

**НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ІНФОРМАТИКИ І ПРАВА  
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ**

**НАЦІОНАЛЬНИЙ ЮРИДИЧНИЙ УНІВЕРСИТЕТ  
імені ЯРОСЛАВА МУДРОГО  
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

Кваліфікаційна наукова праця на правах рукопису

**ЗОЛОТАР ОЛЬГА ОЛЕКСІВНА**

УДК 342.7:004

**ДИСЕРТАЦІЯ  
ПРАВОВІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ**

12.00.07 «Адміністративне право і процес;  
фінансове право; інформаційне право»  
Юридичні науки

Подається на здобуття наукового ступеня доктора юридичних наук.  
Дисертація містить результати власних досліджень. Використання ідей,  
результатів і текстів інших авторів мають посилання на відповідне джерело

\_\_\_\_\_ О.О. Золотар

Науковий консультант –  
Беляков Костянтин Іванович,  
доктор юридичних наук, професор

**Київ – 2018**

## АНОТАЦІЯ

**Золотар О. О. Правові основи інформаційної безпеки людини.** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». – Науково-дослідний інститут інформатики і права Національної академії правових наук України. – Національний юридичний університет імені Ярослава Мудрого, Міністерство освіти і науки України. – Київ, Харків, 2018.

У дисертації вирішено актуальну наукову проблему, що полягає у поглибленні знань і комплексній розробці положень стосовно правових основ інформаційної безпеки людини та підготовці обґрунтованих пропозицій щодо удосконалення чинного законодавства у досліджуваній сфері. Виявлено, що правова і доктринальна основа інформаційної безпеки в Україні розвивались симптоматично і безсистемно, первинно інформаційна безпека розглядалась, насамперед, як інформаційна безпека держави. Проаналізовано етапи становлення українського законодавства у інформаційній сфері в цілому, та щодо інформаційної безпеки, зокрема, і з'ясовано, що на кожному з цих етапів інформаційна безпека людини залишалась вторинним питанням.

Доведено, що кожна історична епоха поглиблювала розуміння соціальних структур і в історичній генезі людина переживала зміну свого соціально-правового статусу. В сучасному українському суспільстві, яке декларує себе як правове, демократичне і інформаційне, можливості і необхідність правового впливу на суспільні відносини знаходяться в прямій залежності від визначення правового статусу людини як суб'єкта і об'єкта соціальних відносин, а насичення інформаційними відносинами усіх сфер суспільного життя і суттєве узалежнення якості життя людини від доступу до інформаційних ресурсів та інформаційних технологій дає підстави говорити про формування інформаційної правосуб'єктності людини та інформаційно-правовий статус як новий галузевий правовий статус людини.

Виокремлено та обґрунтовано зміст двох базових категорій, що є визначальними для правових основ інформаційної безпеки людини - інформаційні права і свободи людини, а також права і свободи людини в інформаційному суспільстві. Під інформаційними правами і свободами запропоновано розуміти комплекс прав, похідних від свободи інформації, як фундаментального права людини, до яких віднесено: 1) інформаційні права, що пов'язані з особою (особистістю) людини; 2) право власності на інформацію; 3) право на доступ до інформації; 4) свободу поширення інформації будь-яким законним способом; 5) право на безпечне інформаційне середовище.

Встановлено, що формування інформаційного суспільства не лише підвищило значення існуючих і появу нових інформаційних прав людини, а й змінило змістовне наповнення усіх прав і свобод людини, а також її обов'язків, в напрямку посилення і ускладнення інформаційної складової кожного з них.

Доведено, що інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, спрямована на реалізацію прав і законних інтересів людини в кожній сфері його життєдіяльності. Не дивлячись на активні наукові дослідження в сфері інформаційної безпеки відсутній єдиний підхід до інформаційної безпеки в цілому, інформаційної безпеки людини зокрема. Зміст і складність цієї концепції є атрибутивною властивістю відносин у сучасному інформаційному суспільстві. Аналіз різних підходів до визначення категорії інформаційної безпеки дозволив зробити висновок про недоцільність суворого дотримання однієї позиції, і найбільш відповідним визначено застосування комплексного підходу, згідно з яким інформаційна безпека визначається через її істотні риси, основні функції, беручи до уваги постійну динаміку інформаційних і соціальних систем.

Розмежовано онтологічне, гносеологічне і логічне розуміння інформаційної безпеки людини. Обґрунтовано, що визначеність логічного змісту інформаційної безпеки залежить від розвитку наукового пізнання, а також від розбудови механізму державного управління. Вказано, що розуміння інформаційної безпеки людини як правової категорії повинне ґрунтуватися на осмисленні комплексності

цього соціального явища, а також враховувати інформаційні права і свободи людини які є змістовним наповненням, що визначає сутність даної категорії.

Окреслено два основні підходи до інформаційної безпеки, базуючись на яких сформульовано авторське бачення структури інформаційної безпеки людини як сукупності інформаційно-психологічної, інформаційно-технологічної (елементом якої є кібербезпека людини) та інформаційно-правової складових. Відзначено, що остання визначається закріпленням на національному та міжнародному рівнях інформаційно-правовим статусом людини, тобто обсягом прав і свобод в інформаційній сфері, а також гарантіями їх реалізації. Обґрунтовано, що інформаційна безпека людини, водночас, є і станом, і процесом, оскільки виступає невід'ємною частиною життя, в якому людина постійно перебуває під дією конкретних інформаційних впливів. При цьому різні категорії осіб знаходяться у неоднакових умовах щодо можливості реалізації своїх прав і свобод в інформаційній сфері, що визначає їх ступінь захищеності в інформаційному суспільстві, види і інтенсивність небезпек, що їм загрожують.

Запропонована типологізація категорій осіб, що характеризуються наявністю спільних інформаційних загроз їх безпеці, дозволила звернути увагу на особливу вразливість цих категорій осіб в умовах інформаційного суспільства. Визначено, що інтегрованість людини в сучасному суспільстві значною мірою залежить від можливості використання інформаційних технологій. Акцентовано, що обмежені фізичні можливості (вади зору, слуху, координації) переважно стають причиною порушення прав людини у зв'язку з неможливістю повноцінно використовувати інформаційні технології, при тому стосуються не лише інформаційних прав, а в умовах інформаційного суспільства – політичних, соціальних, трудових та інших прав людини.

Запропоновано авторське бачення системи інформаційної безпеки, елементами якої вбачаються: 1) правова та наукова (доктринальна) основа; 2) об'єктно-суб'єктний склад, тобто об'єкти інформаційної безпеки, а також система органів (підрозділів), що здійснюють забезпечення; 3) політика інформаційної безпеки; 4) засоби і способи забезпечення інформаційної безпеки. Системний

підхід є необхідною умовою для визначення загроз, а також пошуку оптимальних шляхів їх нейтралізації.

Досліджено існуюче законодавство та зарубіжний досвід регулювання у сфері інформаційної безпеки, що вказує на системну проблему – відсутність єдиного системного підходу до регулювання сфери інформаційної безпеки, в основу якого має бути покладено принцип найвищої цінності людини, гарантування її прав, свобод і законних інтересів. Встановлено, що розвиток законодавства у цій сфері вимагає ефективної співпраці органів державної влади, інститутів громадянського суспільства, комерційних структур і наукового потенціалу держави. Розробка законодавства щодо інформаційної безпеки людини вимагає створення ефективних механізмів активної участі у законотворчій діяльності її суб'єктів – належний доступ до проектів нормативних актів у цих сферах, реальні публічні обговорення, а також врахування їх результатів.

Досліджено ситуацію щодо інформаційної безпеки громадян України в умовах гібридної війни. Запропоновано класифікацію за територіальною ознакою: 1) інформаційна безпека громадян України, що проживають АР Крим та на тимчасово окупованих територіях; 2) інформаційна безпека військовослужбовців та інших осіб, що безпосередньо беруть участь у бойових діях, членів їх сімей, а також мирного населення в зоні бойових дій і на територіях, до них прилеглих; 3) інформаційна безпека населення України, що проживає на «мирних» територіях. Обґрунтовано, що в умовах, коли на території держави відбувається збройний конфлікт, а фактично все населення держави є об'єктом негативних інформаційних впливів, ситуація ускладнена також низкою соціальних, політичних, економічних, історичних передумов, правове забезпечення інформаційної безпеки людини має здійснюватись виходячи не від загроз і небезпек – як це є на сьогодні, а з позицій створення ефективної системи забезпечення основних інформаційних прав і свобод людини. Визначено, що забезпечення інформаційної безпеки людини як функція держави реалізується, насамперед, у складі державної інформаційної політики і політики національної безпеки, але не обмежується ними. Відзначено відсутність скоординованої

діяльності органів державної влади та громадянського суспільства у інформаційній сфері створюють умови для реалізації потенційних та появи нових загроз інформаційній безпеці на всіх рівнях. З огляду на це, обґрунтовано необхідність інституційних змін на рівні державної влади, зокрема, концентрація повноважень по реалізації політики держави щодо розбудови приязного для людини інформаційного суспільства в Україні, в єдиному центральному органі виконавчої влади. Запропоновано визначити сферами відповідальності такого органу: координація розбудови інформаційної інфраструктури держави; забезпечення умов для реалізації інтересів людини, суспільства і держави в інформаційному (в т.ч. кібер) просторі; координація діяльності інших державних органів в інформаційній сфері, забезпечення безвідмовної роботи об'єктів критичної інформаційної інфраструктури, створення умов для формування належного рівня інформаційної культури населення, в тому числі, професійної підготовки населення в умовах розбудови інформаційного суспільства, сприяння розвитку ІТ галузі, забезпечення відкритості та прозорості діяльності влади, а також сприяння формуванню позитивного іміджу України як в середині держави, так і за її межами.

Досліджено політику держави у сфері інформаційної безпеки людини. Визначено необхідність утворення на рівні незалежного органу держави Уповноваженого з інформаційної безпеки людини, діяльність якого має бути спрямована на реалізацію політики держави щодо забезпечення інформаційної безпеки людини, в тому числі захист прав і свобод людини в інформаційній сфері, зокрема, права на доступ до публічної інформації та захист персональних даних. Враховуючи специфіку справ, що пов'язані з порушенням інформаційних прав і свобод громадян, обґрунтовано доцільність створення спеціалізованого суду - Вищого інформаційного суду, запропоновано віднести до його підсудності справи, що стосуються порушення прав людини на доступ до інформації, захисту персональних даних, дифамації, а також щодо реалізації прав громадян на участь у політичному житті, пов'язані з використанням інструментів електронної демократії.

Завдяки аналізу міжнародного досвіду виявлено дихотомію проблеми міжнародної інформаційної безпеки та інформаційної безпеки людини як складової інституту прав людини в міжнародному праві. Встановлено, що узгодження основних питань є необхідним з огляду на економічні інтереси держав, демократичні цінності та глобалізаційні процеси, і, водночас, практично неможливим з огляду на розбіжності в інтересах основних геополітичних гравців; при цьому правове та організаційне забезпечення інформаційної безпеки людини лише на національному рівні є недостатнім з огляду на глобалізацію, інтенсивні транскордонні інформаційні процеси, трудову міграцію, "е-комерцію", втрату ідентичності та ще цілу низку соціальних процесів, що виникають у зв'язку зі становленням глобального інформаційного суспільства.

В результаті аналізу моделей правового регулювання досліджуваної сфери розмежовано підходи до інформаційної безпеки людини в США і країнах ЄС. Акцентовано, що Україна, як держава, що обрала європейський вектор розвитку, зобов'язана враховувати досвід країн ЄС, але з урахуванням національних особливостей формування законодавства і стану демократизації суспільства.

Визначено необхідність закладення правових основ формування таких компонентів інформаційної культури як світоглядний, ціннісний і комунікативний на всіх етапах соціалізації, а також урахування проблеми цифрового розриву і ціннісних відмінностей поколінь та окремих соціальних груп у сучасному українському суспільстві.

У результаті проведеного дослідження визначено низку питань, що потребує вирішення на законодавчому рівні, зокрема: створення правової основи для освіти протягом життя, як необхідної умови існування людини в інформаційному суспільстві; врегулювання питань щодо надання психологічної і психотерапевтичної допомоги, а також інших видів послуг, що використовують методи інформаційно-психологічного впливу; підвищення поінформованості громадян про свої права і свободи через формальні джерела інформації; ефективне регулювання ЗМІ, особливо нових медіа з метою забезпечення дотримання стандартів журналістської діяльності; створення умов для розвитку критичного мислення та оволодіння іншими інструментами, життєво необхідними

в умовах формування інформаційного суспільства, особливо у вразливих категорій населення; подолання цифрової нерівності в географічному та демографічному (віковому) вимірі та інші.

Обґрунтовано, що необхідною умовою ефективної реалізації державної політики щодо інформаційної безпеки людини є проведення фундаментальних та прикладних наукових досліджень. Поруч із вищезгаданими проблемами, які мають відносно добре наукове опрацювання і користуються суспільним схваленням, існують інші, що вимагають етичної оцінки, і тому значно складніше інтегруються у суспільну свідомість, отже і правосвідомість та правову культуру. Зокрема, осмислення на доктринальному рівні потребують питання, пов'язані із правовим забезпеченням використання штучного інтелекту та робототехніки, технологій аналізу великих даних, використання генетичної інформації та ін. Обґрунтовано доцільність завершення процесу виокремлення інформаційного права (разом з правом інтелектуальної власності) в окрему наукову спеціальність.

Сформульовані в дисертаційній роботі висновки, положення, пропозиції й рекомендації можуть бути використані: (а) у науково-дослідних цілях – як основа для подальших досліджень правових основ інформаційної безпеки в цілому, так людини зокрема; а також для подальшого розвитку теоретико-правових та методологічних питань формування та розвитку інформаційного суспільства та його правового; (б) у правотворчій та правозастосовній діяльності – у процесі вдосконалення інформаційного законодавства України, в тому числі з метою використання досвіду інших країн; як методологічна основа наукової та правової експертизи проектів відповідних нормативно-правових актів; а також для удосконалення діяльності системи органів забезпечення інформаційної безпеки; (в) у навчальному процесі – при підготовці навчальних матеріалів з дисциплін «Інформаційне право України», «Інформаційна безпека», «Права і свободи людини в інформаційному суспільстві», «Інформаційна культура», «Інформаційне суспільство» та інших; (г) у просвітницькій і правовиховній діяльності – для підвищення правової та інформаційної культури громадян України, поінформованості з питань їх інформаційних прав і свобод, та з метою виявлення і нейтралізації загроз особистій інформаційній безпеці.



**Ключові слова:** інформаційна безпека, людина, інформаційні права і свободи, державна політика щодо інформаційної безпеки людини, механізм правового регулювання інформаційних відносин, інформаційне право, інформаційне суспільство.

### **Список публікацій здобувача:**

#### **Наукові праці, в яких опубліковані основні наукові результати дисертації:**

1. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. К.: «АртЕк», 2018. 446 с.
2. Золотар О.О. Правова охорона як складова інформаційної безпеки: монографія. К.: ТОВ «ПанТот», 2011. 100 с.
3. Золотар О.О. Генеза суспільних відносин щодо інформаційної безпеки людини. *Інформація і право*. 2018. №1(24). С. 139-148.
4. Золотар О.О. Критичне мислення як необхідна умова безпеки людини в інформаційному суспільстві: соціально-правовий аналіз. *Інформаційна безпека людини, суспільства, держави*. 2018. №1(23). С. 98-105
5. Золотар О.О. Правовий статус людини в інформаційному суспільстві. *Юридичний науковий електронний журнал*. 2018. № 1. С. 84-87.
6. Zolotar O. Legal opposition of informational impact in hybrid warfare in Ukraine /Правова протидія інформаційному впливу в умовах гібридної війни в Україні. *International Journal of Economics and Society*. 2017. Vol. 2. Is. 9. Pp. 93-96.
7. Zolotar O. System prawnej ochrony bezpieczeństwa informacyjnego Ukrainy / Система правової охорони інформаційної безпеки України. *Rocznik Towarzystwa Naukowego Płockiego*. 2017. Ss. 687-702.
8. Золотар О. Информационная безопасность человека: доктринальные подходы к определению категории. *SCI-ARTICLE.RU: науч. период. электрон. журн*. 2017. № 52 (декабрь). С. 260-269.
9. Досвід правового забезпечення інформаційної безпеки в країнах Східного Партнерства ЄС (Молдова, Грузія). *Lex Portus*. 2017. №3 (5) С. 70-80.
10. Золотар О.О. Інформаційні революції: соціально-правове значення. *Публічне право*. 2017. № 2(26). С. 40-46.

11. Zolotar O. Права человека – от эпохи просвещения до информационного общества. *Studia nad Autorytaryzmem i Totalitaryzmem*. 2017. № 38/3. Ss. 7-20.
12. Золотар О.О. Електронна демократія і цифрова диктатура. *Інформація і право*. 2017. №4(23). С. 16-25.
13. Золотар О.О. Особливості інформаційної безпеки людини в умовах гібридної війни. *Інформація і право*. 2017. № 3(22). С. 124-131.
14. Zolotar O. Tożsamość narodowa w erze globalizacji / Національна ідентичність в епоху глобалізації. *Teorie komunikacji i mediów*. Vol.8. 2016. Ss. 111-119.
15. Zolotar O. The rights and safety of women in the informational society: informational gender inequality/ Права та безпека жінок в інформаційному суспільстві: інформаційна гендерна нерівність. *International Journal of Economics and Society*. 2016. Vol. 2. Is. 8. Pp. 118-124.
16. Zolotar O. Informacyjne społeczeństwo a bezpieczeństwo: kwestie teoretyczne i polityko-prawne (na przykładzie Polski, Ukrainy i Rosji) / Інформаційне суспільство і безпека: теоретичний і політико-правовий аспекти (на прикладі Польщі, України і Росії). *Wschodnioznawstwo*. 2015. Ss. 363-376.
17. Zolotar O. Охрана прав человека в правовой системе Украины. *Studia nad Autorytaryzmem i Totalitaryzmem*. 2014. № 36/3. S. 35-49.
18. Золотар О.О. Загрози інформаційній безпеці людини. *Правова інформатика*. 2014. № 2(42). С. 80-89.
19. Золотар О.О., Трубін І.О. Класифікація загроз інформаційній безпеці. *Інформація і право*. 2013. № 3(9). С. 105-114.
20. Золотар О.О. Про поняття “інформаційний шум” у правовідносинах. *Інформація і право*. 2012. № 1(4). С. 70-74.
21. Золотар О.О. Обмеження доступу до інформації: інформаційно-правовий аспект *Інформаційна безпека людини, суспільства, держави*. 2012. № 1(8). С. 74-80.
22. Золотар О.О. Правове регулювання знищення інформації. *Правова інформатика*. 2012. № 2(34). С. 39-44.

23. Золотар О.О. Свобода інформації в контексті концепції природного права. *Правова інформатика*. 2011. № 1(29). С. 12-16.

**Наукові праці, які засвідчують апробацію матеріалів дисертації:**

24. Золотар О.О. Особливості інформаційної безпеки людей похилого віку. *ІТ право: проблеми і перспективи розвитку в Україні*: зб. мат. II міжн. наук.-прак. конф. (Львів, 17 лист. 2017 р.). Львів, 2017. С. 84-88.

25. Золотар О.О. Права і свободи людини: інформаційний вимір. *ІТ право: проблеми і перспективи розвитку в Україні*: зб. мат. наук.-прак. конф. (Львів, 18 лист. 2016 р.). Львів, 2016. С. 59-68.

26. Золотар О.О. Вища юридична освіта в Україні: камінь спотикання чи наріжний камінь? *Правові питання трансформації інформаційного суспільства в суспільство знань як основи інноваційного розвитку України*: мат. круглого столу (Київ, 27 квіт. 2016 р.). К., 2016. С. 107-117.

27. Золотар О.О. Особливості правової соціалізації особистості в інформаційному суспільстві: формування «інформаційного щита». *Філософські та суспільно-правові проблеми становлення і розвитку правового суспільства*: мат. круглого столу (Київ, 20 берез. 2013 р.). Ужгород, 2013. 194 с.

28. Золотар О.О. Віртуальна реальність. *Моделювання колективної безпеки: інформаційний вимір*: зб. мат. (Київ, 27 квіт. 2011 р.) К., 2011. С. 63-66.

29. Золотар О.О. Зміст інформаційного права в контексті концепції природного права. *Інформаційні стратегії в глобальному управлінні*: мат. міжн. наук.-практ. конф. (Київ, 29 жовт. 2011 р.). К., 2011. С. 51-57.

**Наукові праці, які додатково відображають наукові результати дисертації:**

30. Золотар О.О. Інформаційна безпека як право людини. *Інформація та безпека*. 2011. №1-2 (5-6). С. 40-41.

31. Золотар О.О. Класифікація інформаційної безпеки. *Інформація і право*. 2011. № 2. С. 109-113.

32. Концепція кодифікації інформаційного законодавства України / авт. кол.: Баранов О.А., Брижко В.М., Золотар О.О. та ін. *Інформація і право*. 2012. № 1(4) С. 5-16.

## SUMMARY

**Zolotar O. O. Legal bases of the human information security.** - Qualifying scientific work on the rights of manuscripts.

Dissertation for obtaining the degree of Doctor of Law in specialty 12.00.07 "Administrative Law and Process; Finance Law; Information Law ". - Research Institute of Informatics and Law of the National Academy of Law Sciences of Ukraine. - Yaroslav Mudryi National Law University, Ministry of Education and Science of Ukraine. - Kyiv, Kharkiv, 2018.

The dissertation deals with the actual scientific problem, which consists of elucidation of legal nature, essential features and peculiarities of human information security, determination of its place in the system of information and national security, determination of real and potential threats. It was discovered that the legal and doctrinal basis of information security in Ukraine developed symptomatically and insystemically, in addition, in the beginning information security was considered as state one. The stages of formation of Ukrainian legislation in the information sphere in general, as well as on information security, in particular, have been analyzed, and it was discovered that at each of these stages the human information security remained a secondary issue.

It has been proved that every historical epoch deepened the understanding of social structures and in a historical genesis a person experienced a change in his socio-legal status, and in modern Ukrainian society, which declares itself as legal, democratic and informational, the possibilities and necessity of legal influence on social relations are in direct depending on the definition of the legal status of a person as the subject and object of social relations. The saturation of information relations in all spheres of social life and the significant dependence of quality of life, the human's dependence on information resources and information technologies gives grounds to speak about the formation of a person's informational personality and the information and legal status as a new branch legal status of a person.

The content of two basic categories, which are decisive for the legal basis of human information security - information rights and human freedoms, as well as human rights and freedoms in the information society, are singled out and substantiated. Under

the information rights and freedoms, it is proposed to understand a set of rights derived from freedom of information as a fundamental human right, which include: information rights that are related to human personality; 2) ownership of information; 3) the right to access information; 4) the freedom to disseminate information in any lawful manner; 5) the right for secure information environment.

It was discovered that the formation of the information society not only caused the significance of existing and the emergence of new information rights of people, but also changed the content of all human rights and freedoms, as well as its responsibilities, in the direction of forming the information component of each of them.

It is proved that information security is an integral part of the general problem of information provision of a person, as well as the realization of rights and legitimate interests of a person in every sphere of his life. It has been established that despite active research in the field of information security, there is no single approach to information security in general, information security of a person, in particular. The content and complexity of this concept is also an attributive property of relationships in the modern information society. The analysis of different approaches to the definition of the category of information security made it possible to conclude that it is inappropriate to strictly adhere to one position, and the most appropriate is the application of an integrated approach, according to which information security is determined by its essential features, the main functions, taking into account the continuous dynamics of information and social systems.

Ontological, epistemological and logical understanding of human information security were outlined. It is substantiated that the definition of the logical content of information security depends on the development of scientific knowledge, as well as on the development of a mechanism of public administration. It is stated that understanding of human information security as a legal category should be based on the understanding of its complexity as a social phenomenon, as well as the information rights and human freedoms as content, which determines the essence of this category.

Two main approaches to information security are outlined, based on which the author's vision of the structure of information security of a person as a set of information-psychological, informational-technological (the element of which is

cybersecurity of a person) and information-legal components is formulated. It is noted that the latter is defined by the information and legal status of a person, namely, the volume of rights and freedoms in the information sphere, as well as guarantees of their implementation, fixed at the national and international levels. It is substantiated that information security of a person, at the same time, is both a state and a process, because it acts as an integral part of life in which a person is constantly exposed to specific information influences. At the same time, different categories of people are in different conditions regarding the possibility of realizing their rights and freedoms in the information sphere, which determines their degree of security in the information society, the types and intensity of the threats that they are threatened with.

The proposed typology of the category of persons characterized by the existence of common information threats to their safety, has allowed to draw attention to the special vulnerability of these categories of persons in the information society. It is determined that integration in modern society depends to a great extent on the possibility of using information technologies. It is emphasized that limited physical abilities (sight, hearing, coordination) mainly cause violation of human rights in connection with the inability to fully use information technologies, in addition to not only information rights, but in the information society - political, social, labor and other human rights.

The author's vision of the system of information security is proposed, the elements of which are seen: 1) legal and scientific (doctrinal) basis; 2) the object-subjective composition, namely, the objects of information security, as well as the system of bodies (units) that provide security; 3) information security policy; 4) means of ensuring information security. A system approach is a prerequisite for identifying threats, as well as finding the best ways to neutralize them.

The existing legislation and foreign experience of regulation in the field of information security have been researched, indicating a systemic problem - the lack of a unified systemic approach to the regulation of the information security sphere, which should be based on the principle of the highest value of a person, guaranteeing his rights, freedoms and legitimate interests. It has been established that the development of legislation in this area requires effective cooperation between public authorities, civil society institutions, commercial structures and the scientific potential of the state. The

development of legislation on information security of a person requires the creation of effective mechanisms for active participation in the legislative activity of its subjects - proper access to draft regulations in these areas, real public discussions, and the consideration of their results.

It was investigated that the situation regarding information security of Ukrainian citizens is caused by hybrid warfare. The classification is proposed on the basis of a territorial feature: 1) information security of Ukrainian citizens living in the Autonomous Republic of Crimea and temporarily occupied territories; 2) information security of military personnel and other persons directly involved in the ATO, members of their families, as well as the peaceful population of the Ukrainian territory where the ATO takes place; 3) information security of the population of Ukraine, living in "peaceful" territories. It is substantiated that in conditions where an armed conflict occurs in the territory of the country, and in fact the entire population of the state is the object of negative informational influences, the situation is also complicated by a number of social, political, economic and historical conditions; the legal bases of the information security of a person should be grounded not on threats and dangers - as it is today, but from the standpoint of creating an effective system for ensuring basic information rights and freedoms. It is determined that ensuring information security of a person as a function of the state is implemented, but not limited to, state information policy and national security policy.

The lack of coordinated activity of state authorities and civil society in the information sphere has created the conditions for the realization of potential and the emergence of new threats to information security at all levels. In view of this, the necessity of institutional changes at the level of state power, in particular, the concentration of powers on the implementation of state policy towards building a people-friendly information society in Ukraine, in the single central body of state executive power, was substantiated. It is proposed to define the areas of responsibility of such a body: coordination of development of state information infrastructure; provision of conditions for the realization of the interests of the person, society and the state in the information (including cyberspace) space; coordination of activities of other state bodies in the informational sphere, provision of trouble-free operation of objects of

critical information infrastructure, creation of conditions for the formation of the appropriate level of information culture of the population, including the professional training of the population in the conditions of the development of the information society, promotion of IT development, ensuring openness and transparency of the activity of the authorities, as well as promotion of a positive image of Ukraine both in the middle of the state and abroad.

The state policy in the field of human information security is investigated. The necessity at the level of the independent state body of the State to establish the Commissioner for human information security, whose activities should be directed at the implementation of state policy towards ensuring information security of the person, including protection of human rights and freedoms in the information sphere, in particular, the right to access public information and protection of personal data etc. Taking into account the specifics of cases involving violations of information rights and freedoms of citizens, the expediency of creating a specialized court - the High Court of Information, it is proposed to attribute to its jurisdiction cases involving violations of human rights to access information, protection of personal data, defamation, and as well as on the realization of citizens' rights to participate in political life related to the use of e-democracy tools.

Due to the analysis of international experience, the dichotomy of the problem of international information security and information security of human being as a component of the institute of human rights in international law has been identified. It has been established that the harmonization of key issues is necessary in view of the economic interests of states, democratic values and globalization processes, and, at the same time, practically impossible in view of the differences in the interests of the main geopolitical players; while the legal and organizational provision of information security of a person at the national level is insufficient due to globalization, intensive cross-border information processes, labor migration, e-commerce, loss of identity and a whole range of social processes that arise in connection with the formation of an information society.

As a result of the analysis of the legal regulation models of the investigated sphere of legal relations, the approaches to information security of the person in the USA and



EU countries are delimited. It is emphasized that Ukraine, as a state that has chosen the European vector of development, must take into account the experience of the EU countries, but taking into account national features of the formation of information legislation and the state of democratization of society.

The necessity of establishing the legal basis for the formation of components of informational culture as ideological, value and communicative at all stages of socialization, as well as taking into account the problem of digital divide and value differences of generations and separate social groups in modern Ukrainian society is determined.

As a result of the study, it was determined that the legislative level requires a number of issues that are closely related to human information security, in particular: the creation of a legal basis for life-long education as a necessary condition for the existence of a person in the information society; regulation of questions concerning the provision of psychological and psychotherapeutic assistance, as well as other types of services that use methods of information psychological influence; raising public awareness of their rights and freedoms through formal sources of information; effective regulation of the media, especially new media, in order to ensure compliance with journalistic standards; creation of conditions for the development of critical thinking and the mastery of other tools vital in the formation of the information society, especially in vulnerable groups of the population; overcoming of digital inequality in geographical and demographic (age) dimensions and others.

It is substantiated that fundamental and applied scientific research is a prerequisite for the effective implementation of the state policy on information security of the person. Along with the above-mentioned problems, which have relatively good scientific research and enjoy public approval, there are others who require ethical evaluation and therefore are considerably more difficult to integrate into public consciousness, hence the legal consciousness and legal culture. In particular, comprehension at the doctrinal level requires issues related to the legal provision of the use of artificial intelligence and robotics, technologies for analyzing large data, the use of genetic information, etc. The expediency of completing the process of separating

information law (together with the right of intellectual property) into a separate scientific specialty is substantiated.

The conclusions, provisions, suggestions and recommendations formulated in the dissertation can be used: (a) for research purposes - as the basis for further research of the legal foundations of information security in general, such a person in particular; as well as for the further development of theoretical-legal and methodological issues of formation and development of the information society and its legal; (b) in law-making and law-enforcement activities - in the process of improving the information legislation of Ukraine, including in order to use the experience of other countries; as a methodological basis of scientific and legal expertise of projects of the corresponding normative legal acts; as well as to improve the activities of the system of information security authorities; (c) in the educational process - in the preparation of training materials on the disciplines "Information Law of Ukraine", "Information Security", "Human Rights and Freedoms in the Information Society", "Information Culture", "Information Society" and others; (d) in educational and legal activities - for raising the legal and informational culture of Ukrainian citizens, awareness of their information rights and freedoms, and in order to identify and neutralize the threats to personal information security.

**Key words:** information security, a human being, information rights and freedoms, state policy on information security, mechanism of legal regulation of information relations, information law, information society.

**Scientific papers, in which the main scientific results of the dissertation are published:**

1. Zolotar O.O. Information Security of Human Rights: Theory and Practice: Monograph. K.: "Artek", 2018. 446 p.
2. Zolotar O.O. Legal protection as a component of information security: Monograph. K.: "PanTot LLC", 2011. 100 p.
3. Zolotar O.O. The Genesis of Public Relations on Human Information Security. *Information and Law*. 2018. No. 1 (24). Pp. 139-148.

4. Zolotar O.O. Critical thinking as a necessary condition for human security in the information society: socio-legal analysis. *Information security of a person, a society, a state*. 2018. №1 (23). Pp. 98-105.
5. Zolotar O.O. Legal status of a person in the information society. *Legal scientific electronic journal*. 2018. № 1. Pp. 84-87.
6. Zolotar O. Legal opposition to informational impact in hybrid warfare in Ukraine. *International Journal of Economics and Society*. 2017. Vol. 2. Is. 9. Pp. 93-96.
7. Zolotar O. System of legal protection of information security of Ukraine. *Rocznik Towarzystwa Naukowego Płockiego*. 2017. Pp. 687-702.
8. Zolotar O. Information security of the person: doctrinal approaches to categorization. *SCI-ARTICLE.RU: scien. period. electron. journ.* 2017. № 52. Pp. 260-269.
9. Zolotar O.O. The experience of legal security of information security in the countries of the Eastern Partnership (Moldova, Georgia). *Lex Portus*. 2017. № 3(5). Pp. 70-80.
10. Zolotar O.O. Information Revolutions: Socio-Legal Meaning. *Public law*. 2017. № 2(26). Pp. 40-46.
11. Zolotar O. Human rights - from the age of enlightenment to the information society. *Studia nad Autorytaryzmem i Totalitaryzmem*. 2017. № 38 (3). Pp. 7-20.
12. Zolotar O.O. Electronic democracy and digital dictatorship. *Information and Law*. 2017. № 4 (23). Pp. 16-25.
13. Zolotar O.O. Features of human information security in a hybrid war. *Information and Law*. 2017. № 3 (22). Pp. 124-131.
14. Zolotar O. National Identity in the Age of Globalization. *Theory of communication and media*. Vol.8 2016 S. 111-119.
15. Zolotar O. The rights and safety of women in the informational society: informational gender inequality. *International Journal of Economics and Society*. 2016 Vol. 2. Is. 8. Pp. 118-124.
16. Zolotar O. Information Society and Security: Theoretical and Political-Legal Aspects (for example, Poland, Ukraine and Russia). *Wschodnioznawstwo*. 2015. Pp. 363-376.

17. Zolotar O. Protection of human rights in the legal system of Ukraine. *Studia nad Autorytaryzmem i Totalitaryzmem*. 2014. № 36(3). Pp. 35-49.

18. Zolotar O.O. Threats to information security of a person. *Legal informatics*. 2014. № 2(42). Pp. 80-89.

19. Zolotar O.O., Trubin I.O. Classification of threats to information security. *Information and Law*. 2013. № 3 (9). Pp. 105-114.

20. Золотар О.О. About the notion of "information noise" in legal relations. *Information and Law*. 2012. № 1 (4). Pp. 70-74.

21. Zolotar O.O. Restrictions on access to information: information and legal aspect. *Information security of a person, a society, a state*. 2012. № 1 (8). Pp. 74-80.

22. Золотар О.О. Legal regulation of information destruction. *Legal informatics*. 2012. № 3 (34). Pp. 39-44.

23. Zolotar O.O. Freedom of information in the context of the concept of natural law. *Legal informatics*. 2011. № 1 (29). Pp. 12-16.

#### **Scientific works certifying the testing of the dissertation materials:**

24. Zolotar O.O. Features of information security of the elderly. IT Law: Issues and Prospects for Development in Ukraine: *Mat. II intern. scient. conf.* (Lviv, Nov. 17, 2017). Lviv, 2017. C. 84-88.

25. Zolotar O.O. Human rights and freedoms: information dimension. IT Law: Issues and Prospects for Development in Ukraine: *Mat. scient. conf.* (Lviv, Nov. 18, 2016). Lviv, 2016. C. 59-68.

26. Zolotar O.O. Higher legal education in Ukraine: stumbling block or cornerstone? Legal Issues of the Transformation of the Information Society into the Society of Knowledge as the Basis for Ukraine's Innovative Development: *Mat. round table* (Kyiv, April 27, 2016). K., 2016. P. 107-117.

27. Zolotar O.O. Features of legal socialization of the individual in the information society: the formation of an "information shield". Philosophical and socio-legal problems of formation and development of a legal society: *Mat. round table* (Kyiv, March 20, 2013). Uzhgorod, 2013. P. 194.

28. Zolotar O.O. Virtual reality. Collective Security Modeling: Information Dimension: *Mat. scient. conf.* (Kiev, April 27, 2011) K., 2011. Pp. 63-66.

29. Zolotar O.O. Content of information law in the context of the natural law concept . Information Strategy in Global Governance: *Mat. intern. scient.-pract. conf.* (Kyiv, October 29, 2011). K., 2011. Pp. 51-57.

**Scientific works, which additionally reflect the scientific results of the  
dissertation:**

30. Zolotar O.O. Information security as a human right. *Information and security*. 2011. №1-2 (5-6). Pp. 40-41.

31. Zolotar O.O. Classification of information security. *Information and Law*. 2011. № 2. S. 109-113.

32. Concept of codification of information legislation of Ukraine / aut. Number: Baranov O.A., Brizko V.M., Zolotar O.O. etc. *Information and Law*. 2012. № 1 (4) P. 5-16.

## ЗМІСТ

<b>Вступ .....</b>	<b>4</b>
<b>Розділ 1. Теоретико-методологічні засади наукових досліджень інформаційної безпеки людини.....</b>	<b>16</b>
1.1. Онтологічний, гносеологічний та логічний зміст інформаційної безпеки людини.....	16
1.2. Генеза суспільних відносин щодо інформаційної безпеки .....	31
1.3. Місце вчення про інформаційну безпеку в сучасній науці та методологічні засади інформаційно-правових досліджень .....	60
Висновки до розділу 1.....	69
<b>Розділ 2. Правова природа інформаційної безпеки людини.....</b>	<b>74</b>
2.1. Інформаційна безпека людини як системне явище .....	74
2.2. Правове забезпечення інформаційної безпеки людини в Україні.....	84
2.3. Теоретико-правовий аналіз загроз інформаційній безпеці людини.....	100
Висновки до розділу 2.....	137
<b>Розділ 3. Правовий статус і безпека людини в інформаційному суспільстві .....</b>	<b>141</b>
3.1. Парадигма правового статусу людини в умовах становлення інформаційного суспільства.....	141
3.2. Особливості правового забезпечення інформаційної безпеки окремих категорій осіб .....	218
3.3. Проблеми інформаційної безпеки людини в умовах гібридної війни проти України.....	239
Висновки до розділу 3.....	252
<b>Розділ 4. Інформаційна безпека людини в міжнародному праві та законодавстві іноземних держав.....</b>	<b>256</b>
4.1. Інформаційна безпека людини в міжнародному праві.....	256
4.2. Підходи до правового регулювання відносин у сфері інформаційної безпеки людини в США та країнах ЄС.....	285

4.3. Досвід правового регулювання відносин у сфері інформаційної безпеки людини у країнах Східного партнерства ЄС.....	311
Висновки до розділу 4.....	330

<b>Розділ 5. Пріоритети розвитку правових основ інформаційної безпеки людини в Україні.....</b>	<b>335</b>
5.1. Державна політика щодо інформаційної безпеки людини в Україні.....	335
5.2.Механізм правового регулювання відносин у сфері інформаційної безпеки людини.....	353
5.3. Актуальні напрями вдосконалення правових основ інформаційної безпеки людини.....	376
Висновки до розділу 5.....	396
<b>Висновки.....</b>	<b>400</b>
<b>Список використаних джерел.....</b>	<b>409</b>
<b>Додатки.....</b>	<b>468</b>

## ВСТУП

**Обґрунтування вибору теми дослідження.** Аналіз соціальних процесів, що відбуваються останні роки під натиском інформаційної експансії у всіх сферах життя в Україні і світі, дозволяє говорити про наближення до глобального інформаційного суспільства. При цьому, одночасно створюються можливості настання бажаних і загрозових наслідків як для суспільства в цілому, так і для окремої людини. Сучасна людина в суспільстві, що прямує до інформаційного, занурена в світ технологій і надміру інформації. В кожній сфері життєдіяльності суспільства активно використовуються інформаційні технології (ІТ), що спричиняє посилення інформаційних впливів.

Динамічний розвиток дійсності також вимагає перегляду підходів до розуміння безпеки суспільства, держави і, насамперед, людини. Сформоване наприкінці ХХ століття бачення безпеки, яке відштовхувалось від відсутності небезпеки або нейтралізації загроз, і було, насамперед, адаптоване до потреб держави, не спроможне відобразити сутність безпеки людини в сучасному глобалізованому і перенасиченому інформацією світі.

Наприкінці ХХ ст. інформаційно-правові дослідження були сконцентровані на вивченні особливостей суспільних відносин, що виникали у зв'язку з все більш активним використанням ІТ, і намаганням врегулювати видозмінені відносини. При цьому, у світі склалось дві тенденції правового регулювання відносин у інформаційній сфері: використовувати за аналогією законодавство, що існує, при цьому створюючи нові норми лише щодо дійсностей, які повстають у зв'язку з всеосяжною інформатизацією; або творити нове законодавство.

Водночас, врегулювання вже існуючих інформаційних відносин виявилось недостатнім, що підкреслило необхідність ефективної реалізації прогностичної функції права. Становлення законодавства не встигає за здобутками науково-технічного прогресу, у зв'язку з чим виникають нові суспільні відносини, які, доволі часто, вимагають насамперед етичної, а вже потім правової оцінки соціумом. При цьому, пересічний громадянин опиняється в такій же ситуації як і



політичні діячі – значний рівень ентропії при надмірі інформації і вимозі швидко приймати рішення. Так, поруч із зовнішніми (об’єктивними) загрозами інформаційній безпеці людини, які пов’язані з неправомірним використанням ІТ, недостатністю чи неефективністю правового регулювання інформаційних відносин, повстають внутрішні (суб’єктивні) – брак належного рівня інформаційної культури (в т.ч. грамотності, неготовність протистояти негативним чи надмірним інформаційним впливам, нездатність адаптуватись до нових соціальних умов, пов’язаних із постійним посиленням інформаційного насичення усіх сфер життя).

Дослідження реалій суспільства, що прямує до інформаційного, і умов безпечного існування людини в ньому, свідчить про необхідність виявлення закономірностей та тенденцій виникнення та актуалізації інформаційних загроз, а також визначення меж необхідного і можливого втручання держави шляхом правового забезпечення та інституціонального захисту. Окрім того, необхідним є дослідження ролі людини щодо забезпечення власної інформаційної безпеки в умовах глобалізації, розбудови демократичної правової держави та становлення громадянського суспільства. Тому правові основи інформаційної безпеки людини мають досліджуватись не відірвано від системи інформаційної безпеки суспільства, держави і глобальної інформаційної безпеки людства, а з урахуванням їх взаємної детермінації і постійної взаємодії.

З метою дослідження існуючих підходів до розуміння інформаційної безпеки людини та її правового забезпечення було проаналізовано праці з різноманітних сфер наукового знання – окремих галузей правової науки, соціології, політології, наукових знань про безпеку тощо. Серед вітчизняних правників, науковий доробок яких опрацьовано, з урахуванням комплексності та міжгалузевого характеру проблеми, що досліджується, є фахівці не лише в галузі інформаційного права, а й теорії держави і права, конституційного, адміністративного, цивільного, кримінального та інших галузей, зокрема: Арістова І.В., Баранов О.А., Битяк Ю.П., Беляков К.І., Белєвцева В.В., Брижко В.М., Довгань О.Д., Гаращук В.М., Голіна В.В., Гурковський В.І., Калюжний Р.А.,

Капліна О.В., Коновалова В.О., Кормич Б.А., Корж І.Ф., Кохановська О.В., Костецька Т.А., Красноступ Г.М., Логінов О.В., Ліпкан В.А., Матюхіна Н.П., Марущак А.І., Мукомела І.В., Настюк В.Я., Новицька Н.Б., Новицький А.М., Олійник О.В., Пазюк А.В., Панов М.І., Політанський В.С., Пилипчук В.Г., Савінова Н.А., Селіванов А.О., Сухорольський П.М., Тацій В.Я., Тихий В.П., Тихомиров О.О., Фурашев В.М., Цимбалюк В.С., Шепітько В.Ю., Шопіна І.М., та інші. Їх наукові здобутки, а також доробок таких вчених як Баулін Ю.В., Борисов В.І., Гуторова Н.О., Журавель В.А., Криницький І.Є., Кучерявенко М.П., Лукашевич В.Г., Нижник Н.Р., Оніщенко Н.М., Петришин О.В., Пришва Н.Ю., Скаун О.Ф., Степанюк А.Х., Шило О.Г., Шумило М.Є., Щур Б.В. суттєво вплинули на формування світоглядної позиції та наукового підходу автора.

Безперечно, наукову основу дослідження становлять напрацювання з інформаційного та інших галузей права. Проте, для глибшого розуміння соціальної природи людини та аналізу наукових підходів до інформаційної безпеки, в дослідженні опрацьовано наукові погляди Боднара І.Р., Бодрука О.С., Горбуліна В.П., Дзьобаня О.П., Качинського А.Б., Малика Я.Й., Марценюка О.Г., Мельника С.В., Остроухова В.В., Ожевана М.А., Петрика В.М., Петрова В.П., Петрова С.В., Почепцова Г.Г., Скулиша Є.Д., Стрельбицького М.П., Татенка В.О., Шлімакової І.І. та інших.

Також з метою розширення наукового світогляду та вивчення зарубіжного досвіду опрацьовано роботи іноземних науковців, серед яких: Бачило І., Бауман З., Бел Д., Беноа А., де Бон Г., Бостром Н., Врочинські К., Друкер П., Еріксен Т., Земба Р., Кастельс М., Кубі Г., Лідерман К., Лідл К., Лучі Н., Карвалікс Л., Кузьняр Р., Масуда М., Осятинські В., Сен А., Стиляндіс Е., Сишіяк П., Тер-Акопов А., Тофлер Е., Уебстер Ф., Хаяші Й., Хабер Л., Хенкін Л., Хофман Л., Ярочкин В. та інші.

**Зв'язок роботи з науковими програмами, планами, темами.** Дослідження виконано відповідно до основних положень Конституції України; законів України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», «Про основні засади забезпечення кібербезпеки України», Доктрини

інформаційної безпеки України та Стратегії кібербезпеки України. Робота відповідає Пріоритетним напрямам розвитку правової науки на 2016-2020 рр., схваленим постановою Загальних зборів Національної академії правових наук України від 3 березня 2016 р. Дисертація виконана в межах науково-дослідних робіт Науково-дослідного інституту інформатики і права НАПрН України: «Теоретико-правові основи формування і розвитку інформаційного суспільства» (номер державної реєстрації 0113U003154) та «Теоретико-правові основи захисту прав, свобод і безпеки людини в інформаційній сфері» (номер державної реєстрації 0117U007745).

Тема дисертації затверджена Вченою радою Науково-дослідного інституту інформатики і права НАПрН України, протокол № 11 від 9 жовтня 2012 р.

Результати дослідження було розглянуто та обговорено на науково-практичному семінарі в Науково-дослідному інституті інформатики і права Національної академії правових наук України, протокол № 2 від 4 квітня 2018 р.

**Мета й завдання дослідження.** Виходячи з соціально-правової та наукової значущості теми, автор ставить за *мету* розробити правові основи інформаційної безпеки людини, з'ясувавши її правову природу та визначивши реальні та потенційні загрози інформаційній безпеці людини, причини відставання правового регулювання інформаційних відносин в цій сфері, сформулювати теоретичні висновки й розробити пропозиції щодо вдосконалення чинного законодавства.

Для досягнення поставленої мети визначено такі основні *завдання*:

- окреслити історико-правові передумови формування сучасних загроз інформаційній безпеці людини;
- з'ясувати стан дослідженості інформаційної безпеки людини в сучасній правовій науці;
- запропонувати методологію правових досліджень інформаційної безпеки людини;
- узагальнити сучасні наукові концепції щодо розуміння інформаційної безпеки людини та визначити її правову природу і сутнісні характеристики;

- з’ясувати місце інформаційної безпеки людини в системі інформаційної безпеки та національної безпеки, а також визначити співвідношення системи інформаційної безпеки людини та системи її забезпечення;
- виявити теоретико-правові та нормативно-правові підвалини формування інформаційно-правового статусу людини;
- сформулювати та/або уточнити правовий зміст основних понять і категорій інформаційної безпеки людини;
- встановити особливості правового забезпечення прав і безпеки окремих категорій осіб в інформаційній сфері;
- виявити проблеми правового забезпечення інформаційної безпеки людини в умовах гібридної війни;
- з’ясувати можливості і напрями використання іноземного досвіду для визначення правових основ інформаційної безпеки людини;
- визначити концептуальні засади державної політики у сфері інформаційної безпеки людини в Україні;
- розробити пропозиції щодо удосконалення управлінської і нормотворчої практики у сфері інформаційної безпеки людини з урахуванням напрацювань правової науки та науки про безпеку;
- сформулювати науково-практичні рекомендації щодо вдосконалення чинного законодавства України з метою гарантування інформаційної безпеки людини.

*Об’єктом дослідження* є суспільні відносини, що виникають у сфері інформаційної безпеки.

*Предмет дослідження* – правові основи інформаційної безпеки людини.

**Методи дослідження.** Методологічною основою дослідження стала сукупність методів, підходів та прийомів наукового пізнання – як загальнонаукових, так і спеціальних: діалектичний, історико-правовий, логічний, системного аналізу, статистичний, системно-структурний, порівняльно-правовий, логіко-семантичний, формально-юридичний та ін. Задля використання сучасних досягнень світової науки як один з основних був обраний трансдисциплінарний

підхід, як один з основних способів дослідження складних багатфакторних проблем XXI століття. Провідним з класичних методів став загальнонауковий діалектичний метод пізнання, що дозволив дослідити соціально-правову природу інформаційної безпеки людини у взаємозв'язку із сучасною суспільно-політичною ситуацією, зміною історичного типу суспільства та соціально-економічної формації, а також формуванням глобального інформаційного суспільства. В роботі використано також філософський арсенал юридичної герменевтики, онтології та аксіології. Зокрема, історико-правовий метод використовувався для з'ясування особливостей становлення і розвитку правового забезпечення інформаційної безпеки (п. 1.1), а також дослідження передумов формування інформаційних прав людини як онтологічної суті її інформаційної безпеки. Системно-структурний метод дозволив розглянути внутрішню будову інформаційної безпеки та визначити місце і співвідношення інформаційної безпеки людини з інформаційною безпекою як складним суспільно-правовим явищем, окреслити її місце у системі національної безпеки (п. 3.1), а також сприяв визначенню методології дослідження системи правового забезпечення інформаційної безпеки (п. 5.2). Структурно-функціональний метод дав змогу дослідити роль і місце суб'єктів в системі забезпечення інформаційної безпеки людини (підрозділи 3.1 та 5.1). Статистичний метод дозволив виявити тенденції формування і актуалізації загроз інформаційній безпеці людини (розділ 3). Метод класифікації використовувався для осмислення множини загроз інформаційній безпеці людини, виокремлення соціальних груп, які мають певні специфічні характеристики, що обумовлюють спільність підходів до їх убезпечення в інформаційному просторі (підрозділи 3.1 та 3.3). Компаративістський метод застосовувався для порівняння законодавчого регулювання відносин у інформаційній сфері різних країн світу (розділ 4), а також при дослідженні актів міжнародного права та окресленні перспектив адаптації національного законодавства до міжнародних стандартів у досліджуваній сфері (підрозділи 5.1 та 5.3). За допомогою формально-юридичного методу досліджувалися норми конституційного, адміністративного, інформаційного права та інших галузей

права і законодавства, що визначають правові основи інформаційної безпеки людини (підрозділ 2.2). Також цей метод використовувався для формулювання авторських дефініцій понять. Методи теоретико-правового прогнозування і моделювання були використані для висунення та обґрунтування пропозицій щодо внесення змін і доповнень до чинного законодавства про інформаційну безпеку людини (розділ 5).

Нормативну основу дослідження складає національне законодавство України і зарубіжних країн (країн ЄС, США, країн Східного партнерства ЄС, Російської Федерації та КНР), а також міжнародно-правові акти.

Науково-теоретичною основою дисертації є теоретико-методологічні розробки та монографічні дослідження вітчизняних та зарубіжних фахівців з загальної теорії держави і права, у галузях конституційного, адміністративного, інформаційного, міжнародного права та наукові напрацювання з теорії безпеки, соціології, психології та політології.

Емпіричною основою дослідження стали матеріали нормотворчої практики органів державної влади, політико-правова публіцистика, довідкові видання, статистичні матеріали, судова практика українських та зарубіжних судів, а також Європейського Суду з прав людини за темою дослідження.

**Наукова новизна отриманих результатів** визначається тим, що дисертація є першою в Україні працею, в якій на доктринальному рівні запропоноване вирішення наукової проблеми, що виявляється у поглибленні знань і комплексній розробці положень стосовно правових основ інформаційної безпеки людини та підготовці обґрунтованих пропозицій щодо удосконалення чинного законодавства. У результаті проведеного дослідження одержано низку нових наукових результатів, які мають важливе теоретичне і практичне значення, зокрема:

*уперше:*

– на доктринальному рівні встановлено онтологічний, гносеологічний і логічний зміст правової категорії «інформаційна безпека», що дало змогу надати

визначення поняття «інформаційна безпека людини» та визначити її сутнісні характеристики з урахуванням вимог нормотворчої техніки;

- обґрунтовано, що правовий аспект становлення нового соціокультурного простору інформаційного суспільства і ролі людини в ньому проявляється як через появу нових інформаційних прав людини, так і в насиченні інформаційним виміром прав і свобод трьох перших поколінь – особистих, політичних, економічних, соціальних, екологічних тощо;

- розмежовано категорії інформаційні права людини та права і свободи людини в інформаційному суспільстві, визначено їх зміст;

- запропоновано інституціональні зміни в системі органів державної влади з метою ефективного забезпечення інформаційної безпеки людини;

- здійснено класифікацію інформаційної безпеки людини за критерієм спільності інформаційних загроз безпеці окремих категорій осіб, а також обґрунтовано необхідність особливого правового і організаційного забезпечення їх інформаційної безпеки;

- визначено проблеми правового забезпечення інформаційної безпеки людини в умовах гібридної війни проти України;

*удосконалено:*

- базові підходи до структури інформаційної безпеки людини, та її місця в системі інформаційної та національної безпеки;

- теоретичні положення щодо інформаційного суспільства та інформаційних прав і безпеки людини в умовах його формування;

- підходи до формування національного інформаційного законодавства в частині положень про інформаційну безпеку людини;

- понятійно-термінологічний апарат юридичної науки в частині інформаційної безпеки та прав і свобод людини в інформаційній сфері;

- наукові погляди на людину як об'єкт і суб'єкт суспільства, зокрема, надання їй інформаційно-правового статусу, що обумовлює спроможність людини виступати не лише об'єктом інформаційної і національної безпеки, а й суб'єктом їх забезпечення;

*набули подальшого розвитку:*

- положення щодо правових моделей становлення та розвитку інформаційного суспільства у розвинених державах світу та державах, що мають наближене до українського культурно-історичне і геополітичне становище, а також перспектив їх використання їх досвіду для вдосконалення національного законодавства;
- теоретико-методологічні засади інформаційного права, зокрема, акцентовано увагу на доцільності використання трансдисциплінарного підходу;
- ідеї взаємодії органів державної влади, інститутів громадянського суспільства, національних комерційних структур, а також міжнародних та зарубіжних стейкхолдерів, в процесі творення безпечного інформаційного середовища як основи демократичної правової держави та з урахуванням глобалізаційних тенденцій;
- концептуальні положення щодо інформаційної культури людини та суспільства, зокрема, в частині інформаційної грамотності та компетенцій критичного мислення як необхідних умов безпечного існування і розвитку людини в інформаційному суспільстві;
- перспективні напрями розвитку інформаційно-правових досліджень;
- пропозиції та рекомендації до чинного законодавства, спрямовані на нормативне закріплення правових основ інформаційної безпеки людини.

**Практичне значення отриманих результатів** полягає у тому, що вони становлять як науково-теоретичний, так і практичний інтерес, були використані і можуть в подальшому використовуватись у:

*у науково-дослідних цілях* – як основа для подальшої розробки правових основ інформаційної безпеки в цілому, так людини зокрема; а також для подальшого розвитку теоретико-правових та методологічних питань формування та розвитку інформаційного суспільства та його правового підґрунтя (довідка про впровадження результатів дослідження в діяльність Державної наукової установи “Інститут модернізації змісту освіти”, акт впровадження НДІ інформатики і права НАПрН України);



*у правотворчій та правозастосовній діяльності* – у процесі вдосконалення інформаційного законодавства України, в тому числі з метою використання досвіду інших країн; як методологічна основа наукової та правової експертизи проектів відповідних нормативно-правових актів; а також для удосконалення діяльності системи органів забезпечення інформаційної безпеки (довідки про впровадження результатів дослідження в діяльність Кабінету Міністрів України та Верховної Ради України);

*у навчальному процесі* – при підготовці навчальних матеріалів з дисциплін «Інформаційне право України», «Інформаційна безпека», «Права і свободи людини в інформаційному суспільстві», «Інформаційна культура», «Інформаційне суспільство» та інші (акти впровадження НТУУ «КПІ ім. Сікорського», Київського національного університету імені Тараса Шевченка, довідка про впровадження результатів дослідження в діяльність Національної академії державного управління при Президентові України);

*у просвітницькій і правовиховній діяльності* – для підвищення правової та інформаційної культури громадян України, поінформованості з питань їх інформаційних прав і свобод, та з метою виявлення і нейтралізації загроз особистій інформаційній безпеці.

**Особистий внесок здобувача.** Дисертаційне дослідження є самостійною науковою працею. Наукова новизна, висновки та рекомендації сформульовані автором самостійно, обґрунтовані на підставі особистих досліджень та міркувань.

При використанні наукових праць інших вчених, нормативно-правових актів, джерел емпіричної інформації на них зроблено відповідні посилання.

В статті «Класифікація загроз інформаційній безпеці», що опублікована в співавторстві з Трубіним І.О., авторськими є положення щодо загроз інформаційній безпеці людини і суспільства, а також висновки щодо умовного характеру їх класифікації та чинників, що на це впливають. В проекті Концепції кодифікації інформаційного законодавства України, що розроблена авторським колективом Науково-дослідного центру правової інформатики з права науково-дослідного інституту Національної академії правових наук України, особистий

внесок Золотар О.О. відображено в частині, що стосується забезпечення інформаційної безпеки людини, суспільства і держави.

**Апробація матеріалів дисертації.** Результати дисертації обговорювались на понад 30 наукових конференціях, форумах, семінарах та круглих столах, зокрема на міжнародному семінарі «Кібербезпека та нові виклики для інформаційного суспільства» (Київ, 17 трав. 2012 р.); II щорічному круглому столі «Інформаційне суспільство: право, інновації та бізнес» (Київ, 28 лют. 2012 р.); XIII міжнародній науково-практичній конференції «Інформаційні технології та безпека: оцінка стану» (Київ, 18 черв. 2013 р.); Міжнародній конференції „Unia Europejska w roli gwaranta i promotora praw podstawowych” (ЄС в ролі гаранта і промоутера основних прав” (Вроцлав, Польща, 24-25 лист. 2014 р.); міжнародній конференції “International protection of human rights – contemporary problems in the world” („Міжнародна охорона прав людини – сучасні проблеми у світі”) (Вроцлав, Польща, 12-13 лист. 2014 р.); XIV міжнародній науково-практичній конференції «Інформаційні технології та безпека: засади забезпечення інформаційної безпеки» (Київ, 28 трав. 2014 р.); науково-практичній конференції «Проблеми протидії правопорушенням в інформаційній сфері: Інформаційні війни» (Київ, 6 черв. 2014 р.); міжнародній конференції “V Konferencja Absolwentów Programu im. Lane’a Kirklanda” („П’ята міжнародна конференція абсолювентів програми ім. Лейна Кірккланда”) (Варшава, Польща, 15-16 трав. 2015 р.); міжнародній конференції „The Nature of Law in the Context of Morality and Political Authority” (Природа закону в контексті моралі та політичної влади) (Кудова Здруй, Польща, 28-29 трав. 2015 р.); міжнародній конференції «European Legal Education - between Bologna and Efficiency» (Європейська правова освіта – між Болонією і ефективністю) (Бжег, Польща, 10-11 трав. 2016 р.); VII науково-практичній конференції «Актуальні проблеми управління інформаційною безпекою держави» (Київ, 18 берез. 2016 р.); науково-практичній конференції «Проблеми захисту прав людини в інформаційному суспільстві» (Київ, 1 квіт. 2016 р.); круглому столі «Правові питання трансформації інформаційного суспільства в суспільство знань як основи інноваційного розвитку України» (Київ, 27 квіт. 2016 р.); науково-

практичній конференції «Роль і місце інформаційного права і права інтелектуальної власності в сучасних умовах» (Київ, 17 трав. 2016 р.); міжнародній науково-практичній конференції «Кібербезпека та інтелектуальна власність: проблеми правового забезпечення» (Київ, 21 квіт. 2017 р.); міжнародному Форумі «Демократія даних» (Вінниця, 8 верес. 2017 р.); міжнародній науково-практичній конференції «Кібербезпека та інтелектуальна власність: проблеми правового забезпечення» (Київ, 21 квіт. 2017 р.); II міжнародній науково-практичній конференції «ІТ право: проблеми і перспективи розвитку в Україні» (Львів, 17 лист. 2017 р.) та інших наукових зібраннях.

**Структура та обсяг дисертації** зумовлена метою і завданнями дослідження. Робота складається зі вступу, п'яти розділів, що містять п'ятнадцять підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 479 сторінок, з них 405 сторінок основного тексту. Список використаних джерел містить 680 найменувань, які викладено на 59 сторінках; додатки розміщено на 12 сторінках.

# РОЗДІЛ 1

## ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ

### НАУКОВИХ ДОСЛІДЖЕНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ

#### **1.1. Онтологічний, гносеологічний та логічний зміст інформаційної безпеки людини**

Розвиток науки про безпеку в напрямку інформаційної безпеки суттєво залежить від занурення конкретного суспільства і держави в реальність інформаційного вибуху і формування інформаційного суспільства. Рівень розвитку і використання ІКТ в світі дуже нерівномірно, зокрема, інформаційні проблеми 60% населення перебувають на зовсім іншому рівні. Проте, це не означає, що вони не існують. Людина завжди "приречена" на пошук, оцінку та захист інформації (різниця полягає тільки за своїм змістом – інформація про місця для полювання, джерело води, інше плем'я чи щодо комерційної таємниці і персональних даних), тобто, інформаційну діяльність, яка нерозривно пов'язана з інформаційною безпекою. Тільки от за умови формування інформаційного суспільства значення останньої невідмінно зростає.

Переважає більшість наукових праць на тему інформаційної безпеки починається з обґрунтування її актуальності, посилення проникнення інформаційних технологій в усі сфери життя суспільства, а також становлення інформаційного суспільства як нового етапу розвитку (типу) суспільства, в якому питання інформаційної безпеки набуває нової значимості і становить предмет правового регулювання, один з основних напрямів гарантування національної безпеки та безпеки держав, а також передумовою дотримання прав і свобод людини і громадянина. Таким чином, феномен інформаційної безпеки розглядається через призму практично-діяльнісного відношення людини до держави і суспільства, опираючись на потребах і інтересах об'єктів і суб'єктів безпеки. Безперечно, усвідомлена безпека здатна чинити вирішальний вплив на зміст і розвиток суспільних процесів. Цим обумовлена актуальність дослідження інформаційної безпеки як наукової категорії і як суспільного явища.

Інформаційне протистояння, як і кожне інше, є природно обумовленим елементом конкуренції сучасного глобалізованого світу, тому проблематика інформаційної та кібернетичної безпеки набуває особливої ваги з метою встановлення балансу інтересів особи, суспільства, держави та міжнародного співтовариства.

Інформаційна безпека як наукова категорія є тлумачена на різні способи. Мають місце як доктринальні, енциклопедичні, так і нормативно-правові визначення. При цьому, методологічні підходи, логічні способи їх утворення і закріплення, сфери існування і прикладного використання суттєво відрізняються. Це пов'язано також із тим, що сама категорія безпеки неоднозначна і визначається в залежності від наукової області, в якій він вивчається.

Характерною особливістю наукового пізнання є прагнення такого знання, яке ми могли б кваліфікувати як істинне. Історія філософії і науки дає нам привід сумніватися у можливості одностайного тлумачення такого феномена, як істина [483]. Враховуючи, що основною проблемою філософії є відношення "людина – світ, процес усвідомлення людиною сутності світу свого буття і своєї власної сутності в їхньому взаємозв'язку", необхідним вбачається усвідомлення внутрішнього змісту, ознак і особливостей, поняття, що досліджується [482].

Зокрема, в філософському розумінні необхідно звернутись до трьох основних аспектів відображення предмету в теорії - онтологічного, гносеологічного і логічного.

Онтологічний аспект полягає в тому, що зміст філософії є об'єктивним за своїм походженням і відображає об'єктивно існуюче відношення "людина – світ". Філософія ж, як специфічна форма усвідомлення людиною свого буття, як форма суспільної свідомості, претендує на те, щоб дати людині знання про світ і про саму людину в їхньому бутті [482]. Безпека з точки зору філософії є формою і способом існування. Як відзначається в роботах деяких науковців, зокрема Щуровського А. М., Яценка В. Я., існування виступає по відношенню до безпеки як родове поняття, ширше за своїм змістом [527].

В той же час, Ліпкан В. А., стверджує, що безпека у філософському розумінні має соціальний зміст і у своїх проявах несе риси соціальності й історичності,

виступає сутнісною частиною практичної людської діяльності. Поза суспільством нема безпеки, і зміст її залежить від тих змін, що відбуваються в організації життєдіяльності суспільства [236].

Структура явища повстає в динаміці історичного процесу. Її сутність поєднує внутрішній зміст і зовнішні прояви, відображаються в істотних властивостях, які визначають тенденції його розвитку. Таким чином, єдина сутність може знайти відображення і бути пізнаною через множину явищ.

Гносеологічний аспект відображення предмета в теорії полягає в тому, що світ відображається у свідомості людини не дзеркально, не як результат споглядального сприйняття дійсності, а через призму практично-діяльного відношення людини до світу і до самої себе, через призму потреб і інтересів. Саме пізнавальне відношення людини до дійсності є практичним за своєю природою. В основі відношення людини до світу лежать її потреби й інтереси. Вони можуть бути задоволені тільки в процесі практичного освоєння людиною дійсності [482].

У загальному соціологічному розумінні категорія «безпека» характеризує певний стан людського суспільства, при якому забезпечується його нормальне існування і стабільний розвиток. У соціальних моделях під безпекою розуміють розв'язання проблеми умов оптимального функціонування суспільства та його прогресивного розвитку. У широкому філософському та світоглядному аспекті безпека являє собою важливе питання як для наукового пізнання, так і практики існування соціуму в масштабах окремої держави та планети загалом [36].

Безпека є усвідомленим явищем для конкретного суб'єкта суспільних відносин. Вона виступає як прояв активної взаємодії і відносної самостійності суспільної свідомості у відношенні до суспільного буття. Оскільки безпека є усвідомленим явищем, можна зробити висновок, про усвідомлення факторів, що негативно на неї впливають, і необхідності її забезпечення з метою збереження максимальної життєздатності соціальної системи, з урахуванням реальних та потенційних загроз або ризиків її існуванню та розвитку. У основі будь-якої безпеки як системи мають місце життєво важливі інтереси особи, нації, держави чи міжнародного співтовариства. В цьому, як процесі, проявляється розуміння,

сенси, необхідність усвідомленого оволодіння ідеєю безпечного існування заради подальшого існування чи розвитку соціальної системи.

Розкриваючи філософські проблеми безпеки як соціального явища, слід відзначити, що поняття про безпеку і усвідомлення її необхідності проявляється як на чуттєвому (підсвідомому), так і на раціональному рівнях. В дослідженнях К. Лідерман, польський безпекознавець, стверджує, що в той час як забезпечення стосується в більшій мірі заходів (технічних, організаційних, правових тощо), то безпека – суб'єктивного відчуття [616]. Передчуття, негативні емоції, відчуття небезпеки, почуття необхідності самозахисту з подальшим усвідомленим формуванням системи охорони та захисту є проявом багатства різноманітності людської природи, невичерпності людських якостей. Тобто, безпека знаходить відображення у свідомості суб'єкта суспільних відносин як динамічний процес, що має низку варіативних детермінант - стан, рівень розвитку системи, в тому числі культурності й цивілізованості. Тому обґрунтованою є постановка проблеми виявлення і розкриття сутнісних ознак безпеки як соціального феномену. До них можуть бути віднесені усвідомлена самодостатність, здатність до самозбереження, захищеність від загроз, гарантованість власного існування і т. і. В практичній діяльності (в політичній, економічній, правовій, культурній сферах) мають місце статичні ознаки: визначення стану захищеності від загроз у просторі, часі та за колом осіб.

У практичній площині існування соціальних систем безпека не є абстрактним явищем, відірваним від конкретних умов життя. Її зміст узалежнений від конкретних соціальних умов. Безпека виступає як потреба існування особи, нації, держави з огляду на те, що її функціонування пов'язане з задоволенням найважливішої потреби людини. Безпека співвідноситься із самою можливістю життя, виступає умовою його збереження і основний критерій ймовірного розвитку.

В сучасній науковій літературі має місце дискусія про те, що постановка самої проблеми безпеки обумовлена усвідомленням загроз, тобто проблема безпеки, безпечного існування соціальної системи пов'язується до антиподу - небезпеки чи загрози. Такий методологічний підхід обґрунтовує, якщо відсутня

небезпека, то зникає потреба в безпеці, а, отже, і в забезпеченні існування системи охорони, оборони, протидії і захисту. Лише наявність небезпеки обумовлює таку потребу. Подібну позицію висловлює К. Лідел, польський юрист, фахівець з міжнародного тероризму. На його думку, безпека і загрози є нерозривно пов'язаними явищами. Вони становлять протилежні одиниці виміру соціальних явищ [617].

Сутність іншого підходу можна виразити через відомий вислів: прагнеш до миру – готуйся до війни. Тобто, що безпека повинна мати місце завжди, навіть за відсутності очевидних небезпек або загроз.

З філософської точки зору, суть проблеми полягає в тому, що оскільки безпека є усвідомленим явищем, то вона повинна бути і збереженою від усіляких можливих негативних втручань, негараздів, впливів тощо. Це чітко окреслює активний зміст суспільної свідомості, що здатна прогнозувати, передбачити і уявити небезпеки. З цього слідує, що самозбереження є здатністю і основною властивістю свідомості. Прагнення до безпеки є виразом розумності соціальної системи, проявом усвідомленого змісту її буття, її суспільного і морального сенсу. Безпека при такому підході виступає як невід'ємний атрибут існування. Автор власне підтримує цю позицію, що не слід пов'язувати існування безпеки як явища виключно зі своїм антиподом – небезпекою.

Усвідомлення проблеми безпеки набуває повноти з огляду на діалектику життя. Повноцінний розвиток не є можливим без безпеки. Отже, безпека виступає і як гарантія сталого розвитку будь-якої суспільної системи: набуття нею нових ознак, якостей тощо. Популярна концепція сталого розвитку хоча в первинному своєму розумінні насамперед стосувалась необхідності встановлення балансу між задоволенням сучасних потреб людства і захистом інтересів майбутніх поколінь, акцентуючись на потребі в безпечному і здоровому довкіллі [543]. Водночас, на сьогодні, основою такого розвитку визнається системний підхід та сучасні інформаційні технології, за допомогою яких є можливим моделювання різних варіантів напрямків розвитку, прогнозування їх результатів та вибір оптимальних, в тому числі з огляду на безпеку.



Безпека є поняттям, що окреслює стан стабільності, спокою і відсутності загрози. Вона має суб'єктивний характер, виступає однією з підставових потреб людини, суспільних груп і держав. Охоплює задоволення таких потреб як існування, виживання, цілісність, ідентичність, незалежність, спокій (мир), наявність і стабільність розвитку [673, с.27].

Пронизуючи всі напрями діяльності соціальної системи і визначаючи її ефективність, функція безпеки в пізнавальному філософському аспекті виступає в якості методологічної основи для формування теоретичних підходів і практичних дій особи, суспільства, держави. Поняття безпеки при такому підході виступає інструментом пізнання сутності існування системи як цілісного організму, методологічною базою аналізу якості життєдіяльності конкретної суспільної системи, її ефективності та стійкості до різних загроз, спрямованих на порушення бажаного її стану.

Г.А. Пастернак-Таранушенко вважає, що безпека – це стан об'єкта захисту, що відрізняється динамічною стабільністю та своєчасною можливістю вплинути на хід подій з метою збереження цього об'єкта [302, с.29]. По суті ним зроблена спроба через теорію статички довести теорію динаміки безпеки.

Але за будь-яких умов у сучасних умовах задоволення потреби у безпеці на всіх її рівнях (індивідуальному, суспільному, національному, міжнародному) передбачається застосування системного підходу щодо всебічного врахування значної множини факторів, одним з яких є важливість вибору такої стратегії розвитку соціальної системи, за якої досягається гармонія її взаємовідносин з іншими соціальними системами на основі ідей співіснування, взаємодії, співпраці. Про це більше розглянемо в підрозділі «Інформаційна безпека як системне явище».

Таким чином, безпека, в одному аспекті – це тенденції розвитку й умови життєдіяльності соціуму, його структур, інститутів, що визначаються відповідними настановами (політичними, правовими та іншими), за яких забезпечується збереження їх якісної визначеності та вільне, яке відповідає їх природі, функціонування. В другому – це захищеність вказаного функціонування від потенційних і реальних загроз [423, с.278-282].

Третій, логічний аспект розкривається через результат практично-діяльнісного і пізнавального відношення до дійсності, відображеного в змісті філософського знання, яке виражається за допомогою понятійно-категоріального апарату. Поняття і категорії дозволяють окреслити ступінь усвідомлення людиною власного ставлення до світу і до себе. Зміст та структура понятійно-категоріального апарату відбивають динаміку розвитку самої дійсності, людини, і їх взаємозв'язку [482].

Етимологічно термін "безпека" ("security") походить від латинського виразу "sine cura", що означає без (sine) і догляду, турботи, занепокоєння, заклопотаності (cura). Подібною є етимологія українського терміну «безпека».

Академік Тихий В.П. пропонує наступний етимологічний аналіз слова «безпека» [459]. Слово «безпека» створено з прийменника «bez» і основи іменника «река», пов'язаного з дієсловом «ректі» (українською – «пекти»)[135, с.163]. Прийменник «без» має загальнослов'янський індоєвропейський характер. Його вихідне, початкове значення за одними джерелами – «поза», за іншими – «крім»[135, с.161]. Слово «пека» походить від слова «пек», яке запозичене з голландської мови («рек» – смола). У старослов'янській мові – «пъкъ», «пъкъль» – смола; пекло. У християнстві грішники киплять у пеклі в смолі, горять у вічному вогні; через те в народній етимології слово «пекло» пов'язується з дієсловом «пекти». Пекло – найнебезпечніше місце [135, с.328-329]. Етимологія безпеки пов'язана з міфом про Пека – слов'янського бога пекла. У давньоукраїнській міфології Пек – бог пекла, а також війни, кривавих бійок, кровопролиття та всілякої біди, син Чорнобога і Марі. Згідно з повір'ям він був кровожерний, страхітливий, підступний, нещадний, але лякливий, надто боявся Чура (звідси давнє прислів'я «Чур тобі, Пек»). «Пекло» – царство Пека, страхітливе підземелля, куди «провалювалися» душі грішників після своєї смерті. За давніми міфами пекло мало дванадцять ярусів (дванадцять проваль одне нижче одного, з кривими горловинами між ними; чим більше гріхів мала людина, тим важчої була її душа і тим глибше вона падала). Наші пращури вірили, що Пек затягував до пекла і праведників, добрих людей. З усіх богів Вирію лише Чур міг проникати в пекло й відбивати в Пека невинні душі добрих людей чи своїх

лицарів-побратимів, повертати їх на землю чи до Вирію. Битва Чура з Пеком у підземеллі за уявленням давніх українців призводила до землетрусів. Спровадити до пекла (на шибеницю і т. ін.) означає заподіяти кому-небудь смерть [312, с.181-182].

В староросійській мові загальнослов'янське «ректі» існувало в двох похідних формах: «пекъ» (пека) – «жара, спека», і «печа» - турбота, опіка (рос. попечение) [22]. Від цієї другої форми пішло дієслово «обеспечивать», тобто усувати турботи, створювати умови, коли «не пече». Цікаво, що в сучасній польській мові досі залишилась форма «печа» (piecza) – догляд, опіка, турбота». Власне його однокореневим є польське «bezpieczeństwo» - «безпека».

Таким чином, етимологічне походження поняття «безпека» узалежнює його від небезпек, загроз і ризиків. Але в сучасній науковій думці такий підхід є лише одним з існуючих.

Розвиток і удосконалення знання не може успішно здійснюватися без удосконалення, розвитку понятійного апарату, у якому фіксуються результати освоєння світу, ступінь проникнення людського пізнання в сутність предметів, процесів об'єктивної дійсності. Зневажливе ставлення до розробки понятійного апарату, недбалість у використанні термінології часто призводять до значних втрат у дослідженні явищ дійсності і навіть до помилок, до нерозуміння дослідниками один одного [22].

Тому так важливим, на нашу думку, є інтегрований підхід до вивчення феномену інформаційної безпеки, що ґрунтується на суспільно-історичній і соціально-діяльнісній сутності людини, в діалектичній єдності людини і світу. Внаслідок практичної зумовленості пізнавального ставлення людини до світу теоретичне відображення дійсності у свідомості наповняється конкретним змістом. Тому і зміст філософського знання містить у собі відображення світу не у всій його загальності і багатогранності, а в тій мірі, у якій дійсність включається в сферу практично перетворювальної діяльності людини. На цій основі складається і специфічне бачення світу в рамках буття людини [482].

Якщо в такому випадку світ виступає як світ буття людини, то безпека у сучасних соціальних системах виступає основним поняттям оточуючого

середовища, яка характеризує певний стан буття, при якому забезпечується його нормальне існування та стабільний розвиток [36].

Історія виникнення та розвитку поняття «безпека» охоплює значний проміжок часу, що фактично збігається з виникненням та розвитком людства [3]. Трансформація категорії безпеки відбулась разом із визначенням довкілля, пізнанням природних процесів, поширенням науково-технічних знань, культури тощо. В основі фундаментального розуміння цієї категорії лежить утопічна ідея, яка протягом століть мотивує науковців, - це ідея можливості контролювати майбутнє, прогнозувати майбутні події та прораховувати ймовірні сценарії розвитку з максимальною вірогідністю, основною метою якої є створення ідеальних умов розвитку людства [36]. У розуміння ідеального входить поняття безпечного, що визначає їх взаємодоповнюваність у системі соціальних відносин [3].

Згідно енциклопедичному визначенню під категорією «інформаційна безпека» може розумітись: законодавче формування державної інформаційної політики; створення відповідно до законів України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної влади, громадянами та об'єднаннями громадян, іншими суб'єктами права в Україні; гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України; всебічний розвиток інформаційної структури; підтримка розвитку національних інформаційних ресурсів України з урахуванням досягнень науки і техніки та особливостей духовно-культурного життя народу України; створення і впровадження безпечних інформаційних технологій; захист права власності всіх учасників інформаційної діяльності в національному просторі України; збереження права власності держави на стратегічні об'єкти інформаційної інфраструктури України; охорону державної таємниці, а також інформації з обмеженим доступом, що є об'єктом права власності або об'єктом лише володіння, користування чи розпорядження державою; створення загальної системи охорони інформації, зокрема охорони державної таємниці, а також іншої інформації з обмеженим доступом; захист національного інформаційного простору України від розповсюдження

спотвореної або забороненої для поширення законодавством України інформаційної продукції; встановлення законодавством режиму доступу іноземних держав або їх представників до національних інформаційних ресурсів України та порядок використання цих ресурсів на основі договорів із іноземними державами; законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України [216, с.744].

Російська вчена, фахівець з інформаційного права Бачило І.Л. акцентує увагу на багатоплановості поняття «інформаційна безпека» і відносить до кола питань, що ним охоплюються: захист відкритої інформації, охорону державної таємниці, забезпечення захисту інформації з обмеженим доступом, окрім державної таємниці, страхування інформації і інформаційних ресурсів [34, с.253].

На початках становлення наукового розуміння категорії спостерігалось ототожнення «інформаційна безпека» і «безпека інформації». Тер-Акопов А.А. під інформаційною безпекою розуміє також стан захищеності інформації, що забезпечує життєво важливі інтереси людини [457, с.42]. При цьому таке ототожнення мало місце як в працях вітчизняних науковців, так і зарубіжних. Яскравим прикладом може служити визначення, що містилося в одному з перших перекладених на російську мову видань в СРСР щодо методів захисту інформації Л.Дж. Хоффмана: «інформаційна безпека – стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації [495]. В дослідженнях науковців досі можна зустріти подібне безпідставне ототожнення. Редакція наукового журналу «Безпека інформації», який було засновано у 1995 р., визначила основною метою журналу висвітлення результатів наукових досліджень та поширення інформації з усіх аспектів інформаційної безпеки [39].

Водночас, переважна більшість дослідників чітко розмежовує ці категорії, опираючись на тому, що при визначенні безпеки інформації об'єктом виступає власне інформація, а у випадку інформаційної безпеки – безпека як частина цілого [81, с. 53-56].

Небезпідставною вбачається позиція Фурашева В.М., що при вирішенні проблем інформаційної безпеки важливе місце становить дилема між

гарантованістю прав і свобод суспільства збирати, зберігати, використовувати і поширювати інформацію та об'єктивного вимушеного правового обмеження, неможливе без чіткого визначення об'єктів та суб'єктів права у всій його сукупності, виходячи із сутності явища, процесу, процедур тощо [486, с.113]. Близькою за змістом видається позиція Дзьобаня О.П. і Пилипчука В.Г., які визначають інформаційну безпеку як стан захищеності життєво важливих інтересів людини, суспільства та держави в інформаційній сфері від зовнішніх і внутрішніх викликів і загроз, що забезпечує їх сталий розвиток [116, с.150].

В свою чергу, О.А. Баранов деталізує виклики і загрози при визначенні інформаційної безпеки як стану захищеності життєво важливих інтересів особистості, суспільства і держави, за якого зводиться до мінімуму заподіяння збитків через неповноту, несвоєчасність і недостовірність інформації, через негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [27, с.160].

Певною мірою розвиває такий підхід Довгань О.Д., коли під інформаційною безпекою пропонує розуміти результат управління реальними та (або) потенційними викликами і загрозами щодо захищеності важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері, у т.ч. з використанням правових методів [117].

Богуш В. визначає, що інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [55]. Дуже близьким семантично є визначення Фісуна Ю.А. - „стан захищеності інформаційного середовища, що відповідає інтересам держави, за якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх інформаційних загроз” [481].

В межах даного напрямку існує визначення інформаційної безпеки як стану, тенденції розвитку, умови життєдіяльності соціуму, його структур, інститутів та установ, за яких здійснюється збереження якісної, з об'єктивно обумовленими інноваціями в ній, вільне, відповідне власній природі функціонування інформації.

Окремі представники цього напрямку розглядають інформаційну безпеку через відсутність небезпеки, тобто чинників та умов, що загрожують безпосередньо індивіду, спільноті, державі з боку інформаційно-комунікаційного середовища. Прибічники такого підходу вважають інформаційну безпеку лише станом чи процесом захищеності особи, суспільства, держави від реальних або потенційних загроз [148, с.12].

Наступний погляд передбачає, що у самому загальному вигляді під інформаційною безпекою можна розуміти здатність суб'єкта зберігати свої системостворюючі властивості, основні характеристики при патогенних дезорганізуючих, деструктивних впливах на кіберпростір, інформаційно-комунікаційні технології. На думку прибічників цього погляду, серед яких Ліпкан В.А. [236], безпека і забезпечення безпеки становлять собою різні поняття, через те, що безпека виражає характеристику стану соціальної спільноти, тоді як забезпечення безпеки — діяльнісну характеристику, тобто діяльність органів державної влади і управління з підтримання безпеки. Таким чином, безпека виступає основою цілепокладання політики, а забезпечення безпеки — як діяльність з досягнення безпечного стану суспільства або соціальної групи.

Горбатюк О.М. вважає, що інформаційна безпека – представляє собою стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [96, с.46-48].

Ярочкін В.І. визначає безпеку як стан захищеності особи, суспільства та держави від зовнішніх та внутрішніх небезпек та загроз, що базується на діяльності людей, суспільства, держави, світового співтовариства щодо виявлення (вивчення), попередження, послаблення, ліквідації та відбиття небезпек і загроз, здатних знищити їх, позбавити фундаментальних матеріальних і духовних цінностей, завдати неприйнятну шкоду, закрити шлях для прогресивного розвитку [526, с.28].

Гурковський В.І. визначає національну інформаційну безпеку України як суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в

інформаційному просторі, що є необхідною умовою збереження та примноження духовних та матеріальних цінностей нації, прогресивного розвитку України, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів [103].

Литвиненко О. пропонує під інформаційною безпекою слід розуміти одну із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [232, с.47-49].

Кормич Б. А. визначає інформаційну безпеку як захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства і держави. Він також виділяє ряд основних ознак інформаційної безпеки, що обумовлюються специфікою її об'єкта: зони інформаційної безпеки перебувають на перехресті функції національної безпеки та інформаційної функції держави; питання інформаційної безпеки держави носить екстериторіальний характер; суспільні відносини, що входять до сфери інформаційної безпеки, є неоднорідними і різноплановими; компетенція держави у сфері інформаційної безпеки обумовлюється конкуренцією між інформаційними правами особи та функціями держави і її органів по регулюванню інформаційних процесів; у демократичному суспільстві державне регулювання інформаційної сфери можливе лише шляхом встановлення правових норм; політика інформаційної безпеки носить багатовекторний характер, її головними складовими (векторами) є: (1) регулювання інформаційних відносин з метою забезпечення національної безпеки, територіальної цілісності та громадського порядку, підтримання законності; (2) регулювання інформаційних відносин з метою забезпечення прав і свобод громадян, здоров'я та моральності; (3) регулювання інформаційних відносин у сфері комерційної інформації [208, с.93].

Нижник Н.Р. під інформаційною безпекою розуміє стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни [276].



Петрик В. М. зазначає, що природні явища "безпека" і "небезпека" існують в діалектичній взаємозалежності, тобто у природі не існує окремо "стану безпеки" та "стану небезпеки" [306].

Також заслуговує на увагу точка зору О. Логінова, який стверджує, що не слід обмежуватись поняттям «стан» при визначенні категорії «інформаційна безпека», а стверджує, що вона є процесом. Зокрема, на його думку, інформаційну безпеку слід розглядати крізь органічну єдність ознак, таких як стан, властивість, а також управління загрозами і небезпеками, за якого забезпечується обрання оптимального шляху їх усунення та мінімізації впливу негативних наслідків, зокрема у сфері інформаційної діяльності органів виконавчої влади [239, с.155].

Тихомиров О.О., опираючись детально розроблений в теорії держави і права діяльнісний підхід виокремлює положення, що визначають своєрідність його застосування для дослідження державно-правового забезпечення інформаційної безпеки: суб'єктивний аспект забезпечення інформаційної безпеки як діяльності визначається тим, що воно здійснюється певними суб'єктами (державними і недержавними), метою і результатом дій яких є стан інформаційної безпеки, а ефективність цих дій залежить від усвідомлення суб'єктами соціальної зумовленості, спрямованості дій на задоволення відповідних суспільних і індивідуальних інформаційних потреб, необхідності їх реалізації у взаємодії з іншими соціальними суб'єктами тощо; об'єктивність забезпечення інформаційної безпеки визначається конкретними економічними, історичними, соціальними, культурними умовами її здійснення, а отже залежить від реального стану функціонування держави та інститутів громадянського суспільства, рівня розвиненості інформаційного суспільства, інформаційних процесів і технологій, інформаційної культури населення тощо; регулятивна площина забезпечення інформаційної безпеки орієнтує на осмислення впорядкування забезпечення інформаційної безпеки різноманітними соціальними правилами, домінуючим серед яких є право, а також власне нормами інформаційного спілкування та внутрішніми переконаннями суб'єктів забезпечення інформаційної безпеки; процесуальний ракурс вивчення діяльності щодо забезпечення інформаційної безпеки передбачає осмислення послідовності використання різноманітних

засобів, способів, а в результаті - виокремлення відповідних стадій, що складають процес здійснення діяльності або її окремих фрагментів[461].

Російські дослідники А. Урсул і О. Романович переконані, що забезпечення безпеки не зводиться тільки до захисту; ідея національної безпеки тісно пов'язана з концепцією стійкого демократичного розвитку, є її невід'ємною частиною і водночас умовою її реалізації. Такий підхід значно розширює поняття «інформаційна безпека» за рахунок включення в нього «здатності держави ефективно захищати національні інтереси і цінності» [476, с.47-51].

Наливайко Л. Р. вважає, що інформаційну безпеку слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека має включати ефективну протидію сукупності інформаційних загроз [267].

Під час розробки проекту Закону України «Про засади інформаційної безпеки України» було запропоноване наступне визначення: інформаційна безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій [350]. Проте, ця пропозиція досі знаходиться на розгляді.

Різноманітність підходів до визначення категорії «інформаційної безпеки» вказує, що воно являє собою одну з важливих та багатограних концепцій в науці та інших сферах людської діяльності. Зміст і складність цієї концепції є також притаманною складовою сучасного інформаційного суспільства. Аналіз різних підходів до визначення категорії інформаційної безпеки дозволяє зробити висновок про недоцільність суворого дотримання однієї позиції. Найбільш відповідним, на нашу думку, є комплексний підхід, згідно з яким інформаційна безпека визначається через її істотні риси, найбільш важливі основні функції, беручи до уваги постійну динаміку інформаційних і соціальних систем.

Таким чином, онтологічне розуміння інформаційної безпеки опирається на ціннісному вимірі об'єкта безпеки. Тобто, коли йдеться про інформаційну безпеку людини – то це насамперед потреби людини, можливість реалізації яких в правовому полі закріплюється через її права і свободи.

В той час гносеологічно зміст інформаційної безпеки зводиться, з однієї сторони, до небезпек і загроз, що виникають і впливають на існування об'єкта, а з іншої – до діяльнісної складової – можливостей суб'єктів щодо створення безпечних умов існування об'єкта інформаційної безпеки.

Логічний зміст інформаційної безпеки має особливе значення в правовій площині. Адже нормативне закріплення як правової категорії означає, що на ньому буде будуватись система інформаційної безпеки. Через закріплення у відповідних правових нормах виконуються регулятивну і охоронну функції права, а саме закладаються основи захисту об'єктів інформаційної безпеки і правового регулювання діяльності суб'єктів інформаційної безпеки.

Легітимізуючи категорію «інформаційна безпека» в законодавстві як «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації», в один ряд поставлені життєво важливі інтереси людини, суспільства і держави, які в реальності часто є суперечливими і неспіврозмірними.

Визначеність логічного змісту інформаційної безпеки залежить від розвитку наукового пізнання, а також від розбудови механізму державного управління.

## **1.2. Генеза суспільних відносин щодо інформаційної безпеки**

Усвідомлення людиною цінності певного виду інформації, особливостей наявних процесів комунікації, а також можливостей завдання шкоди особистим і суспільним інтересам шляхом інформаційних впливів або використання інформаційного обміну обумовили усвідомлення інформаційної безпеки. Проте,

на нашу думку, не слід говорити про її появу – адже безпека, як умова існування і розвитку людини, завжди була однією з базових її потреб. Водночас, безпека є невід’ємною властивістю соціальних систем (в т.ч. суспільства), яким може бути завдано шкоди шляхом дії на засоби інформаційних комунікацій, наявність і розвиток яких забезпечує інформаційний обмін між всіма елементами.

Інформаційна безпека людини, водночас, є і станом, і процесом, оскільки виступає невід’ємною частиною життя, в якому людина постійно перебуває під дією конкретних інформаційних впливів. З огляду на вищезазначене, в цій праці взято до уваги історичні передумови захисту інформації, використання інформаційних впливів на людину в інтересах держави та інших суб’єктів, а також зародження інформаційних прав людини, зокрема, права на захист персональних даних та доступ до публічної інформації. Очевидно, цим переліком не вичерпується проблема, проте обмежений обсяг роботи і цілі нашого дослідження обумовили саме такий вибір.

*Історія захисту інформації.* Початок історії захисту інформації вчені пов’язують з появою можливості фіксації інформаційних повідомлень на твердих носіях, тобто з винаходом писемності, а першим видом інформації, що підлягала захисту, вважають державну таємницю. Практично одночасно з народженням писемності виникли перші методи захисту інформації, як шифрування і приховування. Один з найстаріших шифрованих текстів з Месопотамії (2000 рр. до н. Е..) Являє собою глиняну табличку, що містить рецепт виготовлення глазури в гончарному виробництві, в якому ігнорувалися деякі голосні і приголосні і вживалися числа замість імен.

З розвитком суспільства удосконалювалися і способи добування необхідної інформації. До IV століття до н. е. Схід значно випередив Захід в мистецтві розвідки. Сунь Цзи писав: «Те, що називають передбаченням, не може бути отримано ні від духів, ні від богів ... ні за допомогою розрахунків. Воно повинно бути видобуто від людей, знайомих з положенням противника»[448, с.112].

Бажанню здобувати конфіденційну інформацію завжди протиставлялось не менше бажання протилежного боку захистити цю інформацію. Стародавні способи захисту інформації по суті перетривали до сучасності, удосконалюється

лише техніка їх реалізації. Наприклад, з метою приховування самого факту наявності інформації у Стародавньому Римі повідомлення, написане на дошці, приховували від сторонніх очей, заливши його воском. У Стародавній Греції обривали раба, писали на його голові і, коли волосся відростало, відправляли до адресата. У середні віки винайдено тайнопис і повідомлення приховували за допомогою невидимих хімічних засобів. В сучасних умовах поширені такі стеганографічні методи, як приховування змісту повідомлень в малюнках, телевізійних і аудіосигналах тощо [417, с. 65]. Паралельно розвивалися методи шифрування і кодування (криптографічні методи), історія яких починається з часів виникнення писемності в Стародавньому Єгипті та Китаї.

Окремі автори процес розвитку захисту інформації розподіляють на відносно самостійні періоди, в основу яких покладено або еволюцію видів носіїв інформації, або розвиток засобів інформаційних комунікацій. Так, Сьомкін С.Н. виділяє три періоди розвитку засобів і методів захисту інформації [417, с. 75]. Перший період визначається початком створення осмислених і самостійних засобів і методів захисту інформації і пов'язаний з появою можливості фіксації інформаційних повідомлень на твердих носіях. Тобто з винаходом писемності. Одночасно з можливістю збереження і переміщення даних виникла проблема, як зберегти в таємниці конфіденційну інформацію, яка існує вже окремо від джерела. Тому практично одночасно з народженням писемності виникли такі методи захисту інформації, як шифрування і приховування. Один з найстаріших шифрованих текстів знайдений в Месопотамії (XX ст. до н. Е.). Він являє собою глиняну табличку і містить рецепт виготовлення глазурі в гончарному виробництві, в якому ігнорувалися деякі голосні і приголосні, а замість імен вживалися числа.

Другий період (приблизно з середини XIX ст.) обумовлений появою технічних засобів обробки інформації і можливістю збереження і передачі повідомлень за допомогою таких носіїв, як електричні сигнали і електромагнітні поля (наприклад, телефон, телеграф, радіо), а отже проблемами захисту від так званих технічних каналів витоку (побічних випромінювань, наведень і ін.). З'явилися способи шифрування повідомлень в реальному масштабі часу (в

процесі передачі по телефонним і телеграфним каналах зв'язку) і т. Д. Крім того, це період активного розвитку технічних засобів розвідки, що багаторазово збільшили можливості промислового і державного шпигунства. Третій період Сьомкін пов'язує з масовою інформатизацією суспільства, тому, на його думку, історія найбільш інтенсивного розвитку захисту інформації пов'язана з впровадженням автоматизованих систем обробки інформації і вимірюється періодом понад 50 років.

Враховуючи вплив на трансформацію ідей інформаційної безпеки, в розвитку засобів інформаційних комунікацій автори іншого російського дослідження виділяють сім етапів [175, с.88]:

I етап (до 1816 р.) використання природних засобів інформаційних комунікацій. В цей період основне завдання інформаційної безпеки полягало в захисті відомостей про події, факти, майно, місцезнаходження тощо, що мали для людини особисто або мікросоціуму, до якого вона належала, життєве значення.

II етап (починаючи з 1816 р.) пов'язаний з початком використання штучно створюваних технічних засобів електро- і радіозв'язку. Для забезпечення безперешкодності радіозв'язку необхідно було використовувати кодування повідомлення (сигналу) з подальшим його декодуванням.

III етап (починаючи з 1935 р.) пов'язаний з появою засобів радіолокацій і гідроакустики. Основним способом забезпечення інформаційної безпеки в цей період було поєднання організаційних і технічних заходів, направлених на підвищення захищеності засобів радіолокацій від дії на їхні приймальні пристрої активними маскуючими і пасивними імітуючими радіоелектронними перешкодами.

IV етап (починаючи з 1946 р.) пов'язаний з винаходом і впровадженням в практичну діяльність електронно-обчислювальних машин (комп'ютерів). Завдання інформаційної безпеки вирішувалися, в основному, методами обмеження фізичного доступу до устаткування засобів обробки і передачі інформації.

V етап (починаючи з 1965 р.) обумовлений створенням і розвитком локальних інформаційно-комунікаційних мереж. Завдання інформаційної безпеки вирішувалися, в основному, методами і способами фізичного захисту засобів

обробки і передачі інформації шляхом адміністрування і управління доступом до мережевих ресурсів.

VI етап (починаючи з 1973 р.) пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань. Загрози інформаційній безпеці серйознішими суттєво ускладнились і потрібно було розробити нові критерії безпеки. Інформаційний ресурс став найважливішим ресурсом держави, а забезпечення його безпеки — найважливішою і обов'язковою складовою національної безпеки. Формується інформаційне право — нова галузь міжнародної правової системи.

VII етап (починаючи з 1985 р.) пов'язаний із створенням і розвитком глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення. Автори цього дослідження припускають, що черговий етап розвитку інформаційної безпеки, буде пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань і глобальним охопленням у просторі та часі, забезпечуваням космічними інформаційно-комунікаційними системами. Для вирішення завдань інформаційної безпеки на цьому етапі необхідним є створення міжнародної макросистеми інформаційної безпеки людства.

Історія інформаційної безпеки на території сучасної України також сягає ще додержавних часів. Першим видом інформації, яку потрібно було охороняти, була військова інформація. Спочатку охорону такої інформації забезпечував князь, потім особа, яку він призначав особисто. Війна була на той час головним і загальновизнаним способом ведення зовнішньої політики будь-якої держави, тому захист військової інформації був головним у політиці князів Олега, Ігоря, Святослава, Ярослава та княгині Ольги. Князі, йдучи в похід, намагалися приховати інформацію про кількість війська і напрям головного удару. Ворог не міг адекватно реагувати на небезпеку, а заздалегідь поширені чутки, перебільшення і дезінформація призводили до паніки [293, с. 11]. Зазначимо, що в 988 р. Володимир розпочав релігійну реформу, і тому ще один вид інформації про віросповідання теж підлягав спочатку охороні. Перші князі тримали своє віросповідання в секреті, зокрема Ольга, а сам Володимир не відразу наважився

прийняти християнське віровчення попри неодноразові пропозиції Візантії. За Володимира та Ярослава особливого розмаху набуває зовнішньополітична, дипломатична діяльність держави, саме інформація про дипломатичні відносини підлягала охороні. Деякі науковці висловлюють припущення, що вже в період Київської Русі з'явилися державні службовці, які здійснювали захист окремих видів інформації. Можливо це були представники молодшої дружини, а саме: отроки, боярські діти та пасинки.

Основним засобом зв'язку в той час були спеціальні князівські гінці, «люди піші та кінні», і «вірні голови» (люди з князівської дружини) [20, с.10]. Використовувалися й інші способи зв'язку: оптична сигналізація за допомогою багать і димів, сигнальних труб і свистків [21, с. 417].

Для забезпечення конфіденційності інформації, що передається використовувалися різні методи. Найбільш важливі повідомлення заучувалися гінцем напам'ять. При цьому часто використовувалися натяки, умовні слова. Суть методу полягала в тому, що зміст переданого повідомлення могла зрозуміти тільки посвячена людина. Надалі, в криптографії такий спосіб забезпечення секретності отримав назву «жаргонного коду» і застосовується досі. Так, наприклад, на жаргоні багатьох розвідок слово «хворіти» означає «арешт» або «взяття під варту»; ЛІКАРНЯ - в'язниця; «лікар» - контррозвідка [21, с. 423]. Таким чином, повідомлення «Майкл арештований контррозвідкою. Йому загрожує ув'язнення », набуває досить «невинного вигляду»: «Майкл захворів. Вчора був лікар і порадив йому лікуватися в лікарні» [93]. Використовувано і так звану «пташину мову» коли в усне повідомлення вставлялися частки-паразити. Подібні способи захисту інформації з давніх часів були поширені не тільки у державних службах, а й серед представників кримінального світу в різних країнах.

Для захисту письмових повідомлень використовувалася фізичний захист, стеганографія і шифрування. В якості гінців використовувалися фізично міцні люди, вони були добре озброєні, нерідко гонець слідував в супроводі охорони. Самі листи скручувалися в сувої, які опечатувалися спеціальними печатками, що



містять напис «ДЬНЕСЛОВО», що перекладається як «приховане, таємне слово» [434, с. 94].

Стеганографічний метод широко використовувався - повідомлення приховувались в одяг, в підошви і каблуки взуття [21, с. 245]. На жаль, шифровані документи, що містять інформацію державного характеру, що відносяться до епохи Київської Русі поки не виявлені. Однак зберігся ряд пам'ятників давньоруської писемності, в яких є зашифровані фрагменти. В основному це літописи і тексти релігійного змісту. У цих джерелах тайнопис застосовується не стільки для забезпечення секретності, скільки для того, щоб підкреслити важливість того чи іншого фрагмента, а також увіковічити ім'я автора або переписувача. Саме ці документи дають можливість описати давньоруські системи шифрування.

В Литовсько-польській державі, до складу якої увійшли українські землі, найважливішою так само визначалась військова інформація, інформація про особу князя (потім короля), і в Литовському статуті Великого князівства литовського (1588 р.) з'являється новий вид інформації, що охоронялася, - державна таємниця. В Речі Посполитій пошуком і знешкодженням шпигунів з метою захисту інформації займалися призначені королем відповідальні особи з його найближчого оточення.

В Російській імперії було встановлено кримінальну відповідальність за розголошення такого виду інформації як державна таємниця. Зокрема, у «Соборному Уложении» (1649 р.) була стаття, що визначала смертну кару за такі дії [293, с.27]. Водночас, централізованої системи охорони державної таємниці не існувало. Найбільш розвиненою була система захисту військової інформації. Її основними напрямками були створення і вдосконалення системи контррозвідувальних органів; організація комплексної системи захисту інформації, що містить військову таємницю; вдосконалення системи фельд'єгерського зв'язку; організація військової цензури.

Наступний період (з середини XIX ст.) пов'язують з появою технічних засобів обробки інформації та передачі повідомлень за допомогою електричних сигналів і електромагнітних полів (наприклад, телефон, телеграф, радіо). У зв'язку

з цим виникли проблеми захисту від технічних каналів витоку. На початку ХІХ століття криптографія збагатилася чудовим винаходом - система шифрування "дисконим шифром", автором якого вважається екс-президент США Томас Джефферсон.

Суттєво вдосконалено систему охорони інформації та її нормативно-правове забезпечення було у ХХ сторіччі, чому суттєво посприяли дві світові війни.

За час існування проблеми захисту інформації змінилися як уявлення про її сутність, так і методологічні підходи до її вирішення. Правове забезпечення захисту інформації у ХХ сторіччі стало складовою частиною ширшої категорії - інформаційної безпеки. Під юридичними аспектами правового забезпечення захисту інформації почали розуміти сукупність нормативно-правових актів, за допомогою яких узаконювались: 1) правила захисту конфіденційної інформації; 2) заходи відповідальності за порушення правил захисту інформації; 3) вирішення питань організаційно-правового забезпечення захисту інформації; 4) процесуальні процедури вирішення ситуацій [417, с. 38].

Хоча правова регламентація охорони інформації недержавного і невійськового змісту має місце лише з другої половини ХХ сторіччя, проте зародження окремих її видів сягає стародавніх часів. Так, Ф. Вальтер зазначає, *лікарська таємниця* має глибоке коріння, ведучи свій початок від часів стародавнього жрецтва (Єгипет, Індія), коли лікування являло собою релігійний акт і жерці, які займалися лікуванням, огортали мистецтво лікування таємницею [110, с. 124]. В Стародавній Індії існувало поняття лікарської таємниці: відомості, отримані від хворого, не розголошувалися, якщо вони могли справити погане враження на близьких людей. Лікар не повинен був повідомляти пацієнту про свої спостереження, які могли негативно вплинути на душевний стан хворого й перешкодити одужанню. Це відповідало аюрведним уявленням про необхідність душевного спокою для збереження здоров'я [254, с. 56].

Наступним витком у спіралі розвитку лікарської таємниці стала клятва Гіппократа, у якій ідеться про таке: «Про що б під час лікування і також без лікування я не побачив або не почув щодо життя людей із того, що не потрібно розголошувати, я промовчу про те, вважаючи подібні речі таємницею» [85]. У

середньовіччі поняття «лікарська таємниця» відображено в статутах Паризького медичного факультету 1600 р., які забороняли видавати таємниці хворих. Крім того, у середньовічній Європі особливою пошаною користувалися «Канони медицини» арабського мислителя Авіценни, у яких, зокрема, йдеться про збереження лікарем у таємниці того, що йому відомо про хворого [474, с. 7].

Проте, у клятві європейських лікарів, яка відома з VI ст. н. е., відсутні згадки про таємницю. Так тривало до XVI ст., коли в різних країнах Європи (Італії, Швейцарії, Німеччині, Франції) були опубліковані праці Гіппократа. Відтоді лікарі, які одержували ступінь доктора медицини на паризькому медичному факультеті, зобов'язані були давати «факультетську обіцянку», створену на основі «Канону», перед бюстом Гіппократа [474, с. 7]. У Франції закон зобов'язував лікарів на рівні з адвокатами, суддями, біржовими маклерами додержуватися професійної таємниці. Взаємини лікаря з хворим мали бути абсолютно довірчими, і саме тоді лікар міг допомогти хворому. У 1666 р. у Франції було прийнято декрет, що зобов'язував лікаря під загрозою штрафів повідомляти квартальних комісарів про всіх поранених, яким було надано медичну допомогу. Згодом лікар отримав право свідчити про туберкульоз (1893 р.) та аборт (1920 р.) [474, с. 7]. У Німеччині лікар зобов'язувався повідомляти про венеричні хвороби (1927 р.), він мав свідчити про насильницьку смерть, тяжкі тілесні ушкодження й каліцтва. Лікарський статут Росії допускав розголошення лікарської таємниці щодо «прилипливих» захворювань і зобов'язував лікарів доводити до відома слідчих всі небезпечні поранення та пошкодження, які мають або можуть мати смертельні наслідки, та про отруєння [310, с. 156].

У дореволюційній Росії лікарі після закінчення медичного факультету промовляли так звану «Факультетську обітницю», повний текст якої розміщувався на оборотній стороні диплома. У ній зазначалось таке: «Допомагаючи стражденним, обіцяю свято берегти довірені сімейні таємниці й не використовувати на зле їхню довіру». [69, с. 36–37]. Ставлення до збереження лікарської таємниці змінилося в 1920-х рр., коли прибічники скасування лікарської таємниці проголосили її пережитком буржуазної медицини. За повідомленнями газетних звітів, на одному з диспутів, що відбулися в Москві в

січні 1928 р., наркомздрав Н. Семашко так визначив ситуацію: «Держа твердый курс на уничтожение врачебной тайны – пережитка буржуазной медицины, каждый советский врач должен быть чутким общественным работником... Мы держим курс на полное уничтожение врачебной тайны. Это вытекает из нашего основного лозунга, что болезнь не позор, а несчастье... Каждый врач должен сам решать вопрос о границах этой «тайны». Далі висловлена точка зору була підтримана, і тим самим питання було нібито вичерпано. Багато пізніше сам Н. Семашко визнав помилковість такої позиції Наркомздраву [502, с. 349]. У Постанові ВУЦВК і РНК РРФСР «Про професійну роботу і права медичних працівників» 1924 р., а потім в Основах законодавства СРСР і союзних республік про охорону здоров'я, прийнятих Верховною Радою УРСР в 1969 р., лікарська таємниця встановлювалась тільки для лікаря. [8, с. 192]

Таким чином, історія виникнення лікарської таємниці свідчить про її перетворення з етичної норми на норму закону.

Комерційна таємниця є одним з найдавніших способів охорони результатів інтелектуальної діяльності. Давні майстри зберігали секрети своєї професійної діяльності задовго до виникнення перших правових засобів охорони виключних прав. Ці секрети передавались з покоління у покоління, і ймовірно, першим захистом таких секретів виступала патріархальне суспільство, де батько мав владу над своїм сином, а господар над рабом. Правова охорона комерційній інформації надавалася ще в Давньому Римі, де законом передбачався подвійний штраф за примушення рабів розкривати секрети своїх господарів.

Держави також приділяли особливу увагу охороні комерційно цінних ідей, навіть історично склався стереотип, що хоронителем таємниці виробництва фарфору, пороху, шовку є Китай; Сирія охороняла секрети виробництва дамаської сталі; Греція берегла секрет «грецького вогню», що використався під час морських боїв, та ін [432, с.272].

Однак не завжди мали місце законні способи суперництва, тому законодавство почало регулювати недобросовісну конкуренцію. Одним із видів правопорушень, визнаних недобросовісною конкуренцією, є неправомірний збір, розголошення та використання комерційної таємниці. Свобода заняття

промисловою діяльністю, що одержала найсильніший розвиток наприкінці XVIII та XIX століть, і пов'язане з нею стрімке зростання економіки призвели до виникнення в конкуренції численних недобросовісних махінацій і методів, які швидко перетворилися на загальну проблему, для вирішення якої необхідне було створення особливого механізму правової охорони [293, с. 77].

Сучасне розуміння комерційної таємниці почало розвиватись в Англії під час промислової революції. У США перше задокументоване судове рішення стосовно комерційної таємниці датується 1837 роком. У Російській Імперії на початку XX ст. Г.Ф. Шершеневич розглядав крадіжку конфіденційної інформації як одну з форм недобросовісної конкуренції: «Проявом недобросовісної конкуренції визнається збір чужих комерційних таємниць, або підкуп службовців, або направлення підставних робітників» [514, с. 116]. Поняття комерційної таємниці припинило існування з прийняттям радянською владою у 1917 р. Декрету «Про робітничий контроль». У радянський період діяло правило про обов'язковість найширшого та безоплатного поширення кожного досягнення, отриманого на окремому підприємстві, про «обмін досвідом» на адміністративній основі. Ще в 1930 р. XVI з'їзд ВКП(б) передбачив необхідність боротьби із секретністю. Хоча, така відкритість обмежувалась сферою цивільного виробництва, а таємниця існувала і захищалась адміністративними заходами, хоча й не мала характеру правової категорії. Повернення інституту захисту комерційної таємниці до законодавства відбулось наприкінці існування радянської державності, у Законі СРСР «Про підприємства в СРСР».

У Європі питаннями дотримання та збереження банківської таємниці вчені та державотворці переймалися ще досить давно. З виникненням перших банків постає питання про додержання банківської таємниці. Вважається, що в установчих документах «Банку св. Амброзіуса», який був заснований у Мілані 1593 р., міститься перша письмова згадка про банківську таємницю [313, с. 65]. Для підтримки довіри до банків у власні державі у XVIII ст. король Пруссії Фрідріх Великий видав указ, за яким особи, які вели банківські операції, були зобов'язані довічно зберігати таємницю про них [409, с. 27].

Швейцарські банкіри понад 300 років тому дбали про збереження інформації про банківські рахунки клієнтів. У 1713 р. на Великій Раді Женеви було ухвалено перший відомий закон, який обмежує право банкірів розголошувати інформацію про своїх клієнтів. У першій половині минулого століття секретність швейцарських банків досить активно почала користуватися попитом, коли багато європейських держав почали підвищувати податки, для виплати боргів після війни, а заможні європейців почали шукати шляхи сховати гроші. Оцінивши позитивний вплив, який подібна практика спричиняє на економіку держави, в 1934 р. у Швейцарії ухвалили закон, що змушував банкірів нести кримінальну відповідальність за розкриття фінансової інформації. Швейцарський Закон про банківську діяльність від 1934 р. був прийнятий після того, як Адольф Гітлер і нацистська партія прийшли до влади у Німеччині [467, с. 389].

На території сучасної України розвиток інституту банківської таємниці розпочався із створенням Державного комерційного банку Росії у 1817 р.. Зокрема, у Статуті Державного комерційного банку було визначено, що кожний вкладник міг щодня (винятком були святкові дні) вимагати для ознайомлення Банківські книги для спостереження за станом свого рахунку. Разом із тим зазначалося, що ніхто у жодному разі не мав права вимагати для ознайомлення рахунки та перекази інших осіб. У даному акті було закріплено, що чиновники банку зобов'язуються зберігати у непорушній таємниці усі рахунки приватних осіб під страхом відсторонення від посади, яку вони обіймали [477]. Значного розвитку банківська таємниця набула з 1903 р. шляхом закріпленням даної категорії у Статуті Державного Банку Російської Імперії. Окремо встановлювалась відповідальність за розголошення банківської таємниці службовцями банку [92, с. 8]. Після подій 1917 р. відбувся певний регрес у розвитку інституту банківської таємниці. Банківська система того часу існувала на принципах про повну непотрібність та, навіть, шкідливість будь-яких таємниць у сфері економічної діяльності, крім державних. Почалися втручання у діяльність приватних банків, існування яких із часом було взагалі заборонено. Як зазначає Г. Б. Романовський, термін «банківська таємниця» в законодавстві СРСР не вживався, та в цьому й не було необхідності, оскільки грошові заощадження

зберігалися в ощадних касах, які належали державі [404, с. 38]. Лише наприкінці існування СРСР розпочалися процеси, пов'язані з реформуванням як політичної системи, так і економічної. Саме з цим періодом можна пов'язувати початок відродження інституту банківської таємниці.

У зв'язку з обмеженим обсягом цієї роботи не можливо розкрити історію становлення всіх видів таємної інформації. Зокрема, не було розглянуто становлення таємниці слідства, адвокатської та нотаріальної таємниці, таємниці страхування та інших.

Сучасний період свідчить про найбільш інтенсивний розвиток засобів захисту інформації починається у зв'язку з масовою інформатизацією суспільства. Проте, наприкінці 20 ст. математично було доведено, що забезпечити повну безпеку інформації в системах її обробки неможливо [496].

***Історія використання інформаційних впливів на людину.*** В різні періоди історичного розвитку людської цивілізації інтенсивність застосування інформаційного впливу, як і досконалість його організації, дуже різнилися. Тому з метою дослідження цієї діяльності з точки зору її історичного розвитку, виявлення основних чинників, які так чи інакше впливали на цей розвиток, науковці умовно поділяють історію інформаційного протиборства на три основні періоди.

Перший період інформаційного протиборства охоплює античні часи, епоху Середньовіччя та частину Нового часу до XVIII ст. включно. Перші письмові згадки про інформаційний вплив на суспільство у Стародавньому Китаї. У вже згаданому Трактаті про мистецтво війни китайського полководця Сунь цзи [448] наводиться опис і яскраві приклади застосування прийомів і методів психологічного впливу, які давали змогу досягати перемоги без битв або з мінімальними втратами. Важливе місце, зокрема, відводиться дезінформуванню противника, психологічній обробці власних населення і війська з метою досягнення єдності в суспільстві напередодні і під час війни, здійснення інформаційних диверсій для розладнання військових союзів ворожої держави з іншими державами тощо.

Подальший розвиток воєнного мистецтва незмінно супроводжувався удосконалюванням форм інформаційно-психологічного впливу. Так, тривалий час у війнах Стародавнього Китаю застосовувався такий самостійний прийом інформаційно-психологічного впливу, як проголошення справедливою війни зі свого боку і несправедливою - з боку противника. Як бачимо, цей спосіб не втратив актуальності й досі і активно використовується в сучасних умовах.

На період греко-перських воєн припадають згадки про спроби використання театру, поезії, образотворчого мистецтва з метою політичної пропаганди, а також протидії цьому з боку політичних опонентів. Новий етап розвитку практики пропаганди мав місце в античному Римі [305, с. 54], зокрема, написання тенденційних біографій з метою уславлення певних аристократичних родів, мемуарний та епістолярний жанри, стають популярними різноманітні легендарні версії з історії Риму та походження римського народу, освячення і обожнення особи імператора. Спеціального розгляду в аспекті порушеної проблеми заслуговує психологічне та ідейно-пропагандистське забезпечення церквою різних воєнних акцій, таких, як, наприклад, збройна відсіч поганським навалам гунів, аварів, вандалів, відвоювання християнських святинь під час хрестових походів, міжконфесійна боротьба та боротьба з єресями. Не менш активно використовували релігійний аспект мусульманські завойовники.

Один з перших історичних прикладів масштабного застосування дезінформації у воєнних цілях пов'язаний із вторгненням монголів до Угорщини у 1241 р. Розбивши угорців та їхніх союзників на річці Шайо, монголи серед захоплених трофеїв знайшли королівську печатку. За наказом Батия грамотні полонені від імені короля Бели написали угорською мовою указ про припинення опору, копії якого, скріплені королівською печаткою, було розіслано в різні кінці країни [305, с.56]

На початку XVI ст. в концепції державної влади, що висунув і обґрунтував Н. Макіавеллі у книзі «Державець» вперше сформулював основні принципи ведення інформаційного протиборства в політичній сфері. Він висунув тезу про те, що політик повинен поєднувати в собі риси лева і лисиці. Володіючи якостями цих тварин, він буде здатний, з одного боку, діяти рішуче, із застосуванням сили, з



іншого - маніпулювати масами за допомогою хитрості, спритності, обману. Брехня на благо суспільства визнавалася допустимою і навіть необхідною, а в роботі з підданими - «наси́льство для тіла і брехня для душі».

Винайдення Й. Гутенбергом друкарського верстату кардинально змінило можливості поширення інформації, прискоривши швидкість тиражування та зменшивши ціну виготовлення книг. В окремих країнах Європи з'являється інформаційне публічне видання - газета, яка спочатку була рукописною, а з часом - друкованою. З цим пов'язують необмежені можливості, причому не лише у військовій, а практично в усіх сферах суспільної діяльності (політичній, економічній, культурній тощо). Перший випадок використання друкованих, а не рукописних листівок, зафіксований під час війни Нідерландів за незалежність від Іспанії в XVI ст. На території Фрісландії було надруковано кілька тисяч примірників звернення до населення, яке стало важливим елементом консолідуючої пропаганди в 1567 р. у війні проти військ герцога Альби та звільнення фламандців від іспанського панування [305, с. 60].

У Запорізькій Січі та державі Б. Хмельницького також вироблені були власні форми захисту військово-політичної інформації, зокрема дезінформації. В спогадах польських урядовців про нього «одне думає, про інше пише», «наміри його жодним чином не можна зрозуміти» [293, с. 48].

Другий період інформаційного протиборства починається з середини XVIII ст. і закінчується Другою світовою війною включно. Найбільш яскравими є діяльність пропагандистського апарату Наполеона Бонапарта і нацистського Третього Рейху.

Наполеон активно використовує можливості поліцейського відомства у справі ідеологічно-психологічного впливу на населення і контролю за ним для збереження власної диктатури. Він був одним із перших можновладців Європи, хто дійсно оцінив роль преси у формуванні громадської думки. "Чотири газети зможуть заподіяти ворогові більше шкоди, ніж стотисячна армія". Усвідомлюючи повною мірою силу вплив преси на формування громадської думки, Наполеон диференційовано підходив до діяльності органів друку усередині країни та за кордоном. У Франції він газет заборонив писати про внутрішню та зовнішню

політику і скоротив кількість газет з 73 до 13. А у кожній окупованій країні засновував офіційний друкований орган: «Газетт де Мадрид», «Газетт де Берлін», «Журналь дю Капітоль» тощо, на сторінках яких широко використовувались методи замовчування і дезінформації [305, с. 62].

На зламі XIX-XX ст. повстає науковий інтерес до феноменів впливу на людську свідомість, зокрема на свідомість мас. У 1879 р. у Лейпцигу за ініціативою вченого В. Вундта відкривається перша психологічна лабораторія. П'ятнадцять років по тому у Франції виходить "Psychologie des foules" (Психологія натовпу) Г. Ле Бона, який заявив про прихід "ери натовпу". Принципово нові завдання ставилися в той же період ідеологами роботи з масовою свідомістю. Відбувається зародження того виду інформаційно-пропагандистської діяльності, який прийнято називати англійським словосполученням "паблік рилейшнз" (ПР). Основним завданням фахівців ПР стало створення досконалих комунікативних технологій, тобто таких варіантів організації подачі інформації суспільству, які зможуть гарантувати, або, принаймні, обіцяти досягнення програмованого ефекту, наприклад, перемоги свого кандидата на виборах, підвищення попиту на рекламований товар тощо.

Реально ПР виник внаслідок індустріальної революції, коли монополісти відчували що для досягнення успіху недостатньо методів управління лише виробничою сферою. Творцями перших технологій ПР дослідники вважають А. Лі та Е. Бернейса. За допомогою методів ПР А. Лі вдалося не тільки уникнути негативних наслідків від страйку шахтарів на шахтах Дж. Рокфеллера, але й використати цю акцію протесту на користь власника, значно підвищивши його імідж як дбайливого хазяїна.

Значного розмаху застосування технологій ПР набуло після закінчення Другої світової війни. У 1948 р. засновуються Інститут ПР у Великій Британії та Асоціація ПР у США. Основними напрямками застосування можливостей ПР є галузь реклами та передвиборна боротьба, але поступово і в інших сферах суспільного та державного життя цей інститут впевнено завойовує позиції. Поява ПР, окрім всього сказаного, означала ще й привернення уваги вчених, підприємців і політиків до роботи з інформацією. Внаслідок цього

вдосконалилися комунікативні технології, що застосовувалися в зовнішньополітичній сфері, зокрема, у війні.

Характерною рисою інформаційно-пропагандистської діяльності в європейських країнах періоду Першої і Другої світових воєн стала її централізація. Так, в часи Другої світової війни, в Англії існувало Міністерство інформації та Департамент пропаганди на противника, у Франції - служба військової пропаганди зосереджувалася при 11-му відділі Генерального штабу, а також "Будинок преси" та неофіційна організація "Альянс Франсе". Хоча США приєдналися до бойових дій на завершальному етапі війни, проте пропагандистську роботу на її потреби здійснювали з широким розмахом. При штабі американської експедиційної армії в Європі функціонувала "Психологічна підсекція", яка, поряд з проведенням широкомасштабних операцій з розповсюдження листівок, займалась і розробленням соціально-психологічної методики вивчення моралі противника, а в США діяв спеціальний орган пропаганди - Комітет громадської інформації, який мав поділ на секції: новин, іншомовних газет, громадської освіти, кінофільмів, відносин з промисловцями, реклами і карикатур.

Пропагандистські машини СРСР і нацистського Третього Рейху не лише масово творили нові методи пропаганди, але й використовували населення своїх країн як своєрідні полігони, на яких проходили випробування нові зразки інформаційної зброї.

Ефективність радянської пропаганди було продемонстровано ще в ході громадянської війни. Вже у грудні 1917 р. при Народному Комісаріаті іноземних справ було створено відділ міжнародної революційної пропаганди, а при видавництві ВЦВК - військовий відділ друку літератури іноземними мовами. Комуністична партія пропаганду за значенням ставила на один рівень з організацією бойових дій. Успішною була політична пропаганда комісарів-пропагандистів Червоної Армії. Маніпулюючи емоціями та свідомістю населення, вони вирішували питання комплектування збройних сил, управління економікою, формування нової структури адміністрації. "Шляхом пропаганди й агітації ми відібрали у Антанти її війська" – цю фразу приписують Леніну [305, с. 64].

Апарат радянської пропаганди та агітації був націлений на радянське населення, щоби перетворити його в покірну безлику масу. Для цього створено нова міфологія з новими "героями", "титанами", "гігантами" і епічними картинами боротьби як на традиційному, так і на трудовому фронті. Схожі методи використовували міфотворці і вожді мас Третього Рейху. Незначна різниця полягала, лише в їх більшій відвертості. Наприклад, з'їзд націонал-соціалістичної партії в Нюрнберзі в 1936 р. прикрашав плакат "Пропаганда допомогла нам прийти до влади. Пропаганда допоможе нам завоювати увесь світ". Процес централізації контролю над пропагандою призвів спочатку до створення міністерства пропаганди, а пізніше міністерства громадської освіти і пропаганди. Характерною рисою фашистської пропагандистської діяльності було ґрунтовне використання наукових розробок у цій сфері. Активно використовувалися напрацювання з психології підсвідомого. Відповідаючи на питання, чому Гітлер не приваблює іноземців, К. Юнг зазначав: "... для будь-якого німця Гітлер є дзеркалом його підсвідомого, у якому не для німця, звичайно, нічого не відображається. Він рупор, настільки посилюючий неясний шепіт німецької душі, що його може почути вухо його підсвідомого". Розроблені німецькими пропагандистами прийоми впливу на маси, до сьогодні використовуються в політтехнологіях. Це передусім театралізовані партійні з'їзди, масові зустрічі на стадіонах, радіотрансляції виступів лідерів на масові аудиторії тощо. Але основною характеристикою фашистської інформаційної політики, безумовно, є інформаційний монополізм.

На сучасному етапі наука має в розпорядженні такі теоретичні надбання, на базі яких здійснюється технологізація інформаційної боротьби, тобто відповідні державні і недержавні структури, що причетні до такої діяльності, здійснюють розробку і апробацію нових інформаційних технологій, прийомів, методів здійснення психологічного впливу, технічних засобів необхідних для такої діяльності. Подібні зрушення не могли не відбитися на зростанні ефективності застосування інформаційних технологій, яке може призводити до кардинальних змін в суспільній, економічній, політичній та іншій сферах окремої країни, або ж у світовому масштабі.

З кінця 1940 до середини 1980-х рр., в епоху так званої холодної війни, протистояння двох супердержав - СРСР і США - спричинило подальше вдосконалення форм і методів пропаганди та психологічної війни.

У 1970-х рр. остання інформаційна революція пов'язана з винаходом комп'ютера висунула на перший план нову галузь - інформаційну індустрію, яка пов'язана зі створенням технічних засобів, методів, технологій для нових знань. Стрімке зростання обсягів інформації й об'єктивна зміна умов психологічної діяльності людини в сучасному світі привели до перерозподілу питомої ваги даних про оточуючий світ, що надходять до індивіда за допомогою генетичних каналів і в результаті безпосереднього сприйняття дійсності, на користь даних, що отримуються ним із засобів масової інформації.

Сучасні можливості техніки в поєднанні з науковою та публіцистичною літературою і періодикою дозволяють ефективно впливати на розум, свідомість і психіку мільйонів людей. Інформація і пропаганда стали сьогодні настільки могутніми, що здатні впливати на появу, перебіг і кінцевий результат політичних подій, в т.ч. глобальних проблем миру і війни.

**Становлення інформаційних прав людини.** На теренах континентальної Європи намагання виділити об'єкт правової охорони, який би відображав суспільну потребу в захисті «автономії» особи, призвів до формулювання теорії «прав особистості», тобто невідчужуваних природних прав, пов'язаних із людиною як біосоціальною істотою [316, с. 125]. В. Осятинський стверджує, що особливість прав людини власне в тому, що не вимагає жодного обґрунтування. Належать вони кожній людині власне як людині, становлять немовби істотну частину буття людиною [630, с. 313]. Гідність людини є нерозривно пов'язана з фактом буття людиною. На буття людиною не мають впливу між іншим такі риси як вік, стан фізичного чи психічного здоров'я, інтелектуальний чи емоційний розвиток, освіченість тощо. Ніхто за жодних обставин не може бути позбавлений гідності [552, с. 43] Гідність людини не може залежати також від громадянства як правового зв'язку з державою [552, с. 42]. Зараз визнається, що гідність людини властива їй від природи, а не з будь-якого рішення влади, є основою прав людини, прав громадянина [607, с. 28].

Творцями сучасної доктрини прав людини вважаються діячі Просвітництва, які розвинули її на основі античної теорії природних прав і теорії суспільного договору як джерела державної влади. Монтеस्क'є сформулював принцип поділу влади на законодавчу, виконавчу і судову, і в його роботі «Про Дух законів» [261] він підкреслив взаємозалежність між свободою і верховенством закону. Ж.-Ж. Руссо в роботі «Суспільний договір» [406] визначає суспільний договір як основу свободи і рівності, при цьому рівність розглядається ним як умова свободи. Метою договору є створення позитивного права і гарантування свободи і інших прав. Ідея свободи, яка займає центральну позицію в моральній філософії Е. Канта, повинна бути відображена в правовій свободі, на яку має право кожна людська істота в силу її людськості [612, с. 22].

Ідеї просвітителів відкрили шлях для радикальних змін в реальності суспільного життя. Ще в кінці XVII століття були закріплені окремі громадянські свободи в Англії. Були окреслені права підданих корони, в тому числі окремі процесуальні гарантії і свободи осіб (Habeas Corpus Act, 1679) і Білль про права (1689). У другій половині XVIII ст.. після великих соціальних революцій: американської та французької, були проголошені епохальні документи, як Декларація незалежності (1776, США) і Декларації прав людини і громадянина (1789 і 1793, Франція). Передісторія і зміст цих декларацій відображає дві західні традиції прав. У країнах без абсолютних монархій в новій історії люди мають права, які обмежують уряд. Конституція є вищим законом, писана або неписана, а не воля володаря або держави. У країнах з постабсолютізмом держава має повноваження, а суспільство – обов'язки. Закон розглядається як свого роду подарунок від держави [630, с.28]. До сьогодні можемо бачити це в культурі англійської мови, яка використовується в правотворчості. В американській традиції, як правило, використовується поняття народу (people) і уряд (government), що свідчить про те, що люди мають той же статус, що і держслужбовці. Незалежні суди захищають права громадянина, докладаючи зусиль для того, щоб уряд діяв в рамках конституційних повноважень. Уряд перебуває в підпорядкуванні суспільству, і якщо порушує права громадян, то має нести за це відповідальність. У законодавстві континентальної Європи поруч з терміном

«народ», як правило, вживається «держава» (state) в різних формах – республіка (republic) або монархії (monarchy), що відображає стійкий характер держави як самого буття (один з буквальних переказів «state» – статус, становище, визначати, встановлювати.) Держава нібито «резервує» за собою монополію на управління суспільством - людьми.

Перша концепція, обґрунтована в ідеях Д. Локка, підкреслює невід’ємні права особистості і таких «природних» соціальних груп, як сім’я або церква; органи державної влади просто зобов’язані їх поважати. Ця традиція взяла гору в XVII ст. в Англії, особливо в американських колоніях, які в XVIII ст., воювали з британською державою. Хоча Англія поступово відійшла від неї, все ще йдеться про англо-американську традицію. Варто відзначити, що в Сполучених Штатах ідея прав людини не завадила знищенню місцевого населення (індіанців) і рабовласництва.

У той час на континенті переважає інша концепція. Держава вважається «гарантом спільного блага і відповідальною за забезпечення індивідуальних потреб» [636, с.11]. Як у російського письменника і публіциста М. Некрасова в «Забытой деревне»: «Вот приедет барин – барин нас рассудит, Барин сам увидит, что плоха избушка, И велит дать лесу», – думает старушка» [274]. Суспільство держав зі стійкими патріархальними традиціями влади очікує «батьківської» турботи від Батьківщини, що передбачає більш широке розуміння суспільних обов’язків і обов’язків уряду. На державу покладається не тільки гарантування безпеки і захисту життя, свободи і власності, але також забезпечення, при необхідності, задоволення основних потреб людини [660, с. 305].

Незважаючи на численні відмінності прототипами актів про права людини вважаються англійський Білль про права (1689), американська Декларація Незалежності (1776), і французька Декларація прав людини і громадянина (1789). Але це ще не були «права людини» в сучасному розумінні, тільки правомочності, які надавалися окремим людям в рамках, визначених суспільством.

XIX ст. відзначене апогеем колоніалізму і зростанням капіталізму, з одного боку, і скасуванням смертної кари, антиімперіалізмом, робітничим рухом і початком руху за права жінок – з іншого. В середині століття був ініційований

міжнародний гуманітарний рух, в основному в результаті злочинів, вчинених в Конго. У 1863 був сформований Міжнародний комітет Червоного Хреста і ратифіковано низку міжнародних конвенцій, що обмежили довільне застосування сили під час збройного конфлікту. Також значення набувають права меншин, особливо після першої світової війни. У ряді договорів і двосторонніх угод в Європі гарантується захист життя і свободи для всіх жителів таких країн, як Австрія, Болгарія, Угорщина і т.д., а також рівні політичні і громадянські права для членів усіх меншин. Хоча ці інструменти виявилися неефективними, положення про захист меншин стали відправною точкою для ідеї кодифікації прав людини в міжнародному праві.

Водночас, в цей же період сформульоване поняття «privacy», що стало прекурсором сучасного права на захист персональних даних. В 1890 р. американські юрист і С. Уоррен і Л. Брандейс визначили його як «the right to be alone». Першим прецедентом, створеним на основі наукових розробок «права бути залишеним у спокої», стало рішення Верховного Суду штату Джорджія у справі *«Павесіч vs. Нью Ігланд Лайф Іншуранс Ко.»* (1905 р.) [401]. Задовольняючи позов чоловіка, зображеного без його згоди в рекламному оголошенні, суд визначив об'єкт і мету правового захисту таким чином: «Той, хто бажає жити життям відносного усамітнення, має право обрати час, місце та способи, у які він буде піддавати себе громадському спостереженню». А у справі *Griswold vs. Connecticut* суддя Верховного суду США Дуглас вивів «право на приватність» з перших п'яти поправок до Конституції США, визнавши, що ці поправки «охороняють різні аспекти недоторканності приватного життя», зазначивши: «правом на недоторканність приватного життя старше ніж Білль про права» [659].

Усвідомлення зміни ролі інформації у суспільстві відбувалось поступово і нерівномірно в географічній перспективі. У 1946 р. Генеральна Асамблея ООН ухвалила одну зі своїх найперших резолюцій, де зазначено: «Свобода інформації є фундаментальним правом людини і ... критерієм для всіх свобод, яким присвячено Організацію Об'єднаних Націй» [410, с.8]. Проте, вперше на міжнародному рівні про право на інформацію було задекларовано в ст. 19



Загальної декларації прав людини. Так, Загальна Декларація прав людини визначила свободу шукати, одержувати і поширювати інформацію та ідеї складовою права кожної людини на свободу переконань і на вільне їх виявлення. Аналогічне закріплення право на інформацію одержало також в інших міжнародно-правових документах, Європейській Конвенції про захист прав людини і основних свобод (п. 1 ст. 10), Міжнародному Пакті про громадянські і політичні права 1966 р. (п. 2 ст. 19) та ін. На основі цього можна зробити висновок, що права на свободу інформації, свободу думки і слова належать до так званих прав «першого покоління» - громадянських і політичних прав, які від початку вважаються невід'ємною частиною людської особистості [210, с.94].

На етапі створення другого покоління прав людини принцип універсальності застосовувався з метою усунення розбіжностей. А. Бенуа, французький академік, політолог і журналіст, зазначає: «теорії прав людини, здається, мало властиве визнання культурного розмаїття з двох причин: по-перше, через фундаментальний індивідуалізм і вкрай абстрактну природу об'єкта, якому надаються права, по-друге, через її тісний зв'язок із Західною культурою». Якщо припустимо, що ідеологія прав людини всупереч її західним корінням, по-справжньому універсальна, виникають труднощі на рівні термінології. Термін «право» в розумінні індивідуальної властивості особи в середньовіччі не існував в жодній європейській мові. Це означає, що тривалий час не існувало навіть слова для позначення прав осіб, які б належали їм в силу їх людськості. Цей факт, а оцінює А. Макінтайр, ставить під сумнів реальність і змістовну наповненість цих прав. В арабській, китайській, японській мовах, а також в івриті і хінді, терміни, використовувані для позначення прав людини не передбачають їх універсальності – *yukt* і *ucita* (правильний), *nyayata* (справедливий), *dharma* (обов'язок), китайський – *chuan* і *li* – влада і інтереси, арабська *haqq* – закон, який перш за все означає істину [540].

Незважаючи на всі невідповідності, концепція XX ст. проклала шлях до прав «третього покоління», яким була потрібна нова роль держави. Концепція прав «третього покоління» визнає суверенітет держави над громадянами, в той же час доповнює його стандартами міжнародного права і міжнародної системою

забезпечення. Забігаючи вперед, Конвенція про захист прав людини і основних свобод та Хартія основних прав ЄС розширить права людини в географічному сенсі – за межі національних держав. Після вичерпання наявних національних засобів захисту, будь-який громадянин може індивідуально звернутися до Європейського суду з прав людини. У той же час, в системі ООН проти держави виступити може не громадянин, права якого були порушено, але інша держава. Численні історичні події свідчать про часте використання подвійних стандартів. Наприклад – один з творців ЗДПЛ Р. Кассін, який виступав за культурний релятивізм в колоніальних війнах, писав: «в відсталіх колоніальних суспільствах права людини можуть поставити під загрозу громадський порядок» [542, с. 962].

Оскільки, процесу розвитку ідеї прав людини властиві як кількісні, так і якісні зміни, то, безперечно, варто погодитись з думкою, що розширює колективні права людини (третє покоління) піднесення та поглиблення права на інформаційний простір світу, на надання різноманітних послуг, що ґрунтуються на інтелектуальних інформаційних технологіях (зокрема на новітніх технологіях досліджень) і технологіях зв'язку (глобальна мережа «Інтернет»), забезпечення інформаційних відносин усередині країни і за кордоном. До розвитку сучасних кібернетичних систем під простором поширення інформації розуміли атмосферу, стратосферу, космос, водні акваторії океанів і морів. Зараз розуміння інформаційного простору включає додатково кібернетичні та віртуальні системи [511, с. 102].

Під час холодної війни політики неохоче згадували про права людини. У кожної держави на те були свої причини. В СРСР панував в сталінський терор, Китай будував комунізм, Сполучені Штати більше дбали про свій суверенітет. Що цікаво, Сполучені Штати не підтримували ідею індивідуальних прав людини на міжнародному рівні. Д. Ф. Даллес заявив, що США «не буде учасником жодного документа з прав людини, прийнятого Організацією Об'єднаних Націй» [603, с.59]. І тільки в 1966 р. стало можливим прийняття наступних актів з прав людини – Міжнародного пакту про громадянські і політичні права та Міжнародного пакту про економічні, соціальні і культурні права. З цього часу, можемо говорити про політизацію прав людини. Більш того, після Конференції з

безпеки і співробітництва в Європі, права людини широкого визнання не лише в Європі набули, а й підтримку правозахисників в країнах Східного блоку. У заключному акті конференції була встановлено право «знати про свої права», яке можна вважати прекурсором інформаційних прав людини.

Помилкою буде вважати, що існували тільки західні модифікації прав. Не вдаючись в подробиці, теоретики комуністичного табору пропонували власну «соціалістичну концепцію прав людини». Відкидаючи природне право і справедливість як джерело, вона ґрунтувалася на нормах позитивного права. Соціалісти проголошували взаємний зв'язок прав і зобов'язань. Кожному праву громадянина повинен відповідати обов'язок держави.

Взаємозв'язок прав та обов'язків знаходимо також в соціальному вченні Католицької Церкви. Однак, згідно з цим вченням, її джерелом є природне право. [631] Персоналістична концепція (від лат. *persona* - особа) є головною в християнському персоналізмі [482, с. 42] К. Войтила сформулював персоналістичну норму, яка визначає людську особу як цінність саму в собі, настільки цінну, що за жодних обставин не можна використовувати її як засіб для досягнення мети, оскільки це вона є самоціллю. Ця виняткова цінність обумовлює належне ставлення до кожної людської особистості [670, с.42]. З цієї точки зору в своєму навчанні Іван Павло II багаторазово підкреслює пріоритет особи перед суспільством, з чого слідує, що жодна людина не може бути ніколи використана як засіб, навіть задля добробуту і розвитку усієї спільноти (людства).

Віросповідання пов'язане з дотриманням певних таїнств. І цікавим з точки зору захисту інформаційних прав людини є таємниця сповіді. Сповідь, є одним із семи християнських таїнств, установлених самим Христом, про що і згадується в Євангеліях. Покаяння, як таїнство, відомо майже всім релігійним конфесіям.

Покаяння – один з найважливіших обрядів християнської церкви. Полягає в усному визнанні гріхів перед священиком, завдяки чому вважається, що людина при каятті, яке йде від серця, одержує прощення через священика від Бога. Зрозуміло, що в поняття «гріх» входять такі дії, що і у світській державі підлягають кримінальному покаранню. Тому дуже часто людина, що сповідує свої гріхи перед священиком, визнаючи себе винною у злочині, залишається

недосяжною для правосуддя. «Західна католицька церква, виходячи з думок Хоми Аквінського і цілого ряду вчених-богословів, встановлює «печатку мовчання» – *sigillum confes-sio-nis*, безумовно забороняючи священикам виказувати будь-кому те, що він почув під час сповіді. XXI стаття IV Латеранського собору попереджає, що за порушення цього правила священика очікує довічне ув'язнення у монастирі «найсуворішого» ордену»[133, с. 493].

Подібних правил дотримувалася і православна церква. Перший, хто зважився порушити таємницю сповіді в Росії, став Петро I, вирішивши використовувати довіру віруючого до священика в боротьбі проти своїх ворогів.

Одночасно варто звернути увагу, що таємниця сповіді в переважній кількості країн світу не проголошується як суб'єктивне право. Чого не можна сказати про деякі інші види особистої інформації, наприклад персональні дані або таємниця листування та іншої кореспонденції.

Так, науковці стверджують, що у інків вже до початку XVI століття існували поштові гінці, які, крім державних повідомлень, доставляли до столу царя свіжу рибу, фрукти та інші продукти. Як вказує Сьєса де Леон в «Хроніці Перу», у інків законами було передбачено збереження таємниці відомостей, що містяться в пересилаються: «І в такому строгому секреті вели свої справи ті, хто проживав на поштових станціях, що ні на прохання, ні під погрозами, ніколи вони не розповідали про те, що збиралися передати в повідомленні, нехай навіть повідомлення вже пішло далі [поштою]»[227].

Поняття таємниці листування з'являється в різні указах і посадових інструкції починаючи з XVII століття і стає поширеною правовою нормою до XIX століття. Систематичні порушення таємниці зв'язку до цього часу сприймаються саме як порушення і причетні чиновники поштових відомств і чорних кабінетів змушені виправдовуватися перед громадською думкою і навіть перед начальством. Так виглядало пояснення з приводу скарг на відкриття листів московським поштамтом в 1791 [175]«... Я починаю сомневаться, не распечатываются ли там [в Берлине] сии письма столь неискусным образом, ибо клеєм подлеплять не есть способ, употребляемый в России. Хотя и после меня рижский почтмейстер свидетельствует письма, но я уверен, что он своё искусство

знает и не подаёт сомнения корреспондентам. Московский почт-директор И. Б. Пестель.»

Право на таємницю листування (пізніше до листування додалися телефон, телеграф та інші види зв'язку) стали вважатись похідними від права на таємницю приватного життя ( «privacy» - приватність).

Причини спеціального відокремлення поняття «персональні дані» із загальної маси різноманітних даних пов'язані з тим, що вони є одним з найбільш важливих, делікатних та вразливих атрибутів недоторканості приватного життя людини, що потребує захисту за допомогою юридичних та організаційних заходів [257, с. 100].

Починаючи з кінця 60-х рр. XX століття на теренах Європи у багатьох країнах почали розроблятись національні закони стосовно регулювання питання автоматизованої обробки та захисту персональних даних. Так, В. Брижко виокремлює основні причини для руху в напрямі удосконалення нормативно-правового упорядкування відносин у сфері захисту персональних даних, із яких виходять європейські та інші країни: усунення передумов та порушень прав людини на її персональні дані; розвиток е-комерції; гармонізація національних законодавств [64, с. 31-32].

Поруч із захистом персональних даних на базі свободи інформації, принципу гласності, свободи слова та друку в другій половині XX ст. як окреме суб'єктивне право виокремлюється *право на доступ до інформації*. Історія цього права корінням сягає ще 1766 р., коли в Швеції було закріплено “права знати” у Декларації прав людини і громадянина 1789 р. [183]. Закон був суттєво послаблений після перевороту Густава III у 1772 р., тим не менше, закладені ним принципи стали основою для принципів, закладених у XX ст. А рівень Швеції за ВВП і соціальними стандартами, а також культура підзвітності й прозорості є найкращим доказом важливості забезпечення права на доступ до інформації й, зокрема, доступу до публічної інформації. Проте, ідея конституційного закріплення права на доступ до інформації була відроджена лише в другій половині XX ст. Проголошення “права знати” у країнах Європи та Сполучених Штатах Америки – це наслідок становлення громадянського суспільства та

демократичних перетворень, а в країнах, які розвиваються, – це умова утвердження громадянського суспільства.

На межі XX і XXI століть інформаційні ресурси стали визначальним фактором розвитку і більшість країн констатували початок нової епохи – інформаційного суспільства. У 2000 р. прийнята Окінавська хартія глобального інформаційного суспільства, у якій було закріплено, що «всі люди повсюдно, без винятку повинні мати можливість користуватися перевагами глобального інформаційного суспільства. Стійкість глобального інформаційного суспільства ґрунтується на стимулюючих розвиток людини демократичних цінностях, таких як, вільний обмін інформацією та знаннями, повага до особливостей інших людей» [287]. У той же час в інформаційному суспільстві руйнується традиційна ієрархічна система цінностей. Кардинально змінюється і трактування понять «людина» і «її особистість». Організаційним принципом культурного життя людини стає принцип трансформації. Свобода особистості стає гарантом її безпеки [259].

Таким чином, проблема прав людини вийшла далеко за межі окремої держави, а обсяг прав і свобод людини в сучасному суспільстві визначається не лише особливостями певного співтовариства людей – національної держави, а й розвитком людської цивілізації в цілому. В науковій думці відсутній однозначний підхід до визначення інформаційних прав людини. П. М. Сухорольський у дослідженні підкреслює, що, наприклад, в англomовних джерелах виділяються так звані цифрові права людини (digital rights), під якими розуміють сукупність загальновизнаних та інших прав людини у контексті поширення нових цифрових технологій, зокрема інтернету [449, с.21].

Розробка «Декларації прав людини і правових норм в інформаційному суспільстві» [560] стала першою спробою визначення міжнародно-правових рамок в цій сфері. Декларація була розроблена Комітетом експертів Ради Європи з інформаційного суспільства. Значну увагу на форумі було присвячено розробці норм відповідальної поведінки в інформаційному суспільстві. Учасники Міжнародного форуму «Права людини в інформаційному суспільстві: відповідальна поведінка головних дійових осіб» ініційованого Радою Європи,

закликали уряди захищати всі права людини, які стосуються інформаційного суспільства, від свободи слова до приватності і копірайту, не забуваючи про завдання подолання інформаційної нерівності і про належне управління. На їхню думку, «цілковита повага свободи слова та інформації державними та недержавними інститутами є необхідною передумовою побудови вільного інформаційного суспільства для всіх, а інформаційно-комунікаційні технології не повинні використовуватися для обмеження цієї фундаментальної свободи» [6].

Інститут інформаційної безпеки людини в Україні і світі є наймолодшим, порівняно з інформаційною безпекою держави чи суспільства. Протягом багатьох тисячоліть інформаційна безпека розглядалась, насамперед, з перспективи інтересів держави. Згодом інтенсифікація процесів інформатизації в усіх сферах, а особливо, зростання значення технічного захисту інформації зумовило становлення правового забезпечення захисту інформації як невід'ємної складової безпеки підприємств, установ та організацій, а також окремих галузей господарства. Так, в соціальній сфері виникла небезпека нового типу нерівності: реальна загроза «інформаційного розшарування», яка веде до потенційну загрозу формування інформаційної еліти суспільства. У духовно-культурній сфері суспільства небезпека застосування в протиправних цілях інформаційних технологій призвела до загрози маніпулювання людською свідомістю, психічної і соціальної дезадаптації людини. Дещо забігаючи наперед зазначимо, що небезпека заподіяння шкоди здоров'ю людини в результаті використання інформаційних технологій породила загрозу розвитку нових видів захворювань.

Військово-політична сфера життєдіяльності сучасного суспільства відрізняється низьким ступенем захисту інформації про особу людини, що міститься в державних системах і комп'ютерних мережах. Небезпека контролю над людиною, маніпулювання, поширення конфіденційної інформації ведуть до потенційної загрози інформаційного тоталітаризму.

На межі тисячоліть гостро повстало питання про міжнародну інформаційну безпеку, а також кібербезпеку у складі інформаційної безпеки. Негативним ефектом застосування сучасних технологій у військово-політичній сфері стали все ширші можливості застосування інформаційної зброї.

Тим не менш, на кожному з вищезгаданих етапів інформаційна безпека людини залишалась і залишається вторинним питанням.

### **1.3. Місце вчення про інформаційну безпеку в сучасній науці та методологічні засади інформаційно-правових досліджень**

Наукові дискусії в сфері інформаційної безпеки особливо актуалізувались в останні роки ХХ сторіччя. При чому, як вже зазначалось, сучасні методи дослідження базуються на різних світоглядних позиціях щодо соціального світу і людини, по-різному також вирішують дослідницькі завдання, а також використовують різні стратегії досліджень.

Первинно, до другої половини ХХ століття, інформаційна безпека розглядалась, насамперед, як інформаційна безпека держави. Згодом інтенсифікація процесів інформатизації в усіх сферах, а особливо, зростання значення технічного захисту інформації зумовило становлення правового забезпечення захисту інформації як невід'ємної складової безпеки підприємств, установ та організацій, а також окремих галузей господарства. На межі тисячоліть гостро повстало питання про міжнародну інформаційну безпеку, а також гостро повстало питання кібербезпеки у складі інформаційної безпеки. Тим не менш, на кожному з цих етапів інформаційна безпека людини залишалась вторинним питанням. Саме до такого висновку призвів аналіз наукових досліджень питань інформаційної безпеки.

Дзьобань О.П. і Пилипчук В.Г. вважають, що ідеал безпечного життя – дотримання в міжнародних відносинах загальноновизнаних норм справедливості – сягає до часів античності, а наукове обґрунтування проблем національної безпеки взагалі й інформаційних її аспектів зокрема, вбачають у творах Т. Гоббса та І. Канта [116, с.140]. З багаточисельних досліджень, що містили філософське осмислення проблем безпеки, зокрема Локка, Маркса, Енгельса, Тойнбі, Расела, Ясперса та інших, хотілось би звернути увагу на концепцію, запропоновану А. Бергсоном, який поєднував [інформаційну] безпеку з розумінням закритого і відкритого суспільства, а також вбачав шлях до безпечного стану людства через



відмову від «штучних потреб», спричинених переважанням розвитку в останні століття «тіла» людства, а не його «душі» [42].

Концептуально погоджуємось з позицією, що «подальші адекватні реальній соціальній дійсності наукові розвідки в царині інформаційної безпеки без опори на класичну спадщину уявляються досить сумнівними» [116, с.146]. При цьому, ці автори окреслюють чотири аспекти, на які звертали увагу класики в своїх працях: (1) інформаційно-етичний – Августин Блажений, І. Кант, Р. Оуен, А. Бергсон, А. Швайцер); (2) зв'язок досягнення безпечного стану і господарської та економічної структури, а також колізії природного й громадянського станів особистості – Цицерон, Гоббс, Локк; (3) Договірні відносини між державами задля формування відповідних організаційно-правових передумов і утворення об'єднань держави – Гроцій, Сен-Сімон, Ясперс, Тойнбі; (4) соціальний характер небезпек, які можна усунути лише змінивши структуру суспільства – Еразм Роттердамський, Франк.

Важливо, що теоретики інформаційного суспільства, також попереджали про врахування інформаційної безпеки як визначальної умови становлення нової інформаційної епохи – Й. Масуда, Ю. Хаяші, Д. Белл, О. Тофлер, М. Кастельс, З. Бжезинський, М. Маклюен, В. Іноземцев, П. Друкер, Ф. Вебстер, Д. Барні, А. Пенті та інші. Інформації у всіх концепціях згаданих дослідників (незалежно від назви) надається телеологічний статус, це обумовлює онтологічний вимір інформаційної безпеки будь-якої соціальної системи сучасності, осьовою детермінантою якої є зростання впливу розвитку інформаційно-комунікативних технологій.

Таким чином, наприкінці ХХ століття правове забезпечення інформаційної безпеки інтегрується з групою інформаційних соціальних відносин, що стрімко розвиваються, і формують на початку інститут у межах адміністративного права, а потім – комплексну галузь інформаційного права.

Тому слід відзначити значну кількість вчених-правників, чиї дослідження інформаційної сфери розпочинались в межах адміністративного права і інших галузей правової науки, а згодом значної уваги в їх працях набули питання інформаційного права – зокрема, Арістова І.В., Брижко В.М., Беляков К.І., Белевцева В.В., Гуцалюк М.В., Калюжний Р.А., Кормич Б.А., Копан О.В.,

Копилов В.А., Логінов О.В. Новицький А.М, Настюк В.Я., Олійник О.В., Рассолов М.М., Тихомиров О.О., Цимбалюк В.С. та ін. Іншу групу дослідників становлять вчені, що починали дослідження в рамках інших галузей наук, як соціальних, так і технічних, проте на сьогодні їх напрацювання становлять інтегральну частину інформаційно-правової науки, зокрема, щодо питань інформаційної безпеки – К.І. Беляков, О.А. Баранов, О.Д. Довгань, О.П. Дзьобань, Д.В. Дубов, І.Б. Жилияєв, Д.В. Ланде, В.А. Ліпкан, А.І. Марущак, М.А. Ожеван, В. Остроухов, І.Н. Панарін, В.М. Петрик, Г.Г. Почепцов, В.Г. Пилипчук, Є.Д. Скулиш, М.П. Стрельбицький, В.М. Фурашев, М.Я. Швець, В.І. Ярочкін та інші.

Однією з перших українських наукових праць, предметом дослідження якої був державно-правовий механізм інформаційної безпеки як системне поняття, стала захищена у 2014 р. Кормичем Б.А. докторська дисертація «Організаційно-правові основи політики інформаційної безпеки України» [210]. В цій праці вперше комплексно було проаналізовано організаційно-правові засади процесу формування і реалізації політики інформаційної безпеки України, а також виявлено специфіку змісту, форм та методів забезпечення інформаційної безпеки людини, суспільства, держави. До правової бази інформаційної безпеки було віднесено норми декількох галузей права, насамперед: конституційного, адміністративного, інформаційного, але її головним системоутворюючим чинником виступають єдині концептуальні засади державної політики інформаційної безпеки. Окрім того, Кормич Б.А. визначав правовий статус людини як об'єкта інформаційної безпеки, що визначається її правами в галузі інформації [210, с.36].

В 2004 р. було видано перший український навчальний посібник з інформаційного права «Основи інформаційного права», де питанням інформаційної безпеки було присвячено окремий розділ – «Інформаційна безпека як об'єкт інформаційного права» [294]. Науковці прогнозували, що в майбутньому інформаційна безпека, у міру розвитку інформаційного суспільства, виокремиться з інформаційного права в окрему субінституцію подібно до права інтелектуальної власності, його провідних складових — авторського права та права промислової власності [294]. Важливо, що вже на цьому етапі фахівці звертали увагу на необхідність створення базового закону в галузі

інформаційного права – Інформаційного кодексу чи Кодексу України про інформацію.

На цьому етапі становлення наукової та правової категорії «інформаційна безпека» ототожнення її із захистом інформації було досить поширеним явищем, а подекуди має місце і досі здебільшого в зарубіжній науковій літературі [617, 616]. Безперечно, правове регулювання захисту інформації є складовою інформаційної безпеки, проте не є їй тотожним.

Адміністративно-правовому захисту інформаційної сфери було присвячено монографію Настюка В.Я. та Белєцева В.В. «Адміністративно-правовий захист інформації», де обґрунтовано, що «захист інформації за своїм змістом передбачає, з одного боку – нівелювання небезпеки, з іншого – підтримання стану захищеності життєво важливих інтересів людини суспільства, держави від різного роду викликів та загроз» [268].

Більш широко і комплексно питання адміністративно-правового забезпечення інформаційної безпеки України досліджує Олійник О.В. в монографії «Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки України» [290]. Автор пропонує широке розуміння забезпечення інформаційної безпеки як здійснення комплексу системних превентивних заходів з надання гарантій захисту від негативних інформаційних впливів: життєво важливих інтересів особи, суспільства, держави, політичного, економічного, науково-технічного, гуманітарного, соціокультурного розвитку, підтримання оборони, державної та екологічної безпеки, системи державного управління на необхідному рівні; забезпечення інформаційного суверенітету та безпечного розвитку національного інформаційного простору; від маніпулювання інформацією, дезінформування та впливів на свідомість, підсвідомість і психіку індивідів, суспільних груп, суспільства в цілому; своєчасність і адекватність заходів протидії та нейтралізації всього спектру негативних безпеко генних чинників, що можуть бути застосовані проти України» [290, с.368-369]. В цьому аспекті одним із важливих завдань, які мають бути вирішені в цьому дослідженні є визначення місця інформаційної безпеки людини у системі забезпечення інформаційної безпеки та зв'язків між її об'єктами

і суб'єктами; виявлення методологічних проблем правового регулювання відносин щодо інформаційної безпеки людини; окреслення пріоритетних напрямів державної політики України у сфері інформаційної безпеки людини.

Розділяючи думку Баранова О.А., що «рафінованих чистих суспільних відносин, які піддаються регулюванню нормами тільки однієї галузі права не існує» [30, с.119], зауважимо, що інформаційні правовідносини щодо інформаційної безпеки людини регулюються також іншими нормами права. Інформаційні відносини становлять додатковий предмет дослідження науковців з інших галузей права, зокрема В.Д. Гавловський, О.В. Кохановська, Л.П. Коваленко, Н.А. Савінова, О.О. Тихомиров та інші.

Окремої уваги заслуговують дослідження у галузі міжнародного інформаційного права, що також переживає свій етап становлення у системі міжнародного права. Серед українських дослідників слід згадати праці Пазюка А.В., Запорожець О.Ю., Забари І.М., Кісілевич-Чорнойван О. М., Боднар І.Р., Шахбазян К. С. та інших. Важливо, що повстає нова плеяда науковців, чие коло наукових інтересів зосереджене на інформаційно-правових дослідженнях, зокрема, Г.М. Красноступ, Т.М. Кронівець, Г.М. Линник, К.С. Мельник, А.Ю. Нашинець-Наумова, О.В. Стоєцький, Д.В. Сулацький, В.С. Шاپіро, І.О. Трубін, Р.В. Радейко, В.С. Політанський, О.В. Шепета та інші.

Значна частина молодих науковців є представниками наукової школи Ліпкана В.А., зокрема М.І. Дімчогло «Консолідація інформаційного законодавства України», В.А. Залізняк «Систематизація інформаційного законодавства України», Ю.Є. Максименко «Теоретико-правові засади забезпечення інформаційної безпеки України», Л.І. Руднік «Право на доступ до інформації», К.Г. Татарнікова «Кодифікація законодавства України про інформацію». Згадані роботи мають різний рівень теоретичної і практичної опрацьованості, зокрема, деякі надають суперечливі за змістом висновки, наприклад, дослідження щодо різних форм систематизації інформаційного законодавства. Водночас, необхідно зазначити, що результати дослідження теоретико-правових засад забезпечення інформаційної безпеки, здійсненого Максименко Ю.Є., містили низку цінних висновків, зокрема, на підставі аналізу

досвід Європейського Союзу у сфері забезпечення інформаційної безпеки, було визначено потенційні загрози інформаційній безпеці України, тенденції та перспективи нормативно-правового регулювання окремих аспектів інформаційної безпеки України. Також серед головних проблем нормативно-правового забезпечення інформаційної безпеки України виокремлено: наявність численних нормативно-правових актів різної юридичної сили у цій сфері; закріплення важливих засад підзаконними нормативно-правовими актами; певна невідповідність чинній Конституції України; неузгодженість нормативно-правових актів та наявність багатьох прогалин; неоднозначність та неузгодженість закріплених дефініцій і відсутність навіть базових з них; наявність значного масиву декларативних положень без механізму їх правореалізації; наявність численних бланкетних норм права, що не призводять до очікуваного ефекту; наявність чисельних абстрактних, суб'єктивних понять, що потребують офіційного тлумачення чи чіткого визначення; низький рівень правореалізації норм права, що регулюють суспільні відносини у сфері забезпечення інформаційної безпеки України [248, с.17-18]. Як можемо бачити, значна кількість означених у 2007 р. проблем й досі залишається не вирішеною.

В 2011 р. Линником Г.М. було здійснено дослідження на тему «Адміністративно-правове регулювання інформаційної безпеки України» в якому обґрунтовано систему адміністративного законодавства в сфері інформаційної безпеки України, а також розроблено пропозиції щодо шляхів підвищення ефективності адміністративно-правового регулювання інформаційної безпеки України, а саме удосконалити адміністративно-деліктне законодавство в сфері інформаційної безпеки України; забезпечити громадський (суспільний) контроль за діяльністю органів державної влади шляхом більш якісного та повного висвітлення їх діяльності в ЗМІ, а також надання можливості безкоштовного доступу громадян до інформації; проводити безкоштовні курси громадянам щодо оволодіння навичками користування інформаційними технологіями; спеціалізовані служби, основним завданням якої було б координація дій державних та недержавних інституцій у сфері забезпечення інформаційної безпеки України [229, с.18].

Політанський В.С. у дисертації «Право на інформацію як фундаментальне право людини» визначає доцільність віднесення права на інформацію в сучасному його вигляді до третього покоління прав людини виходячи з історичних умов, особливостей розвитку та функціонального призначення [316, с.20]. На нашу думку, це твердження суперечить реальності інформаційного суспільства, адже інформаційна складова присутня в кожному праві людини і громадянина, з чим, зрештою, погоджується і сам автор, називаючи право на інформацію фундаментальним. Водночас, заслуговують на увагу проблеми реалізації права на інформацію, серед яких основними Політанський В.С. називає: (а) необхідність законодавчого регулювання відносин у галузі права на інформацію, що виникають при використанні глобальних інформаційно-комунікаційних мереж; (б) правове забезпечення надання відомостей органами публічної влади та місцевого самоврядування, які не відповідають дійсності; (в) порушення права на таємницю приватного життя; (г) несвоєчасне надання інформації чи навмисне приховування інформації; (д) поширення відомостей, які не відповідають дійсності, що ганьблять честь і гідність особи; (е) невиконання обов'язку органів державної влади інформувати про свою діяльність та про ухвалені рішення тощо [316, с.17].

Дискусійним залишається питання щодо методології наукових досліджень інформаційної безпеки. На початках методологічною основою інформаційного права щодо з'ясування нових соціальних явищ визначався цивілізаційний підхід [294]. Згідно такого бачення сучасна методологія наукових досліджень поряд з використанням перевірених часом традиційних методів і підходів потребує нових для усвідомлення складних соціальних процесів, які мають і культурологічно-правову спрямованість. І пропонувалось інтегральне спрямування методології вивчення соціального буття — соціальна синергетика. Погоджуємось з думкою, що методологія інформаційно-правових досліджень має враховувати поліаспектність та комплексність предметної сфери, яка знаходиться на межі соціальних і технічних наук. Задля використання сучасних досягнень світової науки цінним вбачається використання трансдисциплінарної стратегії досліджень Іммануїла Валлерстейна [663, с.13-40]., що дозволяє виявляти подібності та

зв'язки між явищами, і який був запропонований на Всесвітній конференції ЮНЕСКО з вищої освіти – 2009: "Нова динаміка вищої освіти і науки для соціальної зміни і розвитку", як один з основних способів дослідження складних багатфакторних проблем ХХІ століття.

Основними осередками правових досліджень в галузі інформаційної безпеки на сьогодні в Україні є Науково-дослідний інститут інформатики і права Національної академії правових наук України, Навчально-науковий інститут інформаційної безпеки Національної академії Служби безпеки України, Національний інститут стратегічних досліджень. Окремі інформаційно-правові дослідження здійснюються також в Національному юридичному університеті імені Ярослава Мудрого, Київському національному університеті імені Тараса Шевченка, Національному університеті «Одеська юридична академія», Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського», Національному університеті «Львівська політехніка», Національній академії внутрішніх справ, Національному авіаційному університеті та інших наукових установах.

Зокрема, в Науково-дослідному центрі правової інформатики у складі Академії правових наук України (з 2010 р. – Національної академії правових наук України), під керівництвом М.Я. Швеця було започатковано наукову школу правової інформатики, дослідження в її межах заклали підґрунтя для становлення і розвитку інформаційного права як комплексної галузі права. В 2011 р. згідно з рішенням президії НАПрН України діяльність НДЦПІ НАПрН України крім актуальних проблем правової інформатики була зосереджена на дослідженні теорії інформаційного права, правових проблем інформаційної діяльності, державно-правових проблем інформаційної безпеки, юридичної відповідальності за правопорушення в інформаційній сфері, відповідного історичного та іноземного досвіду. Згодом назву було змінено на НДІ інформатики і права, в якому вже сформувалась наукова школа інформаційного права, розпочато формування наукової школи філософії інформаційного права та наукової школи інформаційної безпеки (в галузі юридичних наук), значення яких актуалізується в

умовах інформаційної глобалізації та інтеграції України у світовий інформаційний простір.

В останні роки дослідження питань пов'язаних з інформаційною безпекою, в тому числі правового її забезпечення, особливо актуалізувалось, що має як позитивні, так і негативні наслідки для вітчизняної науки і українського суспільства. Зокрема, 3 березня 2016 р. на загальних зборах Національної академії правових наук України затверджено Пріоритетні напрями розвитку правової науки на 2016-2020 рр., які порівняно з попередніми роками мають більш прикладний характер. Зокрема, в напрямку правового забезпечення інформаційної сфери України визначено необхідність наукового розкриття таких тем як: “Актуальні проблеми забезпечення інформаційної безпеки України, як однієї із основних функцій держави”; “Правові засади захисту персональних даних, інформації з обмеженим доступом, технічного захисту інформації, протидії негативним інформаційним впливам та впливам інформаційних технологій на шкоду людині, суспільству та держави”; “Основи правової інформатики, системної інформатизації нормотворчої, правозастосовної й правоосвітньої діяльності, розвитку електронного державного управління”; “Проблеми впровадження й розвитку інформаційно-правових підсистем електронного парламенту та уряду, електронних систем і баз даних у галузі держави і права в контексті децентралізації влади в Україні”[444].

Слід звернути увагу, що до розробки правового забезпечення питань, які безпосередньо пов'язані з інформаційною безпекою людини, суспільства і держави, що раз більше долучаються громадські організації. Активність громадянського суспільства безперечно є свідченням розуміння проблеми фахівцями в фахових колах – правничих, освітніх, медійних та серед фахівців з безпеки. Проте, такі ініціативні групи зачасти не можуть забезпечити належного наукового осмислення; не володіють правничою, в тому числі нормотворчою, технікою; не спроможні врахувати всі ризики. Водночас, фінансування за рахунок грантових коштів, в тому числі зарубіжних і міжнародних організацій, створює небезпеку нав'язування відповідної ідеологічної позиції певним громадським ініціативам [160].



Водночас, суперечливим залишається питання подальшого системного розвитку науки інформаційного права. В сучасних умовах становлення інформаційного суспільства, національного інформаційного простору та глобального інформаційного протиборства, стрімкого розвитку інноваційних технологій та інших напрямків інтелектуальної діяльності, актуалізується проблема розвитку правової науки та потреба виокремлення інформаційного права і права інтелектуальної власності в окрему наукову спеціальність [230, с.5-17].

І хоча, наказом МОН України від 29.09.14 р. № 1081 було затверджено паспорт наукової спеціальності “Інформація і право” 12.00.13 – “Інформаційне право; право інтелектуальної власності”, а згідно з п. 9 цього наказу Департаменту атестації кадрів вищої кваліфікації МОН України доручалося забезпечити підготовку змін до Переліку наукових спеціальностей, затвердженого наказом Міністерства освіти і науки, молоді та спорту України від 14.09.11 р. № 1057, щодо включення спеціальності 12.00.13 “Інформаційне право; право інтелектуальної власності”, проте його положення досі залишаються нереалізованими [353, с.3].

### **Висновки до розділу 1**

В результаті аналізу доктринальних підходів було встановлено, що наукові підходи до категорії «безпека» і «інформаційна безпека» існують фактично в кожному суспільстві та на кожному історичному етапі існування людства, проте сучасне їх розуміння значною мірою залежить від занурення конкретного суспільства, людини і держави в реальність інформаційного суспільства. Саме в таких умовах проблематика інформаційної та кібернетичної безпеки набуває особливої ваги з метою встановлення балансу інтересів особи, суспільства, держави та міжнародного співтовариства.

Зміст інформаційної безпеки людини було досліджено з огляду на гносеологічний аспект відображення предмета в теорії, який полягає в тому, що явища і процеси відображаються у свідомості людини не дзеркально - як результат споглядального сприйняття дійсності, а через призму практично-

діяльного відношення людини до світу і до самої себе, власних потреб і інтересів. Таким чином, безпека є усвідомленим явищем для конкретного суб'єкта суспільних відносин. Виходячи з того, що безпека є усвідомлене явище, можна зробити висновок, що усвідомлення її необхідності обумовлює глибоке розуміння сутності проблем, що виникають, реальних загроз.

Розкриваючи філософські проблеми безпеки як соціального явища, відзначаємо, що розуміння інформаційної безпеки і усвідомлення її необхідності відбувається і виражається як на чуттєвому (підсвідомому), так і на раціональному рівнях. Оскільки самозбереження є здатністю і основною властивістю свідомості людини, то прагнення до безпеки, в тому числі інформаційної, є виразом розумності людини, проявом усвідомленого змісту її буття, її суспільного і морального сенсу. Безпека при такому підході виступає як невід'ємний атрибут існування. Автор власне підтримує цю позицію, що не слід пов'язувати існування безпеки як явища виключно зі своїм антиподом – небезпекою.

В сучасній правовій науці виявлено наявність множини підходів до розуміння як загальної категорії «інформаційна безпека», так і родової категорії «інформаційна безпека людини». При цьому поширеним є ототожнення інформаційної безпеки людини з її забезпеченням. Це, на нашу думку, є методологічною помилкою, оскільки забезпечення (щодо інформаційної безпеки людини) стосується більшою мірою заходів (технічних, організаційних, правових, кадрових тощо), а сама безпека – суб'єктивного переживання людиною, що відображає активний зміст її свідомості, яка здатна прогнозувати, передбачити і уявити небезпеки, а також своєчасно і адекватно на них відреагувати.

Наступною дилемою, що має місце в правових (і не лише) дослідженнях інформаційної безпеки є протиставлення її як стану і процесу. На нашу думку, у самому загальному вигляді під інформаційною безпекою людини можна розуміти її здатність зберігати свої істотні властивості, і забезпечувати власне існування і розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Тобто, не слід обмежуватись розумінням її як «стану», а найбільш відповідним, на нашу думку, є комплексний підхід, згідно з яким інформаційна безпека

визначається через її істотні риси, найбільш важливі основні функції, беручи до уваги постійну динаміку інформаційних і соціальних систем.

Тому задля визначення категорії «інформаційна безпека людини» було досліджено її онтологічний, гносеологічний і логічний зміст. І встановлено, що онтологічне розуміння інформаційної безпеки опирається на ціннісному вимірі об'єкта безпеки, який виражається через потреби людини, а можливість їх реалізації в правовому полі закріплюється через її права і свободи.

З огляду на вищезазначене, в цій праці взято до уваги історичні передумови захисту інформації, використання інформаційних впливів на людину в інтересах держави та інших суб'єктів, а також зародження інформаційних прав людини, зокрема, права на захист персональних даних та доступ до публічної інформації. Очевидно, цим переліком не вичерпується проблема, проте обмежений обсяг роботи і завдання дослідження обумовили саме такий вибір. В результаті проведеного аналізу встановлено, що інститут інформаційної безпеки людини в Україні і світі є наймолодшим, порівняно з інформаційною безпекою держави чи суспільства. Протягом багатьох тисячоліть інформаційна безпека розглядалась, насамперед, з перспективи інтересів держави. Згодом інтенсифікація процесів інформатизації в усіх сферах, а особливо, зростання значення технічного захисту інформації зумовило становлення правового забезпечення захисту інформації як невід'ємної складової безпеки підприємств, установ та організацій, а також окремих галузей господарства. Так, в соціальній сфері виникла небезпека нового типу нерівності: реальна загроза «інформаційного розшарування», яка веде до потенційної загрози використання інформаційною елітою суспільства новітніх засобів в політичній сфері, зокрема встановлення т.зв. «цифрової диктатури». У духовно-культурній сфері суспільства небезпека застосування в протиправних цілях інформаційних технологій призвела до загрози маніпулювання людською свідомістю, психічної і соціальної дезінтеграції людини. Соціально-політична сфера життєдіяльності сучасного суспільства характеризується низьким ступенем захисту інформації про особу людини, що обумовлює потенційну загрозу інформаційного тоталітаризму. На межі тисячоліть гостро повстало питання про міжнародну інформаційну безпеку, а також кібербезпеку у складі інформаційної

безпеки. Негативним ефектом застосування сучасних технологій у військово-політичній сфері стали все ширші можливості застосування інформаційної зброї.

Водночас, базовою цінністю кожного виду інформаційної безпеки, на нашу думку, є людина, оскільки кожна загроза інформаційній безпеці в той чи інший спосіб спрямована на її права, свободи і законні інтереси, впливає на її життя і можливість задоволення своїх потреб.

Відзначимо також, що наукові дискусії щодо проблематики інформаційної безпеки особливо у інформаційнорозвинених країнах світу особливо актуалізувались в останні роки ХХ сторіччя. При чому, сучасні методи дослідження цього явища базуються на різних світоглядних позиціях, а отже, по-різному вирішують дослідницькі завдання. Якщо говорити про Україну, то наукове осмислення проблематики інформаційної безпеки людини є в процесі становлення і відбувається як вторинне по відношенню до інформаційної безпеки держави. Визначені основні осередки правових досліджень в галузі інформаційної безпеки.

Акцентується необхідність подальшого системного розвитку науки інформаційного права, в межах якої здійснюються правові дослідження інформаційної безпеки. Проте, спроби виділення наукової спеціальності 12.00.13 “Інформаційне право; право інтелектуальної власності (юридичні науки)” не досягнули кінцевого результату. Така ситуація є істотним відображенням ситуації з наукою в державі в цілому, коли питання необхідності розвивати й адекватно фінансувати фундаментальну і прикладну науку є вторинним і вирішується за залишковим принципом. Хоча, сучасних в умовах, коли «проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України» [121, п.1], власне наукові дослідження інформаційної безпеки людини, суспільства і держави, а також використання їх результатів є актуальними і необхідними умовами стабілізації ситуації і розбудови демократичного інформаційного суспільства в державі.

Таким чином, наукове осмислення, визначення і нормативне закріплення категорії «інформаційна безпека людини» (як зрештою і суспільства, і держави) є необхідною умовою для закладення належних правових основ. Визначеність логічного змісту інформаційної безпеки залежить від розвитку наукового пізнання, а також від розбудови механізму державного управління.

## РОЗДІЛ 2

### ПРАВОВА ПРИРОДА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ

#### 2.1. Інформаційна безпека людини як системне явище

Складна політична ситуація, в якій знаходиться Україна останні роки, гібридна війна з Росією і постійне погіршення іміджу держави в міжнародному співтоваристві обумовлені низкою чинників, серед яких не останнім є стан системи інформаційної безпеки. Дехто з науковців вважає, що має місце «фактична відсутність в Україні системи інформаційної безпеки, яка б забезпечувала не тільки виявлення та аналіз інформаційних загроз національній безпеці, а й, що надзвичайно важливо, адекватну обстановці протидію цим загрозам» [226].

Перш ніж перейти до аналізу дійсної ситуації пропонуємо звернути увагу на зміст категорії, що досліджується. Термін «система» походить від давньогрецького *συστήμα* – «сполучення» і буквально означає ціле, складене з частин. Основною змістовною складовою системного підходу вирішення наукових проблем є система. В античній філософії онтологічне тлумачення системи передбачало упорядкованість та цілісність буття. Розуміння системи опирало на організованість Всесвіту як природний порядок, створений богами. Важливими кроками в історії поняття «система» вважають постулати Анаксагора «все у всьому» і «з усього – все»; атомістичне вчення Левкіппа і Демокрита; висловлювання Цицерона про те, що світовий організм є нерозривним цілим і всі елементи світобудови гармонійно пов'язані між собою; систему знань Епікура; ідеї системності знання у давньогрецькій філософії Евкліда, Платона, Арістотеля, стоїків [452, с.130-139].

В працях Г. Гегеля предмети розглядаються як органічна цілісність: «Будь-який предмет – це щось ціле. Як ціле він складається з частин, а частини – з елементів. Відповідно, щоб пізнати предмет (отримати його поняття), необхідно спочатку виявити всі його частини та елементи, а потім подумки зв'язати їх воєдино так, щоб вийшло розуміння цілого. ... Але поодинокі предмети існують не самі по собі, не ізольовано від решти світу. Вони утворюють організовані

системи. Такі системи також є цілим і тому визначають собою зміст всіх своїх частин та елементів. Отже, щоб отримати всебічне розуміння поодинокого предмета, необхідно вивчити не тільки сам предмет, а й ту систему (загальність), якій він належить. Тільки при такому підході поняття предмета буде визначено як з боку його одиничності, так і з боку його загальності» [471].

Подальший розвиток принципів системної природи знання віднайшов у німецькій класичній філософії, зокрема у працях І. Канта (наукове знання як система, в якій ціле панує над частинами), Ф. Шеллінга й Г. Гегеля (системність пізнання – найважливіша вимога діалектичного мислення) [452, с.130-139].

У ХХ столітті в загальній теорії систем Л. Берталанфі об'єкт розглядався як складний з безліччю властивостей, якостей та їхній взаємозв'язків. В кінці ХІХ – на початку ХХ ст. принцип цілісності (холізму) став дуже популярним у наукових дослідженнях. Безперечно, такий підхід є цінний з позиції розуміння людини як складної системи, для якої цілісність її фізіологічного, психоемоційного та соціального станів є необхідною умовою існування і розвитку.

У соціології того часу в основі однієї з перших цілісних концепцій соціальної системи (В. Парето) мало місце механістичне розуміння суспільства як системи, що перебуває у стані рівноваги, але відносної, оскільки вона постійно порушується і відновлюється, оскільки елементи такої соціальної системи механічно впливають один на одного. Поступово відбувся відхід від елементаризму та механіцизму на користь органіцизму – методологічного принципу, за яким соціальні явища досліджувалися за аналогією з природними. В соціології системно-органістичні уявлення про суспільство розвивали О. Конт і Г. Спенсер, визначивши соціальну систему як складне ціле, що формується за законами доцільності. Як кожному живому організму їй властивий постійний розвиток. На відміну від механістичних уявлень про суспільство, органіцизм звертає увагу передовсім на динамічні процеси всередині соціальних систем. Однак таке перенесення біологічних закономірностей на суспільство не сприяло науковому розумінню соціальних законів.

Важливою подією у розвитку системних уявлень вважається публікація у 1948 р. «Кібернетики» Н. Вінера. На думку Д. Гіга, саме з моменту появи

кібернетики системні дослідження почали свій справжній розвиток завдяки У. Ешбі, О. Ланге та багатьом іншим вченим, які забезпечили для цього наукову і технічну базу та досвід проектування автоматизованих систем. [94, с.9]. На відміну від Л. Берталанфі, який особливу увагу приділяв вивченню взаємодії системи із зовнішнім середовищем речовиною, енергією та інформацією, вінеровський підхід передбачав вивчення зв'язків усередині системи, а функціонування системи розглядав як реакцію на зовнішній вплив.

Перетривавши історичну еволюцію, поняття «система» в середині ХХ ст. міцно увійшло у наукову термінологію як одне з ключових філософсько-методологічних і спеціально-наукових понять, фундаментальна й універсальна категорія. Аналіз словникових та енциклопедичних статей дає можливість виділити головні загальні риси категорії «система»: цілісність, єдність елементів, комплексність (сукупність елементів), упорядкованість розташування та взаємопов'язаність її складових частин. Семантика загального визначення поняття «система» пов'язана з термінами «ціле», «єдність», «елемент», «зв'язок», «структура» [452].

Водночас, велика кількість визначень поняття «система» в залежності від контексту, цілей і галузі знань, де воно використовується, обумовлює також різні підходи до визначення властивостей системи. Зокрема, серед них: система прагне зберегти свою структуру (ця властивість заснована на об'єктивному законі організації — законі самозбереження); система має потребу в управлінні (існує набір потреб людини, тварини, суспільства, великого соціуму); у системі формуються складні зв'язки в залежності від індивідуальних властивостей її елементів і підсистем (система може мати властивості не властивих їй елементів, і може не мати властивостей своїх елементів); кожна система має вхідний вплив, систему переробки (обробки), кінцеві результати (вихід) і зворотний зв'язок; на вході система зазнає впливу з боку середовища, а через вихід вона впливає на зовнішнє середовище [70].

Слід також пам'ятати, що безпечний розвиток будь-якого суспільства, держави, людини безпосередньо обумовлений їх інформаційною безпекою, оскільки інформаційне середовище виступає системоутворючим фактором розвитку.



Беручи до уваги вищезазначене, звернімося до бачення інформаційної безпеки як системного явища. Зважаючи на те, що інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки, питання її забезпечення має загальнонаціональне і загально державне значення. Водночас, інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки [120, 306]. Відсутність системи забезпечення інформаційної безпеки унеможливилює надійне забезпечення не лише інформаційної, а й національної безпеки. [178].

Таким чином, обґрунтованим вбачається розглядати систему інформаційної безпеки з урахуванням її місця в системі національної безпеки України та концептуальних питань, опрацьованих на рівні доктрини національної безпеки України. Кожне із великого різноманіття визначень національної безпеки певним чином віддзеркалює її сутнісний чи функціональний аспекти. Зазначене також стосується інформаційної складової у забезпеченні національної безпеки.

Очевидно, що інформаційна безпека є складним, системним, багаторівневим явищем, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні і внутрішні чинники, найважливішими з яких є: 1) політична обстановка у світі; 2) наявність потенційних зовнішніх і внутрішніх загроз; 3) стан і рівень інформаційно-комунікаційного розвитку країни; 4) внутрішньополітична обстановка в державі [262]. Водночас, її компонентами є підсистеми безпеки особистості, держави і суспільства. Саме взаємозалежна, системна єдність останніх складає якісну визначеність, покликану здійснити захист життєво важливих інтересів людини, суспільства і держави, забезпечити їх існування і розвиток.

Розуміння категорії «система інформаційної безпеки» в науковій думці відображає в переважній більшості практично-діяльнісний підхід, водночас, як правило, відрізняється доктринальною складовою. Так, Кормич Б.А. складовими сучасної системи безпеки називає: доктрину і правову основу; інституціональний механізм; методологічна база, що використовується для реалізації конкретних завдань у межах політики безпеки [209, с.119].

Вивчення праць іноземних вчених, дозволило зробити висновок, що таким системам властиві низка ключових ознак: ієрархічність побудови системи; наявність керівного, а не дорадчого органу системи; організація взаємодії між усіма елементами системи; взаємозв'язок національної та міжнародної систем. Загальне керівництво системою здійснюється, як правило, головою виконавчої влади через відповідний робочий орган, який розробляє державну політику інформаційної безпеки і координує діяльність її складових елементів. Найбільш розвинуті системи інформаційної безпеки функціонують у США, Великій Британії, Ізраїлі, ФРН, Російській Федерації, Китаї [226], тобто у тих країнах, які не лише знаходяться під потужним зовнішнім інформаційним впливом, а й володіють можливостями інформаційного впливу на інші держави та міжнародне співтовариство.

Використовуючи методологію системного дослідження, розроблену У. Баклі, К. Бейлі, Н. Луманом та ін., системний підхід при аналізі феномену інформаційної безпеки означає, що всі суспільні зв'язки і опосередковування, елементи і складові суспільства й держави, функції і проблеми, котрі стосуються забезпечення інформаційної безпеки, розглядаються як взаємопов'язане ціле, а застосування системного підходу дозволить встановити загальну орієнтацію досліджень проблем інформаційної безпеки й зафіксувати науковими засобами цілісність, організованість об'єкта (системи, проблеми, соціального явища, процесу тощо), що досліджується, в усій його повноті та в усій багатоманітності й поліаспектності зв'язків в об'єкті. На основі такого підходу пропонуємо власне бачення системи інформаційної безпеки, елементами якої вбачаються:

- 1) правова та наукова (доктринальна) основа;
- 2) об'єктно-суб'єктний склад, тобто об'єкти інформаційної безпеки, а також система органів (підрозділів), що здійснюють її забезпечення;
- 3) політика інформаційної безпеки;
- 4) засоби і способи забезпечення інформаційної безпеки.

При цьому, для досягнення інформаційної безпеки конкретного об'єкта вбачається необхідною побудова системи забезпечення його інформаційної безпеки.

Звернемося до окремих складових запропонованого підходу. Аналізу першого елементу було присвячено увагу в попередніх розділах. Тому відразу перейдемо до об'єктно-суб'єктного складу.

Ст. 3 Закону України «Про основи національної безпеки України» [372] визначає, що об'єктами забезпечення національної безпеки є: людина і громадянин – їхні конституційні права і свободи; суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси; держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

В наступній ст. 4 визначається, що суб'єктами забезпечення національної безпеки є: Президент України; Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; міністерства та інші центральні органи виконавчої влади; Національний банк України; суди загальної юрисдикції; прокуратура України; Національне антикорупційне бюро України; місцеві державні адміністрації та органи місцевого самоврядування; Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України; органи і підрозділи цивільного захисту; громадяни України, об'єднання громадян.

На думку О.О. Тихомирова, суб'єкт забезпечення безпеки – одна з основних категорій, що використовується для розкриття змісту системи забезпечення як національної, так і інформаційної безпеки, якій традиційно приділяється багато уваги законодавцем, оскільки саме законодавство у сучасній правовій державі є засобом визначення повноважень суб'єктів та окреслення сфери їх компетенції [460]. Слід звернути увагу, що більшість суб'єктів системи інформаційної безпеки також є її об'єктами – людина і громадянин, держава, окремі її органи, інститути тощо. Власне тому, вважаємо за потрібне говорити про об'єктно-суб'єктний склад як елемент системи інформаційної безпеки.

Аналіз наукових досліджень і законодавчих норм дозволяє зробити висновок про множинність підходів до суб'єктного складу системи забезпечення інформаційної безпеки. М.Б. Левицька, класифікуючи суб'єкти забезпечення

національної безпеки акцентує увагу на функціях відповідних органів і виокремлює таким чином: 1) суб'єктів, діяльність яких безпосередньо підпорядкована завданням забезпечення відповідного рівня національної безпеки як у комплексі (Рада національної безпеки і оборони України), так і на окремих напрямках діяльності (правоохоронні та інші державні виконавчі органи спеціальної компетенції); 2) суб'єктів, для яких здійснення такої діяльності є суттєвим, але не єдиним напрямком їх діяльності (вищі органи законодавчої, виконавчої та державної влади); 3) суб'єктів, для яких участь у забезпеченні національної безпеки є допоміжним, другорядним завданням порівняно з основною діяльністю (всі інші державні і громадські організації, наприклад, Товариство сприяння обороні України, пункти охорони громадського порядку тощо) [225, с.66].

Теорія національної безпеки відносить до суб'єктів забезпечення національної безпеки всі державні та суспільні інституції, які є учасниками процесу забезпечення національної безпеки, а саме: апарат держави як систему державних органів, органи місцевого самоврядування, громадян та їх об'єднання. З цього переліку виокремлюються дві групи суб'єктів (1) ті, що наділені державно-владними повноваженнями, (2) ті, що ними не наділені, хоча в окремих випадках можуть мати певний обсяг делегованих державно-владних повноважень. [461, с.109]. Екстраполюючи такий підхід, можна говорити про суб'єктів інформаційної безпеки, що здійснюють державне забезпечення і недержавне забезпечення.

Тихомиров О.О. додає ще міжнародний рівень і пропонує серед суб'єктів забезпечення інформаційної безпеки виділяти три групи: міжнародні організації; держава в особі державних організацій; недержавні організації, громадяни та їх об'єднання [461, с.109]. Такий підхід був закріплений в уже згадуваній Доктрині інформаційної безпеки, яка передбачала що діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки України має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства і людини [120]. Окрім того, заходи щодо забезпечення інформаційної безпеки

України фактично відображали міжнародний, державний і недержавний рівні забезпечення інформаційної безпеки.

В.І. Гурковський до системи суб'єктів щодо підтримання інформаційної безпеки відносить: 1) органи законодавчої влади і державного управління загальної компетенції; 2) Конституційний суд, суди загальної юрисдикції; 3) органи виконавчої влади: а) правоохоронні органи; б) галузеві органи державного управління, що регулюють інформаційні відносини в певних галузях; 4) громадські структури [102, с.87].

О.В. Олійник на основі аналізу чинного законодавства та враховуючи досвід інших держав запропонував чотири рівні організаційно-функціональної системи забезпечення інформаційної безпеки. Перший рівень – стратегічний, загальнодержавний, який включає Верховну Раду України, Кабінет Міністрів України та їх консультативно-дорадчі органи [290,с.219]. Це рівень охоплює політичні рішення, законодавче і нормативно-правове забезпечення, встановлення порядку міжнародного співробітництва, застосування сил і засобів інформаційного протистояння, поведінки суб'єктів в критичних ситуаціях. Другий рівень -організаційно-виконавчий, відомчо-територіальний, який включає центральні органи виконавчої влади і органи місцевого самоврядування, воєнну організацію держави, правоохоронні органи і органи судової влади. На цьому рівні здійснюється організаційне і методичне забезпечення інформаційної безпеки у відповідних галузях та адміністративно-територіальних утвореннях, координація і контроль діяльності у сферах відповідальності державно-владних структур [290, с.220]. Третій рівень – критично важливі інфраструктури країни, до яких доцільним вбачається включення підприємств, установ і організацій, комунікацій національного простору та інших об'єктів, управління яким здійснюється з використанням електронно-комунікаційних засобів та інформаційних технологій. На цьому рівні мають виконуватись повноваження, спрямовані на забезпечення безпечного функціонування загальнодержавних, відомчо-територіальних критично важливих інфраструктур, гарантованого попередження зовнішніх та внутрішніх загроз і небезпек, які можуть завдати шкоду громадянам, суспільству і державі[290, с.220].

Хотілося б звернути увагу на важливість правового закріплення критичної інфраструктури держави в цілому, та її інформаційної складової зокрема, звернувшись до іноземного досвіду. В країнах ЄС та у США на законодавчому рівні визначено змістовне наповнення категорії "критична інфраструктура" та визначено план дій на випадок її ураження. У жовтні 2004 р. Європейська комісія здійснила розробку загальної методології із захисту критичної інфраструктури та рекомендувала посилити увагу на технологічних й інформаційних елементах захисту тих об'єктів, припинення функціонування яких матиме транскордонний вплив [590]. Європейська інформаційна мережа попередження загроз критичній інфраструктурі - Critical Infrastructure Warning Information Network (CIWIN) була офіційно затверджено рішенням Ради 2008/0200, а у квітні 2009 р. Європейський парламент прийняв відповідне законодавче рішення про CIWIN[578]. Зокрема, всім країнам ЄС рекомендовано вжити належних заходів: розробити національну програму захисту критичної інфраструктури; забезпечити такий рівень охорони здоров'я, технологічної безпеки, соціально-економічного добробуту, що гарантував би «стійкість» нації до загроз; об'єднати зусилля, спрямовані на захист критичної інфраструктури, визначивши єдиний державний орган, що звітує з цього питання, і наділений функціями координації дій державних органів влади, які спеціалізуються і тісно взаємопов'язані з галузями промисловості, до яких належать об'єкти критичної інфраструктури; визначити органи державної влади, відповідальні за сектори критичної інфраструктури, та відповідні приватні компанії; створити умови для ефективної взаємодії та обміну інформацією, даними і досвідом між країнами-членами ЄС, урядовими структурами та приватним сектором; брати участь у створенні гармонізованої методології на рівні ЄС та загальноєвропейської системи аналізу ризиків [548]. Нормативно-правове визначення критичної інформаційної інфраструктури та органів відповідальних за її безпеку вбачається необхідною умовою створення безпечного інформаційного середовища, а також гарантування національного інформаційного суверенітету.

До четвертого рівня О.В. Олійник відніс суб'єктів невідного характеру, громадян України та їх об'єднання, державні і приватні засоби масової інформації. Для того, щоб на цьому рівні могло здійснюватись забезпечення

інформаційної безпеки необхідним є закладення правових основ такої діяльності, зокрема закріплення їх правового статусу, надання достатнього обсягу прав і свобод, а також створення ефективної системи судочинства. Інакше, існування цього рівня не передбачатиме реального впливу.

Можливості забезпечення інформаційної безпеки значною мірою залежать від сильних та слабких сторін держави. Ф.Х. Гартман серед таких вирізняє: демографічний чинник – кількість населення держави, демографічна структура і тенденції – зростання чи зменшення кількості населення; географічний чинник – положення, розмір території, клімат, географічні особливості; економічний чинник – сировинна база, потреби, об'єми валового виробництва, прогнозоване господарське зростання; історико-психолого-соціологічний чинник – історичний досвід, ставлення до життя, єдність суспільства; організаційно-адміністративний чинник – форма правління, ставлення суспільства до влади, ефективність діяльності влади; військовий чинник – спосіб організації і стан ефективності збройних сил, їх розмір у співвідношенні до населення призовного віку[594].

І.Р. Боднар пропонує національну безпеку України в інформаційній сфері розглядати як інтегральну цілісність чотирьох складових – персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки [57]. Тому в процесі визначення характеру ризиків він пропонує брати до уваги наступні елементи: концептуальні засади політичної безпеки, її принципів, стандартів та правил, погоджених із чинним законодавством й принципами забезпечення безперервності системи інформаційної безпеки особистості, суспільства, комерційних (корпоративних) структур та держави; визначення об'єктів та цілей; визначення прийнятних з погляду забезпечення інтересів усіх суб'єктів структур встановлення контролю над об'єктами безпеки, а також оцінки ризиків та управління ризиками; визначення статусно-функціональних ролей, очікувань та міри відповідальності задіяних суб'єктів включно зі звітністю про події, які несуть потенційні загрози [112].

На нашу думку, діяльність із забезпечення інформаційної безпеки людини має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства та людини за трьома головними напрямками -

інформаційно-психологічному; технологічному, а також правовому. Такий підхід до внутрішньої будови інформаційної безпеки людини обумовлений відображає сфери, в яких можуть бути реалізовані загрози.

## **2.2. Правове забезпечення інформаційної безпеки людини в Україні**

Створення ефективної системи забезпечення інформаційної безпеки є однією з базових потреб сучасної держави, яке вимагає розробки відповідної державної політики, її закріплення і реалізації на всіх рівнях. При цьому політика інформаційної безпеки не може існувати у правовому вакуумі – вона виступає невід’ємною складовою інформаційної політики держави та політики національної безпеки, окрім того має базуватись на міжнародних стандартах інформаційної безпеки і відповідати національним потребам та реальному стану розвитку інформаційного суспільства в державі.

Забезпечення інформаційної безпеки України, безпеки її національних інтересів в інформаційній сфері передбачає пріоритетний розвиток системи нормативно-правового регулювання відносин у цій сфері та впорядкування відповідного правотворчого процесу. О. Олійник стверджує, що система правового регулювання інформаційної безпеки включає масив правових норм, які регулюють відносини в даній сфері, правовідносини, що виникають на основі застосування правових норм, та відповідні правозастосовчі акти [289, с.132-137].

На думку Мельника С.В., взагалі безпека та забезпечення безпеки – це різні поняття, тому що безпека виражає характеристику певного стану, а забезпечення безпеки – дієву характеристику, тобто діяльність, спрямовану на підтримання вказаного стану [257].

Словник української мови дає таке тлумачення слова «забезпечувати»:  
 1. Постачаючи щось у достатній кількості, задовольняти кого-, що-небудь у якихось потребах. 2. Створювати надійні умови для здійснення чого-небудь; гарантувати щось. 3. Захищати, охороняти кого-, що-небудь від небезпеки.

В Словнику синонімів української мови розкривається розуміння цього слова через такі синоніми як: давати, надавати комусь щось потрібне, належне в



достатній кількості), постачати, постачити (кому-чому що), достачати, достачити (кому-чому що й чого), у[в]безпечувати, у[в]безпечити (чим) [82].

Українські мовники схиляють до позиції, що «безпеку» слід «гарантувати», а не «забезпечувати»[431]. Цей вираз прийнятний у побуті, однак не відображає правового змісту категорії. Гарантування має в праві значення зобов'язання, яке бере на себе особа (фізична або юридична, в т.ч. держава, як у випадку Фонду гарантування вкладів фізичних осіб), забезпечити виконання обов'язку іншої особи. Такий термін може бути прийнятним лише у випадку гарантування інформаційної безпеки людини, якщо остання буде надана як суб'єктивне право (порівн. з правом на безпечне довкілля).

В певній мірі поява цієї термінологічної дискусії пов'язана з мовними особливостями і труднощами перекладу. Українська правова і нормативна мова на етапі становлення українського законодавства і нормотворчості була значною мірою узалежнена від російської термінології. В російській мові словосполучення «обеспечение безопасности» не викликає жодних дискусій, оскільки у слів «безопасность» і «обеспечить» різний корінь і різне етимологічне походження. «Без-опасность» – могла би бути перекладена українською як «без-небезпека». А ось слово «обеспечивать» має таке ж походження як і українські слова безпека і забезпечення, про що вже йшлося у попередньому підрозділі.

Окрім того, у зв'язку з ратифікацією значної кількості міжнародно-правових актів, а також з процесами євроінтеграції, посилився вплив перекладів міжнародних правових понять і сталих виразів з англійської мови. В англійській мові вживаними є кілька категорій для означення забезпечення безпеки «to ensure security», «to provide security» і також «to secure» [641]. Відповідно на українську мову кожне з них перекладається як забезпечення.

Безперечно, з точки зору, збереження краси мови і її розвитку добре було б уникати вживання таких термінів. Але, на нашу думку, оскільки на сьогодні відповідник, що в повній мірі відображає явище і є більш прийнятним з мовної точки зору не існує, то в цій праці буде використовуватись словосполучення «забезпечення безпеки» і його похідні, як то «забезпечення інформаційної безпеки». З правової точки зору важливішим вбачається зміст цієї категорії.

На думку деяких дослідників правову основу забезпечення інформаційної безпеки України становлять Конституція України, закони України “Про основи національної безпеки України”, “Про інформаційну безпеку України”, “Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки”, “Про доступ до публічної інформації”, інші закони та інформативно-правові акти, а також ратифіковані або парафовані Україною Договір про безпеку і співробітництво в Європі, Договір “Відкрите небо”, Угода про партнерство і співробітництво між європейським співтовариством і Україною, Додатковий протокол до Європейської конвенції про інформацію щодо іноземного законодавства, які зобов’язують країни-учасниці здійснювати багатосторонній обмін інформацією, потребують створення загальнодержавних механізмів зберігання та споживання отриманої інформації в національних інтересах [248, с.13-20]. Безперечно, окремі з названих актів становлять важливу частину законодавства щодо інформаційної безпеки, водночас, не можемо погодитись з такою думкою.

По-перше, Закону України “Про інформаційну безпеку України” на жаль досі не існує, незважаючи на об’єктивну потребу в час, коли Україна знаходиться в стані гібридної війни, за умов якої інформаційна безпека є найбільш атакованою і, водночас, найбільш вразливою. По-друге, досліджуючи правове забезпечення інформаційної безпеки слід звернути увагу на те, що його становлення і розвиток нерозривно пов’язаний із правовим регулюванням інформаційних відносин, яке містить значну кількість норм що безпосередньо чи опосередковано стосуються об’єкту дослідження.

Не слід також ототожнювати правове забезпечення з нормативним, а тим паче з законодавчим. Підтримуємо думку Остроухова В.В., що нормативна база інформаційної безпеки повинна виконувати в першу чергу три основні функції: (1) регулювати взаємовідносини між суб’єктами інформаційної безпеки, визначати їх права, обов’язки та відповідальність; (2) Нормативно забезпечувати дії суб’єктів інформаційної безпеки на всіх рівнях, а саме - людини, суспільства, держави; (3) встановлювати порядок застосування різних сил і засобів забезпечення інформаційної безпеки [177].

На нашу думку, важливим є створення правової бази на основі поєднання основоположних ідей правового регулювання інформаційної сфери та принципів забезпечення національної безпеки. Адже інформаційна безпека є складовою системи національної безпеки і водночас виступає властивістю інформаційної сфери суспільства.

О.А. Баранов про початки створення нормативно-правового забезпечення становлення інформаційної сфери в Україні зауважив: «Закони покликані не тільки юридично фіксувати суспільні відносини, що вже склалися або достатньою мірою сформувалися, але й активно формувати перспективні відносини, які визначатимуть вектор розвитку суспільства в майбутньому» [28, с.62]. За кілька тижнів після референдуму 1 грудня 1991 р., яким було затверджено Акт проголошення незалежності, Верховною радою вже незалежної України було прийнято Закон України "Про основи державної політики у сфері науки і науково-технічної діяльності" (1991 р.) Цей закон мав на меті створення правових основ державної політики у сфері науки і науково-технічної діяльності, а також визначав правові, організаційні та фінансові засади функціонування і розвитку науково-технічної сфери, створення умови для наукової і науково-технічної діяльності, забезпечення потреб суспільства і держави у технологічному розвитку. Фактично в ньому було закладено підвалини для розвитку інформаційного суспільства, про яке на момент початку розбудови держави особливо ніхто не замислювався. Прийняття цього закону, а також політична воля тогочасного керівництва сформулювали національні інтереси держави, що відображали прагнення нації до розвитку. В ньому визначалось, що розвиток науки і техніки є визначальним фактором прогресу суспільства, підвищення добробуту його членів, їх духовного та інтелектуального зростання. З перспективи часу, цей Закон виглядає як передвісник становлення і розбудови інформаційного суспільства і суспільства знань, як його наступного етапу [452].

В українському національному праві системоутворюючим фактором і поштовхом до виникнення і формування інформаційного права як інституції публічного (державного) права можна вважати прийнятий у 1992 р. Закон України "Про інформацію"[294]. Не можна недооцінювати значення цього акту на

той час. Після довготривалої інформаційної ізоляції за часів УРСР, українська держава і суспільство опинились посеред бурхливих інформаційних процесів, які вимагали від України формування власних пріоритетів і напрямів розвитку інформаційної сфери. Прийняття цього Закону стало знаковою подією в організації безпечного інформаційного простору молодій державі. Фактично, вперше на вищому законодавчому рівні ним були визначені: поняття інформації, її види та галузі; принципи інформаційних відносин; пріоритетні напрями державної інформаційної політики; гарантії права на інформацію; основні види інформаційної діяльності; режими доступу до інформації; процедура інформаційного запиту; коло учасників інформаційних правовідносин, їхні права та обов'язки; питання охорони інформації; підстави відповідальності за делікти в інформаційній сфері; правові форми міжнародного співробітництва в галузі інформації; гарантії інформаційного суверенітету України [307, с.64-68].

Але первинна редакція Закону про інформацію мала низку недоліків і прогалин – недосконалість понятійно-категоріального апарату, полишення без уваги окремих видів інформаційної діяльності, суттєві вади мали місце щодо регулювання відносин з приводу обробки та захисту персональних даних та доступу до публічної інформації. Закон «Про інформацію» зазнавши суттєвих змін, які були спрямовані на створення належної правової бази для формування та реалізації державної інформаційної політики, функціонування інформаційного середовища, здійснення різних форм інформаційної діяльності, забезпечення публічного доступу до інформації, зміцнення інформаційної безпеки, вдосконалення механізмів контролю за дотриманням законності, залишається системоутворюючим для галузі інформаційного права досі.

На основі та на реалізацію положень цього закону було прийнято цілу низку законів, що стосувались окремих видів інформаційних відносин, зокрема, "Про друковані засоби масової інформації (преси) в Україні" [344], "Про науково-технічну інформацію" [365], "Про охорону прав на винаходи і корисні моделі" [375], "Про телебачення і радіомовлення" [387], "Про авторське право і суміжні права" [335], "Про державну таємницю" [342], "Про національний архівний фонд і архівні установи" [366], "Про захист інформації в автоматизованих системах"

[357], "Про зв'язок" [359], Закон України "Про бібліотеки і бібліотечну справу"[336], "Про рекламу"[379], "Про Суспільного телебачення і радіомовлення України"[383], "Про Національну раду України з питань телебачення і радіомовлення"[368], "Про державну підтримку засобів масової інформації та соціальний захист журналістів" [341] та інші.

В тому ж таки 1992 р. у національному нормативно-правовому акті вперше вжито категорію "інформаційна безпека". Розпорядження Президента України "Про затвердження складу Консультативно-експертної групи по підготовці концепції національної безпеки України" [77], а саме витяг з протоколу засідань Комісії при Президенті України по підготовці пропозицій про статус, порядок діяльності і структуру Ради національної безпеки, де одним із основних напрямів розробки концепції національної безпеки України визначено інформаційну безпеку.

Наступним етапом хронологічно, але не змістовно, стало закріплення в Конституції України інформаційних прав, а також проголошення забезпечення інформаційної безпеки України оголошено "справою всього українського народу". Таким чином, інформаційна безпека з вузькоспеціалізованого кола вжитку фахівців прикладного характеру була піднесена до правового закріплення на рівні Основного Закону. Як можна простежити, в науковій думці того періоду спостерігалось значне ототожнення понять «інформаційна безпека», «безпека інформації», «захист інформації», що й досі має місце в багатьох країнах [680, с. 363].

Для питання, що досліджується, має значення п. 5 ст. 92 Конституції України, де закріплено, що виключно законом встановлюються засади організації транспорту та зв'язку, а також основи національної безпеки, складовою якої слід вважати інформаційну безпеку. Забігаючи наперед, слід звернути увагу, що в Україні за 25 років незалежності і вже понад 20 років після прийняття Конституції, все ще не прийнято закону про основи інформаційної безпеки.

Поруч із закріпленням інформаційної безпеки як складової національної безпеки, Конституція України окреслює повноваження суб'єктів, відповідальних

за її забезпечення - Президент України; Рада національної безпеки і оборони України; Верховна Рада України; Кабінет Міністрів України та інших.

В 1998 р. було прийнято два закони, що стосувались інформатизації - Закон України "Про Національну програму інформатизації" [367] та Закон України "Про Концепцію Національної програми інформатизації"[364], які законодавчому рівні створили передумови для забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення.

Протягом наступних років було прийнято кілька законів, що заклали основу для формування телекомунікаційного законодавства України. Так, Закон України «Про радіочастотний ресурс України» [377] встановлював правову основу користування радіочастотним ресурсом України, визначає повноваження держави щодо умов користування радіочастотним ресурсом України, права, обов'язки і відповідальність органів державної влади, що здійснюють управління і регулювання в цій сфері, та фізичних і юридичних осіб, які користуються та/або мають намір користуватися радіочастотним ресурсом України.

В 2002 р. законодавчого закріплення набуло правове забезпечення функціонування загальнонаціональної спеціальної інформаційно-телекомунікаційної системи, яка дістала назву Національна система конфіденційного зв'язку. В 2003 р. було врегульовано на законодавчому рівні питання електронного документообігу - закони "Про електронний цифровий підпис" та "Про електронні документи та електронний документообіг" стали відповіддю на нагальну потребу створення і розвитку інфраструктури електронного документообігу [345, 347]. На реалізацію положень цих законів було прийнято низку підзаконних актів, зокрема Постанови Кабінету Міністрів України «Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу», «Про затвердження Порядку акредитації центру сертифікації ключів», «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та

організаціями державної форми власності», «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади», «Про затвердження Порядку обов'язкової передачі документованої інформації», «Про затвердження Положення про центральний засвідчувальний орган» та інші. Слід зауважити, що законодавчо не було врегульовано питання щодо застосування мов у документообігу.

В 2004 р. було прийнято Закон України "Про телекомунікації" [388], який встановлює правову основу діяльності у сфері телекомунікацій, визначає повноваження держави щодо управління та регулювання зазначеної діяльності, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у даній діяльності або користуються телекомунікаційними послугами [388]. Цей закон став основоположним для телекомунікаційного права, яке є інститутом інформаційного права, визначає повноваження держави щодо управління та регулювання діяльності у сфері телекомунікацій, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у даній діяльності або користуються телекомунікаційними послугами [140].

В цьому Законі слід відзначити два терміни, які вперше були закріплені на законодавчому рівні: «Інтернет – всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на інтернет-протоколі, визначеному міжнародними стандартами». А також «інформаційна безпека телекомунікаційних мереж – здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації».

З прийняттям у 2001 р. нового Кримінального кодексу України [218] було криміналізовано низку «комп'ютерних» правопорушень і об'єднано в окремий розділ XVI – “Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж”. До розділу увійшло три статті: ст. 361 – Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, ст. 362 – Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом

шахрайства чи зловживання службовим становищем і ст. 363 – Порушення правил експлуатації автоматизованих електронно-обчислювальних систем.

Відбулося декілька спроб ухвалити концепцію державної інформаційної політики на законодавчому рівні – 2002, 2009, 2010 та 2011 рр. Проте досі питання відкрите. В Законі України «Про основи національної безпеки України» [372] вперше офіційно визначено інформаційну безпеку як невід'ємну складову національної безпеки України. Зокрема, серед об'єктів національної безпеки названо інформаційне середовище (ст. 3)<sup>1</sup>. Водночас, в ст. 8, були закріплені основні напрями державної політики з питань національної безпеки України в інформаційній сфері: забезпечення інформаційного суверенітету України; вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України; забезпечення неухильного дотримання конституційних прав на свободу слова, доступ до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації та журналістів, заборони цензури, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції, за виконання професійних обов'язків, за критику; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

В період з 2005 до сьогодні було розроблено і прийнято 2 стратегії національної безпеки України (2007 і 2016 рр.). У первинній редакції Стратегії національної безпеки 2007 р. мав місце п.2.8, де зазначалось, що посилюється негативний зовнішній вплив на інформаційний простір України, що загрожує розмиванням суспільних цінностей і національної ідентичності; недостатніми

---

<sup>1</sup> Ані цей закон, ані жоден інший не визначає зміст категорії «інформаційне середовище».



залишаються обсяги вироблення конкурентоспроможного національного інформаційного продукту; наближається до критичного стан безпеки інформаційно-комп'ютерних систем у галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо.

Після затвердження нової редакції Стратегії 2012 р. ці положення зникли. Проте серед ключових завдань політики національної безпеки у внутрішній сфері з'явився підрозділ, присвячений забезпеченню інформаційної безпеки. Передбачалось стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів; забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури; розробка та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними стандартами держав - членів ЄС, у тому числі згідно з вимогами Конвенції про кіберзлочинність; створення національної системи кібербезпеки.

Чинна Стратегія національної безпеки України як при визначенні актуальних загроз національній безпеці України, так і при окресленні пріоритетів забезпечення відокремлює сферу інформаційної безпеки від кібербезпеки і безпеки інформаційних ресурсів. Зокрема, до загроз інформаційній безпеці України віднесено ведення інформаційної війни проти України та відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства, а до загроз кібербезпеці і безпеці інформаційних ресурсів – уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

Як вже згадувалось вище, в 2005 р. Україна ратифікувала Конвенцію про кіберзлочинність [203]. Її проект був розроблений у червні 2001 р. Європейським

комітетом з проблем злочинності. У листопаді того самого р. Конвенція була затверджена комітетом міністрів Ради Європи і підписана 35 державами, як державами-членами Ради Європи, так і державами, що не є членами Ради, які брали участь у її розробці. Зокрема, Конвенцію підписали США і Японія. Ці держави взяли на себе зобов'язання здійснювати погоджену політику боротьби зі злочинністю у цій сфері[203]. В цій конвенції вперше на міжнародному рівні була запропонована класифікація кіберзлочинів.

В 2008 р. Указом Президента введено в дію рішення РНБО "Про невідкладні заходи щодо забезпечення інформаційної безпеки України" [369]. Відповідно до цього указу уряд, зокрема, мав: розробити і внести у шестимісячний строк на розгляд Верховної Ради України проект Концепції національної інформаційної політики, яка визначатиме основні напрями, засади і принципи національної політики, механізми її реалізації та пріоритети розвитку інформаційної сфери; затвердити державну програму формування позитивного іміджу України; виділити фінансування на інформаційно-роз'яснювальну діяльність культурно-інформаційних центрів при закордонних дипломатичних установах України, розширити мережу таких центрів; затвердити заходи щодо розширення вітчизняного мовлення на території інших держав іноземними мовами; вжити невідкладних заходів щодо забезпечення присутності програм вітчизняних телерадіоорганізацій у багатоканальних мережах інших держав. На виконання цього указу РНБО було розроблено проект Доктрини інформаційної безпеки України – сукупності основних офіційних поглядів на мету, задачі, принципи й основні напрямки забезпечення інформаційної безпеки держави. Доктрина була затверджена Указом Президента у липні 2009 р. В підготовці і обговоренні документу було задіяно понад 30 органів державної влади, наукових установ.[120]. Доктрина втратила чинність відповідно до Рішення РНБО України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [358], введеним в дію Указом Президента, яким також передбачено розробку низки законодавчих актів, зокрема, Стратегії розвитку інформаційного простору України, Стратегії кібернетичної безпеки України, проекту Закону України про кібернетичну

безпеку України. Станом на 2017 р. було розроблено і введено в дію Указом Президента України лише Стратегія кібернетичної безпеки України [443], інші ж акти проходять різні етапи розробки – від проектної роботи до експертної оцінки і погодження в комітетах ВР, проте так і не були винесені на розгляд.

Метою стратегії кібербезпеки в Україні визначається створення умов для безпечної експлуатації кіберпростору, його використання в інтересах особистості, суспільства і держави. Окрім того в Стратегії окреслені загрози кібербезпеці, національна система кібербезпеки, основні суб'єкти забезпечення кібербезпеки, пріоритети та напрями забезпечення кібербезпеки України.

Слід зазначити, що у зв'язку з реалізацією Стратегії Національна рада безпеки і оборони України ухвалила рішення про створення спеціального нового органу як робочого органу – Національний координаційний центр кібербезпеки.

У контексті координації функцій забезпечення інформаційної безпеки варто акцентувати на особливому статусі РНБО як суб'єкта інформаційних відносин, оскільки він є єдиним органом, який має повноваження, функції та завдання із координації та контролю діяльності органів виконавчої влади зокрема, центральних органів влади, правоохоронних органів та органів місцевого самоврядування в усіх складових сфери забезпечення національної безпеки і оборони. Окрім цього, при РНБО України існує Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки. До основних її завдань, зокрема, належить аналіз стану і можливих загроз національній безпеці України в інформаційній сфері та узагальнення міжнародного досвіду щодо формування та реалізації інформаційної політики. Як варіант, можливо розглянути розширення повноважень зазначеної структури, в тому числі включення завдання координації [435].

На основі вищезгаданої Стратегії національної безпеки України, а також Конституції і законів України та міжнародних договорів України, Указом Президента України була затверджена Доктрина інформаційної безпеки України. Метою доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни. Доктрина

інформаційної безпеки України визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері.

Однією з нових категорій, яку цим документом введено в правове поле є стратегічний наратив – спеціально підготовлений текст, призначений для вербального викладення у процесі стратегічних комунікацій з метою інформаційного впливу на цільову аудиторію. При цьому визначається «підтримка розвитку механізмів саморегуляції засобів масової інформації на засадах соціальної відповідальності». [119] Представники правозахисних організацій та ЗМІ з огляду на ці положення висловили побоювання утисків свободи слова.

З перших рядків Доктрини відразу є очевидним, що цей документ є певним чином однобічний. «Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України» [120]. Таким чином, автори цього документу визначають основне джерело загрози, а отже і напрям протидії. Безперечно, це є актуальним з огляду на гібридну війну проти України. Однак, на нашу думку, такі «точкові» документи за відсутності комплексного правового регулювання питань інформаційної безпеки є недостатніми.

Слід згадати, що досі залишається чинним Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»[374], яким ще в січні 2007 р. було визначено одним з головних пріоритетів України є прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині

повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвитку та підвищуючи якість життя.

Цим законом, зокрема, було вперше законодавчо закріплено поняття «інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації».

Також визначали шляхи вирішення проблеми інформаційної безпеки. Очікувалось, що впровадження Основних засад розвитку інформаційного суспільства в Україні на 2007-2015 роки дасть можливість забезпечити позитивні зміни в життєдіяльності суспільства і людини. Однак, складна політична і економічна ситуація, а також низка інших чинників, як-то: відсутність чіткого розмежування повноважень органів державної влади та органів місцевого самоврядування при впровадженні інформаційно-комунікаційних технологій у систему державного управління, координації їх діяльності в цій сфері; недостатнє забезпечення доступності якісних адміністративних послуг усім суб'єктам інформаційного суспільства та гарантій їх відповідності затвердженим державним вимогам; недостатній рівень урахування світового досвіду у сфері розвитку інформаційного суспільства; поширеність практики делегування органами державної влади їхніх повноважень з надання адміністративних послуг під приводом необхідності експлуатації інформаційно-телекомунікаційних систем та комплексів, що призводить до втрати контролю над собівартістю адміністративних послуг та над ціноутворенням на такі послуги тощо, призвели до невиконання в Україні низки положень цього Закону та заходів, запланованих Кабінетом Міністрів на його виконання.

Про низькі темпи розвитку інформаційного суспільства свідчить також індекс мережевої готовності (Networked Readiness Index), що визначає рівень розвитку ІКТ у країнах світу. Він складається з чотирьох субіндексів – наявність умов для розвитку ІКТ; готовність; використання та вплив, розподілених за

складовими (індикаторами), які характеризують роль уряду, бізнесу і суспільства у формуванні середовища для розвитку ІКТ. Відповідно до "Глобального звіту про розвиток інформаційних технологій-2015" (The Global Information Technology Report), який, починаючи з 2002 р., щорічно видається Всесвітнім економічним форумом (World Economic Forum), Україна в 2015 р. посіла 71 позицію серед 143 країн світу у рейтингу за рівнем розвитку інформаційно-комунікаційних технологій (ІКТ). Найвищу рейтингову позицію за Індексом мережевої готовності Україна продемонструвала у 2009 р. (62 місце). Після цього упродовж двох наступних років було втрачено 28 пунктів, внаслідок чого у 2011 р. наша країна перемістилася на 90 позицію серед 138 країн світу. В останні роки, з урахуванням розширення кола країн-учасниць рейтингу, Україна знаходиться у сьомому десятку та поступається країнам СНД і Східної Європи. Причиною досить низьких позицій України у світовому рейтингу 2017 р. є, передусім, відставання за складовими, що характеризують політичне і регуляторне середовище – 122 позиція та низький рівень використання ІКТ урядом – 124 позиція [86].

Аналіз становлення законодавства у інформаційній сфері в цілому, та щодо інформаційної безпеки зокрема дозволяє зробити наступні висновки.

Інформаційне законодавство та законодавство щодо інформаційної безпеки є відносно новою галуззю законодавства України і все ще знаходиться на етапі становлення. Можна виокремити наступні етапи його становлення:

I. 1992 -1996 роки – становлення основ інформаційного законодавства;

II. 1996-2003 роки – усвідомлення і формулювання основ інформаційної безпеки як складової національної безпеки;

III. 2003-2014 роки – усвідомлення розвитку глобального інформаційного суспільства, приєднання до міжнародних актів щодо у сфері інформаційного суспільства, права і безпеки, розвиток національного законодавства згідно з тенденціями міжнародного права. При цьому, на нашу думку, у 2010-2014 роках мала місце криза у сфері інформаційної безпеки, обумовлена незваженою інформаційною політикою держави;

IV. 2014 – донині – розвиток законодавства у сфері інформаційної безпеки, спрямований на посилення позицій України у гібридній війні.

Слід відзначити, що за змістом інформаційне законодавство є комплексною галуззю і поєднує норми приватного та публічного права, в той час, як законодавство у сфері інформаційної безпеки містить норми переважно публічно-правового характеру.

Неможливо не погодитись з тим, що на всіх етапах становлення мав місце ситуаційний підхід до ухвалення інформаційних нормативно-правових актів, що призвело до наявності значного кола проблем нормативно-правового регулювання інформаційних правовідносин [191]. Кількість нормативно-правових актів в інформаційній сфері не переростає в якість. Красноступ Г.М. зауважила «не потрібно створювати нові закони у сфері інформації, а систематизувати вже існуючі, визначаючи у них правові гіперзв'язки з метою подальшого їх кодифікування на рівні Кодексу України про інформацію» [217, с.82]. Однак інформаційна сфера розвивається на сьогодні швидше ніж будь яка інша. І потреба в регулюванні нових суспільних відносин виникає постійно.

Таким чином, відповідне нормативно-правове забезпечення формується безсистемно і непослідовно, а отже, не спроможне виконувати своїх функцій і бути ефективним. Сучасний стан нормативно-правового забезпечення інформаційної безпеки України характеризується фрагментарністю вибору об'єктів правового регулювання, недостатньою узгодженістю правових норм, що використовуються для цього, та некоординованістю діяльності суб'єктів законодавчої ініціативи з розвитку та вдосконалення правових норм, тому у ряді випадків не в змозі адекватно вирішувати проблеми що виникають [186, с.5-11].

Нагальною потребою вбачаємо необхідність розробки і прийняття базового для правових основ інформаційної безпеки закону «Про інформаційну безпеку». При цьому важливим вбачається не відокремлювати кібербезпеку від інформаційної безпеки. Відразу, хотілося б обґрунтувати таку позицію. На доктринальному рівні багаторазово досліджувалось питання співвідношення кібербезпеки і інформаційної безпеки, кіберпростір і інформаційного простору. Фактично, сформульовано 2 підходи до цього питання – кібербезпека як окремий напрямок, також кібербезпека як складова частина інформаційної безпеки, яка на думку автора вбачається обґрунтованою [66, 240, 486].

Довший час протиставлення кібернетичної та інформаційної безпеки мало місце в європейській та американській політико-правовій доктринах. Однак, в аналітичній доповіді «Redefining Information Warfare Boundaries for an Army in a Wireless World» [639] від корпорації «ПЕНД» на замовлення сухопутних військ ЗС США зазначено, що в практичній діяльності органів військового управління, суб'єктів забезпечення інформаційної безпеки інформаційне середовище необхідно розглядати як єдине середовище в двох вимірах: людському та технічному. Методологічний підхід, що протиставляв інформаційне середовище та кіберсередовище, а, отже, розглядав інформаційну безпеку та кібербезпеку як окремі паралельні інституції (напрями діяльності) визнано необґрунтованим та штучним (тобто помилковим). Таким чином, позиція, що багаторазово обґрунтовувалась українськими вченими, що кіберпростір є невід'ємною частиною інформаційного простору, а відповідно кібербезпека – складовою інформаційної безпеки, почала розглядатись як можлива і на міжнародному рівні. Хоча в наукових дослідженнях і нормативному регулюванні багатьох європейських країн все ще фігурує перший підхід, що протиставляє інформаційну і кібербезпеку.

На нашу думку, правове забезпечення інформаційної безпеки має поєднувати норми щодо: правового закріплення національних інтересів людини, суспільства і держави у інформаційній сфері; суб'єктивних інформаційних прав людини та громадянина; системи органів, відповідальних за забезпечення інформаційної безпеки; форм участі громадянського суспільства у забезпеченні інформаційної безпеки.

### **2.3. Теоретико-правовий аналіз загроз інформаційній безпеці людини**

Інформаційна безпека зараз безперечно є популярною темою, яку експлуатують ЗМІ, політики, навіть бізнес. Щоб не повертатись до теоретичних розмірковувань, зазначимо, що, на нашу думку, проаналізовані підходи до інформаційної безпеки людини можна узагальнити в два основні. Перший підхід домінує в правових науках та безпекознавстві, і насамперед, наголошує на забезпеченні можливості людини вільно і безперешкодно реалізовувати права та



свободи в інформаційній сфері. Починаючи з 40-х рр. XX ст. у світі набув розвитку власне напрям інформаційної безпеки людини. Тобто це питання почало формуватись не “згори” – від владних органів, а “знизу” – в контексті боротьби за реалізацію інформаційних прав людини, зокрема свободи слова, таємниці приватного життя тощо [208, с.97].

Чинники, що зумовлюють ескалацію загроз інформаційній безпеці, мають комплексний характер – вони охоплюють усі сфери життєдіяльності людини, суспільства і держави, а відповідно мають міжвідомчий характер. Таким чином, на практиці аналіз загроз – це завжди суб’єктивний процес сприйняття певною особою чи соціальною групою певних факторів через призму власних інтересів і фахового рівня. Разом із тим, об’єктивне визначення загроз передбачає чітке усвідомлення параметрів, поза межами яких певне явище втрачає можливості саморегуляції та потребує зовнішнього втручання для збереження стабільності соціальної системи, а також певних умов, що перетворюють ті ж самі фактори або на реальну, або на потенційну загрозу [58, с.37]. Водночас, класифікація загроз дозволяє визначити, які саме загрози становлять переважний пріоритет в науковій чи нормативно-правовій перспективі.

Відповідно до Закону України „Про основи національної безпеки України” до загроз національним інтересам і національній безпеці в інформаційній сфері відносять наступні: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп’ютерна злочинність та комп’ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [372].

Попередня редакція Доктрини інформаційної безпеки України визначала основні реальні та потенційні загрози інформаційній безпеці України класифікуючи їх за сферами життєдіяльності особи, суспільства і держави, зокрема: у зовнішньополітичній сфері, сфері державної безпеки, воєнній сфері,

внутрішньополітичній сфері, економічній сфері, соціальній та гуманітарній сферах, науково-технологічній сфері, в екологічній сфері [120].

Нова редакція 2017 р. актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері визначила: здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні; проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах; інформаційне домінування держави-агресора на тимчасово окупованих територіях; недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України; неефективність державної інформаційної політики, недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства; поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні[121].

У Законі України „Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки”, який все ще залишається чинним, загрозами інформаційній безпеці визначено: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [374, с.102].

У Державному стандарті України „Захист інформації. Технічний захист інформації. Основні положення.” ДСТУ 3396.0-96 безпосереднє формулювання класифікації загроз відсутнє, проте в ньому передбачено можливі шляхи реалізації загроз. Саме вони дають можливість уявити або визначити ймовірні загрози інформаційним відносинам (відносинам щодо збору, обробки й накопичення інформації). В частині 4.1.3 підпункту 4.1 пункту 4 визначено, що загрози можуть здійснюватися: технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали; каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації; несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів [149].

Як критерій можна використати: спосіб впливу на інформацію або шляхи реалізації загроз.

Державний стандарт України „Захист інформації. Технічний захист інформації. Терміни та визначення.” ДСТУ 3396.2-97 містить ряд термінів пов'язаних з інформаційною безпекою та які мають пряме відношення до класифікації загроз [150]. Так, пункт 5 „Загроза для інформації” містить наступні визначення: витік інформації – неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання; порушення цілісності інформації – спотворення інформації, її руйнування або знищення; блокування інформації – унеможливлення санкціонованого доступу до інформації.

Класифікація загроз відповідно має наступний вигляд: загрози витоку інформації; загрози порушення цілісності інформації; загрози блокування інформації.

Можемо зробити висновок, що така різноманітність класифікацій в чинному законодавстві обумовлена не лише різноманітними підходами до вибору класифікаційних ознак та цілями класифікації, але й відсутність належного

теоретичного обґрунтування сутності загроз інформаційної безпеки [173]. До 2016 р. переважна увага приділялась технічному захисту інформації, то Доктрина інформаційної безпеки перемістила акценти на захист від інформаційної експансії з боку держави-агресора.

Науковці також не дотримуються одностайності щодо класифікації загроз інформаційній безпеці. Професор В. Ліпкан пропонує класифікувати загрози інформаційній безпеці відповідно до загальної класифікації загроз національній безпеці: за джерелами походження: природного походження, техногенного походження, антропогенного походження; за ступенем гіпотетичної шкоди: загроза та небезпека; за повторюваністю вчинення: повторювані та продовжувані; за сферами походження: екзогенні та ендогенні; за ймовірністю реалізації: вірогідні, неможливі, випадкові; за рівнем детермінізму: закономірні та випадкові; за значенням: допустимі та неприпустимі; за структурою впливу: системні, структурні та елементні; за характером реалізації: реальні, потенційні, здійснені, уявні; за ставленням до них: об'єктивні та суб'єктивні; за об'єктом впливу - особа; суспільство; держава [236]. В іншій праці, інтегруючи різноманітні підходи, а також пропозиції щодо розв'язання даного питання, запропоновано такі види загроз інформаційній безпеці: розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання [178].

Схожі погляди на перелік загроз інформаційній безпеці висловлює А. Логінов у власному дисертаційному дослідженні. Зокрема вчений визначає загрози як: розкриття інформаційних ресурсів; порушення цілісності інформаційних ресурсів; збій у роботі обладнання [238].

В свою чергу С. Гуцу [104] та О. Литвиненко[233], у сходяться на тому, що основні загрози інформаційній безпеці можна представити у такому вигляді: загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу; загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання); загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання,

передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову).

Л. Євдоченко формуючи власний підхід до класифікації інформаційних загроз та з метою вироблення рекомендацій щодо організації державою дієвих форм і методів забезпечення інформаційної безпеки, визначає і класифікує загрози за кількома критеріями: за способом впливу на об'єкти інформаційної безпеки (інформаційні, фізичні й програмно-математичні, організаційно-правові); за джерелами надходження (внутрішні та зовнішні); за характером вияву (політичні, економічні, організаційно-технічні) [136].

На нашу думку, підхід до розуміння суті інформаційної безпеки різних категорій суб'єктів може істотно відрізнятися, наприклад, безпека пересічних громадян або посадових осіб органів державної влади. Тому цілком логічними та вартими уваги є класифікації загроз які мають більш вузький, або іншими словами спеціальний характер, зокрема, загрози інформаційній безпеці мережевих ресурсів.

У цьому ж контексті більш ширшу класифікацію пропонує А. Погребняк, на його думку загрози можуть бути як випадковими, так і навмисними. До випадкових загроз відносяться: а) помилки обслуговуючого персоналу і користувачів; б) втрата інформації внаслідок не правильного її збереження; в) випадкове знищення або заміна; г) збій у роботі устаткування, електроживлення, дискових систем, комплектуючих елементів мережі; д) некоректна робота програмного забезпечення, зокрема внаслідок зараження комп'ютерними вірусами тощо [314, с.46-47]. До навмисних загроз відносяться: а) несанкціонований доступ до інформації і мережевих ресурсів; б) розкриття і модифікація даних і програм, їх копіювання; в) розкриття, модифікація або підміна трафіка обчислювальної мережі; г) розробка і поширення комп'ютерних вірусів, введення в програмне забезпечення логічних бомб; д) крадіжка магнітних носіїв і розрахункових документів; е) руйнування архівної інформації або навмисне її знищення; є) фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому; ж) перехоплення та ознайомлення з інформацією, яка передана по каналах зв'язку [314,с.50].

Будь-яка з наведених класифікацій, до певної міри, є умовною, оскільки: 1) залежно від мети та методів наукового пізнання може здійснюватись за різними підставами; 2) має суб'єктивний характер, тобто в залежності від суб'єкта що її здійснює та його здатності розрізняти ознаки об'єкта класифікації [173].

Доктриною інформаційної безпеки України визначено як життєво важливі інтереси особи в інформаційній сфері України наступні: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів [101]. Відразу звернемо увагу, що вже в самій назві допущено підміна категорії «людина» на «особа».

Вважаємо, що проблеми захисту від інформації суттєво складніші за проблеми захисту інформації, оскільки загрози, що виникають внаслідок інформаційних впливів надзвичайно різноманітні, їх вплив не завжди очевидний, а відвернення цих загроз або їх нейтралізація вимагають різноманітних неординарних дій. Інформаційні загрози є складним ієрархічним утворенням з множиною різнорівневих зв'язків, їх вплив на людину комплексний і різноманітний.

Варто також звернути увагу, що закріплені інтереси певною мірою відрізняються від тих, що були закріплені в попередній редакції Доктрини: 1) забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; 2) недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних; 3) захищеність від негативного інформаційно-психологічного впливу[120].

Зокрема, слід звернути увагу на пп. 2 і 3 замість більш вузької категорії «персональні дані», нова редакція передбачає «захист приватного життя», а в п.3 уточнено , що захист потрібен від руйнівних інформаційно-психологічних впливів, а не від негативного інформаційно-психологічного впливу.

Таким чином, держава зняла з себе повноваження визначати, що є негативним інформаційно-психологічним впливом. Донедавна єдиним органом, який визначав що саме є негативним інформаційно-психологічним впливом була

Національна експертна комісія України з питань захисту суспільної моралі, яка в різних статусах проіснувала понад 10 років. Досвід її роботи свідчить, що коли державні органи мають повноваження визначати що є моральним, зокрема «сексуальний чи еротичний характер» або «культ насильства, жорстокості, порнографії» призводить до зловживань та цензури. Проте і її вже не існує.

При цьому, чинне законодавство як не передбачало визначення «негативного інформаційно-психологічного впливу», так не передбачає і змісту категорії «руйнівних інформаційно-психологічних впливів». В чинному законодавстві і в правовій науковій літературі часто зустрічається некоректне використання категорій «загрози, ризики, виклики, небезпеки, впливи», що пов'язане з нерозумінням природи цих явищ, та їх місця в системі інформаційної безпеки. Теорія безпеки окреслює категоріальний апарат, який може і, на нашу думку, повинен використовуватись в нормотворчості з метою уникнення підміни понять, а також з огляду на комунікативну правову доцільність [446].

Існує також низка різноманітних визначень виклику, що вказують на наявність протидії (з боку об'єктивних обставин або суб'єктів) реалізації інтересів певного суб'єкта. Виклики не мають чіткого механізму розв'язання, проте ще не вимагають негайного втручання" [58]. Водночас, він характеризується найнижчим ступенем ймовірної реалізації. Коли йдеться про ризики йдеться про усвідомлену можливість небезпеки, а також як можливість збитків або неуспіху у якійсь справі [72].

Сучасний тлумачний словник визначає загрозу як можливість, неминучість небезпеки. З усього різноманіття визначань загрозою можна вважати явище, чинник (и), що спроможні реально створити умови або стати причиною повної або часткової неможливості реалізації істотних інтересів суб'єкта.

Небезпека, за А. Качинським, розуміється як «ситуація, постійно присутня в навколишньому середовищі, що за певних умов може призвести до реалізації небажаної події», має майже стовідсоткову ймовірність [192, с.16.]

Г. Ситником пропонується класифікація видів небезпек, що розкриває взаємозв'язок між цими поняттями, і пропонує при кількісній класифікації небезпек спиратися на поняття „ризик”, а при якісній класифікації – на поняття

„виклик” і „загроза”. Тоді: потенційний виклик (дуже малий ризик); реальний виклик (малий ризик); потенційна загроза (середній ризик); реальна загроза (великий ризик); потенційна небезпека (дуже великий ризик)[291,с.69].

Категорія «вплив», в свою чергу, в теорії безпеки може розглядатись з кількох точок зору. Як взаємодію явищ (чинників) із об’єктом, що призводить до виникнення викликів, ризиків, загроз і небезпек, а також і як цілеспрямовану дію суб’єктів системи забезпечення з метою нейтралізації останніх.

Найбільш широко визначення сутності впливу відкриваються у контексті філософської категорії “взаємодія”. “Філософський енциклопедичний словник” визначає “взаємодію” як філософську категорію, що відображає процеси впливу різних об’єктів один на одного, їхню взаємну обумовленість, зміну стану, взаємопереходи, а також породження одним об’єктом іншого [480, с.81]. Власне з такої позиції Г. Ковальов вплив розуміє як “процес... який реалізується в ході взаємодії двох і більше рівномірно упорядкованих систем і результатом якого є зміна в структурі (просторово-тимчасових характеристиках), в стані хоча б однієї із цих систем”[194, с.4-5].

Категорія впливу є багатовимірною і складною. Існує також позиція, згідно якої феномену впливу має універсальність та всеохоплюючий характер, і може відображати взаємозв’язки, які існують між впливами, різними за своїм походженням та природою (фізичний, хімічний, соціальний, психологічний тощо).

Хоча, фахівці з психології вважають, що результат впливу завжди психологічний, навіть якщо за змістом він є фізичний, хімічний чи соціальний [517]. Слід зауважити, що інформаційний вплив завжди визначає поведінку людини прямо чи опосередковано, через психічні механізми головного мозку. Інформаційні впливи досягають ефекту, коли вони змінюють, реструктурують психологічні властивості, стани і моделі поведінки особистості. Такий підхід певною мірою пояснює, чому терміни «інформаційний вплив» і «інформаційно-психологічний вплив» часто використовуються як взаємозамінні. Хоча, на нашу думку, ці категорії мають певні відмінності, про що буде далі.



Аналіз філософського розуміння категорії впливу дозволяє перейти до визначення інформаційних або інформаційно-психологічних впливів, як таких, що можуть бути руйнівними чи небезпечними.

В теорії безпеки визначається «інформаційний вплив як організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення деструктивних змін у свідомість особистості, соціальних груп чи населення (корекція поведінки), в інформаційно-технічну інфраструктуру об'єкта впливу та (чи) фізичний стан людини» [447]. При цьому інформаційний вплив поділяють на інформаційно-технічний та інформаційно-психологічний впливи, де інформаційно-технічний вплив розглядається як вплив на інформаційно-технічну інфраструктуру об'єкта з метою забезпечення реалізації необхідних змін у її функціонуванні (зупинка роботи, несанкціонований доступ до інформації та її перекручування (спотворення), програмування на певні помилки, зниження швидкості оброблення інформації тощо), а також вплив на фізичний стан людини. Інформаційно-психологічний вплив розглядається як вплив на свідомість та підсвідомість особистості й населення з метою внесення змін у їхню поведінку та світогляд; його базовими методами є переконання й навіювання [44, 367].

Одна з найбільш ґрунтовних, на нашу думку, класифікацій видів психологічного впливу в спілкуванні запропонована О.В. Сидоренко: 1) переконання – свідомо аргументований вплив на іншу людину або групу людей, що має своєю метою змінити їхнє судження, ставлення, намір або рішення; 2) самопросування – відкритий прояв свідчення наявності у людини своєї компетентності й кваліфікації для того, щоб бути оціненою по здобуткам й завдяки цьому отримати перевагу; 3) маніпуляція – прихований від опонента вплив на нього, на його систему ставлень і орієнтацій; 4) прихилиння до наслідування – створення у іншій людини бажання “бути схожою”, подібною до зразка; 5) прохання – словесне звертання до людини із пропозицією задовольнити потребу або бажання ініціатора; 6) примус – вимога виконувати розпорядження ініціатора, підкріплюване прихованими або явними погрозами; 7) деструктивна критика – зневажливі або образливі судження висловлення про особистість опонента, грубий, а іноді агресивний осуд, ганьблення або осміяння його пороків,

вчинків; 8) ігнорування – навмисна неуважність, підкреслене неприйняття людини, при якому ігнорування, найчастіше, виступає як тактична форма примусу або залучення уваги людини до чогось; 9) емоційне зараження – передача свого стану і ставлення іншій людині або групі осіб; 10) навіювання – навмисний свідомий вплив на підсвідомість людини або групи осіб з метою зміни їхнього стану або відношення до питання, а також створення схильності до певних дій [420,с.123-142]. З цієї класифікації видно складність розмежування очевидно правомірних (наприклад, як переконання) і завідомо неправомірних (наприклад, як маніпуляція) способів інформаційного впливу на психіку особи, оскільки всі інші можуть бути використані для досягнення як законних, так і незаконних цілей, отже стати способом вчинення правопорушення. Наприклад, примус використовуватись в рамках закону для забезпечення правопорядку, а, водночас, може стати засобом порушення прав і свобод людини. Навіювання і емоційне зараження часто використовуються маркетологами та психологами в рамках закону, а, водночас, можуть бути використані в шахрайствах та інших правопорушеннях.

За результативністю інформаційні впливи поділяють на ефективні й неефективні; сутнісні, істотні, глибинні й неістотні, поверхневі; стабілізуючі та дестабілізуючі; організуючі та дезорганізуючі. За масштабом трансформацій, спричинених впливами, їх поділяють на глобальні та локальні, часткові. Сам цей масштаб може оцінюватись як за кількістю елементів, що зазнали впливу, так і за ступенем істотності викликаних змін. За масштабом змін може йтися: а) про вплив на актуальну поведінку через породження або зміну ситуативних мотивів, особистісних смислів або смислових установок, як це відбувається в ситуації міжособистісної маніпуляції чи вольової саморегуляції, б) про зміну стійкого ставлення до конкретних речей або людей через породження смислових диспозицій та іноді конструктів, як це робиться, зокрема, в рекламі та пропаганді, а іноді й у психологічному консультуванні; в) про формування чи зміну загальних смислових орієнтацій – світогляду, самостановлення, системи цінностей, із чим має справу практика виховання і психотерапії, а також про ідейну індоктринацію [180, с.47].

Наслідки інформаційних впливів виявляються у цілій низці ефектів, які класифікують таким чином: 1) когнітивні ефекти проявляються у зміні рівня поінформованості, збільшенні обсягу знань (як в усвідомлюваних, так і в неусвідомлюваних формах); формуванні нових когнітивних схем, способів осмислення дійсності, оперування інформацією; 2) емоційні ефекти виражаються у зміні емоційного стану, появі одних та зникненні інших почуттів, у зміні загального емоційно-психологічного фону людського буття, появі імпульсів до активних роздумів, до переробки, трансформації інформації, виникнення прагнення до отримання чи створення нової тощо; 3) ціннісні ефекти виявляються у формуванні нових чи зміцненні або послабленні вже наявних інтересів, смаків, ставлень, оцінок, ціннісних орієнтацій, настанов стосовно світу, окремих предметів, явищ, стосовно інших людей або самих себе; 4) психофізіологічні ефекти також спостерігаються і виявляють себе у зміні психофізіологічного стану особи; 5) поведінкові ефекти спостерігаються у вигляді певних дій, вчинків, відповідної поведінки у сфері предметної діяльності (зокрема, її організації), міжособистісної взаємодії та взаємодії із самим собою [180, с.47]. Особливість інформаційних загроз виявляється в тому, що до появи поведінкових ефектів, їх виявлення і ідентифікація джерела у більшості випадків є неможливою, а отже неможливо і застосувати ефективні заходи щодо нейтралізації їх впливу.

Водночас, слід пам'ятати, що інформаційні впливи є невід'ємною складовою життєдіяльності людини в інформаційному середовищі, необхідною умовою існування суспільної та індивідуальної свідомості, формування людини та її нормальної життєдіяльності, а потреба в інформації – базовою потребою особистості. Інформаційне середовище з його інформаційними потоками та інформаційні впливами різного роду, характеризується сукупністю динамічних факторів, що здатні чинити на людину прямий або непрямий, негайний або відтермінований вплив. Інформаційне середовище є засобом, що опосередковано транслює людині норми, цінності, установки та стереотипи поведінки в суспільстві. Достатність інформаційних впливів на свідомість забезпечує образ реальності, когнітивну модель світу і ситуації, розуміння себе і своїх можливостей. Фундаментальна властивість інформації (щодо людини) полягає в

тому, що вона існує самотійно, відокремлено від об'єкта відображення, стає вмістом пам'яті, тобто самотійно бере участь в психічних процесах, трансформується в уявлення, знання, вміння, навички [243].

Кожна людина, вступаючи в суспільні відносини, одержуючи і передаючи певну інформацію, впливається в це суспільство шляхом засвоєння й дотримання (або незасвоєння чи недотримання) тих норм, які історично в ньому склались. Тому саме суспільство виступає носієм однієї з найбільших загроз інформаційній безпеці людини – інформаційної дискримінації, яка проявляється не лише в розподілі людей на тих, які мають доступ до інформації, і тих, які його не мають. У зв'язку з цим поряд з терміном “інформаційне суспільство” у міжнародній практиці поширюється термін “цифровий розрив” або “цифрова нерівність”, про який ми дещо згадували раніше. На міжнародному рівні питання інформаційної нерівності вперше було порушене в підписаній улітку 2000 р. лідерами країн “вісімки” Окінавській хартії глобального інформаційного суспільства. Згідно з цим документом було утворено міжнародну експертну раду Digital Opportunity Task Force, що виробила план дій, представлений лідерам країн “вісімки” на зустрічі в Генуї влітку 2001 р. [287, с.51-56].

Як відомо, головною метою ООН, сформульованою в Декларації Тисячоліття, є зменшення бідності на планеті. В контексті боротьби з бідністю ООН вирішує й завдання подолання інформаційної нерівності. Що цілком природно, оскільки базовою нерівністю є нерівність економічна, соціальна і культурна, інформаційна ж нерівність є тільки одним з проявів цих базових нерівностей. Без подолання інформаційної нерівності неможливий ні процес глобалізації, ні ефективний розвиток інформаційного суспільства, ні запровадження електронних урядів [426, с.51-62].

Варто звернути увагу, що впроваджуючи в Україні зараз активно процеси е-урядування, пов'язані з ними реалії віддаленого голосування, електронних консультацій, публічних обговорень на сайтах тощо, опираються на ІКТ. І при охопленості близько 60% дорослого населення їх ефективність видається сумнівною [52]. Це не означає, що не потрібно впроваджувати електронну

демократію, а свідчить про необхідність гарантування рівних можливостей доступу до інформаційних технологій.

Міжнародне співтовариство вже з 2000 р. акцентує увагу на необхідності подолання ознак інформаційної та цифрової нерівності, зокрема, в Окінавській хартії глобального інформаційного суспільства серед інших позицій окрема увага зосереджується на необхідності “мобілізації ресурсів для покращення інформаційної та комунікаційної інфраструктур” [287, с.51-56], оскільки інформаційно-комунікаційні технології є найголовнішим чинником, що впливає на формування суспільства XXI ст. ЮНЕСКО визначає головні групи соціальних ознак, відповідно до яких формуються групи розривів: економічні ресурси; географія (асиметрія між міськими і сільськими зонами); вік; стать; мова; освіта, соціальні й культурні підвалини; фізична повноцінність [658].

Економічні ресурси є одним із найважливіших чинників формування світових розривів. Економічно багаті країни мають більші ресурси для втілення технологічних новацій та залучення до них мас. Фінансово незалежні індивіди орієнтуються на найновіші телекомунікаційні та інші технічні засоби для задоволення власних потреб. Географічні розриви базуються на кількох сегментах, зокрема це міжнародний та внутрішній вектори. Міжнародний вектор характеризується суттєвими дисбалансами у доступі до інформації та комунікації через новітні телекомунікаційні канали до світової скарбниці знань між деякими країнами. Наприклад, доступ до Інтернету в країнах Скандинавії перевищує показник у 90 % населення, тоді як в Україні й інших пострадянських країнах цей показник коливається біля позначки 50 % населення [671], причому лєвова частка з них — це мешканці великих міст. Згідно з даними інтернет Асоціація України (опубліковано на їхньому офіційному сайті у квітні 2017 р.), які представляють результати опитування, проведеного протягом лютого 2017 р., на початку р. 64,7% дорослого населення України користуються інтернетом. Частка користувачів інтернет серед людей 15-29 років в Україні сягнула 97%. Старший вік та проживання у сільській місцевості значно зменшують вірогідність користування інтернетом. Опитування проводилось у всіх регіонах України крім окупованого Криму та тимчасово непідконтрольних Україні територій Донбасу.

Кількість користувачів інтернет продовжує зростати. Найчастіше виходять до інтернету за допомогою стаціонарного ПК - 51%, стільникових телефонів - 50%, ноутбуків - 42%, планшетний комп'ютер - 21%, стаціонарний ПК на роботі - 8%, ноутбук на роботі - 5%. В Україні користуються інтернетом близько 21,6 млн. користувачів. Жінки складають - 51% від усіх користувачів, чоловіки - 49%. Мешканці сіл складають 27% у загальній кількості, притому що серед усіх мешканців сіл уже 53% з них користуються інтернетом [52].

Вікові розриви пов'язані з прагненням і відкритістю молоді до інновацій, тоді як люди середнього та старшого віку схильні до стабільності й певної статичності. Все залежить від створених можливостей і мотивації.

Гендерні проблеми виникають у суспільствах, в яких жінка через релігійні чи інші умовності розглядається як неповноправний суб'єкт громадського життя. У Камбоджі законодавчо заборонено ввезення до країни телефонів третього покоління, оскільки "удосконалені моделі сприяють поширенню порнографії" [246]. В Україні ситуація за гендерною ознакою цілком прийнятна – 51 % жінки, 49 % чоловіки.

Однією з суттєвих нерівностей, які перешкоджають реалізації якісного мережевого спілкування, є мовна диспропорція, сформована на основі домінування англійської мови як головної мови інтернету та програмного і технічного супроводу комп'ютерних та телекомунікаційних засобів.

Люди з обмеженими фізичними даними часто не мають можливості спілкуватися в Інтернеті, оскільки не всі комп'ютери налаштовані під потреби інвалідів зору чи слуху, і лише невеликий відсоток сайтів обладнаний програмами звукового супроводу текстового чи графічного матеріалів. Як наслідок, створюється ситуація, коли новітні технології не тільки не сприяють повноцінній реалізації будь-якої особистості, а виступають каталізатором для дискримінації окремих груп населення.

Саме висока інформаційна культура повинна стати перешкодою для розповсюдження інформаційної дискримінації. Інформаційна культура особистості формується в процесі соціалізації, як і інші – правова, економічна, екологічна тощо. На свідомому та підсвідомому рівнях відбувається засвоєння

певних соціальних ролей та поведінкових моделей. В подальшому доросла людина повинна самостійно розвиватись і переживати становлення як особистість в суспільстві. Тому в особливий спосіб акцентуємо увагу на окремих загрозах, які особливо актуальні на початкових етапах соціалізації.

Відбувається помітна уніфікація масової свідомості, оскільки люди “споживають” одні й ті ж інформаційні продукти глобального характеру (новини, реклама, художні твори і т.д.), йде масова пропаганда способу життя, притаманного цивілізації технологічно розвинених країн. Особливо значним є вплив механізму “глобалізації масової свідомості” на дітей та молодь. Втрачається національна ідентичність, відбувається деградація мови, нівелюються морально-етичні принципи, що не може не впливати на правову свідомість.

Інформаційний простір зараз актуалізує багато латентних явищ. Так є, наприклад, з мовою ворожнечі. Єдиного визначення, закріпленого в національному чи міжнародному праві не існує. У різних міжнародних документах в різний спосіб згадується про поняття «hate speech» (у перекладі українською — «мова ворожнечі» або «мова ненависті»). Мова ворожнечі є виявом дискримінації, що виражається в дискримінаційне, некоректне висловлювання до окремих груп чи спільнот або до окремих людей як представників цих спільнот за різними ознаками — етнічною, расовою, національною, віросповіданням, статтю тощо. Як правило, такі висловлювання не просто ображають, а підбурюють до расової ненависті, ксенофобії (страх усього чужого, несвого), антисемітизму (неприятне ставлення до євреїв), гомофобії (страх людей із гомосексуальною орієнтацією), сексизму (зневажливе ставлення до жінки, чоловіка) тощо[530].

В публічному просторі ця тема все більш наголошується, зокрема й завдяки активній і видимій просвітницькій роботі, яку провадять правозахисники у сфері протидії дискримінації. Наприклад, шляхом розміщення рекламних сітілайтів у

великих містах на тему різних проявів дискримінації, одним із яких є мова ворожнечі, вручення символічної премії «Дискримінатор р.»<sup>2</sup>.

Мова ворожнечі — це інструмент маніпуляцій із метою розколу суспільства, це елемент його дестабілізації й зменшення довіри. І найбільшою помилкою тут може бути якраз недооцінювання негативного впливу таких явищ і проявів агресії на суспільну свідомість. У світлі цього окремо варто виділити питання відповідальності за поширення мови ненависті в публічному інформаційному просторі, точніше, її відсутності [531].

Для прикладу, німецький парламент нещодавно обговорював закон проти ненависті та цькування в соцмережах. Цей закон було подано на розгляд міністром юстиції Німеччини, який, з одного боку, він пропонує, щоби слова, вислови, заклики до цькування, якісь маркери ненависті блокувалися, й зобов'язує «Фейсбук» та інші соціальні мережі видаляти такі коментарі протягом 24 годин. У випадках, коли не можна чітко визначити порушення одразу, пропонується сім днів на ухвалення відповідного рішення. Якщо ж адміністрація соцмереж цього не зробить — пропонуються штрафи [419]. Особливого значення набуває питання мови ворожнечі в умовах інформаційної війни.

Існує водночас і критика концепції узаконення відповідальності за мову ворожнечі. Мова ворожнечі як категорія тісно пов'язана з радикальним лібералізмом. Він впроваджується цілком систематично: на рівні державної політики, через широку мережу добре фінансованих громадських організацій, за активної підтримки ЗМІ, зі своєю мовою та системою координат, зі своєю цензурою. Сама по собі цензура є необхідним елементом суспільного життя. Нам дуже важко уявити суспільство, де існувала б абсолютна свобода слова. За адекватних умов цензура має на меті захист суспільного блага, а також універсальних моральних принципів [532]. Прихильники цієї концепції, вважають «Hate speech» універсальним ярликом, за допомогою якого можна затаврувати думки, що суперечать догмам лібералізму. Руйнівне значення концепції “мови

---

<sup>2</sup> Щорічна антипремія «Дискримінатор року» вручається у трьох номінаціях: «Дискримінація «у законі», «Реально Г (ганебний вчинок)» та «Язик мій – ворог мій». В останній номінації 2016 року «переміг» народний депутат Антон Геращенко за коментар в одному з видань щодо нардепа Надії Савченко: він публічно порадив їй вийти заміж і займатися дітьми, а не політикою.



ворожнечі” не можна зводити виключно до того, що ця концепція має на меті заборонити називати речі своїми іменами. Засудження “мови ворожнечі” має сугестивну дію. Воно покликане паралізувати нашу здатність до адекватного етичного мислення.

I. Виртосу пропонує порівняти: «Марш рівності в деяких ЗМІ подається як гей-парад. Здавалося б, яка різниця, яке слово — парад (розвага, гуляння) чи прайд (переклад з англ. — гордість, повага). Однак такі висловлювання формують відповідне ставлення, типу «у нас війна — а в них свої масові гуляння». Наприклад, напад на Марш рівності або підпал кінотеатру «Жовтень» представляється в суді як адміністративне правопорушення і подається ледь не як виправдання: «ну, так же напали на цих геїв, якби ж там були нормальні...» [530].

Запровадження «гендерної рівності» в Україні в багатьох колах небезпідставно сприймається як накидання нової ідеології і культурного перепрограмування. Система освіти активно використовується для реалізації цієї мети. Іншою складовою є розширення розуміння «норми» у сфері сексуальності і дерегуляція відповідних відносин. Так, наприклад, гомосексуальні відносини ще наприкінці ХХ ст. були заборонені на законодавчому рівні у більшості країн. Причиною такої заборони була переважання суспільного осуду і оцінка таких відносин як аморальних і недопустимих. Кілька десятиліть пізніше стала поширюватись концепція гомосексуальних «сімей». Таким чином було практично знищено традиційне визначення сім'ї, як союзу чоловіка і жінки. Те, що колись було маргінальною опозицією, сьогодні є головною політичною силою на глобальному рівні [223].

Проте, під загрозою опинились і абсолютні загальновизнані права людини, наприклад, право на честь і гідність. Порушення цього права, в його специфічному вияві – посмертно, можна побачити на прикладі справи Н. Катсурас [585], дівчини, що в 2006 р. загинула у автокатастрофі у штаті Каліфорнія, США. В інтересах слідства поліція зробила декілька фотографій місця аварії. Декілька співробітників вирішили налякати своїх друзів на Хелоуїн і надіслали їм зроблені фото. Знімки швидко поширилися інтернетом, і батьки дівчини звернулися до суду з вимогою змусити автодорожній патруль Каліфорнії позбутися світлин і

визнати незаконність їх поширення мережею інтернет. На першому етапі справи позов був відхилений. Суд зазначив, що сім'я Катсурас не мала ніяких підстав для позову. Справа була передана до вищої інстанції, і розгляд запланований у Верховному Суді в 2012 р. Проте, відповідач погодилися виплатити родині Н. Катсурас \$ 2375000 на етапі досудового врегулювання.

Родина Катсурас найняли Reputation Defender, щоб видалити фотографії, але вони продовжували поширюватися. За оцінками Reputation Defender, вони переконали сайти, щоб видалити 2500 фотографій, але визнали, що видалення їх з інтернету абсолютно неможливе. Адвокат Т. Франк писав, що хоча засоби масової інформації з розумінням відноситься до важкого становища батьків, але так званий «ефект Стрейзанд»<sup>3</sup> призвів до неконтрольованого поширення фотографій". Величезним питанням є так званий етикет смерті в онлайн-світі. Окрім питань честі гідності, виникають також питання майнового характеру – кому належить цифрова спадщина особи, як в неї вступити?

Ще один приклад щодо права на честь і гідність. Цього разу у зв'язку з використанням технологій Big Data (великих даних). В 2013 р. мережа магазинів роздрібної торгівлі Target мала прецедент з використанням великих даних в маркетингових цілях [601]. Чоловік звинуватив співробітників компанії в тому, що ті надсилають його дочці дисконтні купони на памперси, соски та інші дитячі аксесуари. Чоловік був розлючений, адже його дочка - школярка. Виявилося, що, використовуючи технології і методи обробки великих даних, мережа магазинів дізналася про вагітність дівчинки раніше, ніж її батько. Зі списку регулярних покупок зникли тести на вагітність. Хто і яким чином може оцінювати правомірність і етичність використання таких даних? Чи можливе притягнення в такому випадку до відповідальності?

Іншою загрозою є інформаційні впливи, що становлять загрозу морально-психічному здоров'ю дітей та підлітків. Еротика користується великою популярністю у всіх сферах індустрії розваг, в т.ч. в інтернеті і в мобільному контенті. Аналітики відзначають, що типовим споживачем мобільного

---

<sup>3</sup> Ефект Стрейзанд — феномен, який виражається в тому, що спроба видалити певну інформацію призводить лише до її більш широкого поширення. Наприклад, спроба обмеження доступу до фотографії, файлу або тексту призводить до дублювання даної інформації на інших серверах або появи її в файлообмінних мережах.

порноконтенту є молодь та діти. З цього приводу, наголошу, що існує ілюзія, що це західна проблема і на Україні ще немає підстав хвилюватись.

Водночас, як згадувалось раніше рівні інформаційної культури поколінь значно відрізняються, а за умови, що темп проникнення інформаційних технологій постійно пришвидшується, батьки, вчителі і інші, на кого покладено обов'язок, не володіють необхідним рівнем знань ні щодо загроз, ні щодо способів їх нейтралізації.

Поширення масової культури, неминучість зіткнення з віртуальною реальністю, в якій важко розрізнити ілюзію і дійсність, створюють не лише психологічні і культурні проблеми, але й правові. Створюючи свій образ у віртуальному просторі, людина втрачає адекватне сприйняття реального світу, в тому числі правової дійсності[158, с.63-66].

Важливо враховувати те, наскільки потужним є вплив соціальних мереж і віртуальних світів на психологію людини, перш за все, дітей та молоді. На Заході залежність від соціальних мереж останнім часом досягла апогею: згідно із опитуванням, проведеним у Сполученому Королівстві, із 2,300 респондентів віком від 11 до 18 років, 45 % заявили, що у віртуальному світі вони почуваються щасливішими, ніж в житті[127]. За статистикою, 10-14 % підлітків в Україні страждають від комп'ютерної залежності або ігроманії [79]. Окрім того, не слід забувати про небезпеки віртуального світу, що пов'язані з нездатністю дитини критично сприймати інформацію – 39 % опитаних дітей погодилися з твердженням “Вся інформація в інтернеті є правдивою”[127].

І знову, низький рівень інформаційної, в тому числі комп'ютерної, грамотності більшості батьків, вихователів і вчителів, непристосованість освітніх програм до вимог інформаційного суспільства не дозволяють належним чином захистити дитину від загроз віртуального світу. Інформаційне забруднення як загроза існує як для дітей і підлітків, так і для дорослих. Пропонуємо розглянути це на прикладі реклами по телебаченню. Сучасна дитина майже від народження занурена в інформаційне середовище, яке замість навчити її не мислити, а навпаки, «засмічує» її свідомість надміром неякісної інформації. Рекламні компанії світових концернів часто спрямовані саме на дітей, як потенційних

покупців. Опитування, проведене в 2003 р. компанією “КОМКОН-медіа”, встановило чим старшою стає дитина, тим менше вона дивиться рекламу. Більше половини (52,4 %) глядацької аудиторії, на яку розраховують рекламодавці, становлять дошкільнята. Згідно з отриманими даними, якщо в 9-річному віці телеролик до кінця додивляється 44,8 % дітей, то до 19 р. – тільки 15,9 %. Також встановлено, що діти до 12 років бачать в середньому до 25 000 телереклам в рік [393]. Реклама творить фон життя людини. Не звертати на неї уваги здатна доросла мисляча людина. Свідомо опрацювавши інформацію, є шанс відкинути зайве. Коли інформація сприймається на підсвідомому рівні, вона не обробляється, а сприймається в тому вигляді, в якому була отримана. Пізніше, в конкретних ситуаціях підсвідомість скеровує нашу поведінку відповідно до тої інформації, яка в ній зберігається.

Але й без реклами інформаційний простір забруднений шкідливою для дитячої психіки інформацією. Фільми, передачі, комп’ютерні ігри, на яких дитина зростає, також впливають на її подальшу поведінку. Сцени насильства спричиняють негативний вплив на молодь і підлітків, особливо на тих з них, хто відчуває певні емоційні проблеми. На момент закінчення початкової школи, дитина встигає побачити 8 тисяч вбивств і 100 тисяч інших актів насильства на телеекрані [430].

Вищезазначене показує тенденцію цілеспрямованого забруднення інформаційного середовища особистості таким чином, щоб ця особистість не бачила інших способів поведінки й розвитку, крім тих, що їй пропонуються.

Тому важливим елементом інформаційної культури є інформаційна стійкість. Україна геополітично весь час знаходиться на межі кількох потужних культурних традицій. З одного боку, в Україні, як і в більшості країн Східної Європи відбувається активне насадження прозахідних цінностей. З іншої сторони має місце загроза російської пропаганди, яка в окремих регіонах вже є реалізованою і наслідком якої є гібридна війна (більше в наступному підрозділі).

Безумовно, формування нової системи цінностей і вироблення ідеологічної системи, спрямованої на її підтримку, є складним завданням, яке вимагає ґрунтовного опрацювання і дослідження. Разом з тим, відсутність такої системи

шкодить як інформаційній безпеці окремих громадян, так і безпеці держави загалом. Зазначена ситуація ускладнюється тим, що держава відвернулася від інформаційного й ідеологічного захисту своїх громадян. Це ще раз підтверджує необхідність спрямування інформаційної культури на формування інформаційного імунітету особистості, забезпечення її інформаційної стійкості.

Водночас, не може залишатись поза увагою питання інформаційного забруднення. Велика кількість інформаційних потоків та знаково-символьна архітектура буття сучасної людини, багаторазове дублювання відомостей; перенасичення каналів сприйняття обмежує здатність індивідуальної свідомості впоратися з масивами інформації, що надходить. Інакше кажучи, головною причиною шуму виступає надлишок інформації, особливо якщо остання не затребувана. Шум можливо виміряти лише частково – тоді коли він регулюється певними соціальними нормами. Наприклад, за даними експертів “Лабораторії Касперського”, частка спаму в світовому поштовому трафіку в березні 2014 р. склала 63,5 %, але й ці цифри дозволяють зробити висновок про розмір загрози [438]. Це явище не таке вже безневинне, як може здатися на перший погляд, оскільки зайва, “фонова”, інформація, відволікаючи увагу людини від поставлених цілей, сприяє виснаженню його інтелектуальних сил, підвищує енергетичні витрати.

Сучасна технократична цивілізація нарощує потужність різноманітних шумів та шумових ефектів, не лишаючи при цьому людині ні часу, ні місця для роздумів про життя. Як зазначає Т. Еріксен, “найнеобхідніше вміння в інформаційному суспільстві полягає в захисті себе від 99,99 % пропонованої інформації, якої людина не хоче” [134, с.30].

Проблеми збереження психічного здоров’я громадян України залишаються поза увагою держави. Слід зазначити, що йдеться не про психічно хворих людей, а про право психічно здорової людини зберегти своє психічне, а водночас, і фізичне здоров’я за будь-яких умов життєдіяльності. Особливої уваги на сьогодні заслуговує питання надання професійної психологічної допомоги військовослужбовцям та їх сім’ям, а також внутрішньо переміщеним особам.

Завдяки появі новітніх інформаційних технологій, людство отримало як багато зручностей, так і додаткові несприятливі наслідки для свого фізичного і психічного здоров'я: отримана інформація викликає певну психічну реакцію і залишає відбиток, тобто результат своєї дії, на фізичному тілі людини. Тривале сидіння за монітором або біля телевізійного екрану викликає сухість в очах, проблеми із зором, головні болі; тривале сидіння збільшує навантаження на хребет і призводить до болю у спині, веде до порушення постави; інтенсивне управління мишкою, джойстиком або клавіатурою веде до зайвої напруги в м'язах рук, постійне користування мобільними телефонами, навушниками та голосне прослуховування музики призводять до проблем зі слухом тощо [487, с.82-89].

Принципове значення для сучасного суспільства має факт існування інформаційної картини світу, тобто нашого уявлення про світ. І це уявлення є важливішим, ніж сам світ. Віртуальна реальність впливає на свідомість та підсвідомість людини. Проблема аддикції (патологічної залежності) починається тоді, коли прагнення втечі від реальності, пов'язане зі зміною психічного стану, починає домінувати у свідомості, стаючи центральною ідеєю, що вторгається в життя, веде до відриву від реальності. Відбувається процес, під час якого людина не тільки не вирішує важливих для себе проблем (наприклад, побутових, соціальних), але й зупиняється у своєму особистісному розвитку. У серпні 1997 р. перелік видів “нематеріальної” залежності розширився: патологічне використання інтернету стало позначенням офіційно визнаного психічного розладу. Однак багато психотерапевтів говорять, що інтернет-залежність не є самостійним захворюванням. Як правило, цей діагноз свідчить про інші, серйозні відхилення клієнта – депресію, комунікаційні проблеми тощо. Всі вони, так чи інакше, є ознаками нездатності впоратися зі стресом і формами тієї або іншої дезадаптації в реальному житті.

Влітку 2005 р. на конференції Supernova співробітниця Microsoft Research Л. Стоун зазначила, що в 1997 р. народилося поняття “перманентна часткова увага”, розуміючи під цим режим існування, в якому людина звикає ні на чому довго не зосереджуватися, робити відразу кілька справ, при цьому постійно “скануючи” навколишнє середовище на предмет “нових можливостей”, які в жодному разі не

можна упустити. “Протягом майже двох десятиліть постійна часткова увага була способом існування, способом виконання своїх обов’язків і підтримки відносин”. На думку, дослідниці, з 1985 по 2005 роки тривав цикл, де перманентно розсіяна увага стала цілковитою нормою. Так само як і існування в якості вузла мережі. Відчуваючи себе “на зв’язку” людина відчуває себе “живою”. Але платить вона за це синдромом дефіциту уваги (Attention Deficit Disorder), який є лише варіантом “перманентної часткової уваги”, варіантом, визнаним хворобою[646].

Більш складними наслідками є залежності, пов’язаної з комп’ютером і мережами. Першим в світі центром підтримки інтернет-залежних став центр, створений найвідомішим і авторитетним дослідником в даній області – К. Янг, професором психології Пітсбурзького університету (Бретфорд), автором праці «Спіймані в Мережу»[672]. Створений нею в 1995 р. Центр надає консультації не тільки звичайним людям, а й корпораціям, освітнім установам і психіатричним клінікам. Доктор Янг вперше визначила кілька підтипів залежності, пов’язаної з комп’ютером і мережами (Internet Addiction):

1. Мережева еротоманія або Кіберсексуальна залежність (Sexting і Seks Online Addiction) - Люди, які страждають від цієї залежності, як правило, беруть участь в перегляді, завантаженні і торгівлі порнографією в інтернеті, у дорослих мережевих рольових іграх, соціальних медіа про секс і т.д.,

2. Мережева соціоманія або (Internet Infidelity and Online Affairs) - Люди, які страждають від цього виду залежності занурені в чати, соціальні мережі, або SMS-листування тощо, занадто активні у відносинах, які стають все більш важливими від реальних відносин і життя з сім’єю і друзями, часто призводить до розлучення, роздільного проживання або сімейної нестабільності;

3. [Мережева] ігроманія (Video Games and Gaming Addiction) – відеоігри та комп’ютерні ігри стають все більш складними, детальними і переконливими для зростаючої міжнародної аудиторії гравців. З покращеною графікою, більш реалістичних персонажів і великих стратегічних завдань, то не дивно, що деякі підлітки вважають за краще грати в відеоігри, ніж проводити час з друзями, займатися спортом тощо. Мова йде не тільки про підлітків. Дослідження показують, що від 10% до 15% гравців демонструють ознаки станів, які

відповідають критеріям Всесвітньої організації охорони здоров'я щодо наркоманії, а також в ігрових залежностях (від азартних ігор);

4. Нав'язливий веб-серфінг або Інформаційне перевантаження (Information Overload) – почуття «примусу завантажити інформацію». Наприклад, пошук нової інформації, пошуку в базах даних,

5. Мережеві Компульсії (Net Compulsions) - може бути узагальнена як залежність від перебування в інтернеті, азартні ігри онлайн, покупки тощо [672].

Інтернет-залежні страждають не лише психічно, а отримують серйозні проблеми, пов'язані з фізичним здоров'ям і загальним самопочуттям, а також соціально дезадаптацію. Це може супроводжуватися соматичними порушеннями — різью і сухістю в очах, болем у спині і ліктях. Іншими наслідками інтернет-залежності можуть стати зміни в характері, ігнорування домашніх обов'язків і загальна байдужість.

У 2008 р. уряд Китаю на державному рівні визнав інтернет-залежність загрозою здоров'ю населення номер один і назвали «третьою опіумною війною», а на 2015 рік в Китаї було 350 мільйонів геймерів. Китайські медики офіційно визнали інтернет-залежність хворобою. Визначення захворювання і його діагностичні критерії були розроблені співробітниками Пекінського центрального військового госпіталю за матеріалами 1300 «проблемних» користувачів інтернету. Симптоми залежності включають непереборне бажання увійти до мережі, розумове або фізичне виснаження, дратівливість, порушень сну або концентрації уваги. За останні десятиріччя відкрилося величезна кількість реабілітаційних центрів, більшість з яких очолюють військові у відставці. Центри, як правило, недержавні, представляють собою комбінування армії, в'язниці і психіатричної лікарні.

Відповідно до китайських діагностичних рекомендацій, інтернет-залежною визнається людина, яка проводить в мережі не менше шістьох годин на день і у якої спостерігався щонайменше один з симптомів залежності протягом попередніх трьох місяців. За словами експерта з госпіталю Тао Жання, 80% залежних виліковні. Як показали попередні дослідження, інтернет-залежністю



мають близько 10% китайських користувачів інтернету у віці до 18 років, 70% з них - чоловічої статі [176].

В США для підтримки інтернет-залежних та їх розроблено програму 12 кроків (на зразок 12 кроків «Товариства Анонімних Алкоголіків»). Ознакою одужання вважається здатність людини контролювати час, проведений в мережі.

У Південній Кореї існує «закон Попелюшки», який забороняє підліткам після півночі грати в онлайн-ігри.

У Фінляндії при інтернет-залежності можна отримати відстрочку від армії на три роки. Вважається, що за цей термін «хворий» встигне вилікуватися і стати соціально активною одиницею фінського суспільства.

Для людини зі здоровою психікою електронна пошта, соцмережі та інші ресурси залишаються зручною технологією, проте якщо у користувача вже спостерігаються психологічні труднощі, зокрема проблеми в спілкуванні з іншими людьми, посттравматичний синдром тощо, то ймовірність негативного впливу (аж до виникнення хворобливих станів) збільшується. Хоча інтернет-залежність не є психічним розладом за медичними критеріями (DSM-V і МКБ-10), проте в усьому світі значна увага приділяється інформаційній гігієні і інформаційній культурі.

Джерела загроз інформаційно-психологічній безпеці людини таким чином охоплюють можливості суб'єкта впливу, особливості фізичного і інформаційного середовища, а також стан об'єкту. Аналіз наукової літератури показує, що основними факторами інформаційного середовища, які можуть стати чинниками ризику, а отже, джерелами інформаційно-психологічної небезпеки, є: 1) обсяг, повнота, кількість інформації що циркулює в системі, точність, доступність, своєчасність її надходження; 2) адекватність ергономічних характеристик інформації та їх потоків перцептивним параметрам органів почуттів, властивостям уваги, пам'яті, мислення, стану особистості, поведінковим стереотипам, соціально-психологічним установкам суспільства; 3) наявність в інформаційних потоках специфічних елементів, цілеспрямовано змінюють психофізіологічний стан великих мас людей, або осіб, які приймають важливі для соціуму рішення; 4) наявність в інформаційному середовищі модифікованих

фізичних носіїв інформації, що впливають безпосередньо на її фізіологічне сприйняття [75].

До основних факторів інформаційно-психологічного ризику, що властиві самій людині, відносять: 1) незрілість особистості, що виражається в нездатності до самостійного, свідомого вибору інформації, релевантної своїм змінам, переконанням і планам; 2) установки особистості на конформізм, імітаторство, на готовність до сприйняття маніпулятивних інформаційних впливів; 3) негативні зміни функціонального стану головного мозку і психіки; 4) стан соціуму, що сприяє підвищеній сугестивності, масовому зараженню ідеями, закликами, що може бути спровокований на психофізіологічному рівні хронічним або гострим психоемоційним стресом, фрустрацією, тривожністю [130].

Таким чином, не можна залишити поза увагою ще одну загрозу – низький рівень інформаційної і правової культури, який породжує еклектизм як панівну ознаку інформаційної “культури мас”. В найширшому значенні еклектизм означає механічне поєднання в одному вченні різнорідних, органічно несумісних елементів, які запозичуються з протилежних концепцій. Низький рівень інформаційної культури за умов надміру інформації породжує, як наслідок, порушення цілісності особистості, знижує її спроможність критично сприймати, аналізувати, оцінювати отриману інформацію і формувати власну позицію.

Підтримуємо думку професора Арістової І.В.: “Хоча інформація є дійсно інструментом знання, але сама по собі вона не є знанням. Інформація, яка виникла із бажання обмінюватися знаннями та зробила більш ефективною їх передачу, залишається лише формою знання, точною й стабілізованою, індексованою за часом та користувачем. Інформація, навіть якщо вона може бути “покращена”, не обов’язково має правильне усвідомлення” [16, с.3-13].

Окрему категорію загроз становлять ті, що виникають зв’язку з використанням соцмереж та комунікаторів. Соцмережі містять величезну кількість інформації про особу, яку вона розмістила там особисто і добровільно, при цьому помилково вважаючи, що ця інформація надійно захищена паролем. Зловмисники активно крадуть паролі та логіни до соціальних мереж, які, за

даними експертів «Лабораторії Касперського», на чорному ринку коштують усього близько 5 доларів США[221].

Низький рівень інформаційної і правової культури населення дозволяють зловмисникам використовувати для отримання персональних даних різноманітні квести («Перевір своє знання географії», «Який у тебе словниковий запас», «Визнач свій психотип», «Як ти будеш виглядати через 50 років», «На якого звірати подібний», «Яка машина тобі личить» тощо). Для користування подібними ресурсами людина «логіниться»<sup>4</sup> за допомогою власного аккаунта в соцмережі і надає згоду на використання інформації, що міститься у ньому. Так, «безневинні», на перший погляд, розваги, дозволяють легально стежити за особою – отримувати інформацію про її вподобання, геолокацію, друзів, активність тощо.

Німецькі правозахисники у галузі захисту приватності інформації вимагали видалити кнопку «Like» від адміністрації соцмережі Facebook, яка дозволяє користувачам оцінювати інформацію на сайті в режимі онлайн. Вони заявили, що її використання суперечить німецькому та європейському законодавству, оскільки таким чином персональна інформація про користувачів – інтереси, тривалість перебування на тій чи іншій сторінці, переходи з одного сайту на інший надходить до США, де згодом використовується для таргетування реклами, аналізу поведінки користувачів на сайті тощо. Представники соціальної мережі підтвердили, що, натискаючи цю кнопку, така інформація як IP-адреси, могла передаватися. Вони також зазначили, що ці дані, відповідно до європейського законодавства через 90 днів видаляються [277].

Окремо варто звернути увагу на системи візуального розпізнавання. Спеціальна програма аналізує фотографії і пропонує користувачеві різні варіанти імен того чи іншого знайомого. Ця система успішно впроваджена в США, у тому числі відповідна програма написана для мобільних пристроїв Apple і призначена для поліції [392]. Поліція англійського графства Лестершир в 2014 також вперше в Британії стала використовувати систему NeoFace, яка дозволила порівнювати

---

<sup>4</sup> Від «Логін» (англ. login, logon) — у комп'ютерній безпеці — алфавітно-цифровий набір символів, що ідентифікує користувача комп'ютера або комп'ютерної мережі. Логін разом із паролем зберігаються в обліковому записі та використовуються операційною системою для надання користувачу дозволу на з'єднання з системою та визначення його прав доступу до ресурсів мережі.

особу підозрюваного з наявною у поліції картотекою в 92 тисячі осіб [403]. Як видається, нові технології можуть допомагати швидше і легше ідентифікувати злочинців, адже зафіксовані на камеру спостереження кадри можна порівняти з базами біометричних даних, про які йшлося раніше.

Проте, Й. Каспар зазначає: «Збирання даних – це також засіб соціальної дискримінації. Це у багатьох випадках може призводити до значних зловживань цим інструментарієм»[403]. Наприклад, аналіз індивідуальних рис обличчя може мати випадкові збіги. Як приклад, якщо профіль футбольного фаната буде схожий на профіль якогось футбольного хулігана, йому навіть не продадуть квиток на матч. У зв'язку з рішучими протестами з боку захисників приватних даних спочатку уряд Німеччини, а потім Євросоюз прийняли рішення про заборону цієї технології, яка, на їхню думку, порушує відразу низку законів про захист даних користувача. І соціальна мережа Facebook відключила автоматичного розпізнавання обличчя особи користувачів у Європі. Також було відзначено, що банк із «відбитками облич» мільйонів людей пов'язаний із величезним ризиком зловживань. Як приклад, така система може бути використана в недемократичних країнах з метою стеження за опозицією або злочинцями [235].

З 2015 р. з'явилась інформація про те, що Фейсбук почав збирати інформацію про всіх, хто будь-яким чином скористався Facebook, навіть якщо вони не знали про це. Це означає, що навіть використання Facebook без облікового запису (наприклад, інструменти для коментарів в блогах або «лайки» за допомогою вбудованих ресурсів), призводить до передання даних на сервери компанії [580]. При цьому порушується принцип поінформованої згоди, оскільки пересічний користувач Web, який не має облікового запису Facebook, з такими правилами може ніколи і не ознайомитись. Тому що згадана вище інформація відображається тільки після входу в систему на власний аккаунт Facebook.

Facebook, так само, як Google, заявляють, що збір даних здійснюється в інтересах суспільства. По-перше, тому що вони показують реклами, і тому хочуть, щоб вона відповідала зацікавленням для людей. По-друге, іноді завдяки мережам правоохоронці мають більше можливостей у боротьбі зі злочинністю. Проте, як свідчить практика останніх місяців, і історія з передачею даних Cambridge

Analytica, володіючи метаданими користувачів та мільйонів інших людей, які можуть бути об'єднані і проаналізовані за допомогою технологій Big Data, Фейсбук має і отже використовувати неконтрольовано безпрецедентний обсяг інформації щодо сучасних користувачів технології.

Але збирання інформації і переслідування завдяки соціальним мережам є можливим не лише для поліції, комерційним організаціям, а й самим користувачам, які не завжди використовують його в законних цілях. Кібербуллінг і кібермоббінг, а також розшук лінчування правопорушників за допомогою соцмереж набувають все більшого поширення. Спільним знаменником для них є не лише використання інтернету і соцмереж з метою переслідування конкретної особи чи групи осіб, але й складність притягнення винних до відповідальності.

У первинному розумінні моббінгом вважався систематичний прояв ворожості, знущання та дискримінації на робочому місці, як з боку колег, так і зі сторони керівництва. Проте з часом ця категорія поширилась на будь-яке систематичне, повторюване протягом тривалого часу цькування, образу, приниження гідності іншої людини, наприклад, у школі, на робочому місці, у в'язниці, і через Інтернет (кібермоббінг).

Кібер-буллінг (cyber-bullying), віртуальний терор, (від англійського слова bull – бик) із спорідненими значеннями: агресивно нападати, роз'ятрювати, задирати, прискіпуватися, провокувати, дошкуляти, тероризувати, цькувати. В українському молодіжному сленгу є дієслово аналогічного походження – «бикувати». Кібер-буллінг часто плутають із моббінгом, або масовим цькуванням (від mob – натовп), хоча насправді агресивна поведінка, яка позначається цими двома поняттями, має різні соціально-психологічні механізми [193].

Ззовні і один, і другий виглядають приблизно однаково - це напади з метою завдання психологічної шкоди, а також шкоди репутації особи, які здійснюються через електронну пошту, сервіси миттєвих повідомлень, у чатах, соціальних мережах, на web-сайтах, а також за допомогою мобільного зв'язку. Така багаторазово повторювана агресивна поведінка має на меті зашкодити людині і базується на дисбалансі влади (фізичної сили, соціального статусу в групі).

Американські дослідники Р.Ковальські, С. Лімбер і П. Агатстон виокремлюють такі основні типи поведінки властиві для кібербулінгу [611]:

1. Перепалки, або флеймінг – обмін короткими запальними репліками між двома та більше людьми, що розгортається зазвичай у публічних місцях Мережі. Інколи перетворюється на затяжний конфлікт (holuwar – священна війна). На перший погляд, флеймінг – боротьба між рівними, але за певних умов вона може перетворитися на нерівноправний психологічний терор. Несподіваний випад може привести жертву до сильних емоційних переживань.

2. Нападки, постійні виснажливі атаки (harassment) – повторювані образливі повідомлення, спрямовані на жертву (наприклад, сотні sms на мобільний телефон, постійні дзвінки), з перевантаженням персональних каналів комунікації. Трапляються також у чатах і форумах, а в онлайн-іграх цю технологію найчастіше використовують грифери (grieffers) – група гравців, що мають на меті не перемогу, а руйнацію ігрового досвіду інших учасників.

3. Наклепи (denigration) – поширення принизливої неправдивої інформації. Текстові повідомлення, фото, пісні, які часто мають сексуальний характер. Жертвами можуть бути не лише окремі підлітки – часом трапляються розсилки списків («хто є хто в школі», «хто з ким спить»), створюються спеціальні «книги для критики» (slam books) із жартами про однокласників.

4. Самозванство, втілення в певну особу (impersonation) – переслідувач позиціонує себе як жертву, використовуючи її пароль доступу до аккаунту в соціальних мережах, у блозі, пошті, системі миттєвих повідомлень, або ж створює свій аккаунт із аналогічним нікнеймом та здійснює від імені жертви негативну комунікацію. Організація «хвилі зворотних зв'язків» відбувається, коли з адреси жертви без її відома відправляють друзям провокаційні листи.

5. Ошуканство, видурювання конфіденційної інформації та її розповсюдження (outing & trickery) – отримання персональної інформації і публікація її в інтернеті або передавання тим, кому вона не призначалася.

6. Відчуження (остракізм, ізоляція). Будь-якій людині притаманне бажання бути включеним у групу. Виключення ж із групи сприймається як соціальна смерть. Що більшою мірою людина виключається із взаємодії, то гірше вона

почувається, й то більше падає її самооцінка. У віртуальному середовищі це може призвести до повного емоційного руйнування дитини. Онлайн-відчуження можливе в будь-яких типах середовищ, де використовується захист пароллями, формується список небажаної пошти або список друзів. Кібер-остракізм проявляється також через відсутність відповіді на миттєві повідомлення чи електронні листи.

7. Кіберпереслідування – приховане вистежування жертви з метою організації нападу, побиття, зґвалтування тощо.

8. Хепіслепінг (від англ. slap – ляпас) – назва походить від випадків в Лондонському метро, коли хулігани били випадкових перехожих заради сміху і підняття власного статусу, записуючи це на камеру мобільного телефону. Зараз так називають будь-які відеоролики із записами реальних сцен насильства, які після розміщуються в інтернеті без згоди жертви [611].

Бесіди з київськими підлітками підтверджують наявність більшості описаних типів поведінки в їхньому досвіді чи уявленнях. Навіть хепіслепінг, який виник відносно нещодавно, трапляється серед українських дітей [266].

Відмінності кібер-буллінгу від традиційного реального зумовлені особливостями інтернет-середовища: анонімністю, можливістю сфальшування, наявністю величезної аудиторії, можливістю дістати жертву будь-де і будь-коли. На відміну від реального цькування, для кібер-буллінгу не потрібні м'язи чи високий зріст, а лише технічні засоби, час і бажання когось тероризувати.

Хоча основною категорією ризику кібербуллінгу є підлітки і молодь, проте трапляються і подібні випадки серед дорослих. Так, 31-річну жінку засудили до позбавлення волі за доведення до самогубства через соцмережу. Вона реєструвалася під різними іменами і публікувала на сторінці колишнього хлопця і сторінках його знайомих інформацію про його нетрадиційну сексуальну орієнтацію. Він не витримав цькування і покінчив життя самогубством [296].

Кібермобінг, на думку деяких дослідників, має «ширшу аудиторію» як серед жертв, так і серед переслідувачів. Хоча його види, які виділила N. E. Willard у праці «Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress» є майже повністю подібні [669]: flaming – образа,

що має місце у публічному інтернет-просторі, за допомогою образливих коментарів, вульгарних звернень; harassment – цілеспрямовані, систематичні кібератаки від незнайомих людей, користувачів соціальних мереж, а також від людей з найближчого реального соціального оточення; denigration – навмисне очорнення, поширення чуток за допомогою публікації фото- або відеоматеріалів на інтернет-сторінках, форумах, в групах, через електронну пошту; impersonation – використання фіктивного імені для доступу до ресурсів від імені жертви, наприклад з метою зіпсувати її репутацію; outing and trickery - поширення особистої інформації, наприклад, інтимних фотографій, фінансового стану, роду діяльності з метою образити або шантажувати, наприклад, екс-партнера; exclusion - соціальна ізоляція, відмова спілкуватися (як на діловому, так і на неформальному рівні), що реалізується через видалення з друзів, груп тощо; cyberstalking - систематичне переслідування за допомогою використання електронних засобів, у тому числі інтернету; може поєднувати погрози, заклики до сексу, фальшиві звинувачення, наклепи, крадіжку ідентичності та вандалізм; часто використовується в поєднанні з реальним переслідуванням, оскільки обидва є вираженням бажання контролювати, залякувати або маніпулювати жертвою; cyberthreats – погрози фізичної розправи вбивства або заподіяння тілесних ушкоджень.

Польські дослідники, поєднуючи обидва типи під поняттям «agresja elektroniczna» (електронна агресія) виокремлюють такі типи жертв: 1) жертва, для яких характерною особливістю є нерівність «сил» жертви і нападника, тобто коли жертва слабша; 2) знаменитості (селебріті), де знаменитістю вважається людина, що часто згадується в медіа і викликає громадський інтерес, незалежно від професії чи роду діяльності; 3) особи, що приналежать до певної групи (ang. bias bullying), об'єднаної спільними цінностями, такими раси, етнічної приналежності, сексуальної орієнтації, релігії, віку, сімейного статусу, фізичної або психічної неповносправності і ін.; 4) випадкові жертви, незнайомці «яким не пощастило»; 5) електронне хуліганство, коли правопорушник і жертва, як правило, є членами однієї і тієї ж групи, як онлайн і в реальному житті [635].



Варто нагадати справу М. Майєр [662]. У 2006 р. в маленькому американському містечку посварилися дві 13-річні школярки - Меган Майєр і Сара Дрю. Мати однієї з дівчаток сприйняла цю сварку близько до серця і вирішила встановити стеження за колишньою подругою дочки. Вона не стала наймати для цього приватних детективів, а просто створила в соціальній мережі MySpace аккаунт від імені симпатичного 16-річного хлопця на ім'я Джош Івенс, який втерся в довіру до простодушної Меган Майєр і незабаром завів з нею роман. Лорі писала від імені Джоша втрюх з 13-річною Сарою і зі своєю молодого підпорядкованої на роботі Ешлі Гріллс. Одного дня міфічний Джош, який зумів до того моменту підкорити серце провінційної школярки, раптом почав її всіляко ображати, принижувати і прямо порадив дівчинці позбавити світ від своєї присутності. У той же день Меган Майєр наклала на себе руки, повісившись у шафі. І ФБР, розслідуючи обставини її самогубства, відразу вийшло на слід віртуального Джоша Івенса, чия порада призвела до загибелі дівчинки. Присяжні, під впливом природніх людських почуттів, визнали її винною за трьома пунктами пред'явленого їй звинувачення. А федеральний суддя, керуючись буквою закону, скасував їх вердикт, звільнивши Лорі Дрю від будь-якої відповідальності за вчинене. Лорі Дрю звинуватили в несанкціонованому доступі до комп'ютерних мереж на тій підставі, що вона зареєструвалася в MySpace, використовуючи вигадане ім'я, і, тим самим порушила правила використання цієї соцмережі. Покарання за кожним з трьох пунктів звинувачення могло скласти до трьох років в'язниці і штраф до 300 000 доларів. Але ні американські юридичні експерти, ні професійний суддя не могли погодитися з подібним трактуванням «несанкціонованого доступу».

Відповіддю на цю колізію став внесений до Конгресу США законопроект HR1966, що передбачає відповідальність за «кіберцькування» (cyberbullying) [557]. Перспективи його прийняття в нинішньому вигляді вельми сумнівні: визначити межу між злочинним «цькуванням» і свободою висловлювання для американського законодавця ніколи не було легким завданням. А навіть якщо і приймуть такий закон, проблему, що спонукала до його створення, він все одно не вирішить.

Кількість загроз інформаційній безпеці буде зростати і надалі, з огляду на поширенню інформаційних технологій у всіх сферах життєдіяльності людини і збільшенню їх впливу. В першу чергу, їх розвиток відбувається в комерційних цілях. Так було з Big Data, штучним інтелектом, інтернетом речей. В США з 1 серпня 2017 р. вже почалося чіпування людей. Американська компанія Three Square Market імплантує співробітникам чіпи розміром з рисове зернятко між великим і вказівним пальцями. З його допомогою люди можуть входити в офіс або платити за їжу. 50 із 80 працівників добровільно погодились на чіпування [668]. «Компанії часто стверджують, що ці чіпи безпечні і зашифровані. Але "зашифрований" - досить розмитий термін. Незрозуміло, чи дійсно це безпечно, або все ж цей пристрій можуть зламати», - каже А. Аккісті, професор інформаційних технологій і державної політики в Університеті Карнегі-Меллон.

Ще одна потенційна проблема, за словами Аккісті, полягає в тому, що технологія, розроблена для однієї мети, пізніше може бути використана для іншої. Мікрочіп, імплантований сьогодні, щоб забезпечити прохід до будівлі або платежі, пізніше теоретично може бути використаний інакше. Наприклад, можна відстежувати тривалість обідніх перерв співробітників без їх згоди або в інший спосіб втручатись у їх приватне життя [10].

Ще одним суперечливим питанням є використання чат-ботів. Чат-боти - це програми, які здатні імітувати спілкування користувача з одним або декількома співрозмовниками. Як правило, вони створюються на базі таких додатків, як Telegram, FB, Messenger, Skype, Viber і ін. Для впровадження інновацій, таких як використання чат-бота, добре підходить сфера послуг - страхові, медичні, комунальні, банківські, транспорт, зв'язок, туризм, ресторанний бізнес і, навіть, юридичні послуги. Швидкість і простота виконання сценаріїв, як замовлення послуг, консультування з типових питань, претензії тощо дозволяє залучати нових клієнтів за рахунок підвищення якості обслуговування вже існуючих.

В Україні юристи-боти в основному представлені в двох видах: у вигляді спливаючих вікон на сайтах, прямо або побічно пов'язаних з юридичною практикою, і у вигляді спеціальних сервісів або розділів сервісів (наприклад, юрист-бот в сервісі Telegram). По суті, юрист-бот є чат-ботом - набором

алгоритмів, що обробляють ваш запит, а потім, шляхом пошуку по зовнішніх ресурсах, що видає найкращий за критеріями конкретного бота відповідь [61].

Бот постійно вдосконалюється. В 2015 р. компанія Microsoft впровадила технології, створені для визначення по міміці особи таких основних емоцій як гнів, щастя, апатія, здивування, байдужість, вказуючи їх у процентних співвідношеннях.

В 2017 р. вчені з Массачусетського технологічного інституту розробили алгоритм для аналізу твітів, який може визначати сарказм і емоційний підтекст [536]. Визначення настрою в соціальних мережах корисно для відстеження відношення до брендів і продуктам, а також для виявлення тенденцій на фінансових ринках. Але більш точне розпізнавання сенсу твітів може допомогти комп'ютерам автоматично виявляти і контролювати емоції.

Спочатку дослідники хотіли розробити систему, здатну виявляти расистські повідомлення в Твіттері. Але незабаром вони зрозуміли, що сенс багатьох повідомлень не може бути правильно ідентифікований без розуміння сарказму. Обидві технології використовують глибоке навчання - популярний метод машинного навчання, який базується на навчанні нейронної мережі для розпізнавання тонких патернів з використанням великої кількості даних.

Яким чином ці технології вплинуть на людство? Будь-яка технологія може бути використана в обидві сторони. К. Лоренц писав про « вагомій підставі вважати внутрішньовидову агресію найбільш серйозною небезпекою, яка загрожує людству в сучасних умовах культурно-історичного і технічного розвитку» [241].

Не можливо надати вичерпний перелік інформаційних загроз людині, оскільки вони модифікують з розвитком інформаційних технологій і самого суспільства. Основна частина розглянутих була спрямована на порушення особистих прав людини. Сховатись від інформаційних загроз або закрити інформаційний простір від зовнішнього інформаційного впливу в жоден спосіб, чи то правовий, чи то технічний неможливо. Інформаційна безпека не зводиться винятково до захисту відомостей і даних.

На основі проведеного дослідження вважаємо за необхідне виокремити такі групи загроз інформаційній безпеці людини в залежності від цінностей, яким вони загрожують:

1) технологічні – впливають із постійного вдосконалення технологій та відставання правового забезпечення їх функціонування, реалізують, здебільшого, як загрози безпеці інформації, проте, можуть прогресувати до загроз інформаційній безпеці;

2) соціально-правові – пов'язані із становищем людини у суспільстві і державі, а також можливістю реалізовувати свої соціальні, культурні, політичні і економічні права і свободи;

3) істотні – пов'язані безпосередньо з фізичною і психічною безпекою людини, що є необхідною умовою її якісної життєдіяльності. Реалізація істотних загроз призводить до порушення найважливіших абсолютних прав і свобод людини – на життя, на здоров'я, тілесну недоторканість, повагу людської гідності, недоторканість приватного життя тощо.

Свобода, яка є найважливішою умовою буття людини, обумовлює необхідність гарантування інформаційної безпеки людини. Загрози інформаційній безпеці людини є складним ієрархічним утворенням з множиною різнорівневих зв'язків, їх вплив на людину комплексний і різноманітний. Тому запропонований поділ є певною мірою умовний.

В умовах інформаційного суспільства можливості реалізації прав і свобод людини суттєво залежать від адаптованості до них самої особи, інститутів суспільства і держави, а також системи права. Необхідною складовою такої адаптації і умовою реалізації і захисту прав і свобод людини є високий ступінь інформаційної та правової культури.

Особливої уваги вимагає дослідження загроз, які існують на початкових етапах соціалізації особистості, оскільки на цьому етапі формується інформаційна культура людини, яка в подальшому дозволить (або не дозволить) ефективно протистояти інформаційним загрозам, викликам та ризикам, а також використовувати можливості, які створює інформаційне суспільство.

## Висновки до розділу 2

Розуміння інформаційної безпеки людини як правової категорії повинно ґрунтуватися на комплексності її як соціального явища, а також враховувати її внутрішню будову. Базуючись на міждисциплінарному підході, та тому, що інформаційна безпека людини як соціальне явище вивчається в різних науках (виходячи зі своїх предметних сфер і методів дослідження), сформульовано структуру інформаційної безпеки людини, що поєднує такі елементи – інформаційно-технологічну, інформаційно-психологічну і інформаційно-правову безпеку, а також визначено їх зміст.

Підхід, що був закріплений в Доктрині інформаційної безпеки, декларує конструктивне поєднання діяльності держави, громадянського суспільства і людини, при забезпеченні інформаційної безпеки України. Проте, аналіз чинного законодавства, свідчить про доцільність чотирирівневої системи забезпечення інформаційної безпеки, запропонованої Олійником О.В. – на стратегічному, (загальнодержавному) рівні, організаційно-виконавчому (відомчо-територіальному) рівні, на рівні визначення критично важливої інфраструктури, і четвертий рівень – рівень суб'єктів невідного характеру. Власне на цьому, останньому рівні визначною має стати роль людини як суб'єкта власної інформаційної безпеки і знайти відображення в нормативно-правовому закріпленні її інформаційно-правового статусу.

Аналіз творення системи правових основ інформаційної безпеки свідчить, що це одна з базових потреб сучасної держави, яка вимагає розробки відповідної державної політики, її закріплення і реалізації на всіх рівнях. Акцентується увага, що політика інформаційної безпеки не може існувати у правовому вакуумі – вона виступає невід'ємною складовою інформаційної політики держави та політики національної безпеки, окрім того, має базуватись на міжнародних стандартах інформаційної безпеки і відповідати національним потребам та реальному стану розвитку інформаційного суспільства в державі. Інформаційне законодавство та законодавство щодо інформаційної безпеки є відносно новою галуззю законодавства України і все ще знаходиться на етапі становлення. В результаті дослідження запропоновано виокремити наступні етапи його становлення: I. 1992-

1996 роки – становлення основ інформаційного законодавства; II. 1996-2003 роки – усвідомлення і формулювання основ інформаційної безпеки як складової національної безпеки; III. 2003-2014 роки – усвідомлення розвитку глобального інформаційного суспільства, приєднання до міжнародних актів щодо у сфері інформаційного суспільства, права і безпеки, розвиток національного законодавства згідно з тенденціями міжнародного права. При цьому, на нашу думку, у 2010-2014 роках мала місце криза у сфері інформаційної безпеки, обумовлена незваженою інформаційною політикою держави; IV. 2014 – донині – розвиток законодавства у сфері інформаційної безпеки, спрямований на посилення позицій України у гібридній війні.

Аналізуються наукові дослідження щодо правового забезпечення інформаційної безпеки та регулювання відповідних правовідносин. При цьому наголошується, що правове регулювання доцільно розглядати лише як засіб забезпечення інформаційної безпеки. На основі аналізу доктринальних праць та чинного законодавства визначено, що правове забезпечення інформаційної безпеки має поєднувати норми щодо: правового закріплення інтересів людини, суспільства і держави у інформаційній сфері; суб'єктивних інформаційних прав людини та громадянина; системи органів, відповідальних за забезпечення інформаційної безпеки; форм участі громадянського суспільства у забезпеченні інформаційної безпеки. Слід відзначити, що за змістом інформаційне законодавство є комплексною галуззю і поєднує норми приватного та публічного права, в той час, як законодавство у сфері інформаційної безпеки містить норми переважно публічно-правового характеру.

Нагальною потребою вбачаємо необхідність розробки і прийняття базового для правових основ інформаційної безпеки закону «Про інформаційну безпеку». При цьому важливим вбачається не відокремлювати кібербезпеку від інформаційної безпеки. На його сонові має бути сформоване правове забезпечення інформаційної безпеки, що поєднає положення щодо: правового закріплення національних інтересів людини, суспільства і держави у інформаційній сфері; суб'єктивних інформаційних прав людини та громадянина;

системи органів, відповідальних за забезпечення інформаційної безпеки; форм участі громадянського суспільства у забезпеченні інформаційної безпеки.

Здійснений аналіз змісту категорій «виклики», «загрози», «ризики», а також чинники, що зумовлюють ескалацію загроз інформаційній безпеці людини, свідчить про їх комплексний характер. Їх аналіз завжди є певною мірою суб'єктивним, обумовленим сприйняттям певною особою чи соціальною групою конкретних факторів через призму власних інтересів і фахового рівня. Разом із тим, об'єктивне визначення загроз передбачає чітке усвідомлення параметрів, поза межами яких певне явище втрачає можливості саморегуляції та потребує зовнішнього втручання для збереження стабільності соціальної системи, а також певних умов, що перетворюють ті ж самі фактори або на реальну, або на потенційну загрозу. Водночас, класифікація загроз є необхідною для визначення саме тих загроз, які становлять актуальний пріоритет в науковій чи нормативно-правовій перспективі.

На основі проведеного дослідження вважаємо за необхідне виокремити такі групи загроз інформаційній безпеці людини в залежності від цінностей, яким вони загрожують: 1) технологічні – впливають із постійного вдосконалення технологій та відставання правового забезпечення їх функціонування, реалізують, здебільшого, як загрози безпеці інформації, проте, можуть прогресувати до загроз інформаційній безпеці; 2) соціально-правові – пов'язані із становищем людини у суспільстві і державі, а також можливістю реалізовувати свої соціальні, культурні, політичні і економічні права і свободи; 3) істотні – пов'язані безпосередньо з фізичною і психічною безпекою людини, що є необхідною умовою її якісної життєдіяльності. Реалізація істотних загроз призводить до порушення найважливіших абсолютних прав і свобод людини – на життя, на здоров'я, тілесну недоторканість, повагу людської гідності, недоторканість приватного життя тощо.

Загрози інформаційній безпеці людини є складним ієрархічним утворенням з множиною різнорівневих зв'язків, їх вплив на людину комплексний і різноманітний. Тому запропонований поділ є певною мірою умовний.

Обґрунтовано, що саме суспільство виступає носієм однієї з найбільших загроз інформаційній безпеці людини – інформаційної дискримінації, яка проявляється не лише в розподілі людей на тих, які мають доступ до інформації, і тих, які його не мають, а й суттєво впливає на рівень інформаційної культури його членів, яка безпосередньо пов'язана з інформаційною безпекою людини.

Досліджено окремі види інформаційних загроз, зокрема, пов'язані з дискримінацією; інформаційним забрудненням і перенавантаженням; інформаційним насильством, мовою ненависті і кібер-буллінгом; віртуалізацією реальності і аддикціями, що пов'язані з використанням ІТ; порушенням приватності і неправомірним використанням персональних даних тощо.

Акцентовано, що кількість загроз інформаційній безпеці буде зростати і надалі, з огляду на поширення ІТ у всіх сферах життєдіяльності людини і збільшення їх впливу. Тому особливої уваги вимагає дослідження загроз, які існують на початкових етапах соціалізації особистості, оскільки на цьому етапі формується інформаційна культура людини, яка в подальшому дозволить (або не дозволить) ефективно протистояти інформаційним загрозам, викликам та ризикам, а також використовувати можливості, які створює інформаційне суспільство.

На основі аналізу доктринальних праць, генези суспільних відносин щодо інформаційної безпеки людини і правового регулювання в цій сфері, місця інформаційної безпеки людини в системі інформаційної і національної безпеки, а також сучасних загроз, і пропонується під «інформаційною безпекою людини» розуміти «захищеність людини від шкоди або інших небажаних результатів для її гідності та вільного розвитку, які завдаються негативними інформаційними впливами і порушенням її інформаційних прав та свобод, і полягає у гарантуванні можливості задоволення своїх інформаційних потреб і свободи інформації, а також приязного інформаційного середовища».



### РОЗДІЛ 3

## ПРАВОВИЙ СТАТУС І БЕЗПЕКА ЛЮДИНИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

### **3.1. Парадигма правового статусу людини в умовах становлення інформаційного суспільства**

Сучасний людиноцентрський підхід в праві базується на тезі, що «всі люди народжуються вільними і рівними у своїй гідності та правах», яка закріплена першою статтею «Загальної декларації прав людини». І далі серед основних рис людини визначається розум і совість [145, ст.1].

Рада Європи як основні визначає дві цінності – «людське достоїнство і рівність, а вже з них можна вивести багато інших, наприклад: свобода: оскільки людська воля становить важливу частину людської гідності; примушування робити щось всупереч нашому бажанню принижує людську особистість; повага до інших: оскільки відсутність поваги до інших не дозволяє оцінити їх індивідуальність і їх людську гідність; недискримінація: оскільки рівність людей з точки зору людської гідності означає, що ми не можемо судити про людей на підставі фізичних (або інших) ознак, що не мають відношення до людської гідності; толерантність: оскільки нетерпимість вказує на відсутність поваги до відмінностей, а рівність не означає тотожності або однаковості; справедливість: оскільки люди, рівні у своїй приналежності до людського роду, заслуговують справедливого ставлення; відповідальність: оскільки повага прав інших осіб тягне за собою відповідальність за свої дії і надає зусилля для реалізації прав всіх і кожного» [551]. Таким чином, розуміння сутності людини і її ролі суспільстві визначає підходи до практики співіснування людини, суспільства і держави, необхідними складовими якої є право і закон.

Тому вважаємо за необхідне присвятити цей розділ окресленню підходів до розуміння людини як суб'єкта суспільства і об'єкта суспільних відносин, в яких реалізується інформаційна безпека, і які підлягають правовому регулюванню. Можливості і необхідність правового впливу на суспільні відносини знаходяться

в прямій залежності від відповіді на питання: «хто є людина?» і «яка є людина?». А в цілях цього дослідження вважаємо необхідним розуміння людини з огляду такі питання: Чи є інформаційна безпека суттєвою ознакою кожної людини? Чи може вона вважатись правом людини? Як співвідносяться інформаційна безпека людини, суспільства і держави? Яке місце людини в системі інформаційної безпеки – чи є вона виключно об'єктом, чи може виступати суб'єктом? Які цінності людини є основоположними для визначення об'єкту інформаційної безпеки? Чи є потреба в інформаційній безпеці базовою для людини і як вона співвідноситься з іншими потребами людини і суспільства?

Людина є предметом дослідження природничих і суспільних наук, при цьому в залежності від галузі науки для означення людини має місце використання таких термінів як особистість, особа, індивід, індивідуальність. Право використовує при розумінні людини концепції, опрацьовані, в першу чергу, в таких науках як філософія, психологія, соціологія, водночас, окремі норми права передбачають природничий підхід – людина як біологічний організм. При цьому для означення людини в законодавстві використовуються такі категорії як людина, фізична особа, кожен. З врахуванням окремих біологічних характеристик та соціальних ролей визначається правовий статус учасників соціальних відносин.

В філософії можна спостерігати три підходи до розуміння людини 1) дескриптивний, 2) атрибутивний і 3) сутнісний [278]. У першому випадку дослідники зосереджують увагу на морфологічних, фізіологічних, поведінкових та інших ознаках, які відрізняють людину від представників усіх інших видів живих організмів. Цей підхід з особливою суворістю реалізується саме в природничо-науковій («фізичній») антропології. На початкових етапах йшлося про фізіологічні ознаки (від форми черепа до будови кінцівок), поступово розширилось до спроби виділення кластерних ознак, таких, як прямоходіння, великий обсяг і складну будову головного мозку, використання і виготовлення знарядь праці і захисту, розвинена мова, пластичність індивідуальної поведінки та ін. Однак, в умовах становлення інформаційного суспільства, постає ціла низка проблем, що пов'язані з необхідністю регулювання експериментів з людиною, що змушують переглянути підхід і виділяти в якості ознак, що визначають людину, і

такі, як «унікальність у Всесвіті, здатність мислити і здійснювати вільний вибір, виносити моральні судження і тим самим брати відповідальність за свої дії» [282].

Якщо у 20-му столітті питання створення штучного інтелекту і похідні від того суспільнозначимі питання здавались науковою фантастикою, то на сьогодні більшість експертів у цій сфері сходяться на тому, що є три категорії (або типи) штучного інтелекту: штучний інтелект вузького спектру, або ANI (Artificial Narrow Intelligence) — перший рівень штучної свідомості, яка спеціалізується на прийнятті рішень лише в одній сфері: наприклад, може обіграти світового чемпіона із шахів, але може зробити тільки це і нічого більше; загальний штучний інтелект, або AGI (Artificial General Intelligence) – штучний інтелект другого рівня, який досягає та перевершує рівень звичайної людської свідомості: може розв’язувати математичні та логічні завдання, абстрактно мислити, порівнювати та засвоювати складні ідеї, швидко навчатися, в т.ч. – із власного досвіду; штучний суперінтелект, або ASI (Artificial Super Intelligence) – третій рівень розвитку технологій штучного інтелекту, де він є розумнішим, аніж усе людство разом узятє, спочатку трохи, а згодом як результат самонавчання – у трильйони разів [648].

В багатьох сферах життєдіяльності людини запроваджено системи, котрі використовують ANI: від тих, що покладено в основу роботи пошуковиків до інтернету речей. Складні системи вузькопрофільного штучного інтелекту використовують у виробництві, банківській системі, транспорті, освіті. Їх використання актуалізувало цілу низку питань, пов’язаних з інформаційною безпекою та правами людини, зокрема, інтернет речей (internet of things), великі дані (big data) тощо.

З новим резонансом питання актуалізувались у зв’язку з початком в липні 2005 р. Blue Brain Project – проекту з комп’ютерного моделювання неокортексу людини. Над проектом спільно працюють компанія IBM і Швейцарський Федеральний Технічний Інститут Лозанни. Наприкінці 2015 р. розробниками було заявлено про створення першого штучного мозку з 31 тис. нейронів [649].

Майже завжди, коли йдеться про штучний інтелект, одразу згадують про нанотехнології. Н. Бостром, філософ та директор Oxford Future of Humanity

Institute, стверджує, що суперінтелект, озброєний нанотехнологіями, здатен покласти край низці захворювань, бідності, проблемам із екологією, різного роду фізичним страждань – а на додачу ще й подарувати фактичне безсмертя, уповільнюючи чи взагалі спрямовуючи у зворотному напрямку процеси старіння людського організму. Наскільки етичним може бути варіант створення цифрової копії людської свідомості [60].

В середині липня 2017 р. виникла суперечка між І. Маском і М. Цукербергом з приводу того, чи є штучний інтелект (AI) найбільшим ризиком і загрозою для людської цивілізації. М. Цукерберг зазначив, що позиція засновника Tesla і SpaceX є "безвідповідальною" і що сам Маск песиміст, якщо він так оцінює AI. Однак, вже 1 серпня того ж р. керівництво Facebook прийняло рішення відключити систему штучного інтелекту після того, як чат-боти почали спілкуватися власною невідомою мовою. Експерти висловили побоювання, що боти поступово стануть все більш самостійними і зможуть функціонувати поза контролем IT-фахівців. Тим більше, що навіть досвідчені інженери не можуть повністю відслідковувати хід розумового процесу спамерських пошукових роботів [581]. На нашу думку, це обумовлює потребу врегулювання питання встановлення меж використання штучного інтелекту і нейромереж.

Другий, *deskриптивний підхід* до визначення людини, передбачає такі ознаки, як біологічна непристосованість людини, її органів для якогось певного суто тваринного існування; особлива анатомічна будова, надзвичайна пластичність поведінки; здатність виробляти знаряддя праці, добувати вогонь, користуватися мовою. Лише людина володіє традицією, пам'яттю, вищими емоціями, здатністю думати, стверджувати, заперечувати, вважати, планувати, малювати, фантазувати. Тільки людина може знати про свою смертність, любити, брехати, обіцяти, дивуватися, молитися, сумувати, зневажати, бути гордовитим, зазнаватися, плакати і сміятися, володіти гумором, бути іронічним, грати роль, пізнавати, опредметнювати свої задуми і ідеї, відтворювати існуюче і створювати щось нове [278]. Цей підхід є основою соціологічного розуміння людини і часто протиставляється біологічному. Соціологічний підхід до дослідження особистості спирається як на точку відліку не на індивідуальні особливості людини, а на її

соціальне оточення — систему, елементом якої вона є, і соціальні ролі, які виконує в цій системі, при чому залежно від трактування співвідношення біологічного та соціального виокремлюється біологізаторська, суто соціальна (соціологізаторська) та біосоціальна концепції. Проаналізувавши зміст кожної, вважаємо, що саме біосоціальна концепція має бути основоположною в процесі здійснення правових впливів. Хоча і вона не дає чіткої відповіді на запитання, як в людині взаємодіють соціальне та біологічне.

Значимим з точки зору права вбачається взаємозв'язок і типологізація особистостей на основі співвідношення в них біологічного та соціального, а також розрізнення чотирьох типів: (1) соціально і біологічно повноцінного; (2) соціально повноцінного при біологічній неповноцінності; (3) біологічно повноцінного при соціальній неповноцінності; (4) соціально і біологічно неповноцінного [242, с.168].

Така типологізація дозволяє звернути увагу на особливу уразливість окремих категорій осіб в умовах інформаційного суспільства. Так, інтегрованість в сучасному суспільстві значною мірою залежить від можливості використання інформаційних технологій. При цьому, обмежені фізичні можливості (вади зору, слуху, координації) досить часто в українських реаліях стають причиною порушення прав людини у зв'язку з неможливістю повноцінно використовувати інформаційні технології. Такі обмеження стосуються не лише інформаційних прав, а в умовах інформаційного суспільства – політичних, соціальних, трудових та інших прав людини. Окрім того, особливо гострою залишається проблема доступу до інформації осіб із інтелектуальною та психосоціальною формою інвалідності [325].

Водночас, соціологічне розуміння людини дозволяє розмежовувати поняття "людина - індивід - особа - особистість - індивідуальність" як якісні прояви людини.

При *атрибутивному* підході істотним вважається виокремлення головної, визначальної ознаки, що відрізняє людину від тварин. Найбільш відомий і широко прийнятий з таких атрибутів - «розумність», визначення як людини мислячої, розумної (*homo sapiens*). Інше, не менш відоме і популярне атрибутивне

визначення людини - *homo faber* - як істоти, що творить, виробляє. Третє, що заслуговує уваги - розуміння людини як істоти символічної (*homo symbolicus*), що творить символи, найбільш важливим з яких є слово (Е. Кассіпер) [544]. За допомогою слова він може спілкуватися з іншими людьми і тим самим робити значно ефективнішими процеси уявного і практичного освоєння дійсності. Арістотель відзначив також визначення людини як істоти суспільної.

Історія філософської думки значною мірою відображає пошук розуміння природи людини і сенсу її існування в світі. Людина на ранніх щаблях розвитку не відокремлювала себе від решти природи, відчуваючи свій нерозривний зв'язок з усім органічним світом, що знайшло відображення в антропоморфізмі – несвідомому сприйнятті космосу й божества як живих істот, подібних самій людині. Таким чином, у стародавній міфології і філософії людина розглядалась як малий світ - мікрокосмос, а «великий» світ – як макрокосмос.

Зіткнення з чужої культурою змусило стародавніх греків замислитись про природу власних етичних і правових норм. Софісти першими висунули ідею самоцінності людини, поставивши її в центр світу і вбачаючи в ній міру всіх речей. Саме людина виявляється, на думку софістів, творцем соціальних норм і цінностей, які мають договірну природу і не можуть бути прийняті без відповідного обговорення. З іменем Сократа пов'язують розуміння відокремленої від Космосу людини. Античні філософи вбачали унікальність людини в володінні розумом. Людина розглядалась Сократом як моральна істота, а його етичний антропологізм вбачав справжній сенс життя людини полягає у вічному самопізнанні. Пізніше Епікур загострив увагу на проблемі свободи і щастя людини. Він вважав, що кожна людина здатна обирати власну траєкторію буття, тобто життєвий шлях, а також, що сенс людського життя полягає не в служінні суспільству, а в прагненні до задоволень і щастя.

Протилежною є філософська доктрина буддизму, яка стверджує, що життя людини повне страждань, і важливо покласти їм край. Буддійська ідея звільнення людини від страждань так чи інакше поділялася практично всіма філософськими системами Стародавньої Індії, лише теоретичне підґрунтя ідеї викликало

заперечення прихильників ортодоксальних учень. Буддизм декларував рівність людей незалежно від станової та кастової приналежності.

Християнство утвердило погляд на людину, сотворену за образом і подобою Божою, що володіє свободою у виборі добра і зла, – на людину як особистість. Августин Аврелій по праву вважається засновником християнської філософії. Цей богослов і мислитель створив більше десятка важливих творів, у яких обґрунтував своє онтологічне, антропологічне, етичне вчення. У «Сповіді» він дає зрозуміти, що процес самопізнання повинен поєднуватися з процесом Богопізнання. Перевага душі над тілом у Августина полягає в тому, що саме душа, а не тіло, пізнає Бога, а тіло тільки заважає цьому процесу. Звідси він робив висновок, що людині потрібно якнайкраще піклуватися про душу, а тіло обмежувати в чуттєвих насолодах. На це спрямована, як відомо, вся аскетика християнства. Така подвійність і роздільність людської природи не давала спокою мислителю в антропологічних пошуках, і він вигукував: «Що ж за таємниця - людина! Адже ти, Господи, і число волосся на його голові знаєш, так що жоден з них не впаде без відома Твого. І все ж куди простіше порахувати волосинки, ніж пристрасть і душевні коливання»[4].

Томізм — напрям у схоластичній філософії й теології католицизму, для якого характерне прагнення поєднати християнське вчення з акцентованою увагою до прав розуму і здорового глузду. Згідно Томи Аквінського “існуюче” і “благе” є тотожними, а індивід – особистісним поєднанням душі і животворимого нею тіла. Душа людини нематеріальна і самосуца, проте сама по собі не є “повною” людиною, вона реалізується завдяки тілу. Діяльність людського розуму обмежена чуттєвістю. Людина, як і будь-яка реальність, загалом є благом, проте вона знаходиться на такому ступені досконалості, на якому можливий відхід від благості, тому її діяльність пов'язана і з недоліками, злом. Абсолютного зла, за Ф. Аквінським, не існує [468]. Воно виявляється лише як відхід від блага, приміром у природному світі – натуральне псування речей. У діяльності й поведінці людини зло породжується недосконалою волею, яка не підкоряється законам.

Іслам, на відміну від християнства, твердо упевнений в можливості пізнання Істини і Дійсності. У філософській традиції Ісламу, як свідчить історія, на цю

тему майже не велося дебатів, на відміну від західної філософської традиції, де ця можливість постійно оспорується, починаючи з часів грецької філософії і поглядів Платона. Людина наділена душею і органами сприйняття і створена аллахом, щоб отримувати знання. Згідно Аль-аттасу, ільм (знання) - це відвідини маной (сенсом) істоти, що має душу, або досягнення цієї істоти знання. Отже, душа не лише не пасивна, навпаки, вона теж здатна проявляти активність. По волі Аллаха душа може досягти вахи (одкровення) і інтуїції. П'ять відчуттів сприйняття - це вікна розуму, призначені для отримання емпіричного і раціонального знання [413, с. 57].

У ісламському світогляді існує певна ієрархічна структура пізнання. Оскільки природа людини дуальна, існує і дві категорії пізнання, фард айн і фард кифайя. Ці дві категорії відрізняються ступенем упевненості в знанні і способом його отримання. Знання фард айн чітко визначене і обов'язково для кожного мусульманина. Воно включає знання стовпів релігії, основ віри і Шаріату. Отримання знання фард кифайя обов'язкове для існування в суспільстві. Як свідчить світогляд на основі "таухида" (єдинобожності), знання цілісне або інтегроване, його не можна розділити на релігійну і світську сферу. І фард айн, і фард кифайя мають на меті зміцнення віри, перше за допомогою глибокого вивчення слів аллаха в Корані, а друге - за допомогою ретельного, систематичного вивчення життя людини і природи.

Радикально в напрямку пошуку самотності розвертає людство епоха Відродження. У європейській думці виникає ідея гуманізму, прославлення людини як найвищої цінності. Істинний гуманізм проголошує право людини на свободу, щастя, визнає благо людини основою соціального устрою, утверджує принципи рівності, справедливості, людяності у відносинах між людьми і звільняє їх від релігійних пут. Гуманісти Відродження вважали, що можливості людського пізнання безмежні, бо розум людини подібний божественного розуму. Гуманісти Відродження вважали, що в людині важливо не його походження або соціальний стан, а особистісні якості, такі як розум, творча енергія, підприємливість, почуття власної гідності, воля, освіченість. У якості «ідеальної людини» визнавалася сильна, талановита і всебічно розвинена особистість, людина творець самого себе



і своєї долі. Індивідуалізм породив головну рису культури епохи Відродження - антропоцентризм, який проник в усі сторони життя.

XIX століття ввійшло в історію філософії як антропологічне століття. У центрі німецької класичної філософії поставлено проблему свободи людини як духовної істоти. У працях І. Канта народилася ідея створення філософської антропології. Він визначає людину як творця духовного життя, культури, носія загального ідеального початку - духу і розуму. І. Кантом був сформульований категоричний імператив – внутрішній моральнісний регулятор людської поведінки, покликаний узгодити прагнення максимальної свободи людини з необхідністю підкорюватись вимогам колективного життя людей [148].

Гуманізм став передумовою становлення концепції природного права, яке розуміється усвідомлена людиною можливість і необхідність жити, бути вільною, щасливою та вимагати від держави й суспільства сприяння реалізації своїх прав у межах, визначених принципами співжиття соціуму. Свобода, що складає найнеобхіднішу вимогу природного права, полягає в подоланні страху перед персоналізацією життя, виокремленні себе з колективної маси та виробленні навичок довіри до органів державної влади, до суспільних інституцій та ставлення до них як до таких, що покликані забезпечувати і підтримувати прагнення людини до самореалізації[135, с. 15].

На відміну від концепції природного права філософсько-антропологічна концепція Маркса пов'язувала розвиток людини з процесом зростаючого відчуження: людина стає заручником соціальних інститутів, які сама ж і створила. К. Маркс пов'язував розуміння сутності людини з суспільно-історичними умовами його функціонування і розвитку, з її свідомою діяльністю, в ході якої людина опиняється і передумовою, і продуктом історії. На його думку, саме досвід соціальної співпраці формує свідомість людини. Підкреслюючи значення громадських зв'язків і характеристик людини, марксистки не відкидають специфічних якостей особистості, наділеною характером, волею, здібностями, а також враховують складні взаємодії соціальних і біологічних факторів. Індивідуальне та історичний розвиток людини – процес присвоєння і відтворення соціокультурного досвіду людства.

Шопенгауер обґрунтовуючи свою концепцію ірраціоналізму визначав, що в основі всього світу, живого і неживого, також в людині – не розум, а воля, воля до життя. Це космічний порив, стихійний і несвідомий, який є причиною всього існуючого. І в людині розум підпорядкований волі. Ніцше виступаючи з критикою Шопенгауера, стверджував, що жити може і безвольна істота, проте погоджувався, що в основі світу є не розум, а воля, воля до влади. Влада при цьому ним розглядалась не як політична явище, а прагнення бути вище, досконаліше, вийти за межі існуючого. Важливою вбачається концепція Ніцше, що мораль більшості – це мораль слабких. Він вважав, що необхідно провести переоцінку всіх моральних цінностей. Не повинно вважатися цінністю співчуття і слабкість, а лише гордість і свобода.

Фрейдизм і неофрейдизм мали значний вплив на розвиток філософських досліджень людини. Принциповий крок, зроблений Фрейдом в пізнанні людини, полягав у розкритті ролі несвідомого в людському житті. Ніхто до Фрейда з такою глибиною і всебічністю не описав все багатство і різноманітність сфери підсвідомого, ніхто з такою повнотою не виявив величезного впливу цього підсвідомого на все життя людини, суспільства. Під цим кутом зору Фрейд проаналізував сутність культури, багатьох соціальних процесів в суспільстві, соціальних зв'язків людей, механізмів громадського управління.

Філософія XIX століття, як вже згадувалось, є періодом повстання багатьох антропологічних концепцій, які могли бути діаметрально-протилежними: романтизм та ідеалізм німецької філософії, позитивізм у Франції і Англії, матеріалізм Маркса і Фейєрбаха, філософію окремих великих мислителів (Шопенгауер, Ніцше, К'єркегор), неокантіанство, прагматизм і та інші. Проте ще складнішою і суперечливішою стала філософська наука XX століття, яка значною мірою відобразила перетворення суспільного життя у XX ст.: велика кількість соціальних потрясінь, дві світових війни, декілька десятків революцій, суттєві зміни економічних структур та засобів виробництва, руйнування традиційних укладів життя, відчуження від звичного природного середовища, урбанізація культури, і, врешті, поступове перетворення суспільства на комплекс різних об'єднань та угруповань веде до процесу загальної інституціоналізації,

результатом якої є позбавлення людини власного “я”, втрати індивідуальності. Позитивізм і неопозитивізм, феноменологія і екзистенціалізм, прагматизм і ірраціоналізм, техноутопії, постмодернізм і величезна кількість інших культурологічних та історіософських напрямів власними методами і шляхами шукали відповідь на питання про співвідношення філософії і науки, ролі людини в суспільстві.

Виникнувши на початку ХХ ст., у період занепаду традиційних гуманістичних цінностей, як філософська відповідь на пошуки виходу з глобальної духовної і соціальної кризи, що охопила західне суспільство, екзистенціалізм, або “філософія існування”, сформувався як одна з найбільш особистісно орієнтованих філософських течій, претендуючи на роль єдино істинної “філософії людини ХХ століття” [441, с. 48]. Справжня філософія, згідно з К’єркегором, може бути тільки “екзистенційною”, тобто такою, якій притаманний глибоко особистісний характер. Розглядаючи людину як “екзистенцію”, він аналізує її “буттєву, онтологічну структуру” і вводить такі поняття, як “страх”, “відчай”, “рішучість” тощо, що їх згодом розвинули екзистенціалісти. Водночас К’єркегор встановлює три способи існування особистості, або три типи екзистенції (естетичний, етичний і релігійний), з яких релігійний вважає найвищим [ibid., с. 50].

Ж.-П. Сартр висунув тезу, що люди хочуть бути внутрішньою причиною власного буття, інакше кажучи, людина прагне бути Богом. Тому конфронтація з поняттям “ніщо” спричинює загрозу – екзистенційний страх. У Європі це прагнення стимулювало також виникнення нігілізму, тобто ідеологічного визнання марноти, безглуздості життя та відсутності істинного світу під “стежкою” життя. У відповідь ще один відомий французький екзистенціаліст А. Камю присвятився пошукові шляхів, що вивели б людство за межі нігілізму. Сартр, фактично, змушує особистість брати на себе цілковиту відповідальність за наявний стан справ. Адже якщо “Я”, “творючи” своє майбутнє, актуалізує минуле, то “Я” автоматично відповідальне за все, що відбувається у сфері його минулого, інакше кажучи, за весь світ, у якому “Я” себе знаходить. Сартр пише: “...Людина,

засуджена бути вільною, несе на своїх плечах вагу всього світу; вона відповідальна за цей світ і за саму себе як певний спосіб існування” [640, с.529].

Феноменологія пов'язана з ім'ям Е. Гуссерля, який вважає предметом філософії царство чистих істин, апріорних змістів. Пізнання він розглядав як потік свідомості, внутрішньо організований і цілісний, однак відносно незалежний від суб'єкта пізнання і його діяльності. Назва феноменології походить від «феномен» - ідеальна сутність, зміст, які на думку представників цього напрямку філософії знаходять вираження у мові і психологічних переживаннях. Для феноменології характерний гостра критика позитивізму, усвідомлення духовної кризи сучасності.

Духовна складова стала визначальною у персоналізмі (від лат. *persona* – особистість) – теїстичному напрямі сучасної філософії, який визнає особистість первинною творчою реальністю і вищою духовною цінністю, а увесь світ проявом творчої активності верховної особистості – Бога<sup>5</sup>. Особистість розглядається як основний прояв буття, у якому воляова активність, діяльність поєднується з безперервністю існування, а особистість має джерелом єдиний початок – в Бозі. Е. Муньє вважає християнське вчення про особистість основою революційного перевороту в житті людства, який дозволяє створити "суспільство особистостей", подібне до християнської громади. Оскільки особистість, відповідно до персоналізму, перебуває у ворожих відносинах з дійсністю, життя особистості починається з того, що вона ламає контакт із середовищем; вона вимушена піти в себе, "зосередитися". Внутрішні властивості особистості: "покликання", інтимність, повинні охоронити особистість і суспільство, як від тоталітаризму, так і від індивідуалізму, об'єднати особистостей між собою. Головним способом самоствердження особистості виступає внутрішнє самовдосконалення. Власне, персоналістичну концепцію можна вважати прекурсором права на приватність.

У XX ст. виразним став дуалізм культури - з одного боку, криза духовності, яка насамперед, з засиллям масової псевдокультури, відчуженням і індивідуалізмом, витісненням духовних цінностей на периферію людської

---

<sup>5</sup> Представники: Н. Бердяев, Л. Шестов, Б. Боун, У. Хокинг, Е. Брайтмен, Р. Флюеллінг, П. Ландсберг, М. Недонсель, П. Рікер, Е. Муньє, Ж. Лакруа.

свідомості, стерео типізацією мислення; з іншого – прагнення духовного, що призвело не лише до збереження основних культурних форм, розвитку нових, а й до так званого «релігійного повернення» [138].

Папа Іоанн Павло II в одній зі своїх енциклік (послань) окреслив шлях відновлення сучасної релігійної філософії як відхід від абстрактних вчень про людину і звертання до вивчення «цілісної динаміки життя і цивілізації». Людині треба показати вічні цінності і цінності, які знову з'явилися, допомогти їх правильно зрозуміти і синтезувати. Такий підхід до задач філософії зробив релігійно-філософські доктрини популярними в ХХ в. Під визначення релігійної філософії більшістю підпадали філософські школи, які пов'язані були тим чи іншим чином з християнством та європейською культурою.

Не зважаючи на те, що на початку ХХ століття інтелектуали говорили про секуляризацію, то вже в середині – пророчили релігії зникнення з публічної арени, з буттям винятково в людських душах. Це і стало найбільш вживаною дефініцією секуляризації, під якою розуміють процес втрати релігією впливу на політику, культуру, міжнародні відносини. У 1968 р. автор цієї дефініції, соціолог релігії П. Бергер писав у газеті „Нью-Йорк Таймс”, що на початку ХХІ століття релігійних осіб вірогідно вдасться віднайти лише в маленьких сектах, які тулитимуться одна до одної у спротиві секулярній культурі. Але вже у 1996 р. він був вимушений публічно спростувати власний прогноз „Сучасний світ, за кількома винятками, є так само нестямно релігійним, яким він був завжди, причому у деяких місцях – ще більш релігійним, ніж колись”[138].

Антропологічний напрямок у філософії ХХ століття, прикладами якого є екзистенціалізм, феноменологія і персоналізм, не слід вважати тотожним філософській антропології як розділу філософії. Він ставить значний акцент на протиставленні сцієнтистському напрямку в філософії і культурі 20 століття.

Власне, сцієнтизм або саєнтизм як ідейна позиція, що представляє наукове знання найвищою культурною цінністю і основоположним чинником взаємодії людини зі світом [509], такий світогляд, позитивно оцінює соціальні наслідки НТР, передбачає головним завданням філософії - обслуговування бурхливого розвитку науки. Ця ідея суттєво перекликається з концепцією суспільства знань

як наступним етапом інформаційного суспільства, в якому визначальним ресурсом стане знання, а отже саме з ним має бути пов'язана інформаційна безпека людини.

Неопозитивізм став історично третім етапом позитивістської філософії. Перший, класичний позитивізм, бере свій початок від французького філософа О. Конта, який поставив перед собою завдання перебороти абстрактність і спекулятивність філософії Гегеля на користь науки і осмислення її досягнень. Знання він вважав науковим настільки, наскільки воно відповідає критеріям найбільш розвинутої форми наукового знання – ідеалам і критеріям природничих наук. І насамперед це критерій, що перевіряється у досвіді, шляхом зведення до експериментальних даних чи чуттєвих сприйнять. Саме таке знання О. Конт вважав позитивним, гідним розгляду (звідси і термін – «позитивізм»).

Основні ідеї неопозитивізму стосувались протиставлення філософії і науки, в напрямку утвердження можливості отримання істинного тільки в точних науках. Представники неопозитивізму не було однотайними в підходах, але спільним для них було і є твердження, що: філософія не є справжньою наукою, вона тільки логічний аналіз наукової мови; в основі наукового знання є досвід людини; науковими знаннями можуть бути тільки ті знання, які можливо верифікувати емпірично; істинними можуть бути також і ті знання, які можливо логічно довести.

З огляду на предмет дослідження, хочемо звернути увагу на бачення проблеми мови в філософії неопозитивізму. Мова визначалась як система знаків, яка служить засобом людського мислення і спілкування, і розмежовано природну мову і штучні формалізовані мови. Вітгенштейн висунув і обґрунтував логіко-мовну модель відображення світу, стверджуючи, що ціла хмара філософії концентрується в краплі граматики. А постпозитивізм приходить до необхідності вивчення історико-культурного середовища, в якому існує і розвивається дана мова. Таким чином, неопозитивізм у своїй еволюції прийшов до традиційних світоглядних філософських проблем, від яких на початку відмовився [14, с. 148].

Неопозитивізм, свідомо обмеживши коло філософських проблем, сконцентрувавши всю увагу на методології науки, став передтечею концепцій інформаційного суспільства.

У XX ст. сформувався світоглядний плюралізм, викликаний кризою класичних цінностей і пошуком нових світоглядних засад. Усе це й зумовило сучасне багатство філософських концепцій. Спільною особливістю всіх філософських течій XX ст. є так званий «антропологічний поворот» у філософії, суть якого полягала в переході від захоплення людським розумом, що був властивий попереднім епохам, до критики філософії розуму, яку Шопенгауер сформулював як «бунт проти розуму», тобто критичне ставлення до раціоналізму. На думку О. Шпенглера, криза виявляється як перехід культури в цивілізацію, що призводить до виродження, «обездушення» культури [519]. Криза культури осмислюється дослідниками і в дискурсі протиставлення культури природі, яке також має корені в європейській філософській традиції. В таких міркуваннях штучність культури, як створеної людиною, розглядається як причина відірваності її та, відповідно, людини від природи та ворожого до неї ставлення.

На сьогодні значної критики зазнала теорія ноосфери М. Вернадського, яку він у 1923 р. виклав у Сорбонні, як еволюційно-проективне розуміння про перетворення людини в могутню геологічну силу, здатну переділити у своїх інтересах біосферу Землі, виокремлюючи два етапи формування ноосфери: стихійний і свідомий. Вагоме значення має етична спрямованість вчення про ноосферу, а саме принципи єдності людини і природи; зростання наукової думки; інтернаціоналізації науки як духовної єдності людства; критичності; моральної відповідальності вчених; творчості; соціальності науки [73]. В.І.Вернадський виділяв декілька основних передумов становлення ноосфери: 1) єдність людства на всій Земній кулі - «немає жодного клептика Землі, де б людина не могла прожити, якщо б це було їй потрібно»; 2) перетворення засобів зв'язку та обміну - ноосфера як єдине організоване ціле, всі частини якого на самих різних рівнях гармонійно пов'язані і діють узгоджено, за допомогою швидкого, надійного, всебічного обміну інформацією; 3) відкриття нових джерел енергії; 4) покращення

добробуту працюючих; 5) рівність усіх людей; 6) виключення війн з життя суспільства [73].

Вчення про ноосферу В. Вернадського стало провісником формування нової картини світу, що спрямована перш за все на знання як істину у пізнанні, а не підкорення законів природи (екологічного імперативу), перегляд усієї сукупності традиційних світоглядних уявлень про місце і роль людини у природі і суспільстві, виявленні нових цінностей, пріоритетів і норм буття суспільства [2, с.64].

Однак, друга світова війна, апартеїди, расизм, націоналізм, біполярний світ свідчать про кризу ідеалів європейської культури. Освічена, цивілізована людина ХХ ст. виявилася неспроможною забезпечити ані собі, ані людству справедливість, щастя та мир. Постало питання, чому світ, організований на основі науки, техніки, технологій обернувся проти людини та їй загрожує? [421]

Історія людства в ХХ ст. засвідчила, що науковий та технологічний розвиток не забезпечую апріорі культурне та економічне зростання для всього людства. Навпаки, бурхливий розвиток науки, техніки та технологій здатний створити ілюзію всемогутності людини і - як наслідок – призвести до бездумної вседозволеності.

Дослідивши праці фахівців різних галузей науки, що вивчали концептуальні питання становлення інформаційного суспільства, зокрема Ю. Ханші, Д. Белла, Д. Лайона, М. Маклюєна, Ф. Уїлльямса, А. Даффа, Ф. Вебстера, Р. Абдеева, М. Вершиніна, Л. Землянової, І. Мелюхіна, А. Ракітова, В. Щербини, Г. Почепцова, В. Брижко, А. Кумарасвами, А. Пенті, В. Іноземцева, К. Маркаряна, М. Макарової; М. Кастельса, Д. Барні, Д. Тапскота, З. Бжезинського, С. Джоунса, К. Боулдінга, М. Згуровського, І.Арістової та інших, вважаємо найбільш значимим для становлення інформаційного суспільства як нової історичної фази розвитку людської цивілізації наступні концепції: інформаційного суспільства (яка і стала титульною); постіндустріалізму; мережевого суспільства; суспільства знань.

Появу титульної концепції інформаційного суспільства зазвичай пов'язують з іменами японських вчених Ю. Хаяші та Й. Масуди. Введення самого терміну «інформаційне суспільство» приписується Ю. Хаяші, професору Токійського



технологічного інституту в 60-х рр. XX століття. Й. Масуда, в свою чергу, був учасником розробки практично всіх програм "японської" моделі інформаційного суспільства, зокрема таких, як "Японське інформаційне суспільство: теми і підходи" (1969 р.), "Контури політики сприяння інформатизації японського суспільства" (1969 р.), "План інформаційного суспільства" (1971 р.), "План створення інформаційного суспільства – національна мета до 2000 р." (1972 р.), а його праці "Комп'ютопія" (1966 р.), "Інформаційне суспільство як постіндустріальне суспільство" (1981 р.) та "Гіпотези щодо генезису "Гомо інтелідженс" (1985 р.) стали антологією інформаційного суспільства.

Праці Й. Масуди певною мірою були утопічними, оскільки він описував мрію про «суспільство, в якому буде процвітати людське інтелектуальна творчість, а не матеріальне споживання, проте мали й практичну цінність. Так, в "Комп'ютопії" він вперше обґрунтував та узагальнив основні характеристики інформаційного суспільства, серед яких: глобалізм, вихід людства на космічний рівень свідомості; світовий симбіоз людства і природи; перехід до існування людства у глобальному інформаційному просторі. Окрім того, вчений сформулював принципи концепції "глобальної комп'ютопії", зокрема: прагнення і реалізація цінності часу; свобода ухвалення рішень і рівність сприятливих можливостей для всіх; розквіт різноманітних вільних спільнот; синергетична взаємодія в суспільстві; функціональні об'єднання, вільні від надмірного контролю влади; відродження теологічного синергізму людства і Бога.

Поняття "інформаційне суспільство" набуло всесвітнього визнання після публікації книги І. Масуди "The Information Society as Post-industrial Society" [623], де він сформулював основи майбутнього суспільства: основою нового суспільства буде комп'ютерна технологія, яка покликана заміщати або посилювати розумову працю людини; інформаційна революція перетвориться в нову продуктивну силу суспільства; в новому суспільстві стане можливим масове виробництво когнітивної, систематизованої інформації, технології і знання; точкою насичення ринку стане «межа пізнаного»; зросте можливість співпраці, спільного вирішення проблем; провідною галуззю економіки стане інтелектуальне (наукомістке) виробництво; в інформаційному суспільстві

основним суб'єктом соціальної активності стане «вільне співтовариство»; основною метою в новому суспільстві буде реалізація «цінності часу».

Як вже зазначалось, специфікою японської концепції було те, що вона не була суто теоретичною ідеєю, а була сформульована в аналітичних звітах, поданих до японського уряду декількома організаціями: Агентством економічного планування, Інститутом розробки використання комп'ютерів, Радою зі структури промисловості, і була обрана як перспективний напрямок розвитку держави. Передбачалось, що інформаційне суспільство, в якому процес комп'ютеризації дасть людям доступ до надійних джерел інформації, позбавить їх від рутинної роботи, забезпечить високий рівень автоматизації виробництва. При цьому зміниться і саме виробництво : продукт його стане більш «інформаційно містким», що означає збільшення частки інновацій, дизайну і маркетингу в його вартості; «...виробництво інформаційного продукту, а не продукту матеріального, буде рушійною силою освіти і розвитку суспільства»[623]. В сам же зміст категорії «інформаційне суспільство», насамперед, вкладались примат інформаційних цінностей над матеріальними; економічна цінність капіталу, втіленого у знаннях (Knowledge capital) вища, ніж капіталу, втіленого у матеріальній формі.

Масуда висунув концепцію, згідно з якою інформаційне суспільство буде безкласовим і безконфліктним. Він писав, що на відміну від індустріального суспільства, характерною цінністю якого є споживання товарів, інформаційне суспільство висуває як характерну цінність час. У зв'язку з цим зростає цінність культурного дозвілля. Він навіть приходить до висновку про трансформацію сутності особистості і появу нового типу людей: на зміну «Homo sapiens» приходить «Homo intelligens», так як саме інтелектуальна діяльність стає для людини основним типом діяльності «Homo intelligens» будуватимуть нову цивілізацію, котра суттєво відрізнятиметься від цивілізації «Homo sapiens» - глобальна спільнота громадян, котрі сформують поліцентроване, комбіноване суспільство, схоже на живий організм, з розгалуженою мережею безпосереднього зв'язку, спроможного швидко і динамічно реагувати на зміну зовнішнього середовища[622].

Особливу цінність становлять думки Й. Масуди щодо потенційних небезпек нового типу суспільства. Він передбачав, що людство постало перед вибором між діаметрально протилежними моделями майбутнього: між "Комп'ютопією", тобто справді демократичним, правовим інформаційним суспільством, та "автоматизованою державою". Тобто він передбачав небезпеку «контрольованого суспільства» внаслідок того, що на початках комп'ютери використовувалися, в першу чергу, військовими та іншими урядовими структурами, зокрема – службами безпеки, внутрішніх справ тощо.

Серед головних соціальних загроз він називав футурошоки у зв'язку з швидкими соціальними трансформаціями, дії терористів, а також зазіхання на індивідуальну самотність та кризи підконтрольності [621].

Проблему футурошоку (шок майбутнього) підіймає також в своїй однойменній праці американський письменник, соціолог і футуролог Е. Тоффлер, розуміючи під ними руйнівний стрес і дезорієнтацію, що викликані надто інтенсивними і значними змінами за короткий проміжок часу [656]. Інша праця Е.Тоффлера «Третя хвиля» стала передумовою до концепції постіндустріального суспільства Данієля Бела, найбільш відомого американського теоретика цієї концепції. Тоффлер висунув ідею про три хвилі розвитку суспільства: перша хвиля — аграрне суспільство, друга хвиля — індустріальне суспільство, третя хвиля — постіндустріальне суспільство. Тоффлер зазначав, що " нова цивілізація несе з собою нові сімейні стосунки, інші способи праці, любові та життя, нову економіку, нові політичні конфлікти, і, понад все, це – змінену свідомість"[657].

В 70-ті роки відбувається конвергенція двох майже одночасно створених концепцій: інформаційного суспільства і постіндустріалізму. Концепція професора соціології Гарвардського університету Д. Белла була сформульована у його роботі "Прихід постіндустріального суспільства"(1967), де було виокремлено низку такі риси постіндустріального суспільства, як перехід від індустріального суспільства до сервісного (обслуговуючого) суспільства; визначальне значення теоретичного знання для здійснення технологічних інновацій; «інтелектуальна технологія» у якості основного інструменту при прийнятті рішень.

Особливої уваги заслуговує його бачення розвитку інфраструктури: «Кожне суспільство внутрішньо пов'язане різними каналами, що дозволяє його членам здійснювати матеріальний і духовний обмін. Організація, фінансування, підтримка і керування цими каналами, або інфраструктурою, звичайно знаходилися в компетенції уряду. Першою інфраструктурою був транспорт, другою - засоби передачі енергії, третьою - комунікації; все це зіграло роль каналів колосального інформаційного вибуху, свого роду бомбардування сенсорного апарату людини, розширення соціальної та психологічної взаємодії людей, яка зараз зростає експоненціально» [40, с. 335].

Бел вже тоді передбачив, що на новому етапі розвитку суспільства ускладниться соціальна структура. Проте, більше про цю рису нового типу суспільства пише М. Кастельс, засновник концепції мережевого суспільства. Мережеве суспільство (англ. Network society) — суспільство, яке ґрунтується на горизонтальних соціальних зв'язках і головну роль в якому відіграють не ієрархічні моделі, а соціальні мережі. Значну роль в формуванні такого суспільства відіграють сучасні комунікації, особливо мережевого типу на зразок інтернету.

У своїх роботах М. Кастельс не використовує поняття «інформаційне суспільство», на його думку, всі суспільства використовували інформацію і тому були інформаційними. У трилогії «Інформаційна епоха: Економіка, суспільство і культура» М. Кастельс здійснює аналіз сучасних тенденцій, що приводять до формування основ суспільства, яке він називає «мережевим». Виходячи з постулату, що інформація за своєю природою є таким ресурсом, який легше за інших долає усілякі перешкоди і межі, він називає інформаційну еру епохою глобалізації, де мережеві структури стають водночас, і засобом і результатом глобалізації суспільства. «Саме мережі складають нову соціальну морфологію наших суспільств, а розповсюдження "мережевої" логіки значною мірою позначається на ході і результаті процесів, пов'язаних з виробництвом, повсякденним життям, культурою і владою» [546, с.213]. Таким чином, влада структури виявляється сильнішою за структуру влади. Приналежність до тієї або

іншої мережі, разом з динамікою розвитку одних мереж стосовно інших, виступає, за М. Кастельсом, як найважливіше джерело влади.

М. Кастельс досліджує дві суперечливих тенденції - яким чином глобалізація підсилює інтеграцію людей, економічних і соціальних процесів; та як пов'язані з глобалізацією процеси фрагментації і дезінтеграції. Важливо, що в умовах глобалізації ринків і капіталів змінюється роль національної держави, яка поступово втрачає реальні важелі управління. Інститути і організації громадянського суспільства, котрі будувалися навколо демократичної держави і соціального договору між працею і капіталом поступово втрачають своє значення в реальному житті людей.

Основною суперечністю (і відповідно рушійною силою розвитку) нового суспільства, що формується, заснованого на мережевих структурах, є суперечність між глобалізацією світу й ідентичністю (самобутністю) конкретного співтовариства. М. Кастельс, спираючись на концепцію французького соціолога А. Турена, вводить поняття «Ідентичність опору» і «ідентичність, спрямована в майбутнє» [545, с.16]. Цей опір спрямований проти основної тенденції розвитку сучасного суспільства – глобалізації.

М. Кастельс припускає можливість переходу окремих соціальних груп від ідентичності опору до ідентичності, спрямованої в майбутнє, і тим посприяти перетворенню суспільства загалом із одночасним збереженням цінностей опору інтересам глобальних потоків капіталу й інформації. Поширення логіки мережевих спільнот змінює способи виробництва продуктів, досвіду, культури, влади. На думку Кастельса, мережі стали базовими осередками сучасного суспільства. Кастельс надає великого значення співтовариствам і стверджує, що реальну владу мають саме вони, а не «глобалізовані міста». Простір потоків відіграє центральну роль в розумінні мережевого суспільства за Кастельсом. Це мережі комунікацій з певними центрами, в яких спільноти перетинаються. Еліти в містах не прив'язані до певної місцевості, але прив'язані до простору потоків.

В умовах становлення інформаційного суспільства інтернет виконує функцію інтеграції людства через витіснення безпосереднього людського спілкування штучними формами соціальної комунікації, що призводить до зміни повсякденної

соціальної взаємодії індивідів і соціальних груп, опосередковане спілкування між якими здійснюється за допомогою мережі. Проте інтернет не є єдиною мережею. Мережі в концепції мережевого суспільства розглядаються в широкому значенні – комерційні, освітні, розвідувальна, релігійна, політичні, терористичні тощо.

Мережеве суспільство нівелює колишні форми стратифікації, але творить нові. На думку М. Кастельса, замість капіталізму, керованого правлячим класом, повстає капіталізм без класу капіталістів. У суспільстві основну роль починає відігравати працівники інформаційної сфери. В той же час, робочий клас знецінюється і з'являється маса «працівників загального типу». Інформаційний працівник не прив'язаний до конкретного робочого місця. Поступово зменшується значення традиційних умов праці - нормований робочий день, обладнане робоче місце, чітко окреслені посадові обов'язки, посадова ієрархія. Відбувається певна індивідуалізація праці. Кастельс вважає ядром трансформації сучасного світу технології обробки інформації і комунікації.

Істотних перетворень зазнають політичні процеси. Лідерство стає все більш персоніфікованим, а шлях до влади значною мірою залежить від створення іміджу – політичні діячі активно використовують засоби масової інформації для цієї мети. «Залежність від мови засобів масової інформації, що мають під собою електронну основу приводить до далекосяжних наслідків для характеристик, організації та цілей політичних процесів, політичних діячів і політичних інститутів. В решті-решт, влада, яку мають у своєму розпорядженні мережі засобів масової інформації, займає друге місце після влади потоків, втіленої в структурі та мові цих мереж»[190, с.27]

При цьому, акценти, встановлені Кастельсом, та його розуміння явищ з економічної площини можуть бути екстрапольовані в соціальну. Наприклад, брендінг як символ загальновизнаної здатності додавати товарам і послугам ціннісні якості, зараз працює не лише в економічній, а й у інших сферах. Брендами стають особи, медіа, програми і проекти, історичні місця та пам'ятки, унікальні природні об'єкти та навіть країни. А сам брендінг, не залежно від сфери розвитку, економічна, політична або соціальна, стає не лише соціально-культурним, культурно-історичним, а й політико-правовим явищем.

Наступне, на що звертав увагу Кастельс, інтерактивність. Мережа, реалізована з використанням інтернет-технологій, дозволяє вилучити вертикальні канали зв'язку і забезпечити полівекторний обмін інформацією і спільне ухвалення рішень. Результатом є поліпшення якості інформаційного обміну і досягнення взаєморозуміння між партнерами в процесі їхньої ділової співпраці. Цей принцип на сьогодні є передумовою ефективного функціонування системи державної влади, а також її взаємодії з органами місцевого самоврядування та інститутами громадянського суспільства. Адже демократизація передбачає якісну інформаційну взаємодію і спільне ухвалення рішень в інтересах всього суспільства.

Інтерактивність нерозривно пов'язана з орієнтацією на споживача. Сучасні потреби ринку складно задовольнити через стандартизоване масове виробництво. Завдання знайти оптимальне співвідношення між масовим виробництвом і виробництвом, орієнтованим на споживача розв'язується в багатьох системах через інтерактивну взаємодію, що персоналізується, із замовником в режимі онлайн. Цей підхід Кастельса органічно екстраполюється на політико-правову сферу. Нормотворчість та правозастосування вимагає не лише публічних обговорень на етапі підготовки проектів нормативних актів, а й оцінки ефективності правового регулювання за умови участі інститутів громадянського суспільства, бізнес структур і інших зацікавлених мереж.

Кастельс називає основні проблеми, що, на його думку, перешкоджають розвитку мережевого суспільства у вступі до «Галактика Інтернет» [189]:

1. Управління інтернетом, тобто свобода як така. Інтернет, як мережа мереж поступово стає комунікаційною основою мережевого суспільства, проте є небезпека, що ця інфраструктура може опинитися в чийсь власності, а доступ до мережі може стати об'єктом контролю.

2. Наявність значної кількості виключених з мережі. Така сегрегація відбувається різними шляхами і з різних причин: через відсутність технічної інфраструктури; внаслідок економічних або інституційних перешкод щодо доступу до мереж; недостатність освітніх і культурних можливостей для

використання потенціалу інтернету; недоліків у виробництві мережевого контенту.

3. Проблеми з розвитком здібностей до обробки інформації і генерації відповідних знань. Під цим М. Кастельс має на увазі освіту як фундаментальне явище, тобто набуття інтелектуальної здібності до навчання впродовж усього життя, пошуку і переробці інформації, її використанню для виробництва знань.

4. Проблеми, пов'язані з трансформацією трудових стосунків. Поява мережевого підприємства та індивідуалізація схем зайнятості приводить до зміни механізмів соціального захисту, на яких ґрунтувалися виробничі стосунки індустріального світу.

5. Недостатній темп і гнучкість процедур інституційного регулювання в новій економіці. Йдеться про втрату значимості національних урядів та міжнародних інститутів як регуляторів в умовах глобальних мереж.

6. Небезпека підвищення інтенсивності експлуатації природних ресурсів і посилення деградації навколишнього середовища.

7. Ймовірність втрати людиною контролю над створеними нею технологічними пристроями, особливо в генній інженерії, нанотехнологіях, конвергенція яких може призвести до несподіваних відкриттів, використання яких пов'язане з високою соціальною і етичною відповідальністю. [189]

Ці проблеми порушують велику кількість питань, про які пише М. Кастельс. Хто має взятись за розв'язання цих проблем? «Як ми можемо довірити життя наших дітей владі, контрольованій партіями, які зазвичай діють в умовах системної корупції ... будучи повністю залежними від «політики іміджу», ... відособленою бюрократією, ... що не мають уявлення про реальне життя своїх громадян, що управляє? Проте з іншого боку, чи є їм альтернатива?»[189].

Набуло поширення розуміння, що в основі концепції мережевого суспільства лежить уявлення про інформацію як знання, що породжує конструктивні зміни системи. Знання не підлягають економічному відчуженню й водночас створюють новий тип соціальної нерівності, бо застосування знань потребує відповідного інтелектуального рівня. Характерною тенденцією сучасного виробництва є збільшення питомої ваги висококваліфікованих спеціалістів. Капітал починає



визначатися продуктивністю праці, що залежить від культурно-освітнього рівня працівника. Якщо розглядати капітал як суму предметів споживання, потрібну для відтворення простої робочої сили, то самозростання вартості має обмежений характер. У разі, коли капіталом є знання як стратегічний продуктивний ресурс, що неможливо відчужити, зростання такого капіталу має теоретично необмежений характер. Власне таке розуміння знань і лежить в основі концепції суспільства знань.

Ідею щодо майбутнього суспільства знань ще в XVII ст. висунув Ф. Бекон, а заклав підвалини самої концепції суспільства знань та сформулював її основні положення видатний український мислитель В.І. Вернадський в своїй ще до кінця не оціненій світовим науковим співтовариством концепції ноосфери.

Ф. Махлуп, шукаючи відповідь на питання: «Як нація продукує знання?» написав на цю тему близько 10 праць, найбільш відомою з яких стала «Продукування і поширення знань у США», видана у США в 1962 р. Проте, конкретизував сутність концепції теорії "суспільства знань" П. Друкер американський вчений австрійського походження, був письменником, консультантом в галузі менеджменту, та, як він сам себе називав — «соціальним екологом». У 1966 р. увів у науковий обіг термін "суспільство знань" (knowledge society), що визначає тип економіки, в якій знання відіграють вирішальну роль, а їх виробництво стає джерелом розвитку.

Друкер один із перших у постіндустріальній парадигмі переорієнтував увагу з відносин «людина — техніка» на новий зміст трудових відносин «людина — знання». Новий тип суспільства він називає суспільством знань, оскільки центральним ресурсом розвитку стають знання, або суспільством організацій, адже переважна більшість високоосвіченого населення в такому суспільстві працює за наймом.

Серед основних ідей П. Друкера заслуговують на увагу в цьому дослідженні:

1) Децентралізація та спрощення[568]. Хоча Друкер говорив в основному, про економічний вимір - компанії найкраще працюють, коли вони децентралізовані – проте сьогодення свідчить, що децентралізація є необхідною умовою існування демократичного суспільства.

2) У книзі 1959 р. "Орієнтири майбутнього"[567] він ввів поняття "працівник знань", яке характеризувало роботу, засновану на знаннях і набуває все більшого значення в бізнесі по всьому світу, а також обумовлює необхідність вчитись протягом всього життя.

3) Важливість некомерційного сектора[571] , яку він називає третьою галуззю (приватний сектор і сектор уряду є першими двома). Неурядові організації відіграють вирішальну роль у економіках країн світу.

4) Повага до працівника. Друкер вважав, що працівники є активами, не зобов'язаннями. Він навчав, що обізнані працівники є основними складовими сучасної економіки, і що гібридна модель управління є єдиним способом демонстрації вартості працівника для організації. Центральною у цій філософії є думка про те, що люди є найціннішим ресурсом організації та що робота менеджера полягає в тому, щоб підготувати людей до виконання і дати їм свободу зробити це [569, с.19]

5) Віра у те, що він назвав "хворобою уряду". Друкер стверджував, що недержавні претензії про те, що уряд часто не може або не бажає надавати нові послуги, які люди потребують та / або хочуть [634, с.38].

6) Переконавання, що дії без мислення є причиною кожної невдачі.

7) Потреба в спільноті. На початку своєї кар'єри Друкер прогнозував "кінець економічної людини" і виступав за створення "спільноти рослин"[570, с.205], де можна було б задовольнити соціальні потреби людини. Пізніше він визнав, що така спільнота ніколи не реалізувалася, і у 1980-х роках запропонував, що волонтерство в некомерційному секторі може стати ключем до здорового суспільства, де люди знайшли відчуття приналежності та громадянської гідності [568, с.12].

М. Згуровський відзначає, що суспільство знань та інформації несе людству нові виклики і величезні можливості для розв'язання його головних проблем, а також забезпечення подальшого розвитку [151, с.144]. Але воно вимагає активної участі всього світового співтовариства в осмисленні та втіленні в життя нової парадигми.

Беляков К., Ланде Д. і Ніконова В. відзначають існування «певних етапів інформатизації: електронізація, комп'ютеризація, медіатизація і, нарешті, інтелектуалізація – процес розвитку здатності суспільства до породження і сприйняття знань, тобто підвищення інтелектуального потенціалу, включаючи використання засобів штучного інтелекту. Таким чином, основною ціллю соціальної інформатизації є побудова інтелектуального суспільства – суспільства, побудованого на знаннях» [48, с.14]. Досліджуючи методологічні проблеми правового регулювання становлення суспільства знань, І. Арістова зазначає, що обґрунтованою є наукова позиція щодо існування декількох етапів розбудови інформаційного суспільства. Якщо виходити із того, що перший етап розвитку інформаційного суспільства переважно ґрунтується на досягненнях інформаційних технологій та технологій зв'язку, то наступний етап його розбудови повинний допускати більш широкі соціальні, етичні та політичні параметри — це нове суспільство знань. На її думку, в основі суспільства знання лежить можливість знаходити, виробляти, обробляти, перетворювати, поширювати та використовувати інформацію з метою отримання й застосування необхідних для людського розвитку знань. Це суспільство спирається на концепцію суспільства, яке сприяє розширенню прав і можливостей, що включає в себе поняття чисельності, інтеграції, солідарності та участі [16, с.5]. У своїх роботах І. Арістова робить висновок, що саме суспільство знань є вищою формою існування інформаційного суспільства.

Підсумовуючи, слід відзначити, що в процесі становлення інформаційного суспільства є неминучими певні виклики і загрози самому соціуму і окремим індивідам. Швидке зростання інформаційної складової всіх сфер життєдіяльності людини ставить питання про те, наскільки воно відповідає тенденціям у соціальній та соціопсихологічній сферах. Руйнуються або видозмінюються усталені соціальні структури, повстають нові, що викликає вже згаданий шок майбутнього. І наостанок, все це відбувається в глобальному масштабі.

За таких умов, людина має розглядатись не лише як об'єкт інформаційної безпеки, але й як суб'єкт. Суспільство є складною соціальною системою, елементом якої є людина. Внаслідок залучення людини до багатьох соціальних

систем, вона стає об'єктом системоформуючого впливу, а отже не тільки елементом соціальної системи, а системою, що має складну структуру. При цьому ця структура буде відрізнятися в залежності від наукового підходу. Однак спільним для більшості соціальних наук є використання поряд з категорією «людина» таких понять як індивід, особа, особистість, індивідуальність.

При цьому, людина використовується як широке поняття для визначення переважно біосоціальної сутності, яка означає конкретного представника біологічного виду "*Homo sapiens*", що володіє мовою і свідомістю.

«Індивід» означає конкретну людину, одиничного представника людського роду. Як індивід людина відрізняється від інших не тільки морфологічними особливостями, такими як зріст, конституція тіла, колір очей, тип нервової системи, але і психологічними рисами, такими як здібності, темперамент, характер [439].

«Особа» є суб'єктом і об'єктом соціальних відносин, в праві під особою розуміється « людина, яка має історично зумовлений ступінь розвитку, користується правами, що надаються суспільством, та виконує обов'язки, які ним покладаються» [124, с.65].

Соціальний характер категорії «особа» визначається її розумністю, свободою, індивідуальністю і відповідальністю.

У процесі діяльності людина налагоджує відносини з іншими людьми (суспільні відносини), які формують особистість. Кожна особистість із певного моменту починає робити значимий внесок у життя окремих людей і суспільства. Тому поряд із поняттями особистість, особистісне, виявляється і поняття "суспільно значиме" (те, яке має значення для суспільства), яке може бути як суспільно-прийнятним, так і суспільно-неприйнятним. Таким чином, "особистість" — це стійка система соціально значимих властивостей, ознак і рис, яких набуває індивід у певному суспільстві під впливом інститутів соціалізації, відповідної культури, конкретних соціальних спільнот і груп, до яких він належить і в життєдіяльність яких він залучений. Відповідно поняття "особистість" застосовується стосовно кожної людини, яка пройшла соціалізацію,

оскільки вона індивідуально виражає головні риси певного суспільства, тієї чи іншої соціальної спільноти або групи [439].

Особистість як соціальна якість людини є предметом соціальних наук: філософії, соціології, психології та ін.

"Індивідуальність" свідчить про неповторність, оригінальність, одиничність ознак і їх вияв у конкретної людини. Індивідуальність - це те особливе, специфічне, яке відрізняє одну людину від інших людей, охоплюючи як природні, так і соціальні, як тілесні (соматичні), так і психічні, як вроджені, так і набуті, вироблені в процесі індивідуального розвитку (онтогенезу) властивості. Психолог Б.Г. Ананьев зазначав, що людиною народжуються, особистістю - стають, а індивідуальність завойовують [13, с.38]. Індивідуальність - це поняття для означення винятковості людського індивіда і як біологічного, і як соціального. В ньому фіксується неповторність фізіологічних і психічних рис індивіда, особливість його соціальних якостей.

Одним з основних напрямків соціології є дослідження особистості. Проте розуміння значення цієї категорії є необхідним і визначальним для усіх суспільних наук, адже: 1) саме особистість є одним з головних суб'єктів суспільних відносин; 2) функціонування суспільства неможливе без урахування потреб та інтересів особистості; 3) особистість являє собою індикатор громадського розвитку.

Аналізуючи існуючі соціологічні підходи, в основу системного визначення особистості покладено такі принципи: 1) особистість виступає одночасно суб'єктом і об'єктом як соціальних, так і біологічних відносин; 2) особистість володіє певною свободою вибору своєї поведінки, що обумовлюється розбіжністю соціальних і біологічних умов; 3) особистість, будучи біосоціальним явищем, об'єднує в собі як риси біологічного роду людини, так і соціальної спільноти, в якій вона існує; 4) поведінка особистості залежить від її неповторних особистісних характеристик, через які заломлюється громадський і особистий життєвий досвід [106, с.46].

Вивчення та аналіз особистості як складного соціального явища передбачає виділення її структури, елементами якої є: біологічне, психологічне і соціальне.

Біологічний рівень включає в себе природні, загальні за походженням якості людини (будова тіла, статеві особливості, темперамент і тощо). Психологічний рівень особистості об'єднує її психологічні особливості (почуття, воля, пам'ять, мислення). Психологічні особливості значною мірою обумовлені спадковістю, але також визначаються і середовищем. Третій, соціальний рівень особистості умовно поділяють на три підрівні: власне-соціологічний, специфічно-культурний, та моральний.

Власне цей рівень відіграє визначальну роль у виборі соціальної поведінки особистості як суб'єкта суспільних відносин. Така поведінка де термінується потребами і інтересами.

Потреби - це ті форми взаємодії зі світом (матеріальні і духовні), необхідність яких обумовлена особливостями відтворення і розвитку його біологічної, психологічної, соціальної визначеності і які усвідомлюються, відчуються людиною в будь-якій формі. Потреби розглядають також і як глибинні, неусвідомлені настанови людини щодо самозбереження та самозабезпечення власної цілісності: біологічної та соціальної. Потреби тварин мають більш-менш стабільний характер і обмежені біологічними необхідностями. Потреби людини складніші, постійно розвиваються протягом життя. Людське суспільство через виробництво і сферу послуг створює щоразу нові й нові предмети потреб, які викликають у людей нові й нові потреби [106, с.48].

Зважаючи, що інтереси - це усвідомлені потреби особистості, вони (разом з потребами) особистості лежать в основі її ціннісного ставлення до навколишнього світу, в основі системи її цінностей і ціннісних орієнтацій.

Людина існує не автономно, не сама по собі, завжди є членом тієї чи іншої спільноти, а в ширшому розумінні – певного історичного етапу суспільства. Власне інформаційне суспільство як суспільство споживання обумовлює появу нових потреб та інтересів людини, що призводять до змін у структурі особистості і соціальних функцій, які виконує така особистість.

Як об'єкт соціальних відносин особистість володіє істотними рисами конкретного суспільства, формується під впливом соціальних відносин зовнішнього середовища і творить власне особливе ставлення до зовнішнього

світу. Водночас, соціальні відносини осмислені особистістю, проявляються в її діяльності як особисте ставлення до об'єктивної дійсності. Таким чином, суб'єкт соціальних відносин орієнтований на власні потреби, інтереси, соціальні установки і цінності. Таким чином, соціальні відносини інтегруються особистістю як певна система зв'язків в процесі взаємодії в умовах певного соціального середовища.

В процесі соціалізації особистість виступає об'єктом соціальних відносин, коли силами соціальної дійсності відбувається соціальна і рольова ідентифікації. Як суб'єкт соціальних відносин особистість характеризується самоусвідомленням, нормативною свідомістю і системою ціннісних орієнтацій, а також потребами, соціальними установками і мотивами, що обумовлюють поведінку людини.

Правова соціалізація є невід'ємною складовою загальної соціалізації особистості, зміст якої полягає в засвоєнні особистістю правових цінностей, перетворенні їх у норми власного життя і поведінки [522, с.52]. Менш формалізоване визначення В. Головченко і О. Потьомкіна, які розглядають правову соціалізацію як «... процес, завдяки якому люди вчаться думати і вести себе відповідно до засвоєння та активного відтворення соціально-правового досвіду, набутого в умовах спілкування з іншими людьми і суспільством в цілому, а також різних видів суспільно-правової дійсності» [91, с.100]. Правова соціалізація людини детермінується багатьма чинниками різних рівнів: макрорівня - рівень всього суспільства, мезорівня - рівень великих соціальних груп та мікрорівня - рівень малих соціальних груп. Останнім часом, у зв'язку з процесом глобалізації сучасного світу та переходом до інформаційного етапу розвитку людської цивілізації, все більше впливають на формування правосвідомості чинники мегарівня (міжнародного життя): демократизація сучасного світу, міжнародне право, міжнародні конфлікти, кризи тощо[195].

Вплив інформаційного суспільства на формування особистості є актуальною темою різноманітних наукових досліджень. Відбувається помітна уніфікація масової свідомості, оскільки люди «споживають» одні й ті ж інформаційні продукти глобального характеру (новини, реклама, художні твори і т.д.), йде масова пропаганда способу життя, притаманного цивілізації технологічно

розвинених країн. Особливо значним є вплив механізму «глобалізації масової свідомості» на дітей та молодь. Втрачається національна ідентичність, відбувається деградація мови, нівелюються морально-етичні принципи, що не може не впливати на правову свідомість. Поширення масової культури, неминучість зіткнення з віртуальною реальністю, в якій важко розрізнити ілюзію і дійсність, створюють не лише психологічні і культурні проблеми, але й правові. Створюючи свій образ у віртуальному просторі, людина втрачає адекватне сприйняття реального світу, в тому числі правової дійсності [158, с.64]. Штучно «розмивається» межа правомірної і протиправної поведінки за рахунок інформаційно-психологічного впливу на індивідуальну і суспільну свідомість. Наприклад, факт крадіжки продуктів харчування в супермаркеті і крадіжка інформаційного продукту в мережі не сприймаються однозначно, хоча обидва за змістом є правопорушенням. І це досить «невинний» приклад. Окремої уваги заслуговує «забруднення» інформаційного середовища і проблема «інформаційного шуму». Це питання досліджувалось нами раніше [171], лише зазначимо, що за допомогою «шуму» навколо певних подій, що мають правове і соціальне значення в державі і суспільстві формується негативне ставлення до державних органів, зокрема силових структур, а як наслідок поширення правового нігілізму як масового явища.

Ігнорування особливостей соціалізації особистості, зокрема, формування правової культури в інформаційному суспільстві призводить не лише до послаблення цілеспрямованого впливу на суспільне життя, розбалансування соціальних взаємозв'язків, а й руйнує основи життєдіяльності людини. У міру наростання обсягу інформації стає важче орієнтуватися в її змісті, убезпечувати себе від неякісної інформації, а також від її надлишку. Для людини має значення і якість, і кількість інформації, що потрапляє в її інформаційне середовище. За умови інформаційного перевантаження порушується структура інформаційного середовища людини. Людина не отримує необхідної інформації для оцінки ситуацій, у яких вона діє, тому що вона не встигає переробити всю інформацію та виділити те, що корисно для її адаптування до нових ситуацій. Це призводить до виникнення небезпек. Важлива інформація, від якої залежить безпека



життєдіяльності людини, не потрапляє в зону її уваги та не переробляється, виникає інформаційна криза. Це, по суті, інформаційний голод при інформаційній надмірності. Така ситуація виникає внаслідок відсутності знань про закони та закономірності функціонування інформаційного середовища. Система цінностей та оцінок формує так званий «інформаційний щит», який захищає інформаційне середовище людини від шкідливої і небажаної інформації. Небезпеки виникають насамперед тоді, коли людина не має надійного «інформаційного щита».

Таким чином, людина (в першу чергу діти і молодь) отримує уявлення про правову дійсність на основі інформації, що є в її інформаційному середовищі. Кількість, якість і можливості доступу до такої інформації, а також здатність її критично сприймати («інформаційний щит») значною мірою визначають можливості правової соціалізації особистості. Підтримуємо думку професора Арістової І.В.: «хоча інформація є дійсно інструментом знання, але сама по собі вона не є знанням. Інформація, яка виникла із бажання обмінюватися знаннями та зробила більш ефективною їх передачу, залишається лише формою знання, точною й стабілізованою, індексованою за часом та користувачем. Інформація, навіть якщо вона може бути “покрощена”, не обов’язково має правильне усвідомлення.» [16, с.8].

Окрім того, слід звернути увагу, що в сучасних умовах соціалізація, і освіта як її складова, повинні бути безперервними процесами. Тому актуальним є питання не лише надання можливості доступу до правової інформації, а й створення умов для безперервної освіти з метою формування системи цінностей, що відповідає вимогам безпеки особистості і держави в умовах становлення інформаційного суспільства.

Суспільне буття та історія людства творяться є результатом діяльності конкретних індивідів. При цьому спосіб залучення людини в суспільно-історичний процес обумовлена культурою в широкому розумінні, тобто не тільки суб'єктивними прагненнями і свободою вибору, але й об'єктивними умовами матеріального виробництва, рівнем суспільного розвитку, в тому числі - рівнем свідомості. Отже, те, що має назву «соціальної детермінації», є фактором залежності людей від продуктів та результатів їх, власної діяльності [451, с.54]. Із

сукупної діяльності індивідів розвиваються нові об'єктивні історичні обставини, які, у свою чергу, визначають наступний розвиток людей. Тим самим, не існує закономірних тенденцій історії без діяльності людей. Люди знаходяться в залежності від об'єктивних умов і обставин життя, але разом із тим створюють і змінюють ці обставини.

В умовах нової цивілізації основними факторами людської само детермінації стають не стільки соціально-економічні і технологічні чинники, скільки особистісні - свідомості, вільного вибору, соціально-культурних пріоритетів. Також зазнає змін система культурних цінностей, зростає розуміння цілісності і єдності людства, багатоваріантності і різноманітності культурного розвитку. Розвиваються нові типи соціальних зв'язків людей. Суб'єкти, тобто індивіди та соціальні спільноти, на основі власних інтересів та потреб визначають зміст суспільних відносин у всіх сферах суспільного життя та діяльності - матеріально-економічній (виробничі, технологічні тощо); соціально-політичні (політичні, правові, національні тощо); духовно-культурні (моральні, релігійні, художньо-естетичні, наукові відносини). Хоча такий розподіл певною мірою є умовний, адже всі сфери життєдіяльності є щільно поєднані і взаємообумовлені. Звернемо увагу на окремі аспекти змін в соціальному бутті людини у зв'язку зі становленням інформаційного суспільства.

В інформаційному суспільстві геопростір не зникає, однак суттєво змінюється суспільно-географічне бачення людини. У нових умовах активність людини на протязі певного проміжку часу означає, що вона просторово "розпливається". Завдяки динамічному розвитку світової економіки, комунікаційних систем і міжнародного туризму розвиток контактів між жителями різних регіонів здійснюється швидкими темпами, що сприяє появі нового й універсального міжнародного способу життя.

Новий рівень соціальних відносин призводить особистість до усвідомлення існування нової віртуальної реальності, в якій істотно розширюються рамки її зіткнення зі світом. Багато видів діяльності, важливих для існування, знаходять зовсім нову форму, і слідом за цим, процеси задоволення потреб особистості можуть бути так само перенесені у віртуальну реальність. Внаслідок цього вже в

цій вторинній реальності з'являються і нові потреби, які також вимагають задоволення.

Внаслідок віддаленості, знеособленості або анонімності комунікаційних процесів у віртуальному середовищі змінюється уявлення не тільки про структуру комунікаційного процесу, але і про характеристики суб'єктів комунікації. "Багатоманітність варіантів кожного аспекту життя робить вибір перманентним станом сучасного індивіда. У глобальній цивілізації ніщо не є наперед визначеним, і все підлягає обов'язковому вибору: місце проживання і громадянство, форма сім'ї і характер занять, предмети споживання і духовні цінності. Без вибору дається лише сама ситуація вибору"[41, с.409]. Виникає ситуація множинності життєвих стилів у межах подолання суперечностей між збереженням цілісності та різноманітністю. Таким чином, ідентичність твориться як необхідність впорядковувати різноманітність. Постає проблема якісної характеристики альтернатив, які обумовлюють або можуть обумовити вибір. Критерії та запити вибору походять саме з індивідуальної ідентичності. Показовим моментом у контексті проблеми самоідентичності та вибору, який не можна оминати, є категорія, про яку свого часу говорили С. К'єркегор, представники німецького романтизму, екзистенціалізму, а сьогодні на цьому акцентують увагу багато сучасних філософів, а саме - тип людини-філістера (обивателя, споживача). Основні ознаки такої свідомості - замкненість у собі, боязкість і небажання відповідальності за власні рішення, страх вибору, фрагментарність, корисливість, превалювання емпіричного чинника у житті, закритість до нового досвіду, нівелювання моральних цінностей. "З міщанина-обивателя з його традиційними чеснотами, культивованими поколіннями з часів середньовічних городян, як то гостинність, милосердя, толерантність, працелюбство, поміркованість, - які на сучасному етапі спрощуються й нівелюються, - міщанин перетворюється на "людину масової культури", обивателя, який пасивно "споживає"... товари, культуру, життя" [402, с.125]. З. Бауман подає цю проблему через життєві стратегії сучасності, як "бродяга", "турист", "гравець", кожен з яких прагне до новизни переживань, задоволень відразу і по максимуму, уникаючи завершеної самоідентифікації. "Пережити

враження, про існування яких ти й не підозрював, - це надзвичайне задоволення, а гарний споживач - завжди шукач пригод і любитель утіх... споживачі - це передусім колекціонери відчуттів" [32, с. 68]. У сучасну епоху глобальних змін людина опинилась у ситуації кризи ідентичності, яка проявляється у різноманітних формах (апатія, депресія, відхід від реальності і втеча у віртуальний світ, нігілістичні тенденції, різні форми залежностей та девіантні форми поведінки (наприклад, алкоголізм, наркоманія, статеві збочення). Дослідження у цій сфері Є. Сапожнікова виводять розлади психіки (найперше, депресію) зі споживацьких пріоритетів суспільства [408, с.55]. Механізм споживацтва виглядає так: людина має широкий спектр набору потенційних можливостей, які можна розвинути. Процес їх актуалізації супроводжується задоволенням, проте вимагає постійного відновлення зусиль, а тому часто не реалізується. Це, своєю чергою, призводить до психічних розладів, дискомфорту, незадоволення і відчуженості. Психічне незадоволення можна заглушити сильнішими подразниками нервових рецепторів, або підмінити зовнішніми атрибутами успіху, надаючи речам культового значення. Сучасна людина обирає засоби, що їй пропонуються, - туристичні подорожі, екстремальний відпочинок, азартні і комп'ютерні ігри, алкоголь, наркотики тощо. "Використання вищевказаних способів боротьби з психічною невдоволеністю (яка вкорінена у нереалізованості духовних можливостей) є основою споживацтва" [408, с.55]. Така поведінка уподібнена до різних видів залежностей: наркотичної, алкогольної, азартної. Психічна втома, пригніченість, депресії властиві населенню розвинених країн західного світу, тоді як представники мусульманського, африканського чи китайського світу не мають подібних проблем, хоча об'єктивно рівень їх матеріального добробуту набагато нижчий і причин для психічного незадоволення більше. З цього видається послідовним висновок, що джерелами окреслених негативних явищ сучасного світу є соціокультурні процеси. Всупереч синергетичним прогнозам про посилення значення свідомого вибору соціальних суб'єктів, насправді ми живемо "у світі, де відбуваються неконтрольовані та невпорядковані зміни" [190, с.27]. До чинників, які впливають на вибір та структуру ідентичності сьогодні, можна зарахувати: стан духовного зубожіння,

який породжує некритичність щодо себе, свого досвіду, максимальна увага до матеріальних речей, прагматизм та гіпердинамізм, пошуки психологічного комфорту через незахищеність перед екстремальними змінами фактично в усіх сферах.

Герасимова І., досліджуючи когнітивні аспекти глобальної культурної кризи сучасності, виділяє такі моменти: розмивання "свідомого шару" мислення, пов'язаного з обдумуванням та компетентним прийняттям рішень, чому посприяв культ безпосереднього сприйняття та переживання нав'язаних ЗМІ зразків та стереотипів; культ емоцій нижчої агресивно-біологічної природи; замість оптимального для сучасного культурного рівня розвитку конвенційного рівня спілкування усі більше опускаються до примітивного рівня, коли у співбесідникові бачиться об'єкт для маніпуляцій, самоутвердження, використання; серед раціонально-орієнтованих індивідів утворюється прірва нерозуміння через егоцентризм, нездатність до кооперативного мислення, терпимості; замість породження нових форм логічного синтезу переважає інтелектуальний ізоляціонізм та фрагментарна множинність вторинних, часто відособлених символічних реальностей; еволюційно-об'єктивні процеси індивідуалізації мислення і творчості проходять у формах крайнього індивідуалізму з агресивним нав'язуванням своєї картини світу [83, с. 172].

Перехід від прискореного технологічного розвитку до передових технологій у світовій економіці вимагає нової якості трудових ресурсів і їхньої здатності до інновацій. На ринку найбільше цінується нове. Тому великі корпорації створюють гнучкі децентралізовані організаційні структури, змінюють ієрархічні системи управління мережевими, намагаються привчити працівників відповідати цілям фірми. На зміну принципів жорсткої дисципліни приходить поступове підвищення кваліфікації персоналу, збільшення його самостійності, креативності, передання більшої відповідальності на нижчі рівні. Відносини між суб'єктами будуються на основі комунікативних зв'язків. В управлінні кадрами має місце перехід від цінностей «трудової етики» до цінностей самореалізації.

Бурхливий розвиток цивілізаційної діяльності призвів до експлуатації природи людиною і сьогодні ця проблема стає однією з найфундаментальніших.

Характерною особливістю переходу до інформаційного суспільства є реорганізація відносин у всіх напрямках діяльності суспільства: здоров'я, комерція, освіта, державне управління, дозвілля та багато іншого. Змінюється світосприйняття людей, розуміння ними тих можливостей, які відкриває для них входження в інформаційну добу та поступове створення або перетворення громадянина на е-громадянина – людину, що ефективно використовує можливості інформаційного суспільства. Людина інформаційної доби на якісно іншому рівні веде діалог з державним апаратом.

Рада Європи визначає е-демократію як використання ІКТ урядами, політичними партіями, громадянами та іншими учасниками політичних процесів на місцях, в регіонах, на національному або міжнародному рівнях з метою розширення участі громадян в процесах прийняття державних рішень [131]. Тобто, під терміном «електронна демократія» розуміється така політична система, в якій ІКТ використовуються для забезпечення виконання основних функцій демократичного процесу, зокрема: вільного доступу до суспільно важливої інформації, свободи слова, участі в публічному управлінні (як шляхом вільного обговорення, так й участі у виборах, референдумах тощо).

Електронний уряд будь-якої країни спрямований на вирішення трьох взаємопов'язаних ключових питань: забезпечення громадян та бізнесу ефективними засобами отримання різноманітних е-сервісів; забезпечення держапарату ефективними засобами прийняття управлінських рішень та надання адміністративних послуг; організації електронної взаємодії влади, громадян та бізнесу.

Роль особи, безсумнівно, зростає, і, на перший погляд, здається що людина сьогодні володіє значною кількістю прав і свобод для участі в управлінні державою. Проте її реальні можливості обмежені багатьма чинниками – зокрема, постійно зростаючими можливостями інформаційних впливів, зокрема, технологіями маніпуляції свідомістю, які активно використовуються в політичній боротьбі.

У сучасному світі, коли проблема прав людини вийшла далеко за межі окремої держави, а обсяг прав і свобод людини в сучасному суспільстві

визначається не лише особливостями певного співтовариства людей – національної держави, а й розвитком людської цивілізації в цілому. Виявляється правовий аспект становлення нового соціокультурного простору інформаційного суспільства і ролі людини в ньому як через появу нового покоління прав людини – інформаційних, так і в насиченні інформаційним виміром традиційних прав або прав і свобод трьох перших поколінь – особистих, політичних, економічних, соціальних, екологічних тощо.

Хоча і концепція прав людини, і концепція інформаційного суспільства починали з рівня наукових гіпотез, які від моменту свого зародження і до сьогодні зазнають змістовної критики, все ж шляхом міжнародно-правової легалізації вони виведені на рівень політико-правової дійсності. А їх симбіоз породив феномен інформаційних прав людини. Іноді здається, що інформаційних прав до винайдення комп'ютерів і інтернету не було. Проте, один із засновників постмодернізму Ж. Бодрійяр дав наступну оцінку інформаційного вибуху, який стався в 60-70-ті роки минулого століття: «інформації стає все більше і більше, а сенсу – все менше і менше»[665, с.22].

Правовий статус людини залежить від сутності соціального ладу, в умовах якого він складається і функціонує [428, с. 223], тому становлення інформаційного суспільства обумовлює необхідність юридичного закріплення і державного гарантування правового статусу людини на новому якісному рівні.

Ще у 1946 р. Генеральна Асамблея Організації Об'єднаних Націй ухвалила одну зі своїх найперших резолюцій, де зазначено таке: *«Свобода інформації є фундаментальним правом людини і ... критерієм для всіх свобод, яким присвячено Організацію Об'єднаних Націй»* [410, с.8]. Тому актуальність питання інформаційної безпеки людини визначається, насамперед, в контексті концепції природного права. При цьому природне право людини постає як усвідомлена нею можливість і необхідність жити, бути вільною, щасливою та вимагати від держави й суспільства сприяння реалізації своїх прав у межах, визначених принципами співжиття соціуму.

Вперше на міжнародному рівні про право на інформацію було задекларовано в ст. 19 Загальної декларації прав людини, що в принципі відтворено і в ст. 34

Конституції України. Так, Загальна Декларація прав людини визначила свободу шукати, одержувати і поширювати інформацію та ідеї (ст. 19) складовою права кожної людини на свободу переконань і на вільне їх виявлення. Аналогічне закріплення право на інформацію одержало також в інших міжнародно-правових документах. Серед них — Європейська Конвенція про захист прав людини і основних свобод (п. 1 ст. 10), Міжнародний Пакт про громадянські і політичні права 1966 р. (п. 2 ст. 19) та інші. На основі цього можна зробити висновок, що права на свободу інформації, свободу думки і слова належать до так званих прав «першого покоління» - громадянських і політичних права, які від початку вважалися і вважаються невід'ємною частиною людської особистості[209, с.94]. Хоча окремі науковців зазначають, що права і свободи людини в сфері інформаційних відносин можна віднести до третього покоління [507, с.48].

Оскільки, процесу розвитку ідеї прав людини властиві як кількісні, так і якісні зміни, то, безперечно, варто погодитись з думкою, що розширює колективні права людини (третє покоління) піднесення та поглиблення права на інформаційний простір світу, на надання різноманітних послуг, що ґрунтуються на інтелектуальних інформаційних технологіях (зокрема на новітніх технологіях досліджень) і технологіях зв'язку (глобальна мережа), забезпечення інформаційних відносин усередині країни і за кордоном. Третє покоління прав людини - колективні права народів (націй), тобто права всього людства, що ґрунтуються на солідарності людей, їх належності до якоїсь спільності (асоціації). Це право на мир, безпеку, незалежність (самовизначення народів), на здорове навколишнє природне середовище, на соціальний і економічний розвиток як людини, так і людства в цілому [435, с.64]. В сучасному глобалізованому світі інформаційні права людини неможливо розглядати відокремлено від суспільства і держави. Слід враховувати, що інформаційний вплив, який здійснюється на суспільство та державу, опосередковано діє на кожну людину. Особистість людини є передумовою й продуктом існування суспільства, держави. Сучасна людина постійно перебуває під впливом інформації, що поширюється в просторі цілеспрямовано або довільно. До розвитку сучасних кібернетичних систем під простором поширення інформації розуміли атмосферу, стратосферу, космос,



водні акваторії океанів і морів. Зараз розуміння інформаційного простору включає додатково кібернетичні та віртуальні системи [141].

Визначення інформаційно-правового статусу особи в суспільстві і державі вимагає закріплення достатнього обсягу інформаційних прав людини. В сучасній науковій думці відсутній однозначний підхід до визначення інформаційних прав людини.

Тихомиров О.О. відзначає, відсутність однозначної відповіді на питання щодо співвідношення права на інформацію та інформаційних прав, але виокремлює дві наявні наукові позиції [462, с.105].

Згідно першої – «інформаційні права» ширше за змістом поняття і об'єднує як право на інформацію в сучасному нормативному його розумінні (право збирати, зберігати, використовувати і поширювати інформацію), так і право на свободу думки і слова, право на вільне вираження своїх поглядів і переконань тощо. Тобто інформаційні права і право на інформацію співвідносяться як ціле і часткове [185; 240]

Другій позиції характерне певне змістовне ототожнення права на інформацію та інформаційних прав, що ґрунтується на сучасному сприйнятті права на інформацію не як певним чином відокремленого особистого немайнового права фізичної особи, а крізь призму науки інформаційного права, як універсального конституційного права на інформацію, що містить у собі комплекс можливостей, які в сукупності і становлять так звані інформаційні права суб'єктів [252, с.56].

Водночас, сам науковець вважає недоцільною критику наведених підходів, або ж вибір одного з них за єдину наукову основу не має особливого сенсу, оскільки вони відображають різні етапи еволюції прав в інформаційній сфері: перший – усвідомлення права на інформацію як певного особистого блага і наявну сьогодні його нормативно-правову концепцію, а другий – перспективи становлення комплексного правового інституту «права на інформацію», що охоплюватиме всі інформаційні права, зокрема й цивільні, пов'язані з інформацією [462, с. 106].

Вже згадувана російська теоретик інформаційного права Бачило І. зазначає, що для визначення статусу людини в галузі права на інформацію необхідно

встановити його точну юридичну характеристику, яка передбачає, принаймні, три складових: а) формально-правову, пов'язану з визнанням права в формі його позитивного юридичного оформлення в законі окремої держави і міжнародного співтовариства; б) сутнісну, пов'язану з нормативно закріпленим змістом даного права, що реалізується через певні повноваження і кореспондуючі йому правові обов'язки; в) процесуальну, яка регулює порядок реалізації права [34, с.189].

Марущак А.І. основою інформаційних прав людини визначає право на інформацію, яке включає право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. При цьому основою права на інформацію вважає право людини на доступ (отримання) до інформації, свободу вираження поглядів і переконань, свободу обміну інформацією включає до обсягу поняття “право на інформацію” [251, с.25]. При цьому визначає суб'єктивне право на інформацію як гарантовану державою можливість фізичних, юридичних осіб і держави (державних органів) вільно одержувати, використовувати, поширювати та зберігати відомості, необхідні їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій, що не порушує права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб [252, с.56].

Костецька Т. А. зазначає, що з огляду на те, що до основних структурних елементів права на інформацію Основний Закон включає низку правоможливостей: право збирати, право зберігати, право використовувати та право поширювати інформацію усно, письмово або в інший спосіб – на свій вибір, які, у свою чергу, структуруються в інші численні інформаційні права, можна вважати, що назване право є комплексним [212, с.115].

П. Сухорольський у спеціальному дослідженні підкреслює, що, наприклад, в англomовних джерелах виділяються так звані цифрові права і свободи людини (digital rights and freedoms), під якими розуміють сукупність загальновизнаних та інших прав людини у контексті поширення нових цифрових технологій, зокрема інтернету. Такий підхід дав підстави автору під інформаційними правами людини розуміти певний перелік основних прав людини в різних сферах, на які значною

мірою впливає розвиток інформаційно-комунікаційних технологій в інформаційному суспільстві [449, с.21].

Є.В. Петров пропонує два підходи до трактування права на інформацію, що сформовані у правовій науці та в законодавстві: «у рамках вузького підходу право на інформацію трактується тільки як право на одержання (доступ) до інформації, тобто як відносне право. Широкий підхід же припускає віднесення до права на інформацію усіх видів суб'єктивних прав, спрямованих на інформацію чи на здійснення дій з нею» [309, с. 251].

Професор Арістова І.В. зазначає, що право на інформацію — самостійне конституційне право, що дозволяє людині вільно шукати, одержувати, передавати, створювати і поширювати інформацію будь-яким законним засобом. У літературі висловлюються точки зору, у яких право громадян на інформацію — лише складова частина свободи слова і преси, або, навпаки, свобода інформації — умовне позначення цілої групи свобод і прав: свободи слова або свободи вираження думок; свободи преси та інших ЗМІ; права на одержання інформації, що має суспільне значення; свободи поширення інформації. Вважається, що право на інформацію не охоплюється цілком свободою слова і преси. Воно значно багатіше, змістовніше і має власну субстанцію, грає свою роль у задоволенні певних інтересів суб'єктів; тому зрізаність даного найважливішого права необґрунтовано. На її думку, навряд чи виправданий і такий, надмірно широкий, підхід до змісту права на інформацію. Аргументом на користь таких висловлень є, безумовно, законодавча практика найвищого рівня — конституційна. Йдеться, наприклад, про ст. 34 Конституції України, де закріплені не тільки свобода думки, слова, але і право на інформацію. У Конституції України зовсім не випадково закріплені свобода думки і слова та право на інформацію в різних частинах, хоча й однієї статті. Тобто тим самим підкреслюється як їхній взаємозв'язок і взаємопроникнення, так і відома автономність, самостійність, "суверенність".

Арістова І.В. зазначає, що право на інформацію — дуже не просте суб'єктивне право, бо воно складається з ряду юридичних можливостей [15, с.82]. Важливою складовою є право на безперешкодне ознайомлення з нормативними актами. Передбачена ч. 3 ст. 57 Конституції України: "Закони та інші нормативно-

правові акти, що визначають права й обов'язки громадян, не доведені до відома населення в порядку, встановленому законом, є нечинними". Універсальне право громадянина на інформацію поєднує конкретні правомочності: право знати про створення і функціонування інформаційних систем, що будь-яким чином торкаються сфери особистого життя громадянина або інформації про нього, а також інформації про інші сфери життєдіяльності громадянина; право давати згоду на збирання особистої інформації для соціально-економічних, культурних та інших соціальних цілей; право доступу до такої інформації з метою її перевірки, одержання необхідних довідок; право знати про використання цієї інформації у відповідних цілях і відповідними користувачами систем; право на громадський код (позначення громадянина у відповідній інформаційній системі); право на достовірну інформацію про стан навколишнього середовища; право на достовірну фінансову інформацію й ряд інших прав [15, с.85].

На думку, Марущака А.І., інформаційні права людини – це гарантовані державою можливості людини задовольняти її потреби в отриманні, використанні, поширенні, охороні і захисті необхідного для життєдіяльності обсягу інформації [251, с.21]. Тоді як, універсальне конституційне право на інформацію містить у собі певні конкретні можливості, які в сукупності і становлять інформаційні права суб'єктів інформаційних відносин, якими виступає не лише людина, а й юридичні особи, держава тощо. Зокрема, це такі правомочності як, право кожного вільно збирати, одержувати, зберігати, використовувати і поширювати будь-яку (масову, офіційну, правову, статистичну, науково-технічну інформацію, інформацію як результат творчості та інше) інформацію, за винятком обмежень, встановлених Конституцією України, чинним законодавством; право особи давати згоду на збирання, зберігання, використання та поширення інформації про неї для соціально-економічних, культурних та інших соціальних цілей; право громадянина мати доступ до відомостей про себе (крім тих, що становлять захищену законом таємницю) в органах державної влади, органах місцевого самоврядування, установах і організаціях, право кожного перевіряти достовірність інформації про себе і членів своєї сім'ї, право спростовувати недостовірні відомості у судовому порядку; право вимагати

вилучення будь-якої інформації про себе; право кожного на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням недостовірної інформації про себе і членів своєї сім'ї; право на забезпечення таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції; право на вільний доступ і поширення інформації про стан навколишнього середовища (екологічна інформація), про якість харчових продуктів і предметів побуту; право на правову інформацію — право знати свої права і обов'язки, право на вільний доступ до нормативно-правових актів, що їх визначають; право на офіційну фінансову інформацію; право на інформацію як результат творчості та інші [252, с. 83].

Вказаний перелік інформаційних прав доповнюється правовими можливостями, встановленими чинним законодавством. Серед них: право власності на інформацію; право на заснування друкованих засобів масової інформації, на одержання через них масової інформації; право на заснування телерадіоорганізацій, на заснування інформаційних агентств; право на науково-технічну інформацію; право на захист від поширення відомостей, що не відповідають дійсності, право на їх спростування; право одержувати інформацію про діяльність органів державної влади, місцевого самоврядування, об'єднання громадян та деякі інші [252, с. 89].

Крім загального визначення права людини на інформацію в ст. 34 Конституції, інформаційна свобода є необхідною умовою реалізації багатьох (якщо не всіх) конституційних прав і свобод людини

Погоджуючись концептуально з означеною позицією, вважаємо що інформаційні права є, по суті, змістовними складовими інших конституційних прав і свобод. Зокрема, права: право давати згоду на збирання, зберігання, використання та поширення конфіденційної інформації про неї; право кожного громадянина на доступ до відомостей про себе (крім тих, що становлять захищену законом таємницю) в органах державної влади, органах місцевого самоврядування, установах і організаціях; право кожного перевіряти достовірність інформації про себе і членів своєї сім'ї; право спростовувати недостовірні відомості в судовому порядку; право вимагати вилучення будь-якої

інформації про себе; право кожного на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням недостовірної інформації про себе і членів своєї сім'ї ; право на забезпечення таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції; право на вільний доступ і поширення інформації про стан навколишнього середовища (право на екологічну інформацію), про якість харчових продуктів і предметів побуту (ст.ст. 31, 32, 50) та інші.

Основний Закон України, що значно розширив перелік інформаційних прав, свобод людини і громадянина, таким чином, забезпечив стійкість, перспективність розвитку не тільки відповідних інститутів, а й найбільш динамічних національних суспільних відносин нового типу – інформаційних [212, с.116]. Конституція України закріплює основний зміст прав і свобод в інформаційній сфері, але їх конкретизація відображається в ряді інших нормативно-правових актах, а саме таких як: Закон УРСР "Про мови в Українській РСР", Закон України "Про науково-технічну інформацію", Закон України "Про інформаційні агентства" , Закон України "Про Концепцію Національної програми інформатизації", Закон України "Про захист інформації в автоматизованих системах", Указ Президента "Про додаткові заходи щодо безперешкодної діяльності ЗМІ, дальшого утвердження свободи слова в Україні", Указ Президента "Про вдосконалення державного управління інформаційною сферою", Розпорядження Президента "Про додаткові заходи поліпшення інформаційної діяльності" тощо. Велике значення мають Рішення Конституційного Суду України.<sup>6</sup> Для упорядкування багатьох інформаційних відносин, що існують поки ще стихійно, для визначення оптимальної системи обмежень права людини на інформацію потрібною є розробка і прийняття Інформаційного кодексу України.

---

<sup>6</sup> Наприклад, у справі про офіційне тлумачення положення частини першої статті 7 Цивільного кодексу Української РСР (справа про поширення відомостей) від 10 квітня 2003 р., Рішення КСУ у справі щодо офіційного тлумачення ст. 3, 23, 31, 47, 48 Закону України "Про інформацію" та ст. 12 Закону України "Про прокуратуру" (справа К.Г.Устименка) від 30 жовтня 1997 р., у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України 20 січня 2012 року та інші.

Слід зазначити, що право на інформацію не є абсолютним і необмеженим. Реалізація права на інформацію громадянами, юридичними особами і державою не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб [360, ст.9]. Однією із меж реалізації цього права є принцип, згідно з яким не допускається збирання інформації, що є державною таємницею або конфіденційною інформацією юридичної особи [498, ст.302]. Іншими словами, перефразовуючи стародавній принцип, право особи на інформацію закінчується там, де починається право іншої особи [251, с.23]. В умовах становлення інформаційного суспільства невизначеність у правовій площині цієї межі прав і свобод людини призводить до виникнення нових проблем, які вимагають наукового дослідження.

Розробка «Декларації прав людини і правових норм в інформаційному суспільстві» [559] Комітетом експертів Ради Європи з інформаційного суспільства стала першою спробою визначення правових рамок в цій сфері. Основна увага була присвячено розробці норм відповідальної поведінки в інформаційному суспільстві різних суб'єктів - уряд, приватні компанії, ЗМІ та неурядові організації. На їхню думку, «цілкова повага свободи слова та інформації державними та недержавними інститутами є необхідною передумовою побудови вільного інформаційного суспільства для всіх, а інформаційно-комунікаційні технології не повинні використовуватися для обмеження цієї фундаментальної свободи» [6].

Розділ «Права людини в інформаційному суспільстві» Декларації містить 8 пунктів: право на свободу вираження, інформації та комунікацій; право на повагу до приватного життя і таємниці листування; право на освіту і загальний доступ до інформаційних технологій; заборона рабства і примусової праці; право на неупереджений суд і заборону на позасудове переслідування; захист власності; право на вільні вибори; свобода зібрань [559]. Як можемо бачити – переважна більшість – це права, які вважалися базовими і до становлення інформаційного суспільства.

Проаналізувавши доктринальні підходи, норми міжнародного права та національного законодавства, вважаємо, що слід розрізняти дві різні категорії: інформаційні права і свободи людини, а також права і свободи людини в інформаційному суспільстві. При чому перша категорія є складовою другої.

Під інформаційним правами і свободами розуміємо комплекс прав, похідних від свободи інформації, як фундаментального права людини. До них належать:

1) інформаційні права, що пов'язані з особою (особистістю)<sup>7</sup> людини – право на захист персональних даних, право визначати конфіденційність інформації та розпоряджатися нею;

2) право власності на інформацію;

3) право на доступ до інформації – в широкому розумінні, тобто доступ до публічної, екологічної, правової, наукової та інших видів інформації, в тому числі необхідної для реалізації інших прав та свобод – політичних прав, право на освіту, право на безпечне для життя та здоров'я довкілля, трудових та інших прав;

4) свобода поширення інформації будь-яким законним способом, яка є необхідною умовою повноцінного життя людини в демократичній державі, а також існування самого громадянського суспільства, її реалізація пов'язана з свободою думки і слова, правом на вільне вираження своїх поглядів і переконань;

5) право на безпечне інформаційне середовище.

Зупинимось більш детально на кожній з названих категорій.

*1) Інформаційні права, що пов'язані з особою (особистістю) людини,* виокремлюються нами на основі природно-історичного обґрунтування прав людини. Згідно нього людина є соціальною істотою і володіння правами і свободами має не лише правове значення, але й соціальне. Позбавлення чи обмеження прав людини спричиняє неможливість для задоволення своїх потреб та інтересів. Насамперед, до цієї категорії нами віднесено права, що пов'язані з реалізацією особистої свободи та права на приватність.

Реалізуючи право на свободу та право на особисту недоторканість, фізична особа одночасно реалізує і комплекс прав на інформацію [330, с. 87]. Право на

<sup>7</sup> Різниця в застосуванні категорій «особа і «особистість» в праві та інших соціальних науках розглянута в розділі І. Йдеться про соціальну природу людини, особливості її взаємодії з іншими людьми, соціальними групами та суспільством в цілому.



особисту свободу означає відповідну міру можливої та юридично дозволеної поведінки громадянина розпорядитися собою, своїми вчинками та часом. О.В. Кохановська доповнює цей перелік інформацією [215].

Тихомиров О.О., характеризуючи «інформаційні права першого покоління», які визначають невідчужувані так звані «негативні свободи», відносить до них: право на ім'я, його зміну і використання; право на таємницю особистого життя; право на особисті папери та розпорядження ними; право на таємницю кореспонденції; права особи, пов'язані з фото-, кіно-, теле- та відеозйомкою; право на свободу літературної, художньої, наукової і технічної творчості [462, с.106]. А їх інформаційна природа полягає в необхідності: по-перше, збереження в таємниці певної інформації про життя людини; по-друге, забезпечення цілісності інформації, яка ідентифікує особу, та самостійного визначення ступеня своєї публічності; по-третє, гарантування можливостей вільної творчої діяльності, результати якої у разі їх оприлюднення поповнюють інформаційний простір, перетворюючись у певні загальнодоступні знання.

Чинне законодавство України не містить категорії приватності. Право на приватність – *right to privacy* – належить до основних прав і свобод людини. Його історичні корні сягають праць Арістотеля про дві сфери життя: публічну ("поліс"), пов'язану з політичним життям, та приватну ("ойкос"), пов'язану з домашніми справами. Проте в сучасному розумінні воно було сформульоване в 1890 р. в США професорами права Гарвардського університету Уорреном і Брейндсом [664], як наслідок активного розвитку ЗМІ і їх втручання в приватне життя.

Серед науковців також немає одностайності при визначенні змісту цього права. На думку А. Фат'янова, особиста таємниця базується на неповторності кожної людини. Особисту таємницю в основному становлять відомості про ті факти або події, які можуть спотворити образ особистості, у якому вона хотіла б постати перед суспільством [478, с.14].

Інакший, більш широкий підхід до визначення категорії «приватність» сформулював професор права Університету Д. Вашингтона Д. Солов в праці «Розуміння приватності»: право на усамітнення, можливість особи обмежити

доступ інших осіб до персональної інформації про неї, конфіденційність, або можливість приховати будь-яку інформацію від інших, контроль особи над тим, як інші особи використовують інформацію про неї, стани приватності (самітність, інтимність, анонімність, і захищеність), персональність та автономність, самоідентифікація та розвиток особистості, захист інтимних стосунків [644, с.158].

Нормативне вираження права на приватність знайшло в ст. 17 Міжнародного пакту про громадянські і політичні права, де визначено: «1. Ніхто не повинен зазнавати свавільного чи незаконного втручання в його особисте і сімейне життя, свавільних чи незаконних посягань на недоторканність його житла або таємницю його кореспонденції чи незаконних посягань на його честь і репутацію. 2. Кожна людина має право на захист закону від такого втручання чи таких посягань»

А також в ст. 8 Конвенції про захист прав людини і основоположних свобод, з поправками: «1. Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. 2. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб.»

Дотримання норми, зазначеної у ст. 8, має водночас позитивне і негативне значення. У позитивному сенсі, влада зобов'язана забезпечити захист приватного життя від порушень, в негативному сенсі, зобов'язані утримуватися від втручання в приватне життя, зокрема, заборона криміналізації діянь, пов'язаних цієї сферою.

Коли йдеться про порушення права на приватне життя, визнання такого втручання можливе на основі п.2 ст.8 за наявності трьох умов: 1) втручання здійснюється згідно із законом 2) повинно бути необхідним у демократичному суспільстві 3) захищати визначені в цій статті інтереси.

Законодавство України у сфері захисту недоторканості приватного життя складається з: Конституції України; міжнародних угод, згода на обов'язковість

яких надана Верховною Радою України, Законів України «Про інформацію», «Про захист персональних даних», а також інших законів та підзаконних актів.

Конституція України, норми якої мають пряму дію, досить широко тлумачать право на приватність. Стаття 32 Конституції України передбачає: «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації».

Крім того, Основним Законом гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31). Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинів чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.

Після прийняття Закону України «Про захист персональних даних» для реалізації державної політики у сфері захисту персональних даних було створено Державну службу захисту персональних даних, основними завданнями якої були: внесення пропозицій щодо формування державної політики у сфері захисту персональних даних; реалізація державної політики у сфері захисту персональних даних; контроль за додержанням вимог законодавства про захист персональних даних; здійснення міжнародно-правового співробітництва у сфері захисту персональних даних.

Законом України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [338], з метою

забезпечення незалежності уповноваженого органу з питань захисту персональних даних, як того вимагає Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних [202], повноваження щодо контролю за дотриманням законодавства про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини.

Питанням правового забезпечення права на захист персональних даних присвячено значну кількість напрацювань науковців різних галузей права – конституційного, інформаційного, цивільного, кримінального і, звичайно, інформаційного – Баранов О.А., Бем М. В., Брижко В.М., Мельник К., Пазюк А.В., Поєдинок О.Р., Тихомиров О.О. та інші.

Про те ці відносини є надзвичайно динамічними і відповідно вимагають від держави адекватного і своєчасного реагування змінами правового забезпечення. На сьогодні, зміни політики щодо захисту персональних даних в ЄС вимагають від України відповідної реакції.

Суд Європейського Союзу в жовтні 2015 р. оголосив недійсною угоду між США та країнами ЄС, відому під назвою "SafeHarbor" ("Безпечна гавань"), яка загалом дозволяла передачу даних і їх зберігання в США. У травні 2018 р. набуває чинності новий регламент Європейського союзу про захист даних (General Data Protection Regulation, далі Регламент) [587]. Він ще більше віддаляє дві найбільш поширені моделі правового забезпечення захисту персональних даних – європейську і американську.

Реформа захисту даних Європейського Союзу посилює права громадян, вона спрямована на захист особистої інформації, незалежно від того, де вона введена, обробляється і зберігається, навіть за межами ЄС. Стаття 3.2 Регламенту визначає, що: «Цей регламент застосовується до обробки персональних даних суб'єктів даних, які знаходяться в Союзі, навіть якщо контролер або процесор не засновані в Союзі, де діяльність по обробці пов'язана з: пропонуванням товарів або послуг, незалежно від того, чи вимагається оплата суб'єкта даних таким суб'єктам даних в Союзі; або моніторингом їх поведінки, якщо їхня поведінка відбувається в рамках Союзу». Таким чином, Регламент поширюється на три категорії суб'єктів: 1) організації, засновані в ЄС; 2) інші організації, що здійснюють обробку ПД

європейських громадян у зв'язку з реалізацією товарів або послуг; 3) інші організації, що здійснюють моніторинг поведінки європейських громадян.

Як наголошується у Регламенті, захист фізичних осіб у зв'язку з обробкою персональних даних є фундаментальним правом. При цьому, це право не є абсолютним. Воно повинне розглядатися у зв'язку з його функцією в суспільстві і бути збалансованим з іншими основними правами, відповідно до принципу пропорційності, який має бути визначений у базовому законі країни [63, с.46].

У Регламенті персональні дані означають будь-яку інформацію, що стосується ідентифікованої фізичної особи або фізичної особи, що ідентифікується, водночас дещо уточнюється по тексту - персональні дані можуть включати інтернет - ідентифікатори, надані пристрою, додатку, такі інструменти, такі як IP- адреси, cookies, цифрові ідентифікатори або інші ідентифікатори пристроїв, ідентифікатори і місце розташування по яким може бути ідентифікована конкретна особа.

У Регламенті значна увага приділяється концепції "згоди суб'єкта на обробку своїх персональних даних", яка має бути вільною і яку можна легко відкликати. Визначено 7 основних і 16 додаткових принципів [442].

Регламент стосується не лише питань інформаційної безпеки і відповідності стандарту ISO 27001, він також торкається управління життєвим циклом персональних даних і наявності технологій, що здійснюють це управління. Наприклад, встановлюється обов'язковий мінімальний термін зберігання також згадується в правилі 39 і статті 25, а щодо періоду, протягом якого можна зберігати персональні дані, зазначено,. Що він повинен бути «зведений до строгого мінімуму», і що системи за умовчанням повинні проектуватися таким чином, щоб мінімізувати термін зберігання персональних даних [645].

Окрім, того вперше нормативно закріплене так зване "право на забуття" (англ. right to be forgotten), яке ще в 2014 р. було визнано в судовому порядку Європейським судом у справі Маріо Костеха проти корпорації Google. Тоді громадяни Євросоюзу отримали право звернутися за певних обставин до будь-якої пошукової системи із запитом про видалення неадекватної, такої, що не відповідає дійсності, або застарілої інформації, яка містить їх імена або інші

персональні дані, а справа Костехи стала першим судовим прецедентом у цьому питанні[582]. Але суд також зазначив, що дана справа не є універсальною, а право на забуття — абсолютним: рішення в аналогічних справах виноситимуться на основі конкретних обставин, щоб виключити їх протиріччя з фундаментальними правами людини (свободи слова і друку): принцип a case-by-case assessment [ibid.].

Безперечно, що питання забезпечення права на захист персональних даних є і будуть актуальними. Новий Регламент значною мірою враховує реалії епохи соціальних мереж, де можна зібрати значну кількість інформації щодо її учасників. За даними CareerBuilder, близько 60% європейських роботодавців використовують отриману в соціальних мережах інформацію, перш ніж ухвалити рішення щодо кандидатів. Чи законно це? Чи достатньо захищена приватна інформація? Для України ця проблема ще актуальніша, ніж для ЄС. Для порівняння, в нашій країні, за даними HeadHunter, соцмережі при підборі персоналу вивчають майже 70% роботодавців [85].

## *2) Право власності на інформацію*

Інформацію як об'єкт цивільних правовідносин розглядають у таких проявах: як особисте немайнове благо в комплексі благ, наведених у ст. 201 та Книзі другій ЦКУ; як результат інтелектуальної діяльності, тобто як об'єкт виключних прав, урегульованих у ст. 199 ЦКУ; як інформаційний продукт, ресурс, документ, тобто об'єкт, який може бути інформаційним товаром і предметом будь-яких правочинів, з урахуванням особливостей та специфіки його як особливого об'єкта [214] Якщо в першому розумінні інформація є невіддільним благом від самої особи носія, то два наступних дозволяють розглядати інформацію як товар, що може відчужуватись, хоча йому й притаманні певні особливості.

Баранов О.А., аналізуючи українське законодавство, зауважує його суперечливість щодо визначення права власності на інформацію [26]. В редакції Закону «Про інформацію» в 2011 р. було скасовано категорію право власності на інформацію. Дехто з правників потрактував це в такий спосіб, що інформація не може бути об'єктом право власності [213]. Категорично не погоджуємось з такою позицією, оскільки правомочності володіння, користування і розпорядження є необхідною умовою реалізації інформаційних прав і інформаційної безпеки.

Власниками інформації можуть бути її виробники, тобто власник інформаційного об'єкта (оригіналу документа, першотвору бази даних і т.п.), який створив інформацію, відображену в цьому об'єкті, власник інформації, що його набув на договірних умовах; а також власник - споживач інформації, тобто власник інформаційного об'єкта (тиражованої копії документа, масиву документів і т. п.), який придбав конкретний екземпляр тиражу з метою споживання інформації, що міститься в придбаному їм інформаційному об'єкті. І право власності кожного з них буде відрізнятися.

Ще один аспект права власності на інформацію – як національне надбання, належним чином не відображений в чинному законодавстві. Згідно Закону «Про наукову і науково-технічну діяльність» До наукових об'єктів, що становлять національне надбання, можуть бути віднесені визначені інформаційні ресурси, зокрема, інформаційні фонди. Проте, на нашу думку, слушною є рекомендація ЮНЕСКО вважати публічну інформацію надбанням народу, адже вона створюється в інтересах суспільства і за кошти платників податків. Такий підхід обґрунтовує право на доступ до публічної інформації. З цією метою відповідна норма має знайти відображення в Основному Законі.

Українське законодавство регулює право власності на інформацію нормами цивільного права і інформаційного права. Однак, питання права власності суттєво виходить за межі предмету цього дослідження. Тому називаючи його, автор не заглиблюється у його розгляд. Проте, при здійсненні дослідження автор зіткнувся з такими питаннями, що можуть становити предметне поле для подальшої наукової розвідки, зокрема, питання визначення вартості інформації, реалізації права власності на бази даних, охорони права інтелектуальної власності в умовах постійного вдосконалення інформаційних технологій.

*3) Право на доступ до інформації у сучасній науці інформаційного права визначається як одне з інформаційних прав, що передбачає право кожного вільно збирати інформацію і право отримувати її від осіб, які володіють цією інформацією на законних підставах [139, с.63-72].*

В останнє десятиріччя право на доступ до інформації здебільшого інтерпретували під кутом доступу до публічної інформації. Безперечно воно є

важливим і відображає принцип транспарентності<sup>8</sup>. Принцип інформаційної відкритості є важливою умовою існування демократичного суспільства, виражається в доступності для громадян інформації, що становить суспільний інтерес або зачіпає особисті інтереси громадян; систематичному інформуванні громадян про передбачувані або прийняті рішення; здійсненні громадянами контролю за діяльністю державних органів, організацій і підприємств, громадських об'єднань, посадових осіб та прийнятих ними рішень, пов'язаних з дотриманням, охороною та захистом прав і законних інтересів громадян; створення умов для забезпечення громадян України наданням їм інформаційних послуг іноземного походження.

Як зазначає Т. Мендел, головне значення для гарантування реалізації вільного потоку інформації та ідей має визнання принципу, що державні органи володіють інформацією не для себе, в інтересах суспільства та від його імені [624].

Зміст права на доступ до інформації є похідним від свободи вираження поглядів, передбаченої статтею 10 Конвенції Ради Європи про захист прав людини і основоположних свобод [329]. З аналізу практики Європейського суду з прав людини по застосуванню цієї норми можна зробити висновок, що право на свободу вираження поглядів включає такі складові: свободу дотримуватися своїх поглядів; свободу одержувати інформацію та ідеї; свободу передавати інформацію та ідеї. Щоби мати власні погляди та/або передавати інформацію та ідеї необхідно мати достатній обсяг інформації, що робить право одержувати інформацію та ідеї основоположним.

Органи державної влади самі створюють значний масив інформації, отримують і зберігають великий обсяг даних від фізичних та юридичних осіб. Як правило, це важлива інформація, що впливає на життя усієї спільноти. Можливість кожної окремої людини одержувати всю суттєву інформацію, що існує у суспільстві, напряду залежить від того, чи вчиняє держава активні дії, щоб опублікувати, оголосити чи надати на запит відомості, якими вона розпоряджається, тобто від державної інформаційної політики [329].

---

<sup>8</sup> Від лат. *Transpareo* – відкрите, видиме наскрізь, зрозуміле.



Згідно Закону «Про доступ до публічної інформації» забезпечення права на доступ до інформації здійснюється двома основними способами – шляхом систематичного та оперативного оприлюднення інформації: в офіційних друкованих виданнях; на офіційних веб-сайтах в мережі; на єдиному державному веб-порталі відкритих даних; на інформаційних стендах; будь-яким іншим способом; та шляхом надання інформації за запитами на інформацію.

Відкриті дані (open data) засновані на ідеї про те, що деякі дані повинні бути вільно доступними для всіх, щоб вони використовувались та перевидавали за власним бажанням, без обмежень із авторських прав, патентів та інших механізмів контролю. Цілі відкритих даних подібні до інших "відкритих" рухів, таких як відкриті джерела, відкрите обладнання, відкритий контент, відкритий уряд та відкритий доступ. Філософія відкритих даних відома давно (наприклад, в науковій концепції Мертона), але термін "відкриті дані" останнім часом стає популярним завдяки поширенню інтернету та Всесвітньої павутини та, особливо, запуску урядових ініціатив щодо відкритих даних.

Основні принципи розкриття даних: доступність, відсутність технологічних обмежень, цілісність, відсутність дискримінації осіб та груп, відсутність дискримінації областей і починань і ін.

Так у США у 2009 р. створено ресурс Data.gov, який по суті став першим у світі державним ресурсом відкритих даних. Було також оприлюднено Директиву Відкритого Уряду США. В Європейському союзі існують як загальноєвропейські програми підтримки та розвитку відкритих даних ([open-data.europa.eu/en/data/](http://open-data.europa.eu/en/data/)), так і на рівні окремих держав-членів (Наприклад, Франція [data.gouv.fr/fr/](http://data.gouv.fr/fr/), Німеччина [govdata.de/](http://govdata.de/), Італія [it.ckan.net/](http://it.ckan.net/), Польща [insigos.mg.gov.pl/Glowna.aspx](http://insigos.mg.gov.pl/Glowna.aspx) та ін.). Канада і США на сьогодні є країнами-лідерами по публікаціям даних (опубліковано понад 100 тис. наборів), слідом за ними йдуть Великобританія, Франція, Індія, Японія, Німеччина і Італія (від 10 до 15 тис. наборів)[653]. США, Канада, Великобританія і Австрія не проводять моніторинг цільової аудиторії. У США регулярно оновлюються форуми, і будь-яка людина може взяти участь в «житті» відкритих даних[657]. У Великобританії розвинений громадський контроль за витрачанням державних коштів, визначені пріоритетні набори та

конкретні кроки по їх розкриттю. Запити щодо розкриття державної інформації публікуються на окремому сайті – WhatDoTheyKnow<sup>9</sup>. Запит на розкриття інформації передбачає, що користувач сам оцінює можливу користь від розкриття даних; в разі відсутності соціально-економічних ефектів від розкриття даних дані не публікуються.

Cargemini Consulting в залежності від темпів реалізації принципів відкритості, визначив три групи країн. «Початківці»: Австрія, Марокко, Об'єднані Арабські Емірати, Саудівська Аравія, Естонія. «Група послідовників»: Бельгія, Гана, Данія, Гонконг, Ірландія, Іспанія, Італія, Кенія, Молдова, Нова Зеландія, Норвегія, Сінгапур, Чилі. «Законодавці моди»: Австралія, Великобританія, Канада, США, Франція. Класифікація проводилася на підставі трьох параметрів: доступність даних, державна політика в галузі відкритих даних і функціональні можливості централізованого порталу відкритих даних [653].

В Україні історія розвитку відкритих даних розпочинається після прийняття Закону «Про доступ до публічної інформації» [343], але реально ресурси запрацювали у 2015 р., після того як був прийнятий Закон «Про внесення змін до деяких законів України щодо доступу до публічної інформації в формі відкритих даних» [337] та Постанова Кабінету Міністрів України «Про затвердження Положення про набори даних, що підлягають опублікуванню в формі відкритих даних» [354]. На підставі цих документів державні органи зобов'язані надавати публічну інформацію в формі відкритих даних і регулярно оновлювати її на єдиному державному веб-порталі відкритих даних<sup>10</sup> у визначених форматах, що дозволяють автоматизоване оброблення такої інформації електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання. В тому ж 2015 р. було прийнято Закон «Про відкритість використання публічних коштів», що став правовою підставою оприлюднення інформації про використання публічних коштів функціонують на офіційному державному інформаційному порталі.

---

<sup>9</sup> <https://www.whatdotheyknow.com/>

<sup>10</sup> <http://www.data.gov.ua/>

Відповідно до частини першої статті 212-3 КУпАП неоприлюднення інформації, обов'язкове оприлюднення якої передбачено, зокрема, Законом України "Про доступ до публічної інформації", - тягне за собою накладення штрафу на посадових осіб від двадцяти п'яти до п'ятдесяти неоподатковуваних мінімумів доходів громадян. Складати протоколи про адміністративні правопорушення за статтею 212-3 КУпАП мають право уповноважені особи секретаріату Уповноваженого Верховної Ради України з прав людини або представники Уповноваженого Верховної Ради України з прав людини. Таким чином, особа може звернутись до Секретаріату Уповноваженого Верховної Ради України з прав людини щодо порушення розпорядниками інформації вимог оприлюднення публічної інформації у формі відкритих даних та складення протоколу про адміністративне правопорушення за частиною першою статті 212-3 КУпАП. Порядок звернення до Уповноваженого з прав людини та його Секретаріату, зокрема й щодо складення протоколу про адміністративне правопорушення за статтею 212-3 КУпАП, передбачається статтею 17 Закону України "Про Уповноваженого Верховної Ради України з прав людини". Відповідальність за неоприлюднення відповідної публічної інформації у формі відкритих даних має покладатись на відповідальну особу з питань доступу до публічної інформації розпорядника інформації, яка відповідає за оприлюднення відповідної інформації згідно із Законом України "Про доступ до публічної інформації". Станом на 2016 р. до Секретаріату Уповноваженого Верховної Ради України з прав людини не надходили скарги щодо порушення розпорядниками інформації вимог оприлюднення публічної інформації у формі відкритих даних [231]. Окрім того, створено низку недержавних ресурсів відкритих даних, таких як CityScale<sup>11</sup>, а також ресурсів, що полегшують роботу з відкритими даними, наприклад «Пошуково-аналітична система .007»<sup>12</sup>.

Проблеми, що стали очевидними в правовому регулюванні відкритих даних: низький ступінь поінформованості населення про можливості використання

<sup>11</sup> <http://www.cityscale.com.ua/about.htm>

<sup>12</sup> «Пошуково-аналітична система .007» - це web-ресурс на основі відкритих даних про використання публічних коштів. Проект передбачає сервіс пошуку та візуалізації даних з відкритих джерел про використання державою бюджетних коштів. Основний акцент зроблено на простоті використання та представлення специфічної інформації з масивів великих даних. <http://www.007.org.ua/>

відкритих даних, неефективність системи моніторингу стану оприлюднення та оновлення наборів даних на держаних порталах, сумнівність санкції статті 212-3 КУпАП щодо покладення відповідальності на відповідальну особу з питань доступу до публічної інформації розпорядника інформації (як правило, це державний службовець, який виступає лише виконавцем і немає реальної можливості впливу). Окремим проблемним питанням є громадська думка про недоцільність та безглуздість використання відкритих даних в країні. Деякі пояснюють це історичними особливостями розвитку України і ще не сформованим у наших громадян усвідомленням всієї перспективності демократичних цінностей [231].

Що стосується відкритих даних, що не належать державі, то їх системне правове регулювання відсутнє. Відсутнє на рівні законодавства і визначення відкритих даних, порядок надання такого статусу і його зміст. На нашу думку, інформація (дані) є відкритою, якщо будь-хто має до нього вільний доступ, може вільно використовувати та ділитися нею. При врегулюванні питань відкритих даних важливим видається також нормативно застерегти можливість автору (творцю контенту) визначати заходи, необхідні для збереження походження й відкритості таких даних. Особливої уваги, на нашу думку, заслуговує врегулювання правового режиму відкритості науково-технічної інформації, творів культури і мистецтва, інформації про товари і послуги, а також екологічної інформації (якщо її розпорядником не є держава).

Наступним способом реалізації права на доступ до інформації є отримання інформації на запит. Право запитувати та одержувати інформацію в органах влади було визнано на рівні Ради Європи ще в 1979 р. в рекомендації Парламентської Асамблеї РЄ, де зазначалося, що парламентська демократія може належним чином функціонувати лише тоді, коли люди є повністю поінформовані; що громадськість повинна мати доступ до урядових документів; що така свобода інформації становить інструмент стримування корупції та розкрадання публічних коштів. У документі ПАРЕ йшлося про свободу інформації та систему свободи інформації, оскільки на той час “право на доступ” ще не було сформовано і утверджено. Принагідно слід зазначити, що “свобода інформації” відрізняється

від “права на доступ до інформації”, оскільки перша передбачає негативний обов'язок держави не втручатися в інформаційний обмін між особами, тоді як друге – позитивний обов'язок держави забезпечити доступ активними діями, а не лише утриманням від втручання у свободу особи[90]. У Рекомендації Комітету Міністрів РЄ щодо доступу до інформації, яка була оновлена в 2002 р., наголошувалося, зокрема, на важливості в плюралістичному, демократичному суспільстві прозорості публічної адміністрації та доступності інформації з питань суспільного інтересу [90]. Зазначалося, що широкий доступ до офіційних документів: 1) дозволяє громадськості мати адекватне уявлення та сформулювати критичну думку щодо стану суспільства, у якому воно живе, та щодо органів влади, які ним керують, заохочуючи при цьому поінформовану участь громадськості у спільних справах; 2) сприяє ефективності та дієвості адміністрації та допомагає підтримувати її доброчесність, уникаючи ризику корупції; 3) робить внесок в утвердження легітимності адміністрації як публічної служби та зміцнення суспільної довіри до органів публічної влади.

В Україні право на інформацію визнавалося ще Законом України «Про інформацію» [360] у редакції 1992 р.. У 2011 р. набули чинності Закон України «Про доступ до публічної інформації» та нова редакція Закону України «Про інформацію». Закон «Про доступ до публічної інформації» визначив: 1) порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації; 2) гарантії та принципи забезпечення права на доступ до публічної інформації; 3) суб'єктів відповідних відносин, їх права та обов'язки тощо. Нова редакція Закону «Про інформацію» передбачає «право кожного на інформацію», визначивши при цьому одним із основних напрямів державної інформаційної політики «забезпечення доступу кожного до інформації». Крім того, Закон «Про інформацію» у статті 20 закріпив важливий принцип максимальної відкритості, згідно з яким «будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом»

Законом врегульовано яка саме інформація може запитуватись, та які обмеження щодо доступу існують. Так, запит на інформацію – це прохання особи

до розпорядника інформації надати публічну інформацію, що знаходиться в його володінні (наприклад, інформація щодо використання бюджетних коштів або копія рішення сесії міської ради). Тобто йдеться про вже існуючу інформацію, якою володіє розпорядник. Для відповіді на інформаційний запит розпорядник не повинен створювати нову інформацію.

Доступ до публічної інформації може бути обмежений, якщо вона є інформацією з обмеженим доступом: 1) конфіденційна інформація; 2) таємна інформація; 3) службова інформація.

Обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Таким чином, в законодавстві України знайшов відображення трискладовий тест, що є юридичною конструкцією – засобом для перевірки наявності необхідних умов для обмеження доступу до інформації. Це ті умови, виконання яких є обов'язковим для того, щоб виняток з відкритості інформації був правомірним. Іншими словами – обмеження доступу до публічної інформації без застосування трискладового тесту є незаконним і порушує право особи на інформацію. Будь-якому обмеженню доступу до інформації з боку розпорядника повинно передувати застосування «трискладового тесту» [90].

До 2015 р. органом, що контролював виконання норм щодо забезпечення права на доступ до публічної інформації була прокуратура, від 2015 і до сьогодні - це Уповноважений Верховної Ради України з прав людини.

Рішення, дії чи бездіяльність розпорядників інформації також можуть бути оскаржені до керівника розпорядника, вищого органу або суду. Запитувач має

право оскаржити: 1) відмову в задоволенні запиту на інформацію; 2) відстрочку задоволення запиту на інформацію; 3) ненадання відповіді на запит на інформацію; 4) надання недостовірної або неповної інформації; 5) несвоєчасне надання інформації; 6) невиконання розпорядниками обов'язку оприлюднювати інформацію відповідно до статті 15 Закону «Про доступ до публічної інформації»; 7) інші рішення, дії чи бездіяльність розпорядників інформації, що порушили законні права та інтереси запитувача.

Практика свідчить, що державні службовці досить часто неправильно застосовують на практиці положення тесту, в результаті чого запитувачі не можуть одержати суспільно важливу інформацію. Дані моніторингу виконання органами влади норм Закону «Про доступ до публічної інформації», який здійснюється Центром Політичних Студій та Аналітики з 2011 р., свідчать, що часто це відбувається через незнання чиновниками алгоритму його застосування. Водночас експертами Центру були зафіксовані непоодинокі випадки, коли чиновники зловживали і свідомо неправомірно застосовували тест для того, щоб не надати запитувану інформацію громадянам [90].

Водночас, аналіз звернень до Уповноваженого Верховної ради з прав людини та судової практики щодо порушення права на доступ до публічної інформації свідчить, що неправомірною може бути визнана відповідь розпорядника на запит, у якій він відмовляє в отриманні інформації: оскільки він не вважає себе розпорядником інформації в розумінні Закону України «Про доступ до публічної інформації»; якою він володіє, але з якихось причин вважає «непублічною» чи такою, що не повинна надаватись на запит; через порушення вимог законодавства щодо порядку оплати фактичних витрат на копіювання і друк; через вимогу вказати в запиті відомості, що не передбачені статтею 19 Закону України «Про доступ до публічної інформації»; якою він не володіє, але зобов'язаний відповідно до своєї компетенції; оскільки відповідає не по суті запиту; з будь-яких інших підстав, що не передбачені частиною першою ст. 22 Закону; оскільки запитувану інформацію можна отримати з офіційного веб-сайту чи інших загальнодоступних джерел; оскільки відповідає не по суті запиту; з порушенням встановлених законом вимог до відмови у задоволенні запиту на інформацію

[524]. Серед типових порушень права на доступ до публічної інформації в Україні найбільш поширеними є порушення процедури (недотримання строків та форми), посилення до відкритих даних чи інформації, розміщеної на сайті (коли там відсутні відповідні дані); відмова з огляду на обмеженість доступу до такої інформації. Часто причинами таких порушень є перевантаженість та недостатній рівень обізнаності співробітників з питань права людини на доступ до інформації. Наприклад, при здійсненні моніторингового візиту до Головного управління Національної поліції в Івано-Франківській області з метою перевірки дотримання права громадян на доступ до публічної інформації, було виявлено порушення права на доступ до публічної інформації. При опитуванні співробітники відзначили не проходили підготовки з питань доступу до публічної інформації і жодного разу не брали участь у тематичних навчальних семінарах [78].

Належний рівень правової культури державних службовців, які беруть участь у нормотворчій діяльності, тлумачать та застосовують норми права, а також здійснюють юридичне інформування населення, є необхідною умовою гарантування дотримання прав і свобод людини, а також правового забезпечення розвитку демократичної правової держави.

З питань доступу до публічної інформації заслуговує уваги значна активність громадянського суспільства. За останні роки неурядовими організаціями здійснюється постійна підтримка громадян щодо можливості реалізації цього права, а також захисту і відновлення порушених прав. Центр демократії та верховенства права заснував і активно підтримує Мережу захисників права на доступ до інформації, метою якої є гарантування правового захисту права кожного на доступ до інформації - було підготовлено, перекладено, опубліковано і поширено значна кількість практичних посібників, методичних рекомендацій та науково-практичних коментарів до законодавства, що стосуються прав доступу до публічної інформації, зокрема практичний посібник «Як оскаржити порушення права на доступ до публічної інформації?», Рекомендації розпорядникам публічної інформації, Науково-практичний коментар до Закону України «Про доступ до публічної інформації», навчальний посібник для державних службовців «Свобода інформації» тощо.



У 2014 р. був запущений сайт «Доступ до Правди», що є уніфікованою платформа для надсилання електронних запитів розпорядникам інформації відповідно до Закону “Про доступ до публічної інформації”, отже, для ефективного контролю громадян за діями влади. У 2015 р. Громадська організація «Центр UA» презентував його оновлену версію, що доповнена новим ресурсом, який дозволяє створювати новини і розслідування на основі відповідей на запити громадян. Таким чином, є всі підстави не погоджуватись з раніше згаданою позицією про «несформоване у громадян усвідомленням всієї перспективності демократичних цінностей».

4) *Свобода поширення інформації* будь-яким законним способом є нерозривно пов’язана з свободою вираження думок і поглядів, що є базовою для демократичного суспільства. Ця свобода значно ширша за відсутність цензури. Вона акумулює в собі низку складових - свобода вираження думок і переконань, свобода слова, свобода друку, свобода ЗМІ; свобода журналістської діяльності; свобода творчості; свобода видавничої діяльності; право «виносити сміття з хати» («blow the whistle»)<sup>13</sup>, право мовчати та інші.

Ця свобода закріплена як на найвищому міжнародному рівні (ст. 10 Конвенції про захист прав людини й основоположних свобод від 4 листопада 1950 р.), так і в Основному законі держави (ст. 34 Конституції України), посеред інших інформаційних прав. Водночас, цими ж нормами закріплено випадки обмеження цієї свободи (права – в українському законодавстві): ст. 10 Конвенції про захист прав людини й основоположних свобод: «Здійснення цих свобод, оскільки воно пов’язане з обов’язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров’я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду.»; ст. 34 Конституції України: «Здійснення цих прав може бути обмежене законом в інтересах національної безпеки,

---

<sup>13</sup> Право посадових осіб оприлюднювати інформацію про правопорушення в установі, в якій вони працюють.

територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя».

Це право є «зворотною стороною» інших, в т.ч. інформаційних, прав – права на доступ до інформації, права на захист персональних даних та інших. Саме на межі цих прав і виникає значна кількість конфліктів. Рабінович П.М. зазначав, що в усі часи боротьба йшла не стільки за права, скільки за їх межі [394]. В умовах становлення інформаційного суспільства юридичне закріплення таких меж є визначальним для реалізації інформаційної безпеки людини. Новицька Н.Б. аналізуючи зловживання правом на свободу слова та інформації, дійшла до висновку, що «зловживання правом свободи інформації може призвести до неефективності демократичного ладу, а саме стати причиною національної небезпеки, порушення громадського порядку, неконтрольованості суспільства владою, пропаганди насильницької зміни влади, закликів до національної, релігійної, регіональної, расової ворожнечі, нівелювання правом людини на приватне життя, загрозою її безпеки» [279, с.60-66].

Слід звернути увагу, що право на поширення інформації прислуговує не всім учасникам правовідносин у рівній мірі. Його обсяг залежить від суб'єкта інформаційних відносин (журналісти, адвокати, пересічні громадяни мають різні правомочності) і об'єкта (інформація з обмеженим доступом, інформація, що має суспільне значення, публічна інформація тощо).

Важливою умовою реалізації права на свободу поширення інформації є захист прав осіб, що її поширюють, насамперед, журналісти. Поняття «свобода преси» охоплює не лише засоби масової інформації, як суб'єктів – юридичні особи, колективи людей. Цим поняттям охоплюється також індивідуальна свобода – можливість журналіста, який реалізує свій професійний обов'язок, і будь-якого іншого громадянина висловити свою думку в ЗМІ та прийняти участь в обговоренні суспільно важливих питань. В даному разі засоби масової інформації ефективно забезпечують свободу вираження поглядів будь-якої

фізичної особи, тому обмеження свободи преси неодмінно обмежує індивідуальну свободу громадян, яка впливає зі ст. 10 Конвенції про захист прав людини й основоположних свобод та ст. 34 Конституції України [89].

Обмеження свободи преси, навіть з метою захисту репутації і прав інших суб'єктів, не безпідставно вважається опосередкованим обмеженням права громадян на отримання ідей та інформації. Це, в свою чергу, може обмежити можливості громадян приймати зважені та правильні рішення з питань життя суспільства, що завдає шкоди будь-якому демократичному суспільству. Як зазначає С. Шевчук, якщо «преса не може публікувати різні, навіть образливі, судження, люди позбавлені самостійного політичного вибору. А це означає, що опозиція не має жодних шансів прийти до влади шляхом переконання виборців»[511,с.429]. ЗМІ безпосередньо займаються збором, обробкою та поширенням масової інформації. Можливість вільно збирати та поширювати інформацію, передбачає можливість вільно діяти без втручання інших осіб, зокрема держави, і без наявності в інших осіб певного кореспондуючого обов'язку. У справі „Бусуйок проти Молдови” Європейський суд висловлює таке тлумачення: «журналістська свобода включає також і можливість вдатися до певної міри перебільшення або навіть провокації»<sup>14</sup>.

Проте захисту при реалізації цієї свободи потребують і інші суб'єкти, зокрема, ті, які розкривають інформацію про зловживання. Набув значного розголосу приклад К. Ган, яка працювала на посаді аналітика Головної комунікаційної штаб-квартири електронної організації прослуховування британського уряду. На початку 2003 р. вона одержала копію електронного листа з офіційними детальними планами США щодо прослуховування дипломатів країн-членів Ради Безпеки ООН. Великій Британії і США було конче потрібно отримати рішення Ради Безпеки, яка б санкціонувала заплановане ними вторгнення до Іраку. Ган надала копію електронного листа до газети. Внаслідок цієї історії обидва уряди зазнали значних труднощів. Ган визнала, що вона спричинила витік інформації і була обвинувачена в шпигунстві. У лютому 2004 р. обвинувачення проти неї було знято. Позиція полягала в тому, що британський

<sup>14</sup> Зі справами ЄСПЛ, що розглянуті в роботі, можна ознайомитись на офіційному сайті <http://www.echr.coe.int/>

уряд міг би зіштовхнутися з багатьма труднощами, якби він був зобов'язаний представити у суді конфіденційну юридичну консультацію, яку було використано для підтримки вторгнення до Іраку. У будь-якому випадку, у країні, де половина населення виступала проти війни в Іраку, здавалося малоймовірним, що присяжні визнають Ган винною. К. Ган не була захищена за британським правом. Вона втратила свою роботу і лише уникла кримінального вироку, оскільки уряд побоювався продовжувати її судове переслідування [411]. В українському законодавстві не існує механізмів захисту таких осіб, а рівень ефективності судової системи не дозволяє сподіватись на судовий захист.

Відсутній у українському законодавстві і принцип «Обсяг інформації, доступ до якої обмежується, про публічну особу має бути значно меншим, ніж обсяг інформації про приватну особу», який сформувався в практиці Європейського суду з прав людини<sup>15</sup>.

*5) Право на безпечне інформаційне середовище.* Потреба в безпечному середовищі є необхідною умовою життя і розвитку людини. Погоджуючись значною мірою з М. Кастельсом в твердженні, що кожне суспільство є інформаційним, очевидним є що значення інформаційних суспільних відносин в сучасному світі зросло не порівняно до жодної попередньої епохи. Фізичний і соціальний простір сучасності пов'язаний з інформаційним, і спостерігається тенденція все щільнішого їх поєднання. Таким чином, людина живе в багатовимірному середовищі, одним із важливих вимірів є власне інформаційний.

Сьогодні вченими та фахівцями ставиться питання про необхідність розвитку інформаційної екології - науки, що вивчає закономірності впливу інформації на формування і функціонування людини, і людства в цілому, на здоров'я, як стан психічного, фізичного і соціального благополуччя, розробляються заходи щодо оздоровлення навколишнього інформаційного середовища.

Необхідними складовими права на безпечне інформаційне середовище є як захист інформації, так і захист від негативних інформаційних впливів, яким більше уваги буде присвячено далі в цьому розділі, та в наступному – «Загрози інформаційній безпеці людини».

---

<sup>15</sup> Однією з перших справ, в якій він знайшов відображення була справа «Лінгенс проти Австрії» від 08.06.1986 г.

Перелік означених питань не є вичерпним і потребує подальшого наукового осмислення та вдосконалення нормативно-правового і організаційного забезпечення права на доступ до інформації.

Такий зміст інформаційних прав і свобод відображає доктринальний підхід. Обсяг і зміст правового, зокрема, конституційного, закріплення цих прав залежить від багатьох соціальних, в т.ч. політичних, правових та економічних, чинників: форми держави та її економічного розвитку, рівня демократизації суспільства; геополітичного становища; суб'єктів самих прав (обсяг прав громадян чи інших членів суспільства може відрізнятися); зрештою, етапу становлення самого інформаційного суспільства, на якому перебуває держава.

Правові норми, визначаючи конкретний зміст прав і свобод людини та громадянина, не дають їхнього вичерпного переліку. Водночас, однією з функцій права є прогностична, тобто визначає право покликано передбачати, а певною мірою і визначати, тенденції розвитку державно-правових явищ.

Обсяг і зміст прав і свобод людини в сучасному суспільстві визначається не лише особливостями певного співтовариства людей, а й розвитком людської цивілізації в цілому.

Також заслуговує на увагу твердження, що інформаційні права і свободи людини та громадянина становлять цілісний екзистенціальний феномен, який можна пізнати винятково крізь призму їх системних властивостей, що знаходить свій прояв у наявності прав і свобод інформаційного характеру у різних сферах життєдіяльності суспільства [449, с.21]. Відтак, систему інформаційних прав і свобод реалізуються в екологічній сфері, економічній сфері, політичній сфері, управлінській сфері тощо. В умовах становлення інформаційного суспільства кожні суспільні відносини переломлюються через інформаційну сферу.

Друга категорія, *права і свободи людини в інформаційному суспільстві*, власне відображає зміни в змісті та способах реалізації, вже існуючих, загальноприйнятих та закріплених нормами міжнародного та національного законодавства права, суб'єктивних прав і свобод.

Спробуємо звернути увагу на особливості реалізації окремих прав і свобод людини в умовах становлення чи розвитку інформаційного суспільства.

Для особистості головними системотворчими рисами є цілісність (тенденція до стійкості) та розвиток (тенденція до зміни). Внаслідок руйнування або перекручування цих рис особистість перестає існувати як соціальний суб'єкт. Це означає, що будь-який інформаційно-психологічний вплив на особистість має оцінюватися з позиції збереження чи руйнування її як цілого [416,с.76-88].

В інформаційному суспільстві, на кожному етапі його становлення і розвитку, інформаційно-психологічні впливи збільшуються і поглиблюються. А людська психіка має певні обмеження. Експериментально доведено, що мозок звичайної людини здатен сприймати і безпомилково обробляти інформацію зі швидкістю не більше 25 біт на секунду (в одному слові середньої довжини міститься якраз 25 біт). При такій швидкості поглинання інформації людина за життя може прочитати не більше трьох тисяч книг, за умови, що буде щодня освоювати по 50 сторінок [529].

У той же час сьогодні лише у науковій сфері щорічно з'являється кілька мільйонів книг. Фахівці ввели визначення «макулатурного фактору» для літератури, яка користується нульовим попитом. Німецькі дослідники провели в одній із берлінських бібліотек вивчення попиту на 45 тисяч наукових і технічних видань, які зберігаються в ній. І з'ясувалося, що «макулатурний фактор» спрацював практично для 90 % книг [529]. Значна частина інформації, яка накопичується, швидко застаріває і вимагає заміни. Професійні знання в середньому застарівають за 3-4 роки (потребують оновлення) [416,с.76-88]. Тобто, на момент отримання диплому про вищу освіту, окремі знання з першого курсу навчання можуть бути неактуальними.

Вперше над цим фактом замислились вчені у 70-х роках минулого століття. Тоді і з'явився термін «інформаційний вибух», який означав «лавиноподібне збільшення кількості публікацій у наукових журналах». З'явилися прогнози кінця науки, оскільки вчений втрачає за таких умов відстежувати розвиток його галузі. Згодом термін «інформаційний вибух» почали розглядати під ще одним кутом – непотрібність переважної кількості накопичених людством знань для пересічної людини.

Крім того, виникає і питання якості, адже велика частина всієї людської інформації – нескінченне дублювання одного і того ж з незначними змінами. Особливої уваги заслуговує питання академічної доброчесності і плагіату. Однією з причин його появи є зростаюча кількість творців контенту.

Інформаційне перевантаження «information overload» - термін, що описує труднощі розуміння проблеми і прийняття рішень, причиною якої є надлишок інформації. Поняття згадується в книзі Б. Гросса «Управління організацією» [592] (1964 р.), але популяризував його Е. Тоффлер у своєму бестселері «Шок майбутнього» (1970 р.) [656]. Термін і концепція передували виникненню мережі і становлення інформаційного суспільства.

В останні роки термін "інформаційне перевантаження" модифікувався в «надлишок інформації» (information glut) та «смогу даних» (data smog). Термін, який раніше мав місце в межах когнітивної психології, перетворився в метафору широкого вжитку, яку використовують далеко поза академічними колами. Значним чином, поява інформаційних технологій посилила інформаційне перевантаження: інформаційні технології можуть стати основною причиною інформаційного перевантаження через їх здатність виробляти додаткову інформацію швидше і поширити цю інформацію до широкої аудиторії, ніж будь-коли раніше [579].

Інформаційне перевантаження має не лише психологічні, а й фінансові наслідки. За підрахунками Н. Зельдеса компанія Intel понесла майже в 1 мільярд доларів збитків через зниження ефективності роботи, у вигляді часу, витраченого на обробку непотрібних повідомлень електронної пошти і відновлення від інформаційних втручань. Дослідження Microsoft виявили, що для повернення до виконуваного завдання після перевірки електронної пошти пересічному працівнику необхідно в середньому 24 хвилини [595].

Тобто, якщо говорити про прийдешню соціально-економічну формацію, з тотальними об'ємами різного характеру та сутності інформації, то сучасна людина, просто не готова до цього, її мозок ще не в змозі адекватно реагувати та опановувати такі масиви інформації. З цього приводу влучним є висловлювання наведене у Всесвітній доповіді ЮНЕСКО «До суспільства знань»: «В сучасних

інформаційних потоках, знайти необхідну інформацію, аналогічно до спроби напиться із пожежного крану – води виставить, але треба примудритись не захлинутися» [658]. Звісно, ІКТ фільтрують інформацію, проте, вони не можуть забезпечити рівня фільтрування яким володіє людський мозок.

Надзвичайно важливими з точки зору гарантування інформаційної безпеки людини є володіння достатніми знаннями щодо власних прав і свобод, способів їх реалізації та захисту. Не можна оминати увагою, що в умовах існування відкритих, легкодоступних і легко наповнюваних інформаційних мереж існує проблема дотримання прав і свобод людини в мережевому просторі, зокрема питання обмеження інформації, що вважається соціально чи/і економічно небезпечною, проблема безпеки персональних та інших видів даних, проблема дотримання авторських прав та прав виробників електронної інформації тощо. Заслуговує на увагу думка Городенко Л. М. щодо інформаційного розриву, що виникає щодо свободи поглядів, висловлювань та вільних трактувань [98]. Мережеві форми спілкування уможливили свободу висловлювань, наукового пошуку й творчої діяльності, а також гарантували і продовжують гарантувати можливість створення вільного комунікаційного поля, в якому відбувається обмін знаннями, проходять публічні дебати. Свобода висловлювань, властива мережевим комунікаційним формам, визначає зв'язки, що об'єднують індивідів у життєздатне товариство. Позатериторіальний характер мережових комунікацій сприяє поширенню будь-якої інформації, починаючи від пліток і закінчуючи засекреченими відомостями.

В 1999 р. журналістами BBC чи не вперше було вжито категорію «Cyber rights and cyber liberties», а також «digital freedom»<sup>16</sup>, коли йшлося про необхідність змін в правовому регулюванні відповідно до технологічного розвитку, зокрема, спів розмірного захисту даних на фізичних носіях та в електронній формі [563]. Термін «кіберправо» прижився в англomовному середовищі (поруч з поняттям «кібербезпека») для означення галузі права, що регулює відносини, пов'язані з використанням інтернету, також комп'ютерів, програмного і апаратного забезпечення, інформаційних систем тощо. А термін

---

<sup>16</sup> Кіберправа і кіберсвободи, цифрова свобода



цифрових прав закріпився за означенням суб'єктивних можливостей людини щодо використання цифрових технологій.

На сьогодні існує два основних підходи до розуміння категорії цифрових прав. Перший, цифрові права — це розширення і застосування універсальних прав людини до потреб суспільства, заснованого на інформації [566]. На користь такої позиції свідчить резолюція A/HRC/32/L.20 Генеральної Асамблеї ООН, яка підтверджує, що ті ж самі права, які людина має в офлайновому середовищі, повинні також захищатися в онлайновому середовищі, зокрема, свобода вираження думок, яка може бути застосована незалежно від кордонів і в рамках будь-яких обраних людиною засобів масової інформації, відповідно до статей 19 Загальної декларації прав людини і Міжнародного пакту про громадянські і політичні права [317]. Ця норма фактично повторює визначену 6 грудня 2012 р. в Резолюції L13.

У більш вузькому розумінні під цифровими правами розуміють права людини, які дозволяють отримувати доступ, використовувати, створювати та публікувати цифрові твори, або право доступу і використання комп'ютерів, інших електронних пристроїв або мереж зв'язку.

І в одному, і в другому тлумачення одним із базових цифрових прав вважається право на доступ в інтернет. Коли було підписано вище згадану резолюцію ГА ООН, такі країни, як Росія, Китай, Саудівська Аравія, Південна Африка та Індія, висловились проти. Вони, зокрема, вимагали вилучити з тексту фрагмент, у якому йдеться про “засудження заходів з обмеження та блокування доступу до розміщеної в мережі інформації” [504].

Серед положень цієї резолюції слід звернути увагу на заклики до всіх держав: «боротися з проблемами безпеки "таким чином, щоб забезпечити свободу та безпеку в інтернеті; забезпечити відповідальність за всі порушення прав людини та зловживання, вчинені проти осіб у зв'язку з реалізацією їх прав людини, визнавати, що конфіденційність в інтернеті є важливою; наголошувати на важливості освіти жінок та дівчат у відповідних технологічних галузях» [606].

В кількох країнах світу офіційно визнано право на доступ до інтернету (право на доступ до інформації в інтернеті) і / або заборонено державі

необґрунтовано обмежувати доступ людини до інформації та інтернету. В різний спосіб – шляхом визначення в законах, визнання рішенням Конституційного чи Верховного Суду це право закріплено у понад 10 країнах світу, наприклад, у Фінляндії, Естонії, Франції, Греції, Іспанії, Коста-Ріці.

Була спроба закріпити на законодавчому рівні це право і в Україні. У 2014 р. було запропоновано внести зміни до Цивільного кодексу України, які б гарантували право фізичної особи на доступ до інтернету та встановлювали умови його обмеження [390]. Законопроект не був розглянутий навіть в першому читанні.

Слід розуміти, що право на доступ до інтернету не має на меті лише фізичну можливість доступу до мережі інтернет. Воно базується на комунікаційній цінності інтернету, що передбачає зв'язок цього права із іншими правами і свободами людини та необхідність доступу до інтернету для їх реалізації, зокрема, свободи думки, вираження поглядів та переконань, права на розвиток, політичних прав, екологічних та інших основних прав людини.

Право людини завжди передбачає кореспондуючий обов'язок держави – забезпечити доступ до інтернету належної якості і відповідної ціни, а також не обмежувати без законних підстав доступ осіб до інтернету [620]. Тобто визнаючи це право людини держава зобов'язується створити відповідну інфраструктуру, забезпечити адекватність цінової політики на такі послуги, забезпечити рівні можливості доступу всім індивідам (незалежно від місця проживання, стану здоров'я, віку тощо), створити інші правові і організаційні гарантії реалізації цього права. Мукомела І.В. звертає увагу на ще один важливий аспект цього права - компетенцію населення, звертаючи увагу на її асиметрію в Україні [263].

Проте цифрові права не обмежуються правом на доступ до інтернету. Асоціацією прогресивних комунікацій<sup>17</sup> ще у 2001 р. було розроблено Хартію інтернет прав. Хартія присвячена таким темам як: доступ в інтернет для всіх; свобода вираження думок і асоціацій (зібрань); доступ до знань; спільне навчання

---

<sup>17</sup> Association for progressive communications - це, водночас, мережа і організація, членами якої на квітень 2017 р. було 51 членів-організацій та 30 індивідуальних членів з 75 країн світу. Місія APC: «Всі люди мають легкий та доступний доступ до безкоштовного та відкритого Інтернету для покращення свого життя та створення більш справедливого світу.» <https://www.apc.org/>

і творчість на основі вільного і відкритого програмного забезпечення і розробки технологій; недоторканність приватного життя, спостереження та шифрування; управління інтернетом; обізнаність, захист і реалізація прав.

АПК заявляє, що "можливість обмінюватися інформацією і спілкуватися вільно використовуючи інтернет має життєво важливе значення для реалізації прав людини, закріплених у Загальній декларації прав людини, Міжнародному пакті про економічні, соціальні і культурні права, Міжнародному пакті про громадянські і політичні права та Конвенції про ліквідацію всіх форм дискримінації щодо жінок [204].

К. Беккер, австрійський теоретик інформаційного антиглобалізму, вважає, що «основні цифрові права людини охоплюють право доступу до мережі, право вільно спілкуватися і висловлювати думки в мережі, і право на недоторканність приватної сфери» [539]. Водночас, він звертає увагу на те, що всі інформаційні і комунікаційні технології мають походження з військової промисловості і в сучасних умовах отримали розвиток в якості технологій «несмертельної зброї». Отримання доступу до цих засобів і контролю над ними зі сторони урядів, корпорацій та інших структур може становити загрозу. Тому реалізація цифрових прав людини покликана забезпечити кожному можливість безкоштовно і необмежено користуватися цими засобами і їх потенціалом[539].

Питання обмеження доступу до інформації, в тому числі до інтернету, останні понад десять років постійно мають місце в судовій практиці розвинених країн світу.

Прецедентом стало рішення ЄСПЛ, винесене на користь заявника у справі А. Йилдіріма проти Туреччини (Yildirim v. Turkey), де суд зазначив, що «інтернет став одним із основних засобів здійснення права на свободу вираження поглядів та свободи інформації».

В Україні, після введення в дію Указом Президента Рішення РНБО України «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» [351], було розглянуто низку справ щодо порушення цим рішенням прав і свобод людини. Зокрема, у постанові Вищого адміністративного суду України від 14 червня 2017 р. по справі № 800/198/17

[322] щодо порушення права на свободу вираження поглядів у відповідності зі статтею 10 Конвенції про захист прав людини та основоположних свобод, а також порушення права позивача на свободу доступу до інформації, було відмовлено у задоволенні позову щодо визнання недійсними положень цього акту, які встановлювали заборону на певний період здійснювати надання послуг з доступу користувачам мережі до ресурсів певних російських сервісів.

Серед аргументів суду має місце посилення на Закон України “Про інформацію”, зокрема ч. 2 ст. 6, де визначено, що право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров’я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Ч. 2 ст. 7 цього Закону також передбачено, що ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом.

Доступ до інтернет може бути обмежений в різний спосіб і з різною метою. Єдиною країною, де на законодавчому рівні заборонено доступ до інтернет є Китай. За результатами досліджень Комітету захисту журналістів<sup>18</sup> та деяких інших досліджень обмежено доступ до мережі жителям таких країн як Туркменістан – інтернет недоступний для більшості громадян, підключення до мережі коштує в кілька разів більше середньої заробітної плати; єдиний сервіс-провайдер - уряд, який, до того ж, блокує дуже багато сайтів, веде стеження за всіма обліковими записами своїх громадян в таких поштових сервісах, як Gmail, Yahoo, Hotmail і інші; сайти, що належать правозахисним організаціям (міжнародним або інших країн) блокуються, як і сайти великих інформаційних агентств; В’єтнам - влада цієї країни запитує інформацію в Yahoo, Google, Microsoft про громадян своєї країни, які працюють з сервісами вказаних компаній; урядом створено спеціальний орган для моніторингу роботи громадян своєї країни в інтернеті, в т.ч. розміщення контенту, спілкування по електронній пошті;

---

<sup>18</sup> Комітет захисту журналістів (Committee to Protect Journalists (CPJ)) - міжнародна неурядова організація зі штаб-квартирою в Нью-Йорку, що займається захистом прав журналістів.

блокуються сайти, які не влаштовують уряд; Туніс - провайдери зобов'язані звітувати перед урядом про громадян, які регулярно працюють в мереж; база блогерів, їх імен, паролів, адрес, особистих даних ведеться провайдерами і передається у відповідні урядові служби на регулярній основі; міжнародний трафік контролюється урядом; блокуються тисячі веб-сайтів, які не влаштовують уряд; заборонені торренти і інші види файлообміну; Китай – має чи не найбільш розвинену програму по цензурі мережі у світі; провайдери зобов'язані блокувати сайти, які не бажані уряду, знищувати відповідний контент і вести контроль за поштовим трафіком; заборонені низка соцмереж; Іран – переслідується критика уряд або релігійних діячів, блогери зобов'язані реєструватись в Міністерстві мистецтва і культури; блокуються сайти, де критикується режим правління, а також особливо контролюються сайти організацій захисту прав жінок; Саудівська Аравія – урядом блокується сайти понад 400 тисяч сайтів політичної, соціальної і релігійної тематик; Куба - інтернет важкодоступний, поширеним є користування через урядові точки доступу, де ведеться моніторинг за кожним IP; фільтрується контент, перевіряється історія роботи в мережі; завантажувати контент в мережу дозволено обмеженому колу осіб, наприклад, блогерам і чиновникам, які підтримують режим; Бірма - інтернету практично немає, існуючі точки доступу дуже жорстко контролюються урядом, включаючи електронну пошту, блокуються сайти, де є хоча б найменша згадка про права людини; ті, що належать політичній опозиції (ці сайти розміщуються і наповнюються за межами Бірми); Північна Корея - доступ до мережі має близько 4% населення, серед яких в основному військові та чиновники; для інших існує «Кванмен» — внутрішня закрита мережа; блогінг заборонений, а весь завантажений контент перевіряється відповідними службами безпеки; Саудівська Аравія - цензурі піддається книговидавництво, ЗМІ і доступ в інтернет, весь інтернет-трафік в королівстві проходить через систему проксі-серверів, розташованих в науково-технологічному центрі імені короля Абдулазіза; в країні існує спеціальна Комісія з комунікацій та інформаційних технологій, яка здійснює блокування ресурсів, в т.ч. за персональними заявками громадян; Ефіопія – має низький % інтернет-користувачів - всього 4% населення країни; монополія держави на телеком-послуги, нерозвинена інфраструктура і

політика заборони на розвиток телекомунікацій призвели до неадекватних цін, окрім того мережі повністю відсутні в сільській місцевості, де проживає 85% населення країни; присутня цензура і переслідування за необережні висловлювання.

Неможливо в межах однієї праці розглянути і проаналізувати так значний обсяг питань. Зокрема, поза увагою авторка свідомо залишила питання реалізації політичних прав в умовах е-демократії і засилля політтехнологій, заснованих на маніпуляції інформацією; співвідношення свободи слова і права на захист від шкідливої інформації; трудові права і соціальний захист в умовах віддаленої праці та фрілансерства; свободи совісті і права на національну самоідентифікацію в умовах глобального інформаційного простору та багато інших.

### **3.2. Особливості правового забезпечення інформаційної безпеки окремих категорій осіб**

Оскільки інформаційна безпека людини базується не лише на її захищеності від інформаційних загроз, але й передбачає можливість людини як біологічного організму і соціальної істоти функціонувати, розвиватись і досягати бажаних для себе результатів в інформаційному суспільстві. Сучасні міжнародно-правові акти передбачають обов'язок держав створити рівні можливості для захисту своїх прав онлайн в тій самій мірі, що і в реальному просторі. Комітет Міністрів Ради Європи в Рекомендації CM/Rec (2014)6 [397] зазначає, що існуючі права людини та основні свободи в рівній мірі відносяться як до оффлайн, так і до онлайн простору. Ніхто не повинен бути об'єктом незаконного втручання в здійснення прав людини та основних свобод під час перебування в інтернеті.

Швидкі темпи поширення і популярність інтернету пояснюються світоглядними установками інформаційного суспільства. Інтернет відповідає ціннісним очікуванням сучасної людини: доступність, необмеженість, варіативність, тиражування, оперативність. При цьому різні категорії осіб знаходяться у неоднакових умовах щодо можливості реалізації своїх прав і свобод в інформаційній сфері, зокрема, відрізняється ступінь захищеності в інформаційному суспільстві, види і інтенсивність небезпек, що їм загрожують.

Серед об'єктів інформаційної безпеки можна виокремити категорії, що характеризуються наявністю спільних інформаційних загроз їх безпеці і необхідністю особливого правового забезпечення. Зокрема, в цьому дослідженні спробуємо звернути увагу на наступні:

- 1) окремі вікові групи: насамперед, діти, підлітки і молодь, а також люди похилого віку;
- 2) люди з обмеженими фізичними можливостями, особливостями інтелектуального розвитку та психічними порушеннями,
- 3) люди, що здійснюють діяльність, яка має або може мати важливі соціальні наслідки – державні службовці, медійні особи та журналісти, правозахисники, громадські активісти і політичні діячі тощо;
- 4) населення окремих регіонів країни чи населених пунктів, що володіє специфічними соціокультурними особливостями, в т.ч. релігійними, етнічними, мовними, демографічними;
- 5) люди, що пов'язані з військовими діями на сході України – військовослужбовці, їх сім'ї, а також сім'ї загиблих, населення окупованих територій, «сірої» зони, внутрішньо переміщені особи тощо.

Цей перелік не є вичерпним, його метою є окреслення межі предмету дослідження.

**Діти, підлітки і молодь.** За даними досліджень 2011 р. в США близько 80% дітей у віці до 5 років користувались інтернетом щотижня, більшість дітей проводило принаймні три години на день, дивлячись телевізор, а час загалом витрачений на медіа дітьми дошкільного віку становив 47%. Також зазначається, що 36% дітей у віці від 2 до 11 років одночасно використовують обидва засоби. Загалом, діти у віці від 8 до 10 років щодня проводять близько 5,5 годин використовуючи носій [647].

Використання домашнього інтернету зростає з віком. Кожен з трьох дітей віком від трьох до п'яти років використовує інтернет вдома, у порівнянні з 54% 6-11-річних та 72 % з 12-17-річних. Компанія, що пропонує онлайн послуги щодо захисту дітей від небажаного вмісту мережі «Guardchild» наводить на своїй сторінці результати багатьох досліджень наукових установ і соціальних

інституцій США: 21% дітей дошкільного віку мають доступ до стільникових телефонів, 90% дітей у віці 8-16 років бачили онлайн порнографію, 70% дітей віком від 7 до 18 років виконуючи домашнє завдання натикалися на порнографію в мережі, 31% підлітків у віці 12-18 років завідомо неправильно вказали свій вік, щоб отримати доступ до сайтів з віковими обмеженнями, 95% батьків не знають/не розуміють онлайн сленгу чи скорочень, що використовують їх діти, кожен п'ятий з підлітків у віці отримував повідомлення з пропозиціями сексуального характеру, а 1 з 33 – були переслідуваними в мережі, 65% 8-14 річних були втягнені в кібербулінг<sup>19</sup>, 69% підлітків регулярно отримуючи повідомлення від незнайомих людей не повідомляють про це батькам чи опікунам [593].

Відповідні актуальні статистичні дані щодо України виявилось знайти досить складно. Всеукраїнське соціологічне дослідження, проведене Інститутом соціології НАН України в 2009 р., виявило тривожні тенденції: понад 28% опитуваних дітей готові надіслати свої фотокартки незнайомцям у Мережі; 17% без коливань діляться інформацією про себе і свою родину (адреса, професія, графік роботи батьків, наявність цінних речей у домі тощо); 22% дітей періодично потрапляють на сайти для дорослих; 28% дітей, побачивши в інтернеті рекламу алкоголю або куріння, хоча б один раз спробували їх купити, а 11% – спробували купувати наркотики; близько 14% опитуваних час від часу відправляють платні SMS за бонуси в онлайн-іграх і лише деякі звертають увагу на вартість послуги. Лише у 18% випадків дорослі перевіряють, які сайти відвідує дитина, тільки 11% батьків знають про такі онлайн-загрози, як “дорослий” контент, азартні ігри, онлайн-насилля, кіберзлочинність [38].

Комітет ООН з прав дитини у 2011 р. відзначив, що відвідування порнографічних сайтів становило 70% усього трафіку на території України, а 5 млн. українських користувачів на місяць цікавляться дитячою порнографією. Департамент молоді Ради Європи у 2012 р. провів онлайн-опитування щодо досвіду молоді, пов'язаного з мовою ворожнечі в інтернеті. За його результатами

---

<sup>19</sup> умисні образи, погрози, дифамації і повідомлення іншим даних, що компрометують за допомогою сучасних засобів комунікації, як правило, протягом тривалого періоду часу.



69% не знають, де можна отримати допомогу жертві мови ворожнечі онлайн, 78% респондентів не отримували освіти щодо безпечної поведінки в інтернеті [264]. За даними міжнародної асоціації «INHOPE», видалення матеріалів сексуального зловживання над дітьми в інтернеті допомагає попередити їх подальше перетворення в жертву злочинних посягань. Профайл жертв розміщення матеріалів сексуального характеру у 2014 р. виглядав таким чином: юнацтво – 21% (у 81% випадках жертвами стають дівчата), підлітки – 72% (у 13% випадків жертвами стають хлопці діти), 7% (у 6% випадків – діти обох статей) [604].

Водночас, незалежно від країни чи частини світу діти і молодь вважають інтернет невід’ємною частиною свого життя, благом, навіть якщо воно дороге, недостовірне або доступне лише за допомогою спільних пристроїв (як наприклад у деяких країнах Африки). Всесвітнє опитування показує, що діти вважають його правом людини, необхідністю [600]. З урахуванням віку діти та молодь мають право на особливий захист і консультування при користуванні інтернетом. «Це означає, що: 1. право на вільне вираження своїх поглядів та участь у житті суспільства, на те, щоб бути почутими та вносити свій вклад у вирішення питань. Поглядам повинна приділятися належна увага з урахуванням вашого віку, ступеня зрілості та без дискримінації; 2. можливість очікувати на отримання інформації мовою, що відповідає віку, а також на навчання безпечному користуванню інтернетом, в тому числі щодо захисту вашого приватного життя, з боку вчителів, вихователів, батьків чи опікунів; 3. обов’язок знати, що контент, який створюєте в інтернеті, або контент про дитину, що створюється іншими інтернет-користувачами, може ставати доступним у будь-якому куточку світу і завдавати шкоду гідності, безпеці, приватному життю або іншим чином шкодити особі та її правам у цей час або на наступних етапах життя. На запит такий контент повинен бути вилучений або видалений протягом розумно короткого періоду часу; 4. можливість очікувати на отримання чіткої інформації про те, який онлайн-контент та поведінка є незаконними (наприклад, домагання в інтернеті), а також мати можливість повідомити про потенційно незаконний контент. Така інформація має бути адаптована до віку та обставин, а також повинні надаватись поради та підтримка з належною повагою до конфіденційності та анонімності; 5.

повинен надаватися спеціальний захист від втручання у фізичне, психічне та моральне благополуччя, зокрема, захист від сексуальної експлуатації та насильства в інтернеті та від інших форм кіберзлочинності. Крім того, право на освіту, яка покликана захистити від подібних загроз» [397].

Таким чином, виникає суперечлива ситуація. З одного боку, права дитини на доступ до інформації, на вільний розвиток, персональні дані тощо, з іншого – необхідність забезпечити захист від кіберзагроз та інформаційну безпеку дитини, в цілому. Хто і якою мірою має за це нести відповідальність? Англійська дослідниця С. Лівінгстон [619], підкреслюючи, що один з трьох користувачів інтернету є дитиною, наголошує, що із зростанням технологій дитячі організації, представники приватного сектору, регулюючі органи мають опікуватись тим, що права дітей потребують такої ж реалізації онлайн, як і оффлайн. Права дитини, викладені в Конвенції ООН прав дитини, дослідниця застосовує до онлайн середовища.

Серед загроз з якими дитина зіткнутись при використанні комунікаційних технологій можна виокремити такі: технологічні: загроза як для дітей, так і для дорослих користувачів; доступ до інформації з неприйнятним (часто незаконним) змістом, зокрема, порнографічні, такі, що пропагують наркотики, психотропні речовини й алкоголь, тероризм і екстремізм, ксенофобію, сектантство, національну, класову, соціальну нетерпимість, нерівність, асоціальну поведінку, насилля, агресію, суїцид, азартні ігри, інтернет-шахрайство [234], розголошення персональних даних та іншої конфіденційної інформації, як власної, так і членів сім'ї, друзів чи знайомих, контакт з незнайомцями, що може призвести наслідків як у віртуальному (кібербулінг, дитяча порнографія тощо), так і реальному житті (сексуальне використання, фізичні ушкодження, викрадення).

Не слід залишати поза увагою те, що інформаційна безпека, це не лише кібербезпека і не обмежується безпечним перебуванням у віртуальному просторі. Реалізація численних прав і свобод дитини в сучасному суспільстві залежить від гарантування дотримання її інформаційних прав. Зокрема, це стосується права на рівень життя, необхідний для їх розвитку, права дітей на вираження своїх

поглядів, право на існування власного майна, на свободу думки, совісті і релігії, асоціацій і мирних зборів, доступ дитини до поширення інформації, освіти, користування рідною мовою і культурою, сповідування своєї релігії, відпочинок і дозвілля.

Чи можливим є регулювання взаємодії між медіа і дітьми? Протягом другої половини століття телебачення суворо звинувачувалося в поширенні багатьох соціальних хвороб, тепер цей акцент перенесено на інтернет. Сучасні медіа переважно знаходяться в комерційному використанні, а отже основним регулюючим фактором є фінансовий. Ресурси, які раніше були призначені виключно для дорослих, тепер часто є доступними дітям.

Глобалізаційні процеси в першу чергу в мережевому просторі дозволяють уникати регулювання національним законодавством. Подібною є ситуація щодо телебачення і радіомовлення. Оскільки аудіовізуальні технології спрямовані на сумісність з новими медіа<sup>20</sup>, національні регулятори стикаються з практично нереальними для вирішення завданнями - класифікації, обмеження або планування всього того, що з'являється на екранах країни, а тим більш не мають можливості впливу на споживачів. Виходячи із специфіки дитячого віку, слід сказати, що у профілактичній роботі з даною групою велике значення мають, насамперед, заходи не правового характеру, а педагогічні, психологічні, медичні [74, с.69].

Дослідження свідчать, що з точки зору батьків, ті фактори, які ускладнюють державне регулювання нового медіа-оточення, тягнуть за собою аналогічні складності і для батьків [619]. Батькам було складно відстежувати і впливати на зміст того, що переглядали їхні діти вдома чи у своїх друзів в епоху телебачення. Тим більш, це завдання ускладнилось в епоху інтернету і портативних технологій («гаджетів»). Таким чином, визначення змісту контенту, що споживають діти, виходить за межі можливостей батьківського контролю. Крім цього, як свідчать знову таки дослідження, значна кількість батьків не до кінця розуміють сенс комп'ютерних ігор та сторінок в інтернеті, якими користуються їхні діти.

---

<sup>20</sup> Інтерактивні електронні засоби масової комунікації, засновані, переважно, на технологіях Web 2.0.

На сторінці Майкрософт розміщені правила безпечного користування інтернетом. «Оскільки дорослі самостійно вирішують, який рівень конфіденційності потрібно забезпечити дітям, цей список рекомендацій містить орієнтовні правила користування комп'ютером, зокрема: відстежуйте використання інтернету; попросіть дітей ніколи не надавати особисті відомості, як-от ім'я, місцезнаходження, зображення, паролі, номери телефонів тощо; використовуйте програмне забезпечення для батьківського контролю; дозволяйте дітям переписуватися та спілкуватися лише з тими людьми, яких ви знаєте; розмовляйте з дітьми про незручні або неприємні ситуації в інтернеті; розкажіть дітям, що не слід відповідати на неочікувані або небажані повідомлення електронної пошти; пам'ятайте про те, що практично нічого в інтернеті не є повністю приватним» [37].

Існує думка, оскільки «інтернет здебільшого є продуктом приватних компаній, то реалізація та порушення прав людини в інтернеті має трьохсторонній характер: людина-приватна компанія (провайдер інтернет-послуг чи інтернет-доступу тощо) - держава» [503]. Така позиція, на нашу думку не є однозначною, оскільки гарантування прав і свобод на національному рівні залишається обов'язком держави, тому числі створення належного правового і організаційного забезпечення для їх реалізації. Тоді як зі сторони юридичних і фізичних осіб очікуваною і бажаною поведінкою є дотримання існуючих правових норм, не порушення прав інших учасників правовідносин та виконання покладених на них обов'язків.

Повертаючись до питання щодо інформаційної безпеки дітей та молоді, важливо відзначити необхідність формування належного рівня інформаційної культури, в тому числі опанування навичок критичного мислення, культури безпечної поведінки в інформаційному просторі. Важливим учасником цього процесу є держава, оскільки саме вона через уповноважені органи встановлює зміст навчальних програм, форми навчання і забезпечує підготовку педагогічних кадрів.

Водночас аналіз листів МОН та регіональних органів виконавчої влади у сфері освіти, зміст яких присвячений проблемам інформаційної безпеки: Листи

МОН України "Про захист дітей та молоді від негативних інформаційних впливів", «Про проведення дня безпечного інтернету», «Про проведення конкурсу «Онляндія в моїй школі» свідчить про їх популістський і декларативний характер.

Основним завданням взаємодії батьків, соціальних інституцій і держави в процесі навчання і виховання підлітків з питань інформаційної безпеки повинно бути формування у них інформаційно-комунікаційних компетентностей щодо користування інтернетом. Зокрема серед таких компетентностей слід виділити: 1. Грамотний і успішний пошук інформації: розпізнавання інформаційних потреб; формулювання питань, що відображають інформаційні потреби; знання про існування багатьох інформаційних джерел; пошук, вибір і оцінка інформаційного джерела; зберігання інформації. 2. Критична оцінка інформації: розуміння змісту інформаційного повідомлення; вибір і оцінювання інформації; прийняття рішення про те, що є фактом, а що точкою зору; вирізнення рекламних текстів. 3. Творення, перетворення і презентація інформаційного змісту: творення нового інформаційного змісту; перетворення знайденого в інтернеті або раніше самостійно створеного інформаційного змісту; презентація нового або перетвореного інформаційного змісту. 4. Правові засади творення й поширення інформаційного змісту: усвідомлення правового й етичного вимірів творення інформації; знання, який інформаційний зміст можна перетворювати відповідно до правових засад; знання своїх прав як творця інформації, розміщеної в інтернеті; усвідомлення різниці між інтернет-комунікацією й спілкуванням поза інтернетом. 5. Емпатія й образотворення: знання про те, що інтернет є простором спільної комунікації з іншими людьми; виявлення емпатії в мережі; створення обдуманого й адекватного власного образу. 6. Безпека і приватність: знання про загрози, пов'язані з перебуванням в інтернеті; уміння запобігти небезпекам в інтернеті; здійснення контролю над інформацією, яка передається іншим; усвідомлення різниці між інтернет-комунікацією й спілкуванням поза інтернетом; застосування гігієнічних засад, пов'язаних з використанням комп'ютера. 7. Участь у соціальних електронних мережах: розпізнавання елементів інтернет-культури; активна участь у мережних соціальних спільнотах; ініціативність в розвитку мережних соціальних спільнот, створених для спільних дій [228].

Важливим є створення умов для співпраці батьків та осіб, що їх замінюють, з відповідними органами, що можуть надавати допомогу у випадку актуалізації загроз інформаційній безпеці дітей. Досвід такої допомоги є різний – від створення відповідних підрозділів поліції до сприяння громадським організаціям, які забезпечують роботу інфоліній у випадку виникнення загрози (наприклад, при кібербулінгу чи кібермоббінгу), відслідковують дитячу порнографію онлайн і повідомляють уповноважені органи, а також здійснюють просвітницьку роботу як серед дітей та молоді, так і для батьків та осіб, що ними опікуються.

Процес комп'ютеризації шкіл, що відбувається сьогодні, безперечно, є прогресивним явищем, але без відповідної методичної підтримки, без перепідготовки учителів-предметників, без інтеграції комп'ютерних технологій у навчальний процес не буде забезпечено належного їх використання. Використання технологій мультимедіа при викладанні всіх шкільних дисциплін дозволить підвищити якість засвоєння знань, а також зростання рівня індивідуалізації навчання, що є особливо важливим для дітей з особливими потребами.

За оцінками Всесвітньої організації охорони здоров'я, понад 1 мільярд людей мають якусь форму інвалідності, а це майже 15% населення світу. В Україні понад 2 мільйони 800 тисяч людей мають статус інваліда, з них 151 тисяча – діти. Це 6,1 відсотка до загальної кількості населення. І майже 80 % інвалідів – це люди працездатного віку. **Особи з обмеженими фізичними можливостями, особливостями інтелектуального розвитку та психічними порушеннями** часто бувають виключені з повноцінного життя, зіштовхуючись з дискримінацією різних форм, включно з фізичними і соціальними бар'єрами.

Поняття повноправного члена суспільства, яке є результатом соціалізації, має на увазі, перш за все, визнання членами суспільства іншого як рівного [142, с.184-187]. Інформаційні технології мають значний потенціал для покращення якості життя багатьох людей з обмеженими можливостями. Водночас, можуть стати бар'єром, для прикладу, якщо сторінка має занадто дрібний шрифт, інформація на ній недоступна людям з вадами зору; відсутність написів адаптованих для скрін-рідерів - додатків, які озвучують текст на екрані – стає перешкодою для незрячих

людей; якщо сторінка не містить транскрипти аудіофайлів – інформація недоступна для глухих і слабочуючих людей, це лише найочевидніші перешкоди.

Окрім того, що в суспільстві існує стереотипне мислення і велика проблема під назвою ейблізм<sup>21</sup> [618], то ще й категорія «нормальності» викликає поділ на тих, хто є «нормальним», і тих, хто «нормальним» не є, - поділ на «ми» і «вони» і, як наслідок, аутгрупову гомогенність [589]<sup>22</sup>.

Дослідниця Енн Гібсон змогла нарахувати як мінімум 26 різних ситуацій, коли можливості людей обмежені і у них виникає потреба в доступному інтернеті, наприклад, «хтось впав і зламав пальці - тепер для навігації в інтернеті він може використовувати тільки ліву руку і клавіатуру; хворому на епілепсію, яка іноді викликається яскравими контрастними кольорами, потрібно з обережністю відвідувати сайти з яскравим дизайном; військовослужбовець, що служив на плавучому маяку і, як це трапляється з багатьма, став погано чути на одне вухо - він повертає голову в бік звуку на комп'ютері, але так йому складно бачити екран; а у батьків малих дітей немає фізичних обмеженостей, проте якщо їх більш ніж один, наприклад близнюки, яким по одному року, і це вже успіх, якщо, коли тримаючи когось із них на одній руці, залишається хоча б один вільний палець на іншій руці для навігації по iPad або включення Siri»[589].

У 1999 р. Консорціум Всесвітньої павутини, що займається розробкою єдиних принципів і стандартів для інтернету, створив список рекомендацій WCAG 1.0 (Web Content Accessibility Guidelines), спрямований на забезпечення доступності ресурсів Всесвітньої павутини для людей з обмеженими фізичними можливостями, у 2008 р. вийшла його друга версія рекомендацій WCAG 2.0. У жовтні 2012 р. WCAG 2.0 була прийнята Міжнародною організацією стандартизації як Міжнародним стандартом ISO, ISO / IEC 40500: 2012 [643].

---

<sup>21</sup> Від англ. Ableism — це системна дискримінація людей з хронічними захворюваннями та інвалідністю. Ейблізм характеризує людей, орієнтуючись тільки на їх порушення і ставить їх потреби на другий план, порівняно з іншими людьми. Саме через це, людям з інвалідністю приписують або навпаки відмовляють у певних навичках або рисах характеру.

<sup>22</sup> Ефект аутгрупової гомогенності проявляється в схильності бачити членів своєї групи як різноманітних індивідів, а члени чужій групи здаються нам схожими один на одного. В результаті ми уявляємо собі людей з обмеженими можливостями дуже типовим чином - сліпі з білою тростиною, глухі зі слуховими апаратами, люди на інвалідних візках.

Для осіб з обмеженими можливостями доступність - це можливість використовувати продукт або послугу так само ефективно, як це робила би здорова людина. Це означає, що потрібно використовувати принципи дизайну, які забезпечують доступність продуктів і послуг для більшої кількості людей. У деяких випадках це неможливо, тому для компенсації можуть використовуватися допоміжні технології. Якщо це так, поширені технології повинні забезпечувати безпроблемне програмне або апаратне підключення допоміжного пристрою, як в плані взаємодії, так і в плані портативності даних [127].

Знов таки, як і будь яка соціальна проблема, можливість реалізації прав і свобод людини з обмеженими можливостями в інформаційному суспільстві є комплексною, і її вирішення залежить від співпраці держави, громадянського суспільства, бізнес структур, міжнародного співтовариства і самої особи з обмеженими можливостями. При цьому кожному з них відведено власна роль. Для прикладу, бізнес-група по доступним ІКТ розробила Хартію за доступними технологіями в листопаді 2011 р.. Хартія містить 10 зобов'язань, які повинні дотримуватися корпорації, щоб доступність ІКТ була реалізована у всій організації, включаючи відділ кадрів, політики, поінформованість персоналу, зміни на робочих місцях і закупівлі. Першими цю хартію підписали 17 провідних компаній, включаючи Cisco, Fujitsu, Microsoft і Oracle [126]. Держави ж зобов'язані створити таке правове поле, в якому були б гарантовані права і можливості осіб з обмеженими можливостями. Як свідчить міжнародний досвід, це можливо реалізувати різними шляхами.

Наступна категорія - **люди, що здійснюють діяльність, яка має або може мати важливі соціальні наслідки** - є надзвичайно широкою і неоднорідною. Об'єднати державних службовців, медійних осіб та журналістів, правозахисників, громадських активістів і політичних діячів в одну групу з метою дослідження особливостей загроз їх інформаційній безпеці спонукало суспільна значимість їх діяльності. Адже кожен із них є публічною особою, має власну аудиторію, на яку чинить інформаційний вплив, а окрім того виконує важливу державну чи/та суспільну функцію.



На поверхні знаходяться конфлікти між правом публічних осіб на приватність та правом на свободу вираження поглядів, правом на захист персональних даних і правом доступу до публічної інформації тощо. Ця тема неодноразово досліджувалась в наукових працях, як вітчизняних, так і зарубіжних, існує низка судових прецедентів в національних судах та Європейському Суді з прав людини.

Питання балансу між правом на свободу вираження поглядів і захистом права на приватне життя є досить неоднозначним. [547]. Нагнічук О. І. на підставі аналізу практики Європейському Суді з прав людини<sup>23</sup> формулює принципи співвідношення права на свободу вираження та права на приватність щодо публічних осіб: 1) будь-яке втручання в приватне життя можливе настільки, наскільки це сприяє публічним дебатам з питань загальної важливості; 2) якщо зображення особи, яка вийшла на публічну арену, не містить інформації про її приватне життя, воно може використовуватися, незважаючи на те, чи є ця особа відомою; 3) особи, які стали публічними не з власного бажання, користуються більшим захистом приватного життя порівняно з іншими публічними особами; 4) публічні особи мають право бути захищеними від поширення пліток про їхнє приватне життя; 5) почуттям родичів і близьких померлої публічної особи може бути спричинено шкоду розголошенням конфіденційної інформації про публічну особу, але чим більше часу проходить після смерті публічної особи, тим більше суспільний інтерес в отриманні такої інформації перевищує необхідність конфіденційності такої інформації; 6) не може бути конфіденційною інформацією ставлення політиків до суспільних явищ; 7) комерційні питання не є сферою приватного життя публічної особи [265].

Водночас, право на доступ до інформації, якою володіють органи публічної влади, є основоположним правом людини, а також гарантією функціонування демократичної держави. Право на доступ до інформації вимагає від держави не

<sup>23</sup> Проаналізовані були справи *Cumpana and Mazare v. Romania* (App no 33348/96) ECHR 17 December 2004, *Tammer v. Estonia* (App no 41205/98) ECHR 06 February 2001; *Karhuvaara and Itälenti v. Finland* (App no 53678/00) ECHR 16 November 2004; *Standard Verlags GmbH. v. Austria* (2) (App no 21277/05) ECHR 04 June 2009. 12; *Thorgeir Thorgeirson v. Iceland* (App no 13778/88) ECHR 25 June 1992; *Edition Plon v. France* (App no 58148/00) ECHR 18 May 2004; *Crazy (2) v. Italy* (App no 45737/16) ECHR 17 July 2003; *Fressoz and Roire v. France* (App no 29183/95) ECHR 21 January 1999; *Társaság a Szabadságjogokért v. Hungary* (App no 37374/05) ECHR 14 April 2009.

утримання від втручання, а активних дій – забезпечення нормативних, організаційних та технічних умов реалізації права на інформацію, у тому числі належного розгляду запитів на інформацію та оприлюднення в ініціативному порядку суспільно важливої інформації.

Однак порушення балансу між цими правами призводить до виникнення загрози основним демократичним цінностям, адже право на доступ до інформації є правом інструментальним, тобто таким, що необхідне для реалізації інших прав і свобод людини, – без доступу до певної інформації, яка знаходиться в органів влади чи інших суб'єктів, людина часто не може реалізувати свої інші права (наприклад, на доступ до суду, участь у виборах та в управлінні державними справами, на освіту тощо).

Окрім того, діяльність осіб, яка має соціальне значення, створює значну кількість обставин, що стають передумовами для втручання в приватне спілкування, що здійснюється як санкціоновано – державними уповноваженими органами (право ініціювати таку діяльність мають Національна поліція, Державне бюро розслідувань, Служба безпеки України, Служба зовнішньої розвідки, Державна прикордонна служба, Управління державної охорони, Фіскальна служба, Національне антикорупційне бюро), так і неправомірно – журналістами, політичними опонентами та бізнес-конкурентами.

Згідно ст. 9 Закону України «Про телекомунікації» «охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантуються Конституцією та законами України. Зняття інформації з телекомунікаційних мереж заборонене, крім випадків, передбачених законом» [388, с.155]. При цьому на операторів, провайдерів телекомунікацій покладено зобов'язання вживати відповідно до законодавства технічних та організаційних заходів із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами (ч.3 ст.9).

Кримінально-процесуальним кодексом України передбачено, що для втручання у приватне спілкування необхідна ухвала слідчого судді. При цьому під спілкуванням розуміється передання інформації у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою засобів зв'язку будь-якого типу. Спілкування вважається приватним, якщо інформація передається та зберігається за таких фізичних чи юридичних умов, при яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб. Стаття 258 КПК України визначає різновиди втручання в приватне спілкування є: (1) аудіо-, відеоконтроль особи; (2) арешт, огляд і виїмка кореспонденції; (3) зняття інформації з транспортних телекомунікаційних мереж; (4) зняття інформації з електронних інформаційних систем [219].

Але навіть, за умови дотримання процедури втручання слід пам'ятати, що зняття такої інформації часто зачіпає права і законні інтереси третіх осіб. Важливими гарантіями захисту прав людини при здійсненні втручання в приватне спілкування є: дотримання принципу законності – як щодо процедури, так і щодо обґрунтованості винесенні суддею відповідної ухвали, надійне і обмежене в часі матеріалів, а також невикористання і негайне знищення матеріалів, що не стосуються справи і порушують права третіх осіб.

Прослуховування, фотографування чи відео зйомка є доступними і часто використовуються в незаконних цілях. Поширеним прикладом останнім часом стало фотографування в парламенті та поширення особистої переписки народних депутатів, переважна більшість таких даних не пов'язана з державницькою діяльністю депутатів, є їхньою конфіденційною інформацією. Більше того, поширення фотознімків такої переписки також часто шкодить третім особам, які спілкуються з депутатами, проте не перебувають на державних посадах (наприклад, журналістам, знайомим публічної особи) [319].

Не до кінця врегульованою з точки зору захисту прав третіх осіб залишається ситуація з оприлюдненням електронних декларацій. Безперечно, схема електронного декларування в Україні є важливим кроком у боротьбі з корупцією. Головними завданнями е-декларування є контроль і протидія незаконному збагаченню. Іншим аспектом е-декларування, на думку В. Чумака, є політичний, а

конкретніше той факт, що ці декларації депутатів можуть стати додатковою інформацією для виборців [109]. При цьому не слід забувати, що поруч з інформацією про осіб, уповноважених на виконання функцій держави або місцевого самоврядування, при поданні е-декларацій розкривається інформація їх членів сім'ї. Водночас, самі декларанти висловлювали побоювання, що «відкрите електронне декларування майна чиновників "дає пряму наводку для злочинців" та є питанням безпеки сотень тисяч людей» [528], а також що воно стало «інструментом тиску на суддів для того, аби схилити їх до прийняття тих чи інших рішень» [111].

Ще одна загроза що пов'язана з функціонуванням численних електронних реєстрів. Г. Колесник, голова комітету захисту прав адвокатів та гарантій адвокатської діяльності, зазначає, що через відкритий доступ до інформації про місце проживання або роботи, злочинцям набагато легше тиснути та здійснювати напади на адвокатів. «Кожен завдяки відкритим реєстрам може знайти домашню адресу адвоката. Крім ЄРАУ, де міститься інформація про місце роботи (в адвокатів, які провадять індивідуальну адвокатську діяльність, це домашня адреса), дані щодо проживання адвоката можна знайти, зробивши безкоштовний запит щодо пошуку відомостей в ЄРДР на сайті Мін'юсту (там адреси засновників адвокатських бюро та об'єднань). Та й в судових засіданнях зазвичай (з'ясовуючи особу) суд вимагає в адвоката вказати місце проживання, хоча у прокурора про це не запитують. Як результат, біля під'їздів та у власних квартирах на адвокатів учиняють напади.[408]»

Суперечливим щодо свободи вираження поглядів є намагання останнім часом нормативно регламентувати діяльність окремих груп осіб в соціальних мережах. Зокрема, Правила адвокатської етики доповнили розділом, що врегульовує поведінку в соцмережах та на інтернет-форумах. Відповідно до нових вимог при користуванні соціальними мережами адвокат повинен приймати до уваги обмеження, що встановлені для адвокатської діяльності в частині повноти та сприйняття інформації, забезпечення її конфіденційності та збереження. Адвокату слід обережно здійснювати адвокатську діяльність за допомогою соціальних мереж шляхом надання правової допомоги, професійних порад та

юридичних консультацій, адресованих та/або доступних необмеженому колу осіб. При користуванні соціальними мережами необхідно враховувати параметри їх конфіденційності з метою відповідального їх використання, моніторингу та регулярного аналізу власних соціальних мереж та контентів, що розміщуються в соціальних мережах. При виявленні в них помилок або будь-яких невідповідностей конфіденційності вони підлягають негайному виправленню та/або видаленню.

У соціальних мережах адвокатам рекомендовано обережно відноситись до коментарів, які можуть відображати позицію, що протилежна позиції клієнта. При встановленні адвокатом контактів та спілкування у соціальних мережах, інтернет-форумах та інших формах спілкування в мережі з клієнтами, колегами, суддями, процесуальними опонентами та іншими особами та їх об'єднаннями, він зобов'язаний виключити можливість виникнення конфлікту інтересів.

Висловлювання адвоката в соціальних мережах, інтернет-форумах та інших формах спілкування в мережі не повинні мати притаманний правовий нігілізм, будь-який вид агресії, ворожнечі і нетерпимості. Адвокат зобов'язаний вести себе шанобливо і не допускати образливої поведінки. Будь-які заяви, коментарі адвоката в соціальних мережах, інтернет-форумах та інших формах спілкування в мережі інтернет, в тому числі під час обговорення і роз'яснення правових норм, особливостей судочинства, дій його учасників, повинні бути відповідальними, достовірними і не вводити в оману [328].

Така сувора регламентація, водночас, залишає відкритим питання ідентифікації особи у соціальних мережах. Адже одна із головних цінностей інтернету – це можливість зберігати анонімність. Наприклад, адвокат О. Шевчук із цього приводу зазначив, що в соціальних мережах неодноразово відкрито принижується честь і гідність не лише окремих адвокатів, а й діяльності української адвокатури загалом [327]. При цьому допускається варіант, що такі публікації в соціальних мережах поширюються не просто учасником мережі, а учасником під чужим іменем діючого адвоката, або й учасником-адвокатом, але під чужим іменем адвоката. [327].

Значно менша за обсягом, але подібна за змістом стаття 20 Кодексу суддівської етики визначає, що “участь судді у соціальних мережах, інтернет-форумах та застосування ним інших форм спілкування в мережі є допустимими, проте суддя може розміщувати, коментувати лише ту інформацію, використання якої не завдає шкоди авторитету судді та судової влади” [199].

Щодо поведінки державних службовців, то на сьогодні основними документами, що її регулюють є закон «Про державну службу» та закон «Про запобігання корупції». Кабінет Міністрів скасував кодекс етичної поведінки державного службовця, аргументуючи це уникненням дублювання визначення вимог до етичної поведінки держслужбовців у різних нормативно-правових актах.

Кодекс етичної поведінки держслужбовця передбачав обов'язкову фіксацію телефонних розмов і зустрічей держслужбовців 1-2 категорії з політиками і представниками бізнесу. Також держслужбовцям заборонялося критикувати владу та чиновників. Спеціальних норм щодо поведінки в соціальних мережах та інтернеті він не містив.

В журналістській практиці є по-різному. У більшості закордонних та міжнародних медіа чітко прописані правила поведінки в соціальних мережах. Наприклад, Працівники RFERL вільні використовувати соцмережі, але коли журналіст пише щось у Facebook або Twitter, він має пам'ятати, що є працівником «Радіо Свобода». Тому в соцмережах він не може писати або говорити те, що підриває репутацію «РС» як збалансованого і об'єктивного ЗМІ. Фактично акаунти в соцмережах не діляться на приватні і корпоративні. Навіть на особистих сторінках у Facebook перед поширенням будь-якого посилання існує необхідність переконатися, що інформація правдива, не повинні поширювати фейки чи звертати увагу на діяльність лише однієї політичної сили чи політика. Оскільки така діяльність може створити враження певної заангажованості у читачів. Те ж стосується і «лайків», якщо зміст повідомлення може вдарити по репутації «Радіо Свобода» [427]. В BBC дещо інакше виглядають редакційні стандарти поведінки в соцмережах. Чітко розділені поняття особистого облікового запису і сторінки BBC. Образливі коментарі про працівників видання можуть вважатися дисциплінарним проступком. Журналісти не повинні писати

те, що дискредитуватиме BBC. Працівникам видання заборонено писати образливі пости і коментарі. Не можна використовувати інтернет для атак на колег жодним чином[427].

Українські видання (наприклад, Kyiv Post, «Сьогодні», «Українська правда») здебільшого не мають чітко прописаних правил поведінки у соціальних мережах. Проте очікують від журналістів розуміння, що навіть на особистих сторінках вони є представниками свого видання, і категорично «не вітаються хейтспіч і дискримінаційні висловлювання»[ibid].

Звертаючи увагу на медіа, слід відмітити, що преса, радіо і телебачення України переживають глибоку кризу. Сьогодні в країні фактично немає газет і журналів, телекомпаній і радіостанцій, які б отримали справжню економічну незалежність. Економічний успіх друкованого видання, телеканалу, інформагентство чи онлайн-медіа - в силу діючого законодавства, існуючих правових, адміністративних і економічних регламентів медіаринку - майже зовсім не залежить від чисельності аудиторії. Найбільші та найвпливовіші медіа належать олігархам, які передовсім дбають про власні інтереси, а не інтереси держави чи свободу слова. В той же час журналіст чи особа, що здійснює медійну діяльність<sup>24</sup>, щодня зіштовхується з загрозами, що пов'язані з можливістю знищення чи викрадення інформації, інформаційно-психологічними впливами, зокрема, пов'язаними з тим, що ЗМІ розглядаються як інструмент впливу і досягнення своїх цілей бізнесменами та політиками.

Перш ніж перейти до наступних категорій, вважаємо необхідним зупинитись на соціокультурних особливостях комунікативного процесу. У статті

---

<sup>24</sup> Згідно українського законодавства не кожен, хто здійснює діяльність в медіа є журналістом. У законах України міститься два визначення терміна «журналіст»: одне в Законі «Про пресу» (ст. 25), друге в Законі «Про державну підтримку засобів масової інформації та соціальний захист журналістів» (ст. 1). Сфера дії першого Закону охоплює вужче коло осіб-журналістів і ЗМІ, тому логічно, що визначення з другого Закону як загальне застосовується до всіх журналістів, які не працюють у пресі. За цим визначенням «журналіст – творчий працівник, який професійно збирає, одержує, створює і займається підготовкою інформації для засобів масової інформації, виконує редакційно-посадові службові обов'язки в засобі масової інформації (в штаті або на позаштатних засадах) – відповідно до професійних назв посад (роботи) журналіста, які зазначаються в державному класифікаторі професій України». У Класифікаторі є такі позиції як ведучий програми, випусковий, драматург, журналіст, інокореспондент, коментатор, кореспондент, літературний співробітник, оглядач, письменник, кілька різновидів редакторів, члени редакції й редколегії, в цьому переліку відсутні фотографи і оператори. Ще одною «сірою зоною» журналістики залишається журналістика «онлайн». Але оскільки це питання виходить за межі предмету дослідження, вважаємо за потрібне лише зазначити про існування цієї проблеми як перспективної для подальших наукових досліджень і необхідності її правового регулювання.

"Комунікація" в "Енциклопедії соціальних наук" відзначається, що "для формування суспільства, його об'єднань і підрозділів, а також для забезпечення взаєморозуміння між його членами необхідні якісь процеси комунікації" [418, с.210]. Ефективна комунікація є передумовою становлення демократичного суспільства. Особливого значення вона набуває у багатонаціональних державах, де культура спілкування відрізняється не лише на мікрорівні (особистість, група), а й на макрорівні (регіони, віросповідання, історичний досвід). Таким чином, соціокультурна ситуація значною мірою визначає наскільки ефективним буде комунікативний процес в суспільстві, зокрема між органами влади та населенням, між центральними органами влади, місцевим самоврядуванням та органами самоорганізації населення, між селом та містом, а також між різними регіонами держави. І зрештою від цього залежить, які саме загрози інформаційно-психологічній безпеці людини і суспільства можуть актуалізуватись.

Спілкування є складовою соціокультурної ситуації, яка по-різному впливає на його структуру, функції, способи здійснення. Культура втілює стиль мислення людини, охоплює всі аспекти суспільного життя, характеризує глибину знань особистості, її вихованість, уміння висловлювати свою думку, слухати інших, робити правильні висновки. Складовою культури особистості та соціального середовища, в якому відбувається її взаємодія, є культура спілкування, що віддзеркалює ціннісні орієнтації, позиції, соціальні ролі індивіда у суспільстві. Впливовими чинниками є звичаї та приписи стосовно сім'ї, статевої моралі, розподілу праці, а також відносини власності, особливості політичної влади, товариська етика, магічна практика, віра, уявлення про світ, природу і місце людини в ній. Рівень культури спілкування в групі характеризують: рівень загальнокультурного розвитку країни, її матеріальний, духовний стан на конкретному історичному етапі; рівень розвитку конкретної особистості, стан її комунікативного потенціалу, зв'язки із соціумом; рівень комунікативного розвитку групи, стан її соціально-психологічного простору; система зовнішніх зв'язків, наявність партнерів по взаємодії, каналів доступу іншої культури спілкування, інтенсивність, об'єктивний чи суб'єктивний характер таких зв'язків; комунікативно-правовий та організаційно-культурний порядок у групі;



загальнолюдські, національні, галузеві, групові схеми взаємодії учасників спілкування, які забезпечують запрограмований рівень культури спілкування учасників групи [292].

Слід зважати, що культура спілкування нерозривно пов'язана з культурою мовлення. А. Потебня, досліджуючи соціокультурні особливості особистості як проблему денаціоналізації, бачив органічну участь національної (етнічної) мови не тільки у формуванні народного світосприйняття, але й у самім розгортанні думки. Вчений підкреслював загальнолюдську цінність кожної мови – у якості ще однієї, відбитої саме в цій мові, картини світу: "Якби об'єднання людства за мовою і взагалі за народністю було б можливим, воно було б згубним для загальнолюдської думки, як заміна багатьох почуттів одним, хоча б це одне було не дотиком, а зором... Для існування людини потрібні інші люди; для народності – інші народності" [323, с.229]. Переконавання в тім, що люди бачать світ по-різному – крізь призму своєї рідної мови – лежить в основі теорії "лінгвістичної відносності" Е. Сепіра і Б. Ворфа<sup>25</sup>. Вони прагнули довести, що розходження між культурами обумовлені розходженнями в мовах. І хоча ця теорія й дотепер вважається недоведеною, окремі аспекти її вивчення вплинули на інтерес до аналізу впливу соціокультурних особливостей особистості на проблему трансформації не тільки суспільства в цілому, але й багатьох його структур, у тому числі й мовного середовища як одного із суб'єктів соціокультурного процесу. Причому більшість дослідників приділяли увагу комунікаційним проблемам соціокультурних змін. Так, той же Е. Сепір розглядав вплив комунікативних процесів на життя особистості і суспільства [418].

Тому мовне питання та його правове врегулювання є важливою складовою державної інформаційної політики і необхідною умовою гарантування інформаційної безпеки людини, захисту її інформаційних прав та свобод [292].

Система національно-психологічних особливостей індивіда базується на кількох сферах: мотиваційній (своєрідність мотивів, спонукальних сил діяльності представників тієї чи іншої національної спільноти); інтелектуально-пізнавальній

---

<sup>25</sup>Гіпотеза Сепіра-Ворфа (англ. Sapir-Whorf hypothesis), гіпотеза лінгвістичної відносності — концепція, розроблена в 30-х роках XX століття, за якою структура мови визначає мислення і спосіб пізнання реальності. Названа за іменами американських мовознавців Едварда Сепіра та Бенджаміна Ворфа.

(своєрідність сприймання й мислення носіїв національної психіки, що виражається в наявності специфічних пізнавальних та інтелектуальних якостей, які дають змогу особливо сприймати навколишню дійсність, оцінювати її, будувати плани діяльності, моделі способів досягнення її результатів); емоційно-вольовій (своєрідність емоційних та вольових якостей, від яких в багатьох випадках залежить результативність діяльності); комунікативно-поведінковій (ця сфера охоплює інформаційну і міжособистісну взаємодію, стосунки і спілкування, показує різницю подібних проявів у представників різних національних культур)[292].

Однак потрібно при цьому зважати на те, що специфіка національної психології того чи іншого народу виражається не в яких-небудь неповторних психологічних рисах і особливостях спілкування, а скоріше в їх неповторному поєднанні, прояві в певних звичаях, історичних традиціях, поведінці, вчинках. Об'єктивна оцінка соціокультурних та етнопсихологічних особливостей спілкування свідчить, що властивості національної культури спілкування і властивості індивідів, із яких складається етнос, не тотожні. А це означає, що комунікативні процеси залежатимуть від різних чинників, а отже ймовірність реалізації інформаційних загроз відрізнятиметься.

Савінова Н.А. враховуючи регіональні відмінності населення України, а також необхідність захисту населення від залякування, спотворення офіційної інформації, пропонує систему рівневих комунікативних заходів яка б забезпечувала прямий і зворотній зв'язок населення з владою на макро-, мезо- та мікро- рівні. При цьому кожен з учасників цієї системи має забезпечувати певне коло інформаційних потреб решти, надаючи виключно корисну та легітимну інформацію, утворюючи, таким чином систему спілкування «центральна влада» - «регіональна влада» - «населення» у послідовності та компетенції, чітко визначених на законодавчому рівні.

Оскільки формування первинної комунікації відбувається на вищому рівні, така інформація первинно походить від центральних органів влади і, з використанням, насамперед, офіційних джерел, а у другу чергу – ЗМІ, потрапляє на мезо- та мікрорівень. До населення (на мікрорівень) така інформація нерідко

потрапляє вже неповною, перекрученою, забарвленою ставленням преси, неналежно прокоментована. Внаслідок недоліків офіційної комунікації у суспільстві утворюються відчуття нерозуміння, непочутості, обманутості, покинутості, незадоволення [407].

Реалізація принципу свободи інформації в суспільстві значною мірою залежить від реалізації інтересів особистості у спілкуванні залежить і від того, наскільки послідовно вона дотримується загальнолюдських норм і принципів, етичного кодексу поведінки. До основних етичних принципів спілкування належать: гуманізація і демократизація відносин; повага до співрозмовників і самоповага; соціальна справедливість і толерантність; суверенність особистості (недоторканність гідності кожного); неупереджене ставлення до партнерів по спілкуванню; врахування інтересів співрозмовників та ін. [292].

Не менш важливою є духовна сфера суспільства, складовими якої є не лише релігійність, а, насамперед, суспільна свідомість, громадська думка і соціально-психологічний клімат, на який значний вплив мають системи освіти і виховання, засоби масових інформації і комунікації, що впливають на соціальну поведінку та організацію життєдіяльності людей. Психологічні і культурологічні основи мають знайти своє відображення в праві, насамперед, через мовну політику, врегулювання питань пов'язаних з використанням «мови ненависті», а також побудові ефективної системи комунікації та формування публічного простору, засобів і центрів комунікації, як необхідної умови громадянського суспільства і демократичної держави.

Ще дві категорії розглянемо в наступному підрозділі з огляду на їх обумовленість сучасною соціально-політичною ситуацією на сході країні і в державі в цілому.

### **3.3. Проблеми інформаційної безпеки людини в умовах гібридної війни проти України**

Однозначного визначення гібридної війни не існує. Так, у західній науковій думці орієнтовно вже з середини 2000-х рр. з'являється поняття "гібридна війна", однак у багатьох випадках вона трактувалася в інших термінах та поняттях, ніж

це спостерігається тепер. Для характеристики сучасного протистояння України і Росії можуть бути застосовані такі поняття, як "неконвенційна війна" (unconventional warfare), "нерегулярна війна" (irregular warfare) чи "змішана війна" (compound warfare), або ж спонсоровані державою "гібридні війни" (State-Sponsored Hybrid). В усіх них вказується на "розмивання" обрисів військового конфлікту та залучення до нього невійськових засобів, які у звичному стані не мають прямого стосунку до класичного військового протистояння [97]. В 2010 р., обговорюючи питання гібридної війни в міністерстві оборони США науковці і посадовці окреслювали її «як сукупність загроз з боку держав і недержавних організацій, що використовують комп'ютерні мережі та супутникові атаки; портативні ракети "поверхня-повітря"; саморобні вибухові пристрої; маніпулювання інформацією та засобами масової інформації; хімічну, біологічну, радіологічну, ядерну зброю» [602].

Сутність гібридної війни розкривається через розуміння сучасного суспільства, з одного боку його синергетичності, з іншого - системної кризи світової системи безпеки. По суті, це новітній вид глобального протистояння, що полягає у досягненні політичних цілей агресії шляхом створення внутрішніх протиріч та конфліктів, заволодіння стратегічними ресурсами країни-жертви без оголошення війни, при цьому фактично вона ведеться у різних вимірах: інформаційному, політичному, економічному, соціальному, гуманітарному, воєнному.

Глобальною ціллю гібридної війни є закріплення частини стратегічно важливих ресурсів країни-жертви за агресором. При цьому "передача" таких ресурсів здійснюється добровільно, адже сприймається нею не як загарбання, а як рух шляхом розвитку. Це тягне за собою проблеми у розпізнаванні технологій і засобів гібридної війни та, як наслідок відсутність своєчасної та адекватної відповіді на дії агресора. Якщо «традиційні» війни з часом обов'язково підлягають перегляду результатів, то результати гібридної війни перегляду не підлягають, зважаючи на обов'язковість змін ментальності народу, яка в результаті трансформації губить свої основні цілі і духовні цінності, замінюючи їх морально-психологічними ілюзіями і міфами агресора [489].

Є. Магда визначає гібридну війну як прагнення однієї держави підпорядкувати собі іншу за допомогою політичних, економічних, інформаційних інструментів. Саме тому в умовах гібридної війни бойові дії є другорядними, а на перший план виходять інформаційні операції та інші важелі впливу. Війна полягає у прагненні однієї держави агресивно діяти на свідомість жителів іншого. Іншими словами — це прагнення не знищити мільйони людей, а залякати й деморалізувати їх. Завдяки швидкості поширення інформації світом вона перетворилася не лише на товар, а й на зброю [244].

На думку Ф.Хофмана, гібридна війна включає такі сфери: географічну; економічну; ідеологічну та інформаційну [599]. Проте досвід України свідчить, що поле бою, на якому розгорнула свої операції Російська Федерація, є значно ширшим. Г. Почепцов зазначає, що гібридна війна розгорнута на всіх можливих напрямках, це не лише інформаційна війна. Це одночасно економічна, репутаційна, смислова, людська... На неї повинні працювати всі, хто має вплив на населення: актори, співаки, письменники, режисери. Військові дії задають лише фон для більш масштабної війни в людському розумі[324]. Негативні інформаційно-психологічні впливи закладають підґрунтя для подальших операцій, що спрямовані проти інтересів України на всіх рівнях – особи, суспільства і держави.

Про масштаби інформаційної війни, розгорнуті Росією проти України, влучно сказав Головнокомандувач об'єднаних Збройних сил НАТО в Європі Ф. Брідлав: "Це найбільш дивовижний інформаційний блицкриг, який ми коли-небудь бачили в історії інформаційних воєн". Інформаційний фронт "гібридної війни" розгортається одразу на кількох напрямках. Передусім: (1) серед населення в зоні конфлікту; (2) серед населення країни, проти якої здійснюється агресія, однак територія якої не охоплена конфліктом; (3) серед громадян країни агресора і (4) серед міжнародного співтовариства[97].

При цьому, використовуються різні форми і засоби впливу в залежності від напрямку і сфери впливу. Вплив, що чиниться на політичне становище України різниться в самій Україні, в Російській Федерації і в міжнародному інформаційному просторі. Причому розпочався він задовго до початку активної

фази цієї війни. Російська Федерація у зовнішньополітичній сфері цілеспрямовано послаблювала авторитет України на міжнародній арені. Зокрема, різними шляхами чинила перешкоди євроінтеграції України: через формування упередженого ставлення Європейського співтовариства до української влади, поширення недостовірної, неповної та викривленої інформації про Україну; формування негативного образу Європи, протиставляння близькості «братніх народів» тощо. Значних масштабів набула діяльність різноманітних "фондів", "культурних товариств", "аналітичних центрів" і просто "експертів" проросійської спрямованості в Європі, а також каналу RT і мережі «Спутнік», які використовуються для пропагандистських цілей.

Втручання у внутрішню політику відбувались через підтримку політичних партій та окремих політичних діячів, маніпулювання енергетичною залежністю, використанням підірваного авторитету влади у населення; інвестуванням в українські корпорації, в першу чергу медіа, розпалювання етнічної ворожнечі, маніпулювання мовним питанням.

Важливою умовою ведення гібридної війни є моніторинг ситуації і використання внутрішніх криз. Власне, завдяки цьому, на думку В.Горбуліна, відбулася так швидка анексія території АР Криму. Зокрема, серед передумов, які сприяли, він визначає: ослаблення центральної влади та часткове "безвладдя" на тлі зміни влади; зростання суперечностей (а швидше — актуалізація вже наявних) між Центром і регіонами; незадовільний психологічний і матеріально-технічний стан українських безпекових структур; антагонізм між різними силовими структурами; особливо активна інформаційно-пропагандистська робота Росії саме в Криму протягом усіх років незалежності України[97].

Внутрішньо політичний вплив значною мірою реалізується також через соціо-культурну та гуманітарну сфери. Серед них протидія переосмисленню власної історичної спадщини, нівелювання українських культурних цінностей і формування проросійських настроїв у суспільстві у спосіб насаджування міфу про спільний «русский мир», заперечення існування окремої від росіян української нації з власною мовою, культурою та історією тощо.

Важливим транскордонним простором ведення інформаційного протиборства став кіберпростір. За даними аналітиків на 2014 р. близько 90% телекомунікаційної інфраструктури України знаходилось у власності громадян РФ. Для реалізації сучасних технологій інформаційно-психологічного впливу на індивідуальну, групову і масову свідомість людей використовуються: засоби масової інформації та спеціальні засоби інформаційно-пропагандистської спрямованості; глобальні комп'ютерні мережі і програмні засоби розповсюдження в них пропагандистських інформаційних матеріалів; засоби, що нелегально модифікують інформаційне середовище, на підставі чого людина приймає рішення; засоби створення віртуальної реальності; чутки; засоби підпорогового психосемантичного впливу тощо [469, с.23-28].

На думку психологів, негативні інформаційно-психологічні впливи можуть призвести до таких негативних взаємозалежних змін як зміни психіки, психічного здоров'я людини та зміни в цінностях, у життєвій та інформаційно-психологічній позиціях, орієнтирах, світогляді особистості, що сприяють виникненню антисоціальних учинків та становлять загрозу для всього соціуму та держави загалом [237, с.104].

Враховуючи, що Російська Федерація як наступник «спадщини» школи безпеки СРСР, володіє значним досвідом використання науково розроблених і перевірених на практиці традиційних і нових методів впливу, то весь цей арсенал комплексно використовується в інформаційній війні проти України. Експерти вважають, що інформаційний вплив з метою підготовки плацдарму для гібридної війни розпочався щонайменше «в 2004 р., коли стало зрозуміло, що Україна не має наміру залишатися в фарватері російської зовнішньої політики, прагне бути самостійним суб'єктом міжнародних відносин. Тоді ж розпочався інформаційний вплив РФ, скерований на пропаганду і власного, і українського народів проросійськими/антиукраїнськими ідеями за рахунок підміни справжньої реальності й історичних подій симулякрами (образами того, чого не існує чи не існувало насправді), розповсюдженням напівправди та використанням інших інформаційних технологій [224, с.124-133].

Пропаганда набувала різних форм в залежності від етапу інформаційної кампанії та цільової аудиторії, на яку була скерована. Ще задовго до 2014 р. на російському телебаченні, яке трансливалось також і на всій території України масово з'являлись передачі з «суперечливими історичними» фактами – як Крим раптом став частиною УРСР, чиєю культурною спадщиною є історія Київської Русі, яка мова походить від давньоруської тощо. Вже під час військового протистояння було анімаційний фільм створений нібито дітьми, що втекли з Донбасу в РФ, основним посилом якого було «Рятуйте людей Донбасу».

Напівправда використовувалась активно під час анексії Криму, коли російські ЗМІ заявляли про масовий перехід українських силовиків на сторону агресора або про добровільну здачу військових частин, складів, зброї, інших військових об'єктів російським військовим.

Використовувалось також поєднання фактів, наприклад, у програмі «Сьогодні» на НТВ світ від 02.03.2014 р. йшлося про референдум щодо статусу Криму, що має відбутись 30 березня 2014 р. нібито цілком в дусі сучасних європейських реалій, нагадавши при цьому про заплановані аналогічні заходи в Шотландії (18 вересня 2014 р.) та Каталонії (9 листопада 2014 р.)[412].

І великого поширення набули симулякри<sup>26</sup> (або в поточній публіцистиці – «фейки») Симулякр - це знак, слово, що позначає те, чого насправді немає. Іншим словами, симулякр - це порожнє поняття, тобто поняття, яке не має змісту і / або обсягу. Найбільш вдале визначення симулякра, на нашу думку, дано американським літературним критиком Ф. Джеймісоном - "точна копія, оригіналу якої ніколи не існувало". Прикладами симулякрів є: "фашисти в Києві", "звірства каральних батальйонів", "розіп'яті хлопчики", використання Україною заборонених озброєнь. Стратегічна мета експлуатації цих симулякрів — замінити об'єктивні уявлення цільових груп про характер конфлікту тими "інформаційними фантомами", які потрібні агресору.

Використання симулякрів є поєднання вербальних та невербальних механізмів впливу, адже в основі останнього лежить підсвідоме сприйняття

---

<sup>26</sup> Симулякр (фр. Simulacres, від лат. Simulo, "робити вигляд, прикидатися") - "копія", яка не має оригіналу, термін який ввів в обіг постмодерніст Жорж Бата



людиною інформації. Чим тонша психічна організація людини, тим емоційно вразливіша вона до неконтрольованого людиною інформаційного впливу: застосування нових спеціальних засобів маніпулювання суспільною свідомістю через звук, колір, запах, малюнок, тощо; специфічні штучні щеплення; підшкірне вживлення; чипізація; гіпноз; деструктивний вплив на психіку людини природних комплексів, антропогенних зон, генераторів фізичних полів, випромінювання та інший інформаційно-енергетичний та психофізичний вплив з метою програмування дій та поведінки людини для створення «потрібних» подій та маніпулюванням громадською свідомістю [493, с.184-191].

Інформаційно-психологічні впливи підсилюються традиційними адміністративно-силовими методами порушення інформаційних прав і свобод людини – перешкоджання діяльності ЗМІ, обмеження доступу до мережі чи окремих ресурсів. Наприклад, на початках збройного протистояння було використано механізми блокування ресурсів, що активно спростовували (могли спростовувати) неправдиві повідомлення. Зокрема, свого часу на виконання вимог Роскомнадзору в соцмережі ВКонтакте було заблоковано сторінки «Правого сектору» та «Євромайдану» [521]. Окрім нових ЗМІ, активно використовуються традиційні способи пропаганди за допомогою преси, радіо, телебачення, кіно- та і друкована продукції. Захист інформаційного простору України розпочато навіть не відразу після початку АТО, численні серіали та фільми, раїдо та телепередачі з антиукраїнськими настроями масово трансливалися загальнонаціональними в українському теле і радіоефірі.

Іншим прикладом інформаційно-психологічного впливу на свідомість дітей в умовах протистояння між Україною та Росією є друкована продукція. В окупованому Луганську було представлено новий ілюстрований дитячий пізнавально-розважальний журнал «Вежливые человечки». Продукція розрахована на дошкільнят та дітей молодшого шкільного віку. Головними героями оповіді є героїчні дітлахи в образах так званих «бійців Малоросії», а в негативних героях цієї оповіді можна було впізнати президента України, Прем'єр-міністра та Секретаря РНБО. Таке перекручування фактів, паплюження та зневага до посадових осіб держави формує у дитячій свідомості викривлену картину

сприйняття сьогодення і навряд чи зможе виховати з них гідну особистість з високим рівнем правосвідомості та громадянською позицією [68].

Використання інформаційної зброї для впливу на широку аудиторію, в тому числі міжнародну, передбачає існування мережі установ, що використовуються як інструменти інформаційного впливу РФ. Зокрема, на забезпечення пропаганди в інтересах російської влади працюють інтернет-ресурс «Sputnik», що є інтерактивним майданчиком з можливістю підключення інтернет-радіостанції «Sputnik», а також інтернет-доступу до телеканалів RT, де мовлення здійснюється 45 мовами [405].

Окрім того, існує мережа так званих наукових установ і громадських організацій, що діють за межами РФ («Институт стран СНГ», «Международный институт политической экспертизы», «Русский институт», «Институт национальных стратегий», «Кавказский институт демократии» та «Институт евразийских исследований»), спеціально-створені молодіжні «недержавні» організації (Кримський «Прорив», закарпатський Русинський «Прорив», «Євразійський союз молоді», та фонди («Русский мир»)) [304, с.30-37].

Поширеним явищем є приклади використання медіаресурсів, що знаходяться у приватній власності громадян РФ в цілях пропаганди. Наприклад, на початку 2016 р. телеканал Life news повідомив, що ФСБ РФ отримала інформацію про підготовку терористичних нападів з боку ІДІЛ в місцях масового скупчення людей в Києві. За декілька днів британське видання The Independent опублікувало матеріал, в якому лейтмотивом стало планування Україною відправки військ в Сирію. При цьому наводиться «анонімне джерело з Міністерства оборони України». На відміну від попередньої новини, дана «сенсація» мала певний резонанс в Україні. Міністерство оборони України заперечило і звернуло увагу, що The Independent належить російському олігархові Лебєдеву, що має вагомі частки в таких гігантах російського бізнесу як РАО ЄЕС «Россия» і «Аерофлот» [326].

Слід звернути увагу, що ситуація щодо інформаційної безпеки населення України за територіальною ознакою умовно може бути класифікована на кілька категорій: 1) інформаційна безпека громадян України, що проживають АР Крим

та на тимчасово окупованих територіях; 3) інформаційна безпека військовослужбовців та інших осіб, що безпосередньо беруть участь у бойових діях, членів їх сімей, а також мирного населення в зоні бойових дій і на територіях, до них прилеглих; 3) інформаційна безпека населення України, що проживає на «мирних» територіях.

Моніторинговий огляд підготовлений Кримською правозахисною групою на підставі матеріалу, зібраного у травні 2017 р., зазначає про порушення права на свободу зібрань, свободу слова і висловлювання думки [333]. На порушення свободи слова припадає близько 20 % з 246 правопорушень, зафіксованих «Крим SOS» станом на травень 2016 р. Журналісти зазнають утисків у вигляді обшуків, допитів, переслідувань, криміналізації висловлювань [326]. Під таким тиском велика кількість журналістів, не згодних з окупаційною політикою російської влади, були вимушені залишити територію півострова. Так само, як і на російській території, в окупованому Криму знищуються незалежні ЗМІ. В аналітичній доповіді Національного інституту стратегічних досліджень на основі аналізу широкого спектру інформаційно-пропагандистських заходів РФ під час операції з захоплення Криму, визначається, що найбільш поширеними технологіями маніпулювання масовою свідомістю є:

- інформаційна блокада, що була спрямована на формування інформаційного вакууму для українських ЗМК в Криму та подавала факти під єдиним вигідним для Кремля кутом зору. Серед основних заходів – позбавлення місцевих теле- та радіокомпаній ліцензій мовлення, фізичні погрози розправи з журналістами, стеження за ними, «профілактичні» бесіди з спецслужбами, прослуховування їх розмов і читання листування. Як результат – станом на лютий 2015 р. на півострові не залишилося вільних медіа;

- використання медіаторів, або так званих «лідерів думки» – політичних діячів, представників релігійних конфесій, діячів культури, науки, мистецтва, спортсменів, військових;

- методи ефекту першості та упереджувального удару завдяки оперативності донесення матеріалу до отримувача дозволяв ЗМК Росії формувати бажане уявлення про події;

- переписування історії відіграло потужну роль в процесі руйнування історичної пам'яті;
- метод зворотного зв'язку передбачав проведення штучно інсценованих масових акцій на підтримку відторгнення Криму від України;
- прийоми емоційного резонансу, сенсаційності та психологічного шоку використовувалась для створення у широкої аудиторії антиукраїнських та антиісламських настроїв;
- повторення одних і тих же тверджень мало на меті сформувати у населення єдине бачення подій та спрямовувалось не на ідеологічні установки, а на буденну свідомість громадян;
- рейтингування застосовувалось кремлівськими медіа для виправдання агресивних дій російської влади, мотивуючи це вимогою суспільства [182].

Окрім того, мають місце порушення прав, що безпосередньо пов'язані зі свободою інформації – права на освіту, свободи совісті, релігії та віросповідання, права на правову допомогу тощо. Особливих переслідувань зазнають представники кримсько-татарського народу.

Звичайно на фоні незаконних затримань та утримань, залучення дітей до збройних формувань, сексуального насильства та інших злочинів, що пов'язані з військовим конфліктом на сході України, порушення інформаційних прав виглядають не так значимими, проте забезпечення реалізації більшості прав людини не є можливим у сучасному суспільстві без свободи інформації[318].

На території самопроголошених ЛНР і ДНР у 2014-15 роках заблоковано доступ до українських та міжнародних ЗМК, ліквідовані місцеві проукраїнські ЗМІ, створені відповідні інстанції - Міністерство інформації та зв'язку ДНР та інформаційна комісія ЛНР - завданням яких є моніторинг ЗМК та повне вилучення проукраїнських [472]. При цьому, за масштабної військової, матеріальної, інформаційної допомоги і координації Російської Федерації, зокрема, фахівців з інформаційно-психологічних операцій, створюється інформаційно-пропагандистська система, метою якої є виправдання насильства бойовиків, легітимізація сепаратистських «урядів», дегуманізація образу

української нації (а також європейців та американців), дискредитація української влади, а також деморалізація Збройних Сил України [182].

Стан масової свідомості в «ЛНР-ДНР», за оцінками спостерігачів, також є досить типовим для територій збройних конфліктів і визначається ними як «фрустраційний, травмований»[123]. За характеристикою директора донецької ГО «Інститут соціальних досліджень і політичного аналізу» В. Кіпеня, «це свідомість поляризована, чорно-біла, закрита для сприйняття «чужого» погляду. [...] Більшість дезорієнтована, втрачає чітке розуміння добра і зла, допустимого і неприпустимого»[ Ibid.].

Інформування населення на тимчасово окупованих територіях залежить від сукупності чинників: технічної можливості - переважна частина обладнання знищена, те що збереглось захоплене; психологічної складової – значна частина населення не готова сприймати інформацію з позицій української держави; мешканці обирають ті джерела, які забезпечують психологічний комфорт; сприйняття інформації обумовлене родинними зв'язками з бійцями ДНР і ЛНР, а також соціальною складовою – надходження гуманітарної допомоги, існуючою комунальною інфраструктурою тощо; змістовної (контентної) складової - приховання особливо важливої інформації про стан справ у будь-якій сфері; занурення важливої інформації в масив «інформаційного сміття»; підміна термінів або трансформація сенсу; відведення уваги на події в інших сферах; керування термінами, які легко сприймаються суспільством, але які не мають не тільки чіткого визначення, але і за своєю суттю не відповідають цій предметній галузі; заповнення інформаційного простору неприйнятною інформацією тощо; невизначеність державної інформаційної політики в Україні, а також рівнем фінансування.

Інформаційна безпека другої категорії є пов'язана з особливою значимістю інформаційно-психологічного впливу для безпосередніх учасників бойових дій, членів їх сімей та населення території, де здійснювалось АТО, а тепер тривають бойові дії. Насамперед йдеться про захист військ від інформаційно-психологічного впливу противника з метою зниження небезпеки негативного інформаційно-психологічного впливу на органи військового управління, особовий

склад військ (сил) та населення; забезпечення ефективного управління військами (силами); зміцнення морально-психологічного стану особового складу військ (сил) [9, с.77-86].

Основними складовими завданнями захисту військ (сил) від інформаційно-психологічного впливу супротивника є: роз'яснення особовому складу військ рішень військово-політичного керівництва країни та задач, що стоять перед військами (силами); аналіз і прогнозування інформаційної обстановки в районі операцій (бойових дій), рівня її впливу на війська (сили) та населення; збір і узагальнення інформації про вірогідні джерела та об'єкти негативного інформаційно-психологічного впливу противника; нейтралізація інформаційно-психологічного впливу противника з метою недопущення деморалізації, дезінформації військ (сил) та зниження їх морально-психологічного стану; проведення інформаційно-психологічних заходів (акцій), спрямованих на свої війська і населення в районі бойових дій; організація запобіжних (профілактичних) заходів щодо поширення неправдивих чуток серед особового складу, упередження неправдивих слухів, тривожних висловлювань і протиправних дій, спрямованих на зниження морально-психологічного стану військ (сил), та ін. [9, с.77-86] Важливою складовою інформаційної безпеки цієї категорії осіб є якісне і своєчасне надання психологічної допомоги як під час перебування в зоні бойових дій, так і після повернення додому. Значення має також інформаційна та правова підтримка учасників бойових дій на сході України та їх сімей.

Таким чином, на нашу думку, державна інформаційна політика має враховувати специфіку різних категорій населення, які зазнають інформаційно-психологічних впливів з різною інтенсивністю та різними методами.

Окрім, того важливим вбачається морально-етичний аспект діяльності ЗМІ та інститутів громадянського суспільства. Адже, рівень довіри до влади в Україні залишається вкрай низьким. За даними опитування Центру Разумкова на травень 2017 р., Президенту України довіряють 22% громадян, не довіряють – 71,9%, свідчать, що уряду довіряють 12,8%, не довіряють - 81,9%, Національному банку – відповідно 11,7% і 81,5%), Верховній Раді – відповідно 9% і 86,6%, прокуратурі

– відповідно 9,5% і 83,3%, судам – відповідно 7% і 86,6%. Національному антикорупційному бюро України довіряють 21,3% опитаних, не довіряють – 64,8%. Довіру до державного апарату (чиновників) висловили 7,9% опитаних, не довіряють – 87%. Вкрай низький рівень довіри мають також політичні партії (відповідно 8,6% і 83,5%) і комерційні банки (відповідно 10,4% і 83,9%)[125]. При цьому, рівень довіри до ЗМІ є значно вищим. У лютому 2017 р. найбільш високий рівень довіри українці відчували до такого постачальника політичної інформації, центральні ТВ канали країни (49%). Далі за рівнем довіри йдуть українські інтернет-ЗМІ – 19%, родичі і знайомі – 12%, соціальні мережі – 9%, місцеве ТВ – 6%, місцева преса – 4%, місцеве радіо – 3%, центральна преса України – 3%, центральні українські радіоканали – 3%, розмови і чутки – 3%, інше – 7%. Не довіряють нікому 31% опитаних.

Рівень довіри українців до ЗМІ певною мірою пов'язаний з такими соціальними характеристиками аудиторії споживачів, як вік, місце та регіон проживання. Наприклад, старша частина значимо частіше довіряє центральним ТВ каналам, ніж особи у віці до 40 років. А ті, в свою чергу, значно частіше довіряють українським інтернет-ЗМІ і соціальним мережам. Мешканці обласних центрів значимо рідше, ніж жителі звичайних містечок і сіл довіряють центральним ТВ каналам країни. А ось вітчизняним інтернет-ЗМІ міські жителі довіряють частіше, ніж жителі сіл [520].

Враховуючи історичний досвід використання інформаційних технологій, наприклад, пропаганда фашизму у Німеччині, сталінізму у Радянському Союзі, геноциду у Боснії та Руанді, створення належної правової бази для функціонування незалежних ЗМІ є необхідною умовою інформаційної безпеки на усіх рівнях – людини, суспільства і держави.

Підтримуємо думку Требіна М., що «будь-яка війна, у тому числі й «гібридна», колись закінчиться, а інформаційна боротьба за розум і серця людей не закінчиться ніколи, оскільки ми вступили в інформаційну епоху, де головним джерелом багатства та благополуччя людей стає інформація» [470, с. 64-68]. Тому національна та міжнародна інформаційна політика має враховувати реалії становлення інформаційного суспільства і бути спрямованою на забезпечення

цілісності особи та її здатності до розвитку, як визначальних категорій буття людини.

### **Висновки до розділу 3**

Сучасний людиноцентристський підхід в праві базується на тезі, що «всі люди народжуються вільними і рівними у своїй гідності та правах», тому окреслення підходів до розуміння людини як суб'єкта суспільства і об'єкта суспільних відносин, в яких реалізується інформаційна безпека, є необхідною умовою ефективного правового регулювання, а також визначення особливостей правового забезпечення інформаційної безпеки людини в залежності від об'єктивних і суб'єктивних властивостей.

Аналіз трьох філософських підходів до розуміння людини - дескриптивного, атрибутивного і сутнісного, дозволив зробити висновок, що людина як об'єкт соціальних відносин індивідуально відображає істотні риси певного суспільства, інтегрує соціальні відносини зовнішнього середовища і виробляє своє, особливе ставлення до зовнішнього світу. Водночас, завдяки сприйняттю внутрішнім когнітивно-емоційним світом (свідомими і несвідомим), в її діяльності виявляються характеристики суспільства через особисте ставлення до об'єктивної дійсності. Зміни, що відбуваються у зв'язку із формуванням інформаційного суспільства в Україні та світі, обумовлюють необхідність юридичного закріплення і державного гарантування правового статусу людини на новому якісному рівні. Формування інформаційного суспільства обумовило не лише значення існуючих і появу нових інформаційних прав людини, а й змінило змістовне наповнення усіх прав і свобод людини, а також її обов'язків, в напрямку формування інформаційної складової кожного з них.

Роль людини в такому суспільстві, безсумнівно, зростає, і номінально володіючи значною кількістю прав і свобод для участі в соціальному житті і в управлінні державою, проте реальні можливості людини обмежені багатьма чинниками – зокрема, постійно зростаючими можливостями інформаційних впливів, зокрема, технологіями маніпуляції свідомістю; змінами в системі культурних цінностей, що загрожують дезадаптацією; розвитком нових типів



соціальних зв'язків людей тощо. Ігнорування особливостей соціалізації особистості в інформаційному суспільстві призводить до розбалансування соціальних взаємозв'язків, а також руйнує основи життєдіяльності людини, здійснюючи, таким чином, деструктивний вплив і на суспільство, і на державу. Аналіз змін, що відбулись в трьох основних сферах суспільного життя - матеріально-економічній, соціально-політичній і духовно-культурній, на нашу думку, дозволяє зробити висновок про актуальність нормативно-правового закріплення інформаційної правосуб'єктності людини та інформаційно-правового статусу як нового галузевого правового статусу людини, основою якого є інформаційні права і свободи людини.

При цьому, проаналізувавши доктринальні підходи, норми міжнародного права та національного законодавства, вважаємо, що слід розрізняти дві різні категорії: інформаційні права і свободи людини, а також права і свободи людини в інформаційному суспільстві. При чому перша категорія є складовою другої.

Під інформаційним правами і свободами пропонуємо розуміти комплекс прав, похідних від свободи інформації, як фундаментального права людини, зокрема: 1) інформаційні права, що пов'язані з особою (особистістю) людини; 2) право власності на інформацію; 3) право на доступ до інформації; 4) свобода поширення інформації будь-яким законним способом; 5) право на безпечне інформаційне середовище.

Правовий статус людини залежить від сутності соціального ладу, в умовах якого він складається і функціонує, але, водночас, різні категорії осіб знаходяться у неоднакових умовах щодо можливості реалізації своїх прав і свобод в інформаційній сфері, зокрема, відрізняється ступінь захищеності в інформаційному суспільстві, види і інтенсивність небезпек, що їм загрожують. Тому в межах цього дослідження увагу присвячено аналізу окремих категорій об'єктів інформаційної безпеки, що характеризуються наявністю спільних інформаційних загроз їх безпеці і необхідністю особливого правового забезпечення, зокрема: 1) окремі вікові групи: насамперед, діти, підлітки і молодь, а також люди похилого віку; 2) люди з обмеженими фізичними можливостями, особливостями інтелектуального розвитку та психічними порушеннями; 3) люди,

що здійснюють діяльність, яка має або може мати важливі соціальні наслідки – державні службовці, медійні особи та журналісти, правозахисники, громадські активісти і політичні діячі тощо; 4) населення окремих регіонів країни чи населених пунктів, що володіє специфічними соціокультурними особливостями, в т.ч. релігійними, етнічними, мовними, демографічними; 5) люди, що пов'язані з військовими діями на сході України – військовослужбовці, їх сім'ї, а також сім'ї загиблих, населення окупованих територій, «сірої» зони, внутрішньо переміщені особи тощо. Що дозволило окреслити актуальні проблеми та перспективні напрямки розвитку правових основ інформаційної безпеки.

Збройний конфлікт на сході України, та гібридна війна, істотна частина якої ведеться в інформаційному просторі, і в яку перманентно є втягнутим все населення держави, вимагають переосмислення загроз інформаційній безпеці людині, суспільству і державі. Від розуміння сутності і небезпек стану гібридної війни, значною мірою залежить державна політика гарантування безпеки людини, її прав та свобод в кожній сфері, в т.ч. інформаційній. Зважаючи, що Російська Федерація володіє значним досвідом використання науково розроблених і перевірених на практиці традиційних і нових методів інформаційного впливу, який використовується в інформаційній війні проти України, має місце як комплексний вплив на населення України в цілому, так і цілеспрямовані інформаційні атаки на окремі соціальні групи. Запропоновано класифікацію інформаційної безпеки населення України за територіальною ознакою: 1) інформаційна безпека громадян України, що проживають АР Крим та на тимчасово окупованих територіях; 2) інформаційна безпека військовослужбовців та інших осіб, що безпосередньо беруть участь у бойових діях, членів їх сімей, а також мирного населення в зоні бойових дій і на територіях, до них прилеглих; 3) інформаційна безпека населення України, що проживає на «мирних» територіях. Державна інформаційна політика має враховувати специфіку різних категорій населення, які зазнають інформаційно-психологічних впливів з різною інтенсивністю та різними методами. Визначається значна роль створення належної правової бази для функціонування незалежних ЗМІ як необхідна умова інформаційної безпеки на усіх рівнях – людини, суспільства і держави.

Враховуючи геополітичне становище України, а також реалії становлення інформаційного суспільства, доводиться необхідність врахування досвіду гібридної війни і напрацювання відповідної правової бази у інформаційній сфері з метою забезпечення інформаційної безпеки людини, українського суспільства та держави.

## **РОЗДІЛ 4**

### **ІНФОРМАЦІЙНА БЕЗПЕКА ЛЮДИНИ В МІЖНАРОДНОМУ ПРАВІ ТА ЗАКОНОДАВСТВІ ІНОЗЕМНИХ ДЕРЖАВ**

#### **4.1. Інформаційна безпека людини в міжнародному праві**

Інформаційна безпека людини як наукова і правова категорія перебуває на етапі становлення як в національному, так і міжнародному політичному, правовому та науковому дискурсі. Глобальний характер інформаційного простору зі слабкими механізмами ідентифікації користувачів, складністю визначення їх місця та наслідків дій, всесвітній розвиток соціальних мереж, ринки міжнародної злочинності обумовлюють суттєвий вплив на сталий розвиток стабільного суспільства як основи особистого розвитку та економічного процвітання. Уразливість міжнародних та національних інформаційних інфраструктур, відсутність або часткова неможливість встановити обмеження для збору даних загрожують особистій свободі і міжнародній стабільності.

Люди очікують від держави та міжнародних організацій захисту миру, безпеки і добробуту від загроз, що обумовлені новим етапом розвитку суспільства. На глобальному рівні є необхідними політичні дії, спрямовані на вирішення цих проблем, засновані на переконливому аналізі тенденцій і наслідків в технологічній, соціальній, економічній і політичній сферах.

І.Г. Ханін вважає, що глобалізація підходів до досягнення і підтримки інформаційної безпеки зумовлена декількома причинами [490]. По-перше, зміною інформаційних потреб, які вийшли на загальносвітовий рівень. Це пов'язано зі зростанням рівня інтернаціоналізації економіки і, зокрема, транснаціоналізації виробництва і капіталу. По-друге, індустрія, що забезпечує процеси інформатизації (включно зі стандартами, технічною інфраструктурою, протоколами передачі даних тощо) набуває загальносвітового значення, насамперед у плані уніфікації. Глобальність стосується і світового рівня інформаційних послуг. По-третє, інформаційні загрози розглядаються відносно всього світового співтовариства та організації сучасної світогосподарської

системи. По-четверте, рівень інформатизації зріс настільки, що стало можливим говорити про виникнення глобального інформаційного суспільства з багатьма концепціями його проектування на майбутнє. По-п'яте, комп'ютерна або кіберзлочинність та загрози, що створюються нею, все більше набувають транснаціонального характеру. Все це виводить завдання досягнення і підтримки інформаційної безпеки у розряд міжнародних і світових, від вирішення яких залежить прогрес людства. Це створює новий порядок денний і закономірно веде до зростання ролі міжнародних правових інститутів та організацій. Відповідно виникає правове поле та нові напрями діяльності і компетенції міжнародних організацій. МСІБ, що формується, охоплює: правові інститути, різноманітні стандарти і методи досягнення безпеки, технологічні компоненти, а також структури, що забезпечують практичну реалізацію відповідних заходів.

Водночас, інформаційна безпека людини є складовою частиною міжнародної інформаційної безпеки. Під міжнародною інформаційною безпекою в термінології ООН розуміється захищеність глобальної інформаційної системи від т.зв. «тріади загроз» - терористичних, злочинних і військово-політичних. На думку Забари І.М., сучасні концепції міжнародної інформаційної безпеки характеризуються однаковим усвідомленням і розумінням: 1) місця і значення інформаційних технологій, їх взаємозв'язку в рамках інформаційного простору (кіберпростору), ролі в реалізації загальної концепції інформаційного суспільства; 2) необхідності захисту найважливіших національних інфраструктур, глобальних інформаційно-комунікаційних мереж і систем, а також цілісності накопиченої інформації; 3) складності, серйозності та чисельності загроз для ІКТ, пов'язаних як з процесами природнього і антропогенного характеру, так і діяльністю людини; 4) неефективності традиційних стратегій; 5) державних завдань, що постають на національному і міжнародному рівнях; 6) необхідності об'єднання зусиль з метою збереження і розширення внеску, який ІКТ роблять у забезпечення безпеки і цілісності держав; 7) необхідності міжнародної взаємодії в питанні розробки стратегій зменшення ризиків для ІКТ [143].

Серед доктринальних визначень заслуговує на увагу визначення міжнародної інформаційної безпеки як взаємодії акторів міжнародних відносин з операцій

підтримання сталого миру на основі захисту міжнародної інфосфери, глобальної інфраструктури та суспільної свідомості світової спільноти від реальних і потенціальних інформаційних загроз [260]. Автори цього визначення називають серед актуальних проблем міжнародної інформаційної безпеки: 1) формування належної соціальної бази інформаційної безпеки та подолання інформаційної нерівності між країнами; 2) практичну реалізацію потенційних можливостей інформаційної безпеки для різних соціальних верств населення з метою забезпечення їхньої нормальної діяльності та інтеграції у світову систему; 3) ефективне використання національних і наднаціональних структур інформаційної безпеки у системі вільної міжнародної комунікації, співробітництва в різних сферах життя з метою формування взаєморозуміння й довіри та попередження міжнародних і регіональних конфліктів; 4) переорієнтацію систем інформаційної безпеки від виконання завдань суто охоронних і захисних на завдання конструктивної модернізації структур національної свідомості та формування єдиної планетарної свідомості як "інфраструктури" збереження цивілізації й забезпечення виживання людства [260].

Водночас, визначаючи основні напрями міжнародно-правового регулювання в інформаційній сфері, Пазюк А.В. називає: а) міжнародно-правове регулювання змісту поширюваної інформації (інформаційний контент), б) міжнародно-правове регулювання інформаційної і комунікаційної діяльності; в) міжнародно-правове регулювання використання обмежених інформаційних ресурсів як-от: позиція на геостаціонарній орбіті, радіочастотний спектр, телефонний номерний ресурс, номери та назви (доменні імена) в інтернеті; г) міжнародно-правове співробітництво з питань інформаційної безпеки; д) міжнародно-правове регулювання використання інформаційно-комунікаційних технологій в інтересах людства, запобігання та подолання наслідків стихійних явищ тощо [299]. Таким чином, вчений відносить питання інформаційної безпеки до предмету міжнародного інформаційного права.

На основі вищезазначеного, а також розуміння інформаційної безпеки, що було нами сформульовано в попередніх розділах, вважаємо, що інформаційна безпека людини у глобалізованому суспільстві належить до предметної сфери

міжнародного публічного права. Тому, серед джерел, слід звернути увагу на 1) міжнародні договори, 2) міжнародно-правові звичаї і 3) загальні принципи права, а також 4) судові рішення і 5) доктрини фахівців з публічного права різних націй як допоміжний засіб для визначення правових норм, що закріплені у пункті 1 статті 38 Статуту Міжнародного суду ООН в якості застосовуваних джерел міжнародного права, крім згаданих трьох основних джерел. До джерел міжнародного права також відносяться рішення (акти) міжнародних міжурядових організацій. Хоча вони і не застосовуються при розгляді спорів Міжнародним судом ООН, в той же час виконують регуляторну функцію, визначаючи поведінку держав як основних суб'єктів міжнародного права.

Аналізуючи приписи міжнародного права, вважаємо, що норми, спрямовані на підтримання інформаційної безпеки людини за предметною ознакою можуть бути згруповані наступним чином: 1) що визначають принципи міжнародного права, в т.ч. в інформаційній сфері та щодо міжнародної безпеки; 2) щодо глобального інформаційного суспільства, глобальної інформаційної інфраструктури та міжнародного інформаційного порядку; 3) що визначають права і свободи людини в інформаційній сфері, а також міжнародні механізми їх захисту; 4) щодо кібербезпеки.

Основні принципи міжнародного права становлять фундамент системи міжнародного права, а отже виступають вихідними при творенні норм, що регулюють відносини щодо інформаційної безпеки. Основні закріплені в Статуті ООН, Декларації про принципи міжнародного права та в Заключному акті Наради з безпеки та співробітництва в Європі (НБСЄ).

Дев'ять з десяти принципів мають універсальний характер - принцип незастосування сили або загрози сили; принцип мирного вирішення міжнародних спорів; принцип невтручання; принцип співробітництва; принцип рівноправ'я і самовизначення народів; принцип суверенної рівності держав; принцип добросовісного виконання зобов'язань за міжнародним правом; принцип територіальної цілісності; принцип поваги прав людини; а принцип непорушності кордонів – регіональний, оскільки не визнаний усіма країнами світу. Що є суттєвим – що власне на цих принципах має базуватись міжнародно-правове

забезпечення інформаційної безпеки. Хоча на момент створення цих актів ще не існувало сучасного розуміння інформаційних загроз, глобальної інформаційної інфраструктури, інформаційних прав людини тощо, але власне вони є своєрідним мірилом відповідності норм міжнародного права його основоположним цінностям.

Водночас, їх застосування має бути основою для всієї системи міжнародного права і у випадку необхідності – використовуватись для заповнення прогалів, тобто для регламентації відносин у разі відсутності прямого регулювання. Це має особливе значення в умовах постійного відставання правового забезпечення від реальних суспільних відносин в умовах інтенсивного розвитку інформаційних технологій.

Доповідь Комісії Макбрайда, політичного діяча Ірландії, правозахисника, лауреата Нобелівської премії миру 1974 р., опублікована під назвою «Багато голосів – один світ», відображала результати роботи експертів, які брали участь у роботі Комісії. Вони виявили істотний дисбаланс у міжнародних потоках інформації, а також «інформаційний голод», властивий для країн і регіонів «третього світу». Діяльність Комісії Макбрайда була пов'язана з активізацією руху за новий, більш справедливий, міжнародний інформаційний та комунікаційний устрій (НМІКУ, або НМІУ). Багато ідей руху знайшли відображення в «Декларації про основні принципи, що стосуються внеску засобів масової інформації у зміцнення миру та міжнародного взаєморозуміння, у розвиток прав людини і в боротьбу проти апартеїду та підбурювання до війни» (ЮНЕСКО, 1978 р.).

На симпозіумі спеціалістів з питань інформації і на п'ятій зустрічі глав держав і урядів країн в Коломбо були дані загальні визначення Концепції нового міжнародного інформаційного порядку. У цій програмі розглядалися проблеми диспропорції міжнародних інформаційних потоків, справедливого розподілу прибутків транснаціональних інформаційних корпорацій. Основними завданнями НМІУ вбачались забезпечення використання інформації в інтересах миру, співробітництва і розвитку всіх народів на основі більш збалансованих інформаційних обмінів між розвиненими країнами і країнами, що розвиваються,



забезпечення чесного і справедливого характеру переданої інформації, надання допомоги країнам, що розвиваються, у справі розвитку власних систем інформації. З огляду на значення інформації для країн, що розвиваються, держави запропонували кваліфікувати інформацію як “соціальне благо” і “міжнародний ресурс”.

На VI Конференції глав держав чи урядів країн, що не приєдналися (Гавана, 1979 р.), була прийнята резолюція, відповідно до якої принципами НМІУ є: незалежність, суверенітет і територіальна цілісність держав, невтручання у внутрішні справи держав; право кожної держави розвивати власну систему інформації; право кожної держави використовувати власні засоби інформації для інформування світової громадськості про свої інтереси і сподівання; право кожного народу на швидку, об’єктивну і повну інформацію; рівність у міжнародному інформаційному обміні, відповідальність різних суб’єктів процесу інформації за її об’єктивність, вірогідність та інформативність; право кожної держави боротися в рамках своєї конституції проти поширення невірогідної і перекрученої інформації, здатної стати на перешкоді розвитку добросусідських відносин між народами.

Проте, своєрідним антиподом НМІУ стала Таллуарська декларація (міжнародна конференція «Голос свободи», Франція, Таллуар, 1981 р.). Прихильники Декларації 1978 р. звинувачували Захід у нав’язуванні світові одностороннього потоку інформації, яку отримують, виробляють і розповсюджують крупні медіа-монополії. Ті, хто підписав Таллуарську декларацію, вважали, що НМІУ підтримує прагнення авторитарних і тоталітарних режимів встановити державний контроль над засобами масової інформації у світовому масштабі.

Таким чином, кілька десятиріч тривало протистояння в розумінні шляхів подальшого розвитку міжнародних відносин щодо інформації. Основними аспектами проблеми встановлення були політико-юридичний, тобто необхідність розробки і прийняття відповідних міжнародно-правових принципів і норм, на основі яких ґрунтуватимуться міжнародні інформаційні обміни; а також економіко-технічний, що полягав у створенні всесвітньої системи комунікацій,

яка надала б можливість усім народам на рівноправній і справедливій основі користуватися її вигодами.

Через майже 3 десятиліття дискусій міжнародне співтовариство сформулювало політико-правові принципи, які знайшли закріплення в Декларації принципів «Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті»: принцип інклюзивного, загального і недискримінаційного доступу до ІКТ і благ інформаційного суспільства – інформації, ідей і знань; принцип справедливого розподілу благ, привнесених ІКТ, між розвиненими і країнами, що розвиваються, а також всередині країн; принцип збереження спадщини і культурного надбання; принцип (цифрової) солідарності, партнерства і співробітництва між органами державного управління, приватним сектором, громадянським суспільством та міжнародними організаціями; принцип багатостороннього співробітництва в управлінні розвитком глобальної інформаційної інфраструктури [108].

Принципи побудови інформаційного суспільства мають декларативний характер, проте їх цінність полягала в тому, що для багатьох держав вони стали дороговказами щодо подальшої внутрішньої і зовнішньої політики, а також спонукали прийняття відповідних національних нормативних актів<sup>27</sup>.

Необхідною умовою становлення глобального інформаційного суспільства є розвиток глобальної інформаційної інфраструктури (ГІІ). В середині 90-х рр. країни "Великої сімки" та Світовий банк у зв'язку усвідомленням економічного впливу цифрового розриву, створили Комісію з глобальної інформаційної інфраструктури. Її створення було спробою відповіді на визнання того, що традиційні інститути та регуляторні основи вже не можуть задовольнити все більш складні проблеми та можливості глобалізованої інформації. Комісія з глобальної інформаційної інфраструктури (ГІІК) - це незалежна недержавна ініціатива, в якій беруть участь керівники галузі, пов'язані з інформацією та зв'язком, з країн, що розвиваються, а також промислово розвинених країн.

---

<sup>27</sup> Зокрема, в Україні було прийнято Закон «Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015», що залишається чинним досі.

ГПК відзначають також, що інформаційна революція відбувається хаотично і суперечливо. Тому ГПК зобов'язується забезпечити унікальну, нейтральну та об'єктивну платформу для своїх уповноважених з метою просування ідей, що сприяють впровадженню інформаційної інфраструктури у всьому світі. Згідно з їхньою задумкою, ГП являтиме собою інтегровану загальносвітову інформаційну мережу масового обслуговування населення нашої планети на основі інтеграції глобальних і регіональних інформаційно-комунікаційних систем, а також систем цифрового телебачення і радіомовлення, супутникових систем і пересувного зв'язку.

Базові технології ГП включають такі складові: комп'ютерну; телекомунікаційну; побутову (побутових електронних приладів); контентно-сервісну (інформаційних сервісів).

Інформаційна інфраструктура сильно впливає на міжнародні, національні, регіональні та індивідуальні інтереси. ГПК, зокрема, визначає чотири фактори:

1. Країни, що розвиваються, а також промислово розвинені країни мають високу частку в розвитку інформаційної інфраструктури;
2. Зобов'язання та можливості розвитку інформаційної інфраструктури переходять від урядів до приватного сектору;
3. Розуміння та бачення приватного сектору мають важливе значення для формування ефективної політики при розбудові інформаційної інфраструктури, яка має бути економічною та безпечною;
4. Політичні виклики, як і ринки інформаційної інфраструктури, по суті, є глобальними [652].

Водночас, розбудова інфраструктури не є самоціллю, а лише засобом. Під побудовою інформаційного суспільства в Декларації принципів вбачалась *орієнтоване на інтереси людей (вид. автором)*, відкрите для всіх і спрямоване на розвиток суспільство, в якому кожен міг би створювати інформацію та знання, мати до них доступ, користуватися і обмінюватися ними, з тим щоб дати окремим особам, громадам і народам можливість повною мірою реалізувати свій потенціал, сприяючи своєму сталому розвитку і підвищуючи якість свого життя на основі цілей і принципів Статуту Організації Об'єднаних Націй і дотримуючи в

повному обсязі і підтримуючи Загальну декларацію прав людини. Окрім того, «як необхідний фундамент інформаційного суспільства було визнано проголошене в статті 19 Загальної декларації прав людини право кожної людини на свободу переконань і на вільне їх вираження; це право включає свободу безперешкодно дотримуватися своїх переконань і свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів. Спілкування є одним з основних соціальних процесів, однією з базових людських потреб і фундаментом будь-якої соціальної організації. Воно становить серцевину інформаційного суспільства» [108].

Таким чином, підтверджувалась особлива значимість у сучасному суспільстві інформаційних прав людини, які визнані на міжнародно-правовому рівні у Міжнародній хартії прав людини<sup>28</sup>.

Свобода інформації отримала своє міжнародне визнання завдяки розвитку міжнародного права захисту прав людини. Загальна декларація прав людини, передбачає такі права і свободи в цій сфері: захист приватності (Стаття 12), свобода думки (стаття 18), свобода переконань і їх вираження (Стаття 19), свобода мирних зібрань (стаття 20).

Міжнародний Пакт про громадянські і політичні права визнає право на приватність (стаття 17), свободу думки (стаття 18), свободу поглядів і їх вираження, що включає свободу шукати, одержувати і поширювати будь-яку інформацію та ідеї, незалежно від державних кордонів, усно, письмово чи за допомогою друку або художніх форм вираження чи іншими способами на свій вибір (стаття 19), заборону пропаганди війни, національної, расової чи релігійної ненависті (стаття 20), право на мирні зібрання (стаття 21), право брати участь в управлінні державними справами, голосувати і бути обраним, мати доступ до державної служби (стаття 25), право етнічних, релігійних та мовних меншин на рівні права користування своєю культурою, сповідувати свою релігію і виконувати її обряди, а також користуватися рідною мовою (стаття 27).

---

<sup>28</sup> Загальна декларація прав людини (1948); Міжнародний пакт про економічні, соціальні і культурні права; Міжнародний пакт про громадянські і політичні права; Факультативний протокол до Міжнародного пакту про громадянські і політичні права (1976); 2-й Факультативний протокол до Міжнародного пакту про громадянські та політичні права про відміну смертної кари (1991)

Міжнародний Пакт про економічні, соціальні і культурні права, визнає такі права людини, як право на освіту (стаття 13), на участь у культурному житті, користування результатами наукового прогресу та їх практичного застосування, а також право користуватися захистом моральних і матеріальних інтересів, що виникають у зв'язку з будь-якими науковими, літературними чи художніми працями, автором яких він є (стаття 15).

Окрім Міжнародної хартії прав людини, яка передбачає універсальні права людини, існує також низка міжнародних актів, що визначають спеціальні права і свободи – для забезпечення правовими засобами можливості користуватись своїми правами особам, що з різних причин зазнають чи можуть зазнавати дискримінації.

Так, Конвенція про права дитини, передбачає права дитини на свободу вираження своїх поглядів, що включає свободу шукати, одержувати і поширювати інформацію та ідеї будь-якого типу, незалежно від кордонів в усній, письмовій чи друкованій формі, у формі творів мистецтва чи за допомогою інших засобів на вибір дитини (стаття 13), свободу думки, совісті і релігії (стаття 14), право дитини на свободу об'єднань та свободу мирних зібрань (стаття 15), право на приватність (стаття 16), свободу засобів масової інформації, доступ дитини до інформації, спрямованої на сприяння соціальному, духовному і моральному благополуччю, а також здоровому фізичному і психічному розвитку дитини, передбачає також захист дитини від інформації і матеріалів, що завдають шкоди її благополуччю (стаття 17).

Відповідні норми, що мають на меті надання особам з інвалідністю можливостей вести незалежний спосіб життя й усебічно брати участь у всіх аспектах життя, містить Конвенція про права осіб з інвалідністю. Нею на державу покладено обов'язок вживати належних заходів для забезпечення інвалідам доступу нарівні з іншими до фізичного оточення, до транспорту, до інформації та зв'язку, включаючи інформаційно-комунікаційні технології і системи, а також до інших об'єктів і послуг, відкритих або які надаються для населення як в міських, так і в сільських районах. Заходи, які включають виявлення й усунення перешкод і бар'єрів, що заважають доступності, повинні поширюватися, зокрема: а) на

будівлі, дороги, транспорт та інші внутрішні та зовнішні об'єкти, включаючи школи, житлові будинки, медичні установи та робочі місця; б) на інформаційні, комунікаційні та інші служби, включаючи електронні та екстрені служби.

На виконання статті 21 Конвенції з забезпечення інвалідів можливістю користуватися правом на свободу вираження поглядів і переконань, включаючи свободу шукати, одержувати і поширювати інформацію та ідеї нарівні з іншими, користуючись за своїм вибором усіма формами спілкування, визначеними у статті 2 Конвенції, держави вживають усіх належних заходів, включаючи: а) постачання інвалідів інформацією, призначеною для широкої публіки, у доступних форматах і з використанням технологій, що враховують різні форми інвалідності, своєчасно і без додаткової плати; б) прийняття та сприяння використанню в офіційних зносинах: жестових мов, абетки Брайля, підсилювальних і альтернативних способів спілкування й усіх інших доступних способів, методів і форматів спілкування за вибором інвалідів; с) активне спонукання приватних підприємств, що надають послуги широкій публіці, зокрема через інтернет, до надання інформації та послуг у доступних і придатних для інвалідів форматах; d) спонукання засобів масової інформації, в тому числі тих, що надають інформацію через інтернет, до перетворення своїх послуг на доступні для інвалідів; е) визнання і заохочення використання жестових мов. Конвенція також гарантує права інвалідів на приватність (ст. 22), освіту без дискримінації та на основі рівності можливостей на всіх рівнях і навчання протягом усього життя (ст. 24), участь у політичному і громадському житті (ст. 29), участь у культурному житті, проведенні дозвілля і відпочинку та занятті спортом (ст. 30).

Існують також норми, що визначають інформаційні права і свободи на регіональному рівні. Вперше на регіональному європейському рівні ці права були підтверджені в Конвенції Ради Європи про захист прав людини та основоположних свобод, укладеній в Римі 4 листопада 1950 р. Право людини на повагу до приватного життя гарантується у статті 8, свобода думки, совісті і релігії – у статті 9, свобода вираження – у статті 10 Конвенції. Американська Конвенція про права людини, прийнята на Міжамериканській спеціальній конференції з прав людини в Сан-Хосе (Коста-Ріка), проголошує право на

приватність (стаття 11), свободу совісті і релігії (стаття 12), свободу думок і їх вираження (стаття 13), а також право на спростування (стаття 14). Африканська хартія прав людини і народів бали прийнята в рамках Організації африканської єдності в Найробі, 26 червня 1981 р. і набула чинності 21 жовтня 1986 р. Хартія гарантує право на повагу до життя (Стаття 4), право отримувати інформацію, висловлювати і поширювати свої погляди (стаття 9), право на освіту, участь у культурному житті своєї спільноти (стаття 17).

У Хартії основоположних прав Європейського Союзу, передбачаються, окрім «класичних», також «нові» інформаційні права людини, що з'явилися, на нашу думку, у зв'язку з поступовим розвитком саме міжнародного інформаційного права: захист персональних даних (стаття 8), право на належне управління (стаття 41), право на доступ до документації (стаття 42). Хартія не має обов'язкової юридичної сили, але береться до уваги Судом Європейських співтовариств (ЄС) та Європейським судом першої інстанції (ЄСПІ).

В цілому, зміст прав, визнаних основними міжнародними актами, постійно переосмислюється через правозастосування міжнародними судами. Так, для прикладу, рішення у справах, що розглянуті Європейським Судом з прав людини вважаються єдиним джерелом динамічного тлумачення Європейської Конвенції з прав людини. При цьому, слід звернути увагу власне на динамічну складову, адже позиції Суду щодо тлумачення тієї самої норми не є усталеними, визначаються особливостями національних правових систем держав, а також культурними цінностями конкретного суспільства та змінами, що відбуваються у ньому.

Так, у практиці Європейського Суду можна простежити зміну розуміння права на доступ до інформації та його співвідношення з іншими правами людини. В початкових коментарях Європейського суду щодо десятої статті Конвенції наголошувалось, що ця стаття гарантує право громадськості бути *«належним чином поінформованою»*<sup>29</sup>. В подальшому, у своїх рішеннях ЄСПЛ зазначив, що

---

29 Справа Sunday Times v. United Kingdom, 26 квітня 1979 року, § 66.

громадськість має право отримувати інформацію та ідеї, що становлять суспільний інтерес<sup>30</sup>.

У рішенні по справі *Leander v. Sweden*, суд зазначив: «...Право на свободу отримувати інформацію головним чином забороняє Уряду обмежувати особу в отриманні інформації, яку інші хочуть або можуть хотіти передати їй. Стаття 10, у ситуації, описаній у цій справі, не надає особі права доступу до реєстру інформації про його особисті характеристики, а так само не покладає на Уряд обов'язок надавати таку інформацію особі»<sup>31</sup>.

Таким чином, Європейський суд з прав людини визначив, що у цьому випадку право передбачене ст. 10 Конвенції не охоплює доступ до адміністративної інформації. Подібним було тлумачення і у справі *Gaskin v. the United Kingdom*<sup>32</sup>. Але один із суддів Європейського суду оприлюднив окрему думку про те, що забороняючи надання адміністративної інформації особі, держава втручається у свободу одержувати інформацію та ідеї.

Згодом у справі *Guerra and others v. Italy*<sup>33</sup> заявники поскаржилися на те, що органи влади їх міста не вжили належних заходів щоб поінформувати населення про ризики, пов'язані з функціонуванням хімічного заводу біля міста. Всупереч позиції Європейської комісії, яка до 1998 р. приймала скарги приватних осіб на порушення Європейської конвенції, Велика палата ЄСПЛ дійшла висновку, що стаття 10 не підлягає застосуванню у цій справі. При цьому, вісім суддів з двадцяти висловили окремі думки у цій справі, відповідно до яких за певних обставин у ситуації, подібній до розглянутої, стаття 10 могла б бути застосована. Так, суддя П. Ямбрек зауважив, що якби особи подали запит до органу влади, і цей орган безпідставно відмовив у наданні інформації, то таким чином держава перешкодила б отриманню інформації, і це відповідало б формулюванню статті Конвенції.

30 *Thorgeir Thorgeirson v. Iceland*, 25 червня 1992 року, § 63; *Jersild v. Denmark*, 23 вересня 1994 року, § 31; *Ukrainian Media Group v. Ukraine*, 29 березня 2005 року, § 38 та ін

31 Рішення ЄСПЛ у справі *Leander v. Sweden*, 26 березня 1987 року, §74-75.

32 Рішення ЄСПЛ у справі *Gaskin v. the United Kingdom*, 7 липня 1989 року, §50-53 та Окрема думка судді Уолша, що не збігається з рішенням.

33 Рішення ЄСПЛ у справі *Guerra and others v. Italy*, 19 лютого 1998 року, §52-54 та Окрема думка судді Ямбрека, що збігається з рішенням.



Теоретичне значення має, на нашу думку, тлумачення Європейської комісії з прав людини: «надання громадськості інформації є одним з основних способів захисту благополуччя і здоров'я населення у ситуаціях, де є загроза довкіллю. Відповідно, слова «Це право включає свободу... одержувати... інформацію» у частині 1 статті 10 повинні тлумачитися таким чином, що вони надають право одержувати інформацію, зокрема від органів влади, членам місцевих громад, які зазнали чи можуть зазнати шкоди від індустріальної чи іншої діяльності, що загрожує довкіллю. Стаття 10 поклала на Держави не лише обов'язок робити доступною інформацію з питань довкілля., а також і позитивний обов'язок збирати, обробляти і поширювати таку інформацію, яка за своєю природою не може інакшим чином стати відомою громадськості». Європейська комісія також підкреслила, що стаття 10 має запобіжну роль і попереджає порушення інших основних прав, таких як право на життя чи на повагу до приватного і сімейного життя.

Проте, вже 2006 р., ЄСПЛ розглянув справу *Sdružení Jihočeské Matky v. Czech Republic*<sup>34</sup>, щодо відмови у наданні громадській екологічній організації документів і планів атомної електростанції в місті Темелін, і рішення у ній передбачало вже зовсім інакше тлумачення: «У цій справі заявник попросив дозволу ознайомитися з адміністративними документами, які були у розпорядженні органів влади, і до яких громадяни могли мати доступ на умовах, передбачених статтею 133 Постанови про будівництво, яку оспорує заявник. За цих умов Суд визнає, що відхилення зазначеного запиту становило втручання у право заявника отримувати інформацію». Рішення містило також твердження, що про висновок суду «що із Конвенції складно вивести загальне право доступу до адміністративних даних і документів».

Таким чином, Європейський суд у цій справі прямо визнав, що відмова надати інформацію на запит з боку державних органів була формою втручання у право на свободу одержувати інформацію.

Професор Гентського університету Д. Воорхоф та викладач Амстердамського університету В. Хінс, аналізуючи цю справу, дійшли висновку,

<sup>34</sup> Рішення ЄСПЛ у справі *Sdružení Jihočeské Matky v. Czech Republic*, 10 липня 2006 року, §1.1.

що у розглянутій судом ситуації було три фактори, які сприяли застосуванню до неї статті 10 Конвенції:

1) Заявники подали до органу влади запит, і їм було відмовлено у наданні інформації. Отже, держава вчинила конкретну дію, втручання у процес обміну інформацією.

2) Запитані відомості містилися в адміністративних документах, що були у розпорядженні органу влади. Отже, ці відомості не треба було ані збирати, ані створювати.

3) За чеським законодавством громадяни могли мати доступ до такої інформації, однак у розглянутому випадку заявнику було відмовлено у доступі до неї.

Вони також відзначили, що заявники не запитували інформацію про себе. За умов подання подібних запитів, як показала практика ЄСПЛ, Суд не схильний вважати, що справа може розглядатися за статтею [598, с.124-125].

І найбільш фундаментальним рішенням ЄСПЛ щодо розширення розуміння статті 10 винесено було у справі *Társaság a Szabadságjogokért v. Hungary*<sup>35</sup>. Угорська громадська організація «Угорське об'єднання громадських свобод» звернулася до Конституційного Суду Угорщини з проханням надати їй скаргу, що знаходилася на розгляді Суду. Цю скаргу подав депутат угорського парламенту, і у ній містився запит щодо конституційного розгляду останніх змін до кримінального кодексу, які стосувалися злочинів, пов'язаних із наркотиками. Конституційний Суд відмовив у наданні документа, не запитавши про це у депутата, і вказав запитувачу, що скарга не може бути надана третім особам без згоди її автора. Посилаючись на норми угорського законодавства із доступу до інформації, громадська організація оскаржила відмову до судів усіх рівнів. На всіх рівнях позов не був задоволений з огляду на захист права народного депутата на приватність. ЄСПЛ, розглянувши цю справу, звернув увагу на те, що метою громадської організації було отримання інформації задля її поширення, зокрема з метою суспільної дискусії із питань протидії обігу наркотиків. Органи влади перешкождали. Європейський суд назвав «монополію Конституційного Суду на

---

<sup>35</sup> Рішення ЄСПЛ у справі *Társaság a Szabadságjogokért v. Hungary*, 14 липня 2009 року; §26-39.

інформацію» однією з форм цензури. Водночас, ЄСПЛ вважає, що втручання органів влади ґрунтувалося на законних підставах і мало легітимну мету – захист прав особи (зокрема, на приватність). На думку ЄСПЛ, відсутня умова допустимості такого втручання - воно не було необхідним у демократичному суспільстві. Стаття 10 не покладає на державу обов'язки з надання інформації, і про те, що право на доступ до адміністративних відомостей з неї складно вивести. «Тим не менше, Суд нещодавно наблизився до ширшого розуміння поняття «свобода одержувати інформацію... і відповідно до визнання права на доступ до інформації».

У розглянутому випадку, на думку ЄСПЛ, мало місце втручання у здійснення організацією функцій watchdog суспільства через «цензуру інформаційної монополії», а не лише відмова у доступі до офіційних документів. Європейський суд також підкреслив, що запитана інформація була вже готова і могла бути надана. Водночас, на державі лежав обов'язок не перешкоджати суспільному рухові такої інформації.

Принципи, вироблені Європейським судом у цій справі, лягли в основу наступних рішень - *Kenedi v. Hungary*<sup>36</sup>, де ЄСПЛ підтвердив, що «доступ до оригінальних документальних джерел з метою легітимного історичного дослідження є основною умовою реалізації права заявника на свободу вираження поглядів».

Вирішуючи справу, Європейський суд дійшов висновку, що відмова надати інформацію хоч і переслідувала легітимну мету (захист національної безпеки), але не була передбачена законом. Отже, суд визнав порушення статті 10 Конвенції.

Знаковою для науковців стала справа *Gillberg v. Sweden*<sup>37</sup>. Вчений К. Гілберг досліджував дитячу психіатрію в Гетеборзькому університеті. Два інших науковці звернулися до нього із проханням надати їм окремі документи щодо дослідження. Гетеборзький університет як розпорядник зазначеної інформації відмовив у її наданні. Запитувачі звернулися до суду і отримали рішення, яким їм було дозволено отримати потрібні їм документи на певних умовах секретності. Гілберг

<sup>36</sup> Рішення ЄСПЛ у справі *Kenedi v. Hungary*, 26 серпня 2009 року; §40-45.

<sup>37</sup> Рішення Великої палати ЄСПЛ у справі *Gillberg v. Sweden*, 3 квітня 2012 року; §82-97

та університет знову відмовили запитувачам і знищили документи, пов'язані із дослідженням. За це вченого, його колег і віце-президента університету було піддано кримінальному покаранню.

К. Гілберг звернувся до Європейського суду із заявою про порушення його прав за статтями 8 (право на повагу до приватного життя) та 10 Конвенції. Він стверджував, що стаття 10 передбачає, разом із позитивними правами передавати та одержувати інформацію, також і негативне право не надавати відомості, які він не хоче поширювати. Справу у 2010 р. розглянула палата суддів, а у 2012 її переглянула Велика палата ЄСПЛ. У фінальному рішенні Європейського суду припущення заявника щодо такого негативного права було спростоване.

За законодавством Швеції університет є публічною установою, його працівники – посадовими особами університету, а інформація, якою розпоряджається такий навчальний заклад має статус публічної. У розглянутій ситуації посадова особа університету відмовилася надати інформацію третім особам, К. та Е., всупереч рішенням національних судів. ЄСПЛ зауважив, що такі дії професора перешкоджали вільному обміну думками та ідеями щодо проведеного дослідження.

І навпаки, Європейський суд вказав, що визнання позиції професора Гілберга «становило б зазіхання на права К. та Е. за ст. 10 ...отримувати інформацію шляхом доступу до запитаних публічних документів»<sup>38</sup>.

Таким чином, відбулася зміна в підходах Європейського суду, що повинно визначати також і позиції національних судових установ. Адже, в Конституції України практично відтворені майже всі права, закріплені в Конвенції, але їх розуміння у національній правозастосовній практиці дуже часто помітно відрізняється від того, яке демонструє при її застосуванні Європейський суд з прав людини [512].

Важливо зауважити, що рішення ЄСПЛ на користь заявника, не тільки зобов'язує державу виплатити заявникові справедливую компенсацію, а також спонукає розвиток національного законодавства в напрямку зближення до

---

<sup>38</sup> Рішення ЄСПЛ у справі *Gillberg v. Sweden*, 2 листопада 2010 року; §120-127 та Рішення Великої палати ЄСПЛ у справі *Gillberg v. Sweden*, 3 квітня 2012 року; §82-97.

міжнародних стандартів, визначаючи обов'язок держави усунути ті недоліки національного законодавства, які спричинили таке порушення.

Оскільки глобальний інформаційний простір став полем для конкурентної боротьби у економічній, політичній та інших сферах, то це породило існування багатоманітних випадкових та створених інформаційних загроз, серед яких сьогодні розглядаються інформаційні війни (кібер, електронні, мережеві та ін.), інформаційний тероризм, інформаційна зброя (у тому числі технічного характеру), хакінг, кіберзлочинність, кібершпіонаж, агресія у кіберпросторі по відношенню до держав та людей [490].

Відповідною реакцією на це стала постановка питання про кібербезпеку та інформаційну безпеку на міжнародному рівні.

Універсальний міжнародний договір з питань міжнародної інформаційної безпеки відсутній. Проте, склався цілий комплекс норм soft law, закріплений у резолюціях ГА ООН, які дозволяють визначити риси, окреслити контури, а у певних випадках і визначити елементи майбутнього механізму міжнародно-правового регулювання міжнародної інформаційної безпеки, зокрема, це Резолюції ГА ООН «Створення глобальної культури кібербезпеки і захист найважливіших інформаційних структур» №57/239, № 58/199, № 64/211 (2009), Глобальна програма кібербезпеки МСЕ та ін.[508]

Перша з названих Резолюцій – «Створення глобальної культури кібербезпеки» 57/239 – визначила дев'ять основоположних елементів глобальної культури кібербезпеки: обізнаність, відповідальність, реагування, етика, демократія, оцінка ризику, проектування та запровадження засобів забезпечення безпеки, управління забезпеченням безпеки та переоцінка [132].

Проте виявилось, що розуміння необхідності створення системи забезпечення міжнародної інформаційної безпеки не означає єдності в підходах, зокрема щодо принципу відповідальності за власний інформаційний простір. Фактично, науковці говорять про існування двох концепцій [144, 67, с.42-44, 515, с.76-81, 220].

Прихильники першої концепції не підтримують ідеї побудови складної ієрархічної і розгалуженої системи міжнародної безпеки, де окреме місце було б

визначено міжнародній інформаційній безпеці. Вони вважають, що в основу міжнародної інформаційної безпеки має бути покладено боротьбу із злочинами у сфері інформаційно-комунікаційних технологій, в т.ч. боротьбу із тероризмом у сфері ІКТ. При цьому прихильниками цієї концепції не вбачається необхідності міжнародно-правового регулювання використання ІКТ у військовій сфері, оскільки, на їх думку, достатньо існуючих міжнародно-правових засобів - Конвенції про кіберзлочинність від 23.11.2001 р. та Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобського характеру, вчинених через комп'ютерні системи від 28.01.2003 р.

Прихильники другої концепції розглядають міжнародну інформаційну безпеку в якості одного з ключових аспектів системи міжнародної безпеки, що безумовно потребує міжнародно-правового регулювання. На їх думку, в основу проблематики міжнародної інформаційної безпеки в широкому розумінні мають бути покладені принципи неподільності безпеки та відповідальності держав за свій інформаційний простір. Таким чином, протидія загрозам військового (військово-політичного), терористичного і кримінального характеру з використанням ІКТ, повинна здійснюватись системно і узгоджено. Відповідно, міжнародно-правове регулювання повинно бути поширено на всі зазначені структурні елементи, і задля досягнення цього запропоновано прийняття міжнародної угоди на універсальному рівні.

Прикладом реалізації такого поєднання виступає Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки від 16.06.2009 р., в якій знайшли відображення відповідні положення цієї концепції.

На думку фахівців – політологів і соціологів – проблема криється глибше. За нині пануючих умов головним двигуном формування глобальних цінностей виступає північноатлантична цивілізаційна спільнота, через що процес глобалізації набув ознак культурно-ціннісної експансії західної цивілізації – із поширенням на інші країни ідеалів та ціннісних символів, притаманних саме західним ринковим демократіям. Але такі процеси, які функціонально можуть

бути полегшені через застосування певних стандартизованих і навіть подекуди шаблонних підходів, можуть наражатися на істотні перешкоди, пов'язані зі специфікою минулого історичного шляху розвитку глобальних «культурно-ціннісних донорів» – історичним досвідом, який відсутній у країн – реципієнтів ціннісних засад Заходу. Але, можливо, ще більшу проблему становить те, що різні цивілізаційні утворення в сучасному світі де-факто знаходяться на різних етапах суспільного розвитку і на якісно різних стадіях суспільної модернізації. Модернізація в нинішніх країнах «золотого мільярда» – це процес, для якого характерні, зокрема, цінності епохи постмодерну, з її пріоритетами індивідуалізму, нематеріальних прагнень особистості, особистого задоволення та емоційності, мережевої взаємодії, а не чітких ієрархій. А модернізація в країнах «третього світу» (країнах, що розвиваються) – це за змістом дещо інший процес, який більшою мірою має спирається на традиційні цінності сім'ї та національної держави, прагнення до матеріального благополуччя, прагнення до ієрархії, чіткого визначення повноважень та статусного утвердження. Фактично це якісно два різні підходи, які дуже важко поєднати в якусь єдину глобальну систему[425, с.7-21].

Проте, на нашу думку, причини такого розподілу є подібними до ситуації, що спостерігалась при визнанні основних прав і свобод людини, коли держави, які мали проблеми з дотриманням відповідних прав всередині держави виступали проти або утримувались від їх визнання на рівні міжнародно-правових актів. Другу концепцію підтримують такі держави як Росія, КНР, в деяких питаннях – США, тобто держави, які або здійснюють розробки інформаційної зброї, концепцій ведення мережових та інформаційних війн, або виступають «природними» монополістами на глобальному інформаційному ринку, або намагаються легітимізувати на міжнародному рівні вже існуючі всередині держави обмеження, посиляючись на пріоритетність забезпечення інформаційної безпеки як на національному, так і на міжнародному рівнях.

Таким чином, фахівці мають всі підстави стверджувати, що на сьогоднішній день проблема міжнародної інформаційної безпеки виокремлена в самостійну наукову проблему, яка «має соціологічні, економічні та правові аспекти»[450].

Тим не менш, і за відсутності єдності, що пошуки прийнятного для усіх сторін варіанта врегулювання проблеми міжнародної інформаційної безпеки тривають. Координуюча роль належить ООН, діяльність якої зосереджена на питаннях пов'язаних із (1) боротьбою із злочинним використанням інформаційних технологій (резолюції ГА ООН «Боротьба із злочинним використанням інформаційних технологій» № 55/63 від 04.12.2000 р., № 56/121 від 19.12.2001 р.), (2) міжнародною інформаційною безпекою (резолюції ГА ООН «Досягнення в сфері інформації та комунікації в контексті міжнародної безпеки»), (3) створенням глобальної культури кібербезпеки і захистом найважливіших інформаційних структур (резолюції ГА ООН «Створення глобальної культури кібербезпеки і захист найважливіших інформаційних структур» № 57/239 від 20.12.2002 р., № 58/199 від 23.12.2003 р., № 64/211 від 21.12.2009 р.)[143].

При цьому до основних елементів міжнародної системи інформаційної безпеки, що формується, на думку І.Ханіна, слід відносити: 1) міжнародні доктринальні документи універсального характеру, присвячені інформатизації, інформаційному суспільству та інформаційній безпеці; 2) міжнародні стандарти у галузі інформаційної безпеки; 3) міжнародні професійні (спеціалізовані) установи, які займаються питаннями інформаційної безпеки у різних галузях; 4) міжнародно-регіональні інститути та структури, які створюються інтеграційними об'єднаннями (наприклад, ЄС); 5) інститути, що створюються військово-політичними організаціями (наприкладі НАТО); 6) національні доктрини, концепції та стратегії [490].

Окремої уваги заслуговує зацікавленість неурядових і некомерційних організацій в питаннях інформаційної безпеки. Головними і найбільш авторитетними міжнародними професійними установами, які займаються питаннями інформаційної безпеки є: International Telecommunication Union; Institute of Electrical and Electronics Engineers; Association for Computing Machinery; W3 Consortium; Information Systems Security Association; Center for Internet Security; International Organization for Standardization; Internet Engineering Task Force; International Computer Security Association; Internet Security Alliance; Information System Audit and Control Association [143].



Після Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства і Повноважній конференції МСЕ 2006 р. було визначено фундаментальну роль МСЕ як створення довіри і безпеки при використанні інформаційних і комунікаційних технологій. Глави держав і урядів, інші глобальні лідери, які брали участь в ВСІС, а також Держави - Члени МСЕ доручили МСЕ зробити конкретні кроки до стримування загроз і небезпек, пов'язаних з інформаційним суспільством.

Протягом багатьох років, Всесвітня федерація вчених, яка була залучена до відповідних програм МСЕ, розробляла концепцію кібермиру, а МСЕ, зокрема через свого Генерального секретаря, сприяла її конкретизації [660].

Термін кібермир використовувався і раніше, але без однозначного підходу до його розуміння. Зокрема, у 2007 р. в рамках Міжнародного жіночого мирного руху, з прямим посиланням на Декларацію і Програму дій ООН по культурі миру, було проголошено ініціативу щодо розширення прав і можливостей молоді будь-якої нації, за рахунок використання потенціалу ІКТ, в напрямку безпеки інтернету і заохочення інновацій [654].

Міжнародні експерти відзначають, що проблема визначення глобальної позиції щодо кібермиру і кібербезпеки постійно актуалізується, адже «руйнування кіберпростору (а) негативно відбивається на правах людини на приватне, сімейне життя, на право мати будинок і спілкуватися без перешкод або атак, (b) створює перешкоди прав на свободу думки, совісті і віросповідання, (c) обмежує право на свободу переконань і виразів і (d) обмежує право на отримання і передачу інформації та ідей в будь-якому середовищі передачі і незалежно від кордонів» [488].

Термін "кібермир" на сьогодні розуміється набагато ширше, і призначений служити основним принципом у створенні "універсального порядку в кіберпросторі". Спроба сформулювати концепцію миру і культури миру була зроблена Генеральною Асамблеєю ООН в "Декларації і Програма дій по культурі миру" від жовтня 1999 р. містить каталог складових і передумов миру, а також окреслює шляхи досягнення і підтримки його за допомогою культури миру[535]. Посилаючись на Хартію Організація Об'єднаних Націй з питань освіти, науки і

культури, в якій стверджується, що "війни починаються в розумах людей, тому захист миру повинен бути побудований в свідомості людей", МСЕ сформулював п'ять принципів кібермиру, які також встановлюють конкретні дії і зобов'язання задля забезпечення миру і стабільності в кіберпросторі: кожна держава має взяти на себе зобов'язання надати своєму народові доступ до засобів зв'язку; кожна держава візьме на себе зобов'язання захищати своїх людей в кіберпросторі; кожна держава візьме на себе зобов'язання не приховувати терористів/злочинців на своїх територіях; кожна держава повинна взяти на себе зобов'язання не застосовувати першою кібератаки до інших країн; кожна держава повинна взяти на себе зобов'язання взаємодіяти з іншими країнами в рамках міжнародного співробітництва для забезпечення миру в кіберпросторі.

Всесвітня федерація вчених деталізувала ці та інші загальні принципи, затверджені ООН, що стосуються кіберсередовища в Декларації Еріче про принципи кіберстабільності і кібермиру [572]. Ця Декларація показує, що досягнення кіберстабільності і кібермиру тісно взаємопов'язані. Декларація є короткою і концентрується на основних робочих моментах кібермиру, до яких належать:

1. Всі уряди повинні визнати, що міжнародний закон гарантує особам вільний потік інформації та ідей; ці гарантії також поширюються на кіберпростір. Обмеження повинні встановлюватись тільки в міру необхідності і їх повинен забезпечувати процес правового перегляду.

2. Всі країни повинні спільно розробити загальний кодекс кіберповедінки і глобальногармонізовані правові рамки, включаючи процедурні положення, що стосуються допомоги в проведенні розслідувань і співпраці, які поважають недоторканність приватного життя і прав людини. Всі уряди, постачальники послуг і користувачі повинні підтримувати міжнародні правоохоронні дії, спрямовані проти кіберзлочинців.

3. Всі користувачі, постачальники послуг і уряди повинні домагатися того, щоб кіберпростір не використовувалося будь-яким чином, який призводить до експлуатації користувачів, особливо молодих і беззахисних, за допомогою насильства або деградації.

4. Уряди, організації та приватний сектор, в тому числі фізичні особи, повинні впроваджувати і підтримувати комплексні програми безпеки, засновані на міжнародно визнаному передовому досвіді і стандартах з використанням технологій конфіденційності та безпеки.

5. Розробникам програмного і апаратного забезпечення слід прагнути до розробки безпечних технологій, які сприяють стійкості і протистоять уразливості.

6. Уряди повинні брати активну участь в зусиллях Організації Об'єднаних Націй щодо заохочення глобальної кібербезпеки і кібермиру, з тим щоб перешкодити використанню кіберпростору для конфлікту.

Складність реалізації цих принципів, як вже згадувалось раніше, лежить в площині політичних перешкод. Необхідність пошуку спільних рішень щодо протидії інформаційним та кіберзагрозам, вироблення спільної стратегії інформаційної безпеки для протидії кібервійнам, інформаційному тероризму та інформаційній злочинності не знаходить однозначного розуміння, а процеси розробки стратегій міжнародного співробітництва у сфері інформаційної безпеки свідчать про суттєву диференціацію бачення пріоритетів світової, регіональної і національної політики у контексті протидії новим загрозам.

Дубов Д.В. відзначає, що кіберпростір став новим виміром геополітичного суперництва, «винятковість якого пов'язана з тим, що він єдиний з усіх п'яти наразі опанованих людиною просторів є екстериторіальним, адже практично позбавлений географічних обмежень. При цьому залежність сучасної людини від кіберпростору є лише трохи меншою, ніж від інших. Саме від кіберпростору, від його стану, функціональності, передбачуваності та прогнозованості залежить стабільність світової економіки, безпека людей, всезагальне зростання добробуту, суспільний розвиток» [128, с.9].

При цьому науковець акцентує увагу на відсутності принципів існування та використання кіберпростору, пріоритеті практичних міркувань над правилами співіснування людей характеризують політику використання кіберпростору як своєрідну *realpolitik*, яку часто намагаються поєднати з радикальними ліберальними теоріями, створюючи химери уявного світу, який нібито

регулюється загальноприйнятими нормами на кшталт Вестфальського миру та міжнародним законодавством [ibid.,с.12].

Для європейських держав діяльність у сфері спільної політики безпеки, зокрема й інформаційної, спрямована на інтеграцію європейського інформаційного простору, розвиток інформаційного суспільства, створення європейських правових норм у галузі комунікації, забезпечення свободи слова та обміну інформацією, функціонування засобів масової комунікації на основі новітніх технологій, оскільки в умовах становлення інформаційного суспільства регіональні організації захищають стандарти Європейської Конвенції з прав людини, соціальні пріоритети європейського суспільства, плюралістичні принципи ЗМК, європейський зміст електронної демократії тощо. В цих цілях було розроблено і прийнято Європейську Конвенцію з кіберзлочинності. Хоча в самій конвенції фахівцям не вдалось домовитись про єдине розуміння категорії «кіберзлочинність», і тому обмежились лише визначенням переліку таких посягань. Важливою метою цієї Конвенції було розширення повноважень урядів при розслідуванні звичайних злочинів, при вчиненні яких був задіяний обмін інформацією чи передача сигналу через мережу. На сьогодні, крім європейських держав, Конвенцію підписали також Канада, Японія та США, які брали активну участь у підготовці її тексту, які багато в чому пов'язують продовження міжнародного співробітництва в галузі міжнародної інформаційної безпеки з виконанням положень Конвенції.

Однак, політика США позначена виразним поворотом до мілітаризації інформаційної сфери, яка означає більш тісну координацію політичних і силових структур з «кібербезпеки», а також визначенням військових й невійськових аспектів психологічних та інформаційних операцій. У забезпеченні регіональної безпеки США, а отже і Організація Американських Держав готові на далекосяжні ідеологічні компроміси з Росією та Китаєм аж до згоди на закріплення за цими та іншими потужними державними чи наддержавними утвореннями «сфер відповідальності» для підтримання регіональної безпеки й стабільності. Така політика супроводжується активним використанням високих технологій подвійного призначення, які дозволяють конфіденційно створювати й

використовувати «інформаційні озброєння» під прикриттям реалізації загальних науково-дослідних програм, коли йдеться не лише про заходи превентивно-оборонного характеру, але й про наступальні «інформаційні озброєння», здатні забезпечувати переваги у кризових ситуаціях та регіональних конфліктах [245,с.51-62].

Проблематика міжнародної інформаційної безпеки<sup>39</sup> стабільно займає одне з центральних місць в порядку денному ШОС. Учасники організації ще в 2006-му на саміті в Шанхаї прийняли Заяву глав держав-членів ШОС по міжнародній інформаційній безпеці. У документі висловлювалася стурбованість «Використанням ІКТ з метою, що завдають шкоди безпеці людини, суспільства і держави ». Пріоритетною метою виражався намір держав скоординовано вживати заходів для реагування на загрози безпеки в інформаційній сфері. В ході подальших заходів ШОС приймалися нові документи, що регулюють поведінку держав у інформаційному просторі і відповідальне використання ІКТ, що базувався на єдиному баченні і довірі між країнами об'єднання. В 2009 р. був підписаний основоположний документ, який визначив формат, цілі та принципи співробітництва країн Організації в галузі міжнародної інформаційної безпеки - Угода між урядами держав-членів Шанхайської організації співробітництва про співпрацю в області забезпечення міжнародної інформаційної безпеки. Угода визначила загальну термінологічну і концептуальну базу підходу ШОС, зокрема, загальне розуміння таких базових понять як «Розробка та застосування інформаційної зброї, підготовка і ведення інформаційної війни», «інформаційний тероризм», «інформаційна злочинність » тощо. У 2011 р чотири країни-учасниці ШОС (Росія, Китай, Узбекистан, Таджикистан) вперше представили в ООН своє бачення проблем, пов'язаних з МІБ, в розроблених і спрямованих листом на ім'я Генерального секретаря ООН “Правила поведінки у сфері забезпечення міжнародної інформаційної безпеки”. Їх головною метою декларувались визначення прав і обов'язків держав у інформаційному просторі, стимулювання конструктивної і відповідальної поведінки та співробітництва держав з метою протистояння загальним викликам і загрозам у цій сфері, спонукання до

---

<sup>39</sup> А власне таке формулювання прийняли для себе держави учасниці ШОС

використання інформаційно-комунікаційних технологій виключно для повномасштабного соціального і економічного розвитку та добробуту народів, забезпечення миру і безпеки.

Ці правила по суті повторювали основні положення Конвенції про забезпечення міжнародної інформаційної безпеки, що була внесена для обговорення на рівні ООН Російською Федерацією [201].

Проте, пропозиції держав-учасниць ШОС не знайшли належної підтримки на міжнародному рівні. Це, на нашу думку, обумовлено не лише розбіжностями в розумінні змісту і загроз міжнародній інформаційній безпеці, а й тим, що Російська Федерація та Китай, які є найбільш активними учасниками ШОС щодо розвитку кіберпростору та кібербезпеки, декларуючи намір «Стимулювати побудову мирного, безпечного, справедливого і відкритого інформаційного простору, ґрунтуючись на принципах поваги державного суверенітету і невтручання у внутрішні справи інших країн»<sup>40</sup>, демонструють внутрішню і зовнішню політику, що суперечить таким намірам.

В свою чергу, інформаційна безпека в діяльності регіональної організації АТЕС<sup>41</sup>, розглядається передусім в контексті економічного співробітництва з питань лібералізації торгівлі та інвестицій, зокрема проблем захисту критично важливої інфраструктури від терористичних загроз. З спільних документів - Заяви з питань безпеки інформаційних і телекомунікаційних інфраструктур на саміті АТЕС в Шанхаї (2002 р.), Закону про кіберзлочинність, «Декларації Бангкока», стратегії «Електронний АТЕС» та декларації, прийнятій на зустрічі міністрів АТЕС з питань розвитку телекомунікації і інформаційної індустрії в Лімі простежується важлива роль державної політики в розвитку інформаційної інфраструктури, розширенні спектру інформаційних послуг, що надаються громадянам (електронне управління), створення сприятливого інвестиційного клімату для інвестицій в інформаційний сектор, необхідність співпраці на політичному рівні між всіма державами-членами АТЕС з метою вироблення комплексної стратегії протидії інформаційним загрозам і розвитку регіональної

---

<sup>40</sup> Бішкекська декларація глав держав-членів Шанхайської організації співпраці

<sup>41</sup> Азійсько-Тихоокеанське економічне співробітництво (англ. The Asia-Pacific Economic Cooperation, скорочено АТЕС)

системи інформаційної безпеки, а також удосконалення законодавств країн регіону відносно регулювання інформаційного сектора в контексті інформаційної безпеки, відповідно до міжнародних норм і принципів.

Це свідчить про те, що важливими елементами миру і культури миру є не лише незастосування сили і утвердження практики ненасильства, а й загальний набір цінностей і моделей поведінки, міжнародний порядок і законність, позитивні, динамічні процеси участі та права людини (зокрема, дотримання принципів свободи, справедливості, демократії, толерантності, солідарності, співпраці, плюралізму, культурного розмаїття, діалогу і взаєморозуміння, сприяння у врегулюванні конфліктів). Важливою є також роль міжнародних стандартів в сфері інформаційної безпеки. Загальними їх показниками фахівці називають: універсальність, гнучкість, гарантованість, реалізацію та актуальність. Міжнародною організацією стандартизації (ISO) прийняті такі основні стандарти: ISO/IEC 27002:2013 «Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги» та ISO/IEC 27002:2013 «Інформаційні технології. Методи забезпечення безпеки. Кодекс практики управління інформаційною безпекою» та інші стандарти серії ISO/IEC 27002, ISO/IEC 27005:2011 «Інформаційні технології. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки» [605]. При цьому, слід звернути увагу, що стандартам мають відповідати не лише комерційні структури, а й урядові та інші організації, адже їх дотримання сприяє прозорості взаємодії суб'єктів, свідчить про відповідність систем і структур належному рівню захисту інформації, зокрема, персональних даних, комерційної таємниці тощо.

Оскільки сфера міжнародної інформаційної безпеки є надзвичайно динамічною, то вона потребує постійного моніторингу і аналізу. Група урядових експертів ООН вперше була створена на виконання Резолюції ГА ООН 56/19, мандат якої передбачає розгляд існуючих і потенційних загроз у сфері інформаційної безпеки і можливих спільних заходів по їх усуненню, а також вивчення міжнародних концепцій, які були б спрямовані на зміцнення безпеки глобальних інформаційних і телекомунікаційних систем. За результатами її роботи Генсекретар ООН доповідав на Генеральній Асамблеї в 2005 р. про

результати цього дослідження. В подальшому така група скликалась ще декілька разів - 2009-2010 рр., 2010-2013 рр. і, в останнє, 2016-2017 рр.

Важливим кроком щодо виявлення актуальних проблем інформаційної безпеки є проведення відповідних конференцій. Уперше саміт із кібербезпеки – CyberSecurity Summit – у рамках Мюнхенської безпекової конференції проведено не в Німеччині, а у Кремнієвій долині. Обговорювались такі проблеми безпеки кіберпростору як протидія кібератакам, майбутнє ведення війн, розвиток норм і правил для кіберпростору, боротьба проти кібертероризму, а також економічне значення кібербезпеки[154]. Останній глобальний саміт з кібербезпеки (Global Cybersecurity Summit-2017) відбувся в Києві, де обговорювались актуальні питання інформаційної безпеки: створення нового покоління кіберпрофесіоналів; новий світ в сфері IoT (інтернет речей); штучний інтелект і машинне навчання; безпечне голосування (вибори в епоху цифрових технологій); співпраця та взаємообмін інформацією про загрози; зростаючі тренди в області автоматизації і безпеки додатків; шифрування майбутнього, а також можливості використання переваг штучного інтелекту в боротьбі з кіберзагрозами і атаками.

Ханін І.Г. вважає, що головними трендами у сфері міжнародної інформаційної безпеки в останні роки є: безпека стає пріоритетом (перевагою) найвищого рівня для держав і бізнесу; підвищується значущість інформаційних ризиків; відбувається розвиток і розширення сфер кіберзлочинності; з'являються нові виміри інформаційної безпеки (наприклад, інтернет речей, операції з великими даними і знаннями, прийняття рішень, що базується на обробці даних, та ін.); посилюється асиметричність заходів щодо підтримки інформаційної безпеки у різних країнах і регіонах світу; відбувається розвиток спеціальних технологій у сфері безпеки (включно з інформаційними); загострюються проблеми захисту інформації та інтелектуальної власності (особливо в інтернеті) ".[490]

Підсумовуючи, зазначимо, що забезпечення інформаційної безпеки людини, суспільства і держави, на рівні національного законодавства і зусиллями виключно однієї держави, в сучасних умовах вбачається неефективним; оскільки



загрози інформаційній безпеці набувають глобального виміру, отже вимагають спільних зусиль на міжнародному рівні.

На нашу думку, міжнародна інформаційна безпека як складова міжнародної безпеки відображає сучасні геополітичні процеси. На фоні глобалізаційних процесів політичного, економічного та соціального розвитку протистояння основних геополітичних гравців відбувається, насамперед, у інформаційному просторі. Дубов В.Д. називає таке протистояння ключових геополітичних суб'єктів, яке відбувається переважно в кіберпросторі «холодною війною v2.0.[490,с.13]». До цих ключових суб'єктів науковець відносить, насамперед США, КНР, РФ та ЄС. Власне їх внутрішня та зовнішня інформаційна політика суттєво впливає на стан міжнародної, в т.ч. інформаційної безпеки, а їх протистояння обумовлює вибір позицій іншими учасниками міжнародних відносин і формування їх політики щодо інформаційної безпеки. Тому в наступному підрозділі пропонуємо дослідити правове забезпечення інформаційної безпеки в законодавстві цих суб'єктів. Також приділимо увагу інформаційному законодавству та реаліям інформаційної безпеки окремих держав, чий досвід з огляду на історичні, геополітичні, правові чи економічні тенденції може бути цінним для України.

#### **4.2. Підходи до правового регулювання відносин у сфері інформаційної безпеки людини в США та країнах ЄС**

Становлення правового регулювання сфери інформаційної безпеки розпочалось наприкінці ХХ століття. Насамперед, усвідомлення загроз, що виникають у зв'язку з розвитком інформаційних технологій, соціально-економічними, військовими та політичними наслідками останньої інформаційної революції, мало місце в країнах, що перші розпочали активну трансформацію у напрямку побудови інформаційного суспільства. Одними з перших держав, які розпочали розробку національної інформаційної політики та політики у сфері інформаційної безпеки стали Сполучені Штати Америки та Японія, а слідом за ними – переважна більшість розвинених країн світу.

При цьому вибір означених напрямів політики та форм їх закріплення у національній правовій системі суттєво відрізняється і обумовлений низкою історичних, культурних, правових та економічних чинників. Так, наприклад, у США увага акцентується на технологічних аспектах, у Європі – на соціальних вимірах. Всі держави-члени Євросоюзу мають власні програми національної політики щодо побудови інформаційного суспільства, а також кібербезпеки; окрім того мають спільні директиви ЄС щодо питань, які досліджуються. Японія, розпочавши активно після Другої світової війни побудову власної моделі інформаційного суспільства, на початку нового тисячоліття втратила оберти. Натомість, швидкими темпами почав розвиватись ринок інформаційних технологій в азіатських країнах – Республіці Корея, Тайвані, Гонконгу та Сінгапурі. Велика Британія послідовно проводить політику максимального надання інформації і послуг громадянам з боку держави через інтернет. Канада намагається максимально зберігати культурну різноманітність і національну ідентичність перед загрозою інформаційної експансії США. Російська Федерація та інші країни пострадянського простору розпочавши від єдиних вихідних позицій за менш як 30 років сформували власні підходи до інформаційної політики, що відрізняється як за змістом, так і за формами та ступенем реалізованості.

Перш ніж перейти, до розгляду правового регулювання інформаційної безпеки людини у різних країнах світу, вважаємо за необхідне зазначити, що ці питання визначаються на межі інформаційної політики держав та політики національної безпеки. При цьому, має значення сукупність історичних чинників, політичного і економічного розвитку, фінансових і матеріальних ресурсів, що впливають в цілому на розбудову інформаційного суспільства та демократизацію процесів, зокрема:

геополітичне становище – вибір моделі правового регулювання питань інформаційної безпеки значною мірою залежить від зовнішньо політичних пріоритетів держави; інформаційної політики сусідів, а також приналежності до міжнародних організацій;

макроекономічна ситуація – умовою належного ступеня інформаційної безпеки людини, суспільства і держави є розбудова надійної інформаційної інфраструктури, існування якої, в свою чергу, є основою для подальшого розвитку;

особливості ідеології та національної культури – найбільш яскравим прикладом, напевно, будуть держави з комуністичною ідеологією та тотальним контролем за інформаційним простором з боку держави; але не лише – в демократичних країнах з різними традиціями державотворення віддається перевага різним аспектам інформаційної безпеки;

специфіка правової системи – чи вона сприяє і забезпечує, чи навпаки гальмує становлення інформаційного суспільства, дотримання в ньому прав і свобод людини, а також захист національних інтересів держави в інформаційній сфері.

Слід звернути увагу, що правове регулювання питань інформаційної безпеки людини є складовою системи права окремої держави, а отже обумовлено особливостями такої системи і традиціями нормотворчості. Чим більш еластичним є правотворчий процес, тим швидше відбувається становлення нових інститутів права і законодавства. Певною мірою, швидкі темпи становлення інформаційного законодавства в США були можливі завдяки системі загального права, яка дозволила реагувати на появу нових суспільних відносин, що виникали у зв'язку з інтенсифікацією інформаційних процесів в усіх сферах життя людини, суспільства і держави.

Брижко В. вважає, що навіть Японія, яка вважається меккою виробництва цифрової техніки та використання найсучасніших ІТ-технологій, відстає від США більше ніж на п'ять років у сфері розповсюдження персональних комп'ютерів, кабельного телебачення, цифрової телефонії та в інших аспектах інформаційної політики [62, с.32-36].

Створена в США система державного регулювання в інформаційній сфері, має на меті ефективне використання сучасних інформаційних технологій для прискорення розвитку економіки, водночас, враховує питання інформаційної безпеки у складі національної безпеки. В США вже на початок ХХ сторіччя

сформувалась система забезпечення інформаційної безпеки, яка спрямована насамперед на убезпечення єдиного інформаційного простору США, проте лише частково відповідає на питання щодо інформаційної безпеки людини.

Американська модель покладена в основу багатьох моделей формування інформаційного суспільства. Американська модель, або модель Кремнієвої долини, побудови інформаційного суспільства була заснована на індивідуалізмі, розвиненості ринку ідей, ризикованому підприємництві при задекларованих мінімальних функціях держави, що обмежуються створенням умов для розвитку ринкових сил.

На думку Бусола О., державна політика США у сфері інформаційної безпеки пройшла тривалий еволюційний шлях, який складається з чотирьох етапів: виникнення – 1939–1947 рр.; становлення – 1947–1982 рр.; активний розвиток – 1983–2001 рр.; докорінне вдосконалення – 2001 р. – дотепер [67]. Її історичні корені сягають початку значно глибше, ніж утворення у 1957-му р. військового агентства передових досліджень ARPA (Advanced Research Projects Agency), мережевий проект якої ARPANET і став першим кроком до повстання інтернету.

Очевидно, що ключовим напрямом розвитку інформаційної безпеки, стало забезпечення національної безпеки. Початки нормативно-правового регулювання сфері інформаційної безпеки сягають початку ХХ століття. Зокрема, перший закон у сфері інформаційної безпеки держави - "Про захист інформації" був прийнятий у США ще у 1906 р. Проте інтенсивний розвиток законодавства щодо інформаційної безпеки розпочався після винайдення комп'ютерів та створення мережі ARPANET, в основу якої були покладені ідеї, спрямовані на: цілковиту приватизацію і лібералізацію ринку інформаційних технологій, зокрема, підкреслювалась непотрібність громадського контролю за розвитком мереж і їх контенту; первинну роль побудови мереж, на базі яких і розвиваються послуги (на відміну від європейської моделі, де відзначається пріоритетний розвиток сектора послуг, а вже потім - його технічного, мережевого забезпечення); універсалізацію телекомунікаційного обслуговування для всіх.

Важливим етапом розвитку інформаційного суспільства в США стало прийняття в 1966 р. Акту про свободу інформації та у 1976 р. Акту про

висвітлення діяльності уряду. Ці документи, стали основою для реалізації прав громадян на доступ до інформації.

У 1974 р. був прийнятий Акт про охорону персональних даних, що визначав категорію «право на приватність» як особисте і фундаментальне право, яке охороняється Конституцією США. Також було встановлено заборону на збір і збереження інформації про те, як індивід здійснює свої права, передбачені першою поправкою до конституції (свободу слова і друку, свободу віросповідання, свободу зборів і подачі петицій), за винятком випадків, коли це прямо передбачено законом або дозволене самим індивідом, або коли це має безпосереднє відношення до правоохоронної діяльності.

У 1986 р. було прийнято Акт про комп'ютерну безпеку (Computer Security Act), яким визначено значимість безпеки інформаційних систем для всього суспільства. Створено Національний інститут стандартів і технологій, на який покладались обов'язки щодо моніторингу можливих загроз, та напрацювання шляхів захисту, як у державних інформаційних системах, так і в приватному секторі. Також цим актом фактично регламентувалась координація діяльності міністерств і відомств, включаючи Міністерство оборони, Міністерство енергетики, Агентство національної безпеки та інших з метою уникнення дублювання і несумісності.

Важливою складовою системи правового забезпечення інформаційної безпеки стало встановлення на федеральному рівні кримінальної відповідальності за злочини у сфері комп'ютерної інформації в Акті про підробку засобів доступу, комп'ютерне шахрайство та зловживання (Counterfeit Access Device and Computer Fraud and Abuse Act). Цей акт встановлює відповідальність за сім основних протиправних діянь, якими визнаються: (1) комп'ютерне шпигунство, яке полягає в несанкціонованому доступі до інформації або перевищенні його меж, а також отриманні інформації, що стосується державної безпеки, міжнародних відносин і питань атомної енергетики; (2) несанкціонований доступ до інформації з урядового відомства США з будь-якого захищеного комп'ютера, котра має відношення до внутрішньої або міжнародної торгівлі, або перевищення меж такого доступу, а також одержання інформації з фінансових записів банківської

установи, емітента карт чи інформації про споживачів, що містяться у файлі управління обліку споживачів; (3) вплив на комп'ютер, що перебуває у виключному користуванні урядового відомства США, або порушення нормального функціонування комп'ютера, котрий повністю чи частково використовується урядом США; (4) шахрайство з використанням комп'ютера – доступ, здійснений із шахрайськими намірами, і використання комп'ютера з метою отримання будь-якої цінності за допомогою шахрайства, включаючи незаконне використання машинного часу вартістю більше п'яти тисяч доларів протягом р., тобто без оплати користування комп'ютерних мереж і серверів; (5) умисне або необережне пошкодження захищених комп'ютерів; (6) шахрайство шляхом торгівлі комп'ютерними паролями або аналогічною інформацією, що дозволяє одержати несанкціонований доступ, якщо така торгівля впливає на торговельні відносини між штатами та з іншими державами або на комп'ютер, що використовується урядом США; (7) погрози, вимагання, шантаж й інші протиправні діяння, вчиненні з використанням комп'ютерних технологій.

Відповідальність за комп'ютерні злочини в інформаційному просторі встановлена й іншими параграфами Зводу законів США, зокрема, за торгівлю викраденими або підробленими пристроями доступу, які можуть бути використані для отримання цінностей (грошей, товарів чи послуг); за умисне пошкодження майна, устаткування, контактних пунктів, ліній або систем зв'язку. Передбачена також відповідальність за перехоплення й розголошення повідомлень, переданих по телеграфу, усно або з використанням комп'ютерів; за порушення конфіденційності електронної пошти шляхом незаконного доступу до збережених повідомлень, а також за створення перешкод для санкціонованого доступу до таких повідомлень.

Важливою ознакою американської моделі правового забезпечення інформаційної безпеки є пріоритет національних інтересів при вирішенні питань безпеки інформації (у тому числі і приватної). Зокрема, вже згадуваний Computer Security Act декларує, що вимоги державних органів щодо забезпечення необхідного рівня захисту інформації можуть бути поширені на будь-яку "важливу інформацію". При цьому встановлено, що "важливою" є така

інформація, "втрата якої, неправильне використання, несанкціонована зміна якої чи доступ до якої можуть призвести до небажаних впливів на національні інтереси". Крім того, в США законодавчо закріплено така категорія як "несекретна інформація, важлива з точки зору національної безпеки". До цієї категорії віднесено практично всю несекретну інформацію урядових відомств, а також велику частину даних, які циркулюють чи обробляються в інформаційно-телекомунікаційних системах приватних фірм і корпорацій, що працюють за урядовими замовленнями.

Поступово роль Національного інституту стандартів і технологій посилювалась, так у 1997 р. з'явився Computer Security Enhancement Act, положеннями якого був зобов'язаний на запит приватного сектора готувати стандарти, посібники, засоби і методи для інфраструктури відкритих ключів, які дозволяють сформувати недержавну інфраструктуру, сумісну з федеральними інформаційними системами, а також з урахуванням аналізу засобів і методів оцінки уразливих місць інших продуктів приватного сектора в сфері інформаційної безпеки.

Хоча на початкових етапах США декларували мінімальне втручання держави в сферу розвитку інформаційних технологій та наприкінці XX століття ситуація суттєво змінилась. У 90-х роках забезпечення інформаційної безпеки здебільшого було прерогативою ФБР, Міністерства юстиції та Міністерства оборони США. Зокрема, останнє здійснювало реалізацію концепції "Інформаційного протиборства", яка в 1996 р. була закріплена нормативно як польовий статут армії США "Інформаційні операції".

А початком сучасної цілеспрямованої систематичної організаційної діяльності у сфері інформаційної безпеки на національному рівні можна вважати директиви адміністрації Президента Б. Клінтона Presidential Decision Directive 63 "Захист критично важливої інфраструктури" 1998 р., та підписаний на його основі "Загальнонаціональний план захисту інформаційних систем" у 2000 р., який визначив основні напрями діяльності держави та суспільства у сфері забезпечення інформаційної безпеки.

Суттєвих змін зазнала система інформаційної безпеки США після подій 11 вересня 2001 р.. Актом про посилення повноважень спецслужб було визначено як одна з форм тероризму, несанкціоноване проникнення в державні комп'ютерні мережі з метою отримання вигоди чи нанесення шкоди, а також суттєво збільшено повноваження ФБР США щодо моніторингу інтернету. Повноваження поліції та федеральних агентств щодо нагляду за громадянами були розширені іншим Актом про патріотизм (USA Patriotic Act).

Важливою також була норма, що визначала критичну інфраструктуру як «сукупність фізичних чи віртуальних систем і засобів, важливих для США в такій мірі, що їхній вихід з ладу чи знищення можуть призвести до згубних наслідків в галузі оборони, економіки, охорони здоров'я і безпеки нації».

Актом про боротьбу з тероризмом (Combating Terrorism Act) у 2001 р. було скасовано необхідність отримання дозволу суду для прослуховування приватних переговорів і моніторингу мережі. Достатньо було обґрунтувати наявність однієї з двох обставин: існування "нагальної загрози" інтересам національної безпеки США або атака на функціональну дієздатність комп'ютера, який знаходиться під захистом, щоб отримати дозвіл прокурора.

При Міністерстві оборони США було створене Бюро оперативно-інформаційного реагування задля побудови пошукової системи, яка з метою виявлення підозрілих осіб чи груп зможе мати доступ практично до всіх існуючих баз даних.

В 2002 р. Актом про внутрішню безпеку (Homeland Security Act) було змінено систему національної безпеки США і утворено Міністерства внутрішньої безпеки (Department of the Homeland Security), якому підпорядковувались всі урядові структури безпеки. Цей же акт передбачував заснування мережевої гвардії (NET Guard) з метою ліквідації наслідків атак терористів на інформаційні ресурси і мережі зв'язку.

Акт про підвищення кібернетичної безпеки (Cyber Security Enhancement Act) 2002 р. посилив відповідальність за злочини у сфері високих технологій, а також визначав нові заходи кібербезпеки критичної інфраструктури .



Формування нової системи безпеки було визначено Національною стратегією боротьби з тероризмом (The National Strategy for Combating Terrorism), Національною стратегією фізичного захисту критичної інфраструктури (The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets) та Національною стратегією безпеки кібернетичного простору (The National Strategy to Secure Cyberspace). Цими документами з огляду на залежність інфраструктури США від стану захищеності інформаційних систем і мереж, було передбачено створення Єдиної національної системи реагування на кібернетичні напади (National Cyberspace Security Response System), як перший з п'яти головних пріоритетів діяльності США по забезпеченню інформаційної безпеки. Наступними були: реалізація комплексної системи заходів по зменшенню загроз інформаційної безпеки; забезпечення підготовки спеціалістів у сфері комп'ютерної безпеки та відповідального відношення всього населення до питань захисту інформації; забезпечення захисту інформаційних систем, які мають відношення до державних органів; розвиток різних форм співпраці у сфері забезпечення інформаційної безпеки [286].

Пріоритетами національної інформаційної політики США було визначено: підтримку досліджень і розробок у галузі інформації і комунікації; вплив на їхнє спрямування та заохочення до поширення технічних знань і можливостей в економіці; сприяння обміну технологіями між лабораторіями та фірмами, запровадження нововведень на ринках; побудову та вдосконалення інформаційної інфраструктури, контроль за її діяльністю, побудову глобальних систем комунікації і дослідження впливу систем на міжнародні, національні та приватні пріоритети; збереження порушеної новими технологіями рівноваги між чотирма основними інформаційними цінностями: конфіденційність інформації, інформацію як суспільне благо, інформацію як товар, інформацію як невіддільний компонент існування держави; недоторканність приватного життя, конфіденційність інформації приватного характеру на різних рівнях і в різних сферах державного управління та в приватному секторі; творення урядової політики в галузі інформації і комунікації [436,с.24-25].

Подальша політика США в сфері інформаційної безпеки поєднувала такі аспекти: зміцнення системи забезпечення інформаційної безпеки США; домінування США в глобальному інформаційному просторі; намагання поєднати ринкові інструменти в регулюванні інформаційної сфери з широкими повноваженнями держави в особі уповноважених органів по контролю над інформаційними ресурсами.

З 2009 р. було прийнято кілька Актів про кібербезпеку (The Cybersecurity Act), проте в першому з них було передбачено повноваження Президента США відключати доступ до мережі на всій території США у надзвичайних випадках загроз національній безпеці [650].

Тодішній президент США Б. Обама виклав власні погляди на проблему кібербезпеки у Зауваженнях щодо кібербезпеки 2009 р., де назвав цифрову інфраструктуру США "стратегічною національною цінністю", а захист цієї інфраструктури – національним пріоритетом [626]. На початку березня 2010 р. Президентом США була затверджена чергова "Ініціатива зі всеосяжної національної кібербезпеки" Ради національної безпеки США у складі розділу Воєнної доктрини США, що стосується кібернетичної оборони. Документом передбачено створення єдиної федеральної мережі, пов'язаної захищеними каналами зв'язку, а також об'єднання всіх центрів оперативного реагування на кіберзлочини з метою підвищення ефективності їх діяльності та проведення більш глибокого аналізу хакерських атак.

Стратегія кібербезпеки США 2011 р., запропонована Президентом США Б. Обамою, якою передбачено право США приймати заходи у відповідь на ворожі дії у кіберпросторі, розглядаючи їх як будь-які інші загрози. Тобто, хакерські атаки прирівняні керівництвом США до оголошення війни.

В 2012 р. Сенат США прийняв Акт CISPA (Cyber Intelligence Sharring and Protection Act), який дозволив Уряду США, приватним агентствам безпеки та будь-яким приватним компаніям за наявності підозр про вчинення кіберзлочину отримати доступ до конфіденційної інформації користувачів і комерційних організацій, також посилив можливості американських правоохоронних органів

та правовласників у боротьбі з незаконним контентом в інтернеті, торгівлею інтелектуальною власністю, захищеною авторським правом, і контрафактом.

А в 2015 р. Сенат США проголосував за Акт про обмін інформацією в галузі кібербезпеки (The Cybersecurity Information Sharing Act), метою якого визначалось "забезпечення кібербезпеки в Сполучених Штатах шляхом посилення обміну інформацією про загрози кібербезпеки та для інших цілей " [565] Цим актом визначається порядок надання технологічними та виробничими компаніями інформації про трафік в інтернеті уряду США. Цей акт мав значну кількість противників, на думку яких він підвищує ступінь вразливості особистої приватної інформації та дозволяє доступ до особистої приватної інформації семи державним установам, в т.ч. місцевій поліції.

Слід зазначити, що правовідносини щодо інформаційної безпеки, урегульовані здебільшого на федеральному рівні, і становить понад 300 актів. Тоді як на рівні штатів здебільшого визначається відповідальність за злочини в інформаційній сфері.

Аналіз федерального законодавства щодо інформаційної безпеки свідчить про пріоритет національної безпеки перед дотриманням прав і свобод людини. Тим не менш, має місце значний масив нормативних актів що регулює питання дотримання інформаційних прав і свобод людини, які закріплені в поправках до Конституції США. Зокрема, інформаційну безпеку людини в США слід пов'язувати з гарантованістю прав та свобод, передбачених першою поправкою до Конституції США, яка гарантує, що Конгрес США не буде видавати закони щодо впровадження будь-якої релігії чи заборони вільно сповідувати її, а також не має права видавати закони, що обмежують свободу слова, друку і права народу мирно збиратися і звертатися до уряду з проханням усунути якусь кривду.

Позицію США щодо інформаційної безпеки в міжнародних відносинах та зовнішній політиці відображає Міжнародна стратегія щодо кіберпростору. «Процвітання, безпека та відкритість мережевого світу». В ній відображено орієнтацію на мілітаризацію інформаційної сфери, більш тісну координацію політичних і силових структур з кібербезпеки, а також визначенням військових й невійськових аспектів психологічних та інформаційних операцій.

## **Країни ЄС та Сполучене Королівство Великої Британії та Північної Ірландії.**

Країни ЄС демонструють спільну позицію щодо інформаційної безпеки та стандартів прав людини в інформаційній сфері, при чому така позиція є динамічною і постійно зазнає переосмислення. При цьому вона значною мірою базується на передумовах побудови інформаційного суспільства в країнах Європи – розвиненій економіці та соціальній спрямованості політики. Європейці, які мають певний обсяг благ, що гарантований певною мірою, системою соціальної захищеності, значно більше цінують можливість самореалізації, вільний час, можливість спілкування, а також захищеність приватного життєвого простору. Тому в інформаційній політиці ЄС спостерігається пошук деякого балансу між контролем з боку держави і ринковими законами. ЄС намагається віднайти формулу динамічного поєднання державних і суспільних інтересів. Тому основні відмінності між американською і європейською моделями розбудови інформаційного суспільства, а також розумінням інформаційної безпеки лежать в площини соціального спрямування внутрішньої політики ЄС.

Позиція, що відображала спільну європейську політику щодо інформаційної безпеки була окреслена Європейською Комісією в документі під назвою «Мережева та інформаційна безпека: європейський політичний підхід» у 2001 р. [550]. Під «мережевою та інформаційною безпекою» визначались здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі і системи. Більш широкий підхід до розуміння щодо змісту поняття "інформаційна безпека" був сформульований представником Швеції при обговоренні питань міжнародної інформаційної безпеки на 56-й сесії Генеральної Асамблеї ООН, згідно з якою інформаційна та мережева безпека означає захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації і створення надійного джерела постачання обладнання, послуг та

інформації, а також охоплює захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. При цьому, недостатній захист життєво важливих інформаційних ресурсів та інформаційних і телекомунікаційних систем може створити загрозу міжнародній безпеці [575].

Таким чином, в ЄС спостерігається чітке розмежування особливостей інформаційної безпеки людини і суспільства, інформаційної безпеки держави та міжнародної інформаційної безпеки. При цьому основоположними стали власне інтереси людини і суспільства, що й обумовило інтенсивний розвиток таких напрямів як безпека персональних даних, доступ до інформації, а також забезпечення реалізації демократії в умовах побудови інформаційного суспільства. Окремим рядком слід відзначити правове забезпечення протидії кіберзлочинності, яке обумовлене як обраним напрямом на розбудову інформаційного суспільства, так і традиційно визначальною роллю держави в захисті прав та законних інтересів її громадян.

Базовий міжнародний нормативно-правовий документ, що регулює суспільні відносини у сфері боротьби з кіберзлочинністю - Конвенція Ради Європи "Про кіберзлочинність" від 23 листопада 2001 р., був створений власне під впливом європейської правової думки. Найбільш близьким за змістом до нього є Кримінальний кодекс ФРН.

В Резолюції Ради ЄС № 2003/С 48/01 від 18 лютого 2003 р. про європейський підхід до культури мережі та інформаційної безпеки, державам-членам було запропоновано сприяти забезпеченню безпеки, як важливій складовій управління на державному і приватному рівнях, шляхом розподілу відповідальностей; надавати належну освіту та підвищувати рівень обізнаності у питаннях безпеки, особливо в молодіжних колах; вживати відповідних заходів з метою запобігання та усунення випадків порушення безпеки, зокрема, шляхом: безперервного вдосконалення ідентифікації і оцінки проблем безпеки та застосування відповідних способів управління; визначення ефективних способів повідомлення всіх зацікавлених сторін про необхідність вчинення певних дій, через покращення діалогу на Європейському і національному рівнях та, якщо необхідно, на міжнародному рівні, особливо, з тими, хто забезпечує технологіями інформаційне

суспільство та надає послуги; забезпечувати належний обмін інформацією відповідно до потреб суспільства у поінформованості щодо належних практик у сфері безпеки; заохочувати до співпраці і партнерства наукових та ділових кіл з метою розробки технологій безпеки і розробки та затвердження загальновизнаних стандартів.

Зусилля, що робляться на міжнародному рівні, пов'язані з діями з реформування кримінального законодавства на національному рівні. Насамперед, кожна з країн ЄС має власну стратегію кібербезпеки – наприклад, Стратегія безпеки та оборони інформаційних систем Франції, Національна стратегія кібербезпеки Королівства Нідерланди, Стратегія кібербезпеки Німеччини, Політика захисту кіберпростору Республіки Польща та інші.

У 2004 р. було створено європейське агентство по мережевій і інформаційній безпеці з метою підвищення ефективності функціонування внутрішнього ринку. Агентство виступає в ролі консультанта і центру передових технологій у сфері мережевої і інформаційної безпеки для країн-членів і інститутів ЄС. Агентство сприяє розвитку зв'язків між країнами-членами ЄС, інститутами ЄС, господарюючими суб'єктами і приватним бізнесом [99].

У січні 2013 р. в Гаазі повстала наступна інституція ЄС - Європейський центр боротьби з кіберзлочинністю, завдання якої є припинення діяльності організованих злочинних мереж. Найбільше уваги приділяється протидії в трьох напрямках - онлайн-шахрайство, що заподіює великий збиток фінансовим організаціям і їх клієнтам; поширення дитячої порнографії, кібератаки на ключові інфраструктури і інформаційні системи [129].

У 2016 р. Європейський парламент прийняв Директиву ЄС щодо мережевої та інформаційної безпеки, метою якої є встановлення загальних стандартів кібербезпеки та покращення співпраці між країнами ЄС [651]. Її положення мають допомогти компаніям більш ефективно боротися з хакерами та запобігати нападам на цифрову інфраструктуру, над якою мережа охоплює багато країн або весь Союз.

Інциденти, пов'язані з кібербезпекою, часто є транскордонними і, таким чином, охоплюють більше однієї держав-членів ЄС. Фрагментарний захист

безпеки поставив під великий ризик інформаційну інфраструктуру у всій Європі, ця директива встановила загальний рівень мережі та інформаційної безпеки з метою запобігти майбутнім кібератакам на важливі взаємопов'язані європейські системи [556]. Згідно з директивою, держави-члени повинні підготувати списки "ключових постачальників послуг". Це підприємства, що працюють у ключових галузях економіки, а також важливі для суспільства, і тому потребують спеціального захисту. Це суб'єкти господарювання з таких секторів, як енергетика, транспорт, охорона здоров'я, банківське та водопостачання (питною водою). Держави-члени ЄС повинні будуть ідентифікувати підприємства, що працюють у цих регіонах, відповідно до критеріїв, викладених у Директиві. Цей список включає, наприклад, провайдерів послуг, які мають вирішальне значення для "підтримки критичної соціальної або економічної діяльності", а інциденти, пов'язані з безпекою мережі, "мають суттєвий негативний вплив на надання послуги". Деякі інтернет-провайдери, хоча і не визнаються ключовими (оператори комерційних платформ, пошукових систем і хмарних сервісів), також зобов'язані, хоча й у меншій мірі, забезпечити свою інфраструктуру та повідомляти про серйозні інциденти національним властям.

Кожна країна ЄС зобов'язана була прийняти стратегію національної мережі та інформаційної безпеки. Передбачено створення стратегічних "груп співпраці" для обміну інформацією та підтримки держав-членів у створенні можливостей забезпечення безпеки мережних та інформаційних систем.

Наступним важливим напрямом є творення е-демократії та е-урядування. У цілому європейський підхід до інформатизації від самого початку значно більше був орієнтований на функціональне і практичне інформування населення, а не на розваги, як у США. Континентальна Європа творила більш суворе законодавство щодо регулювання ринку праці, продуктів і послуг, аніж приміром США чи Об'єднане Королівство. Державі відводилась значна роль у формуванні інформаційного суспільства, про що свідчать положення Резолюції Європейського Союзу «Біла Книга. Зростання, конкурентоспроможність, зайнятість: виклики та стратегії XXI століття»[667], Директиви ЄС «Зелена Книга.

Життя і працевлаштування в інформаційному суспільстві» [591] та Рекомендації «Інформаційна магістраль для глобального суспільства» [625].

У Декларації 1999 р. Європейського Союзу було сформульоване бачення "істинно демократичного інформаційного суспільства, заснованого на фундаментальних цінностях Ради Європи, може бути побудоване за наявності основ політики, яка заохочує доступ і участь, компетентність і підготовленість, творчість і різноманіття та забезпечує відповідний захист.

В 2000 р. була підтримана ініціатива Європейської Комісії під назвою «Електронна Європа» (eEurope), яка пізніше була закріплена в документі «Електронна Європа — інформаційне суспільство для всіх». Процес розвитку електронного урядування в Європейському Союзі відображають програмні документи: - План дій «e-Europe 2002» [574], План дій «e-Europe 2005» [575], План дій «e-Government i-2010» [576], а також Цифровий порядок денний для Європи (Digital agenda for Europe) як складова Стратегії Європа 2020 [576].

Перший зі згаданих планів передбачав розвиток за трьома напрямками:

1) Дешевий, швидкий, безпечний інтернет: дешевий і швидкий доступ до інтернету; швидкий інтернет для дослідників та студентів; безпечні мережі та смарт-карти;

2) Інвестиції в людей і вміння: європейська молодь у цифрову добу; робота в економіці, заснованій на знаннях; участь для всіх в економіці, заснованій на знаннях;

3) Стимуляція використання інтернету: розвинена е-комерція; урядові он-лайн: електронний доступ до публічних послуг; медицина в мережі; європейський цифровий зміст (контент) для глобальних мереж; розумні транспортні системи.

Резолюція Ради № 2003/С 48/02 від 18 січня 2003 р. щодо імплементації Плану дій e-Європа 2005 заохочувала держав-членів робити все можливе, з допомогою контрольних індикаторів, що містяться в Додатку, для досягнення мети Плану дій, стимулювати мережеву безпеку та широкополосні мережеві послуги, а також електронне управління, електронний бізнес, електронне здоров'я та електронне навчання, беручи до уваги особливості національних, інституційних та адміністративних структур; працювати з усіма зацікавленими



особами для ефективної імплементації Плану дій; до середини 2003 р. надати оглядові матеріали національних заходів та дій які були застосовані для досягнення мети Плану дій; призначити високого представника для керуючої групи.

Кожен наступний план певною мірою конкретизував, а часом і змінював підходи до розуміння перспектив інформаційного розвитку держав Європейського співтовариства. Спільним було бачення, що держави мають щодо доступу до нових інформаційних технологій і участі в них: сприяти максимально широкому доступу усіх до нових інформаційних і комунікаційних послуг; надати можливість усім особам відігравати більш активну роль у житті суспільства на національному, регіональному і місцевому рівнях за допомогою використання нових інформаційних технологій; заохочувати вільний обмін інформацією, думками й ідеями з використанням нових інформаційних технологій; заохочувати розробку і виробництво матеріалів культурного й освітнього призначення та їх широке поширення; заохочувати ефективне міжнародне співробітництво з метою реалізації переваг розширення доступу і збільшення прозорості; сприяти створенню рівних можливостей використання нових інформаційних технологій усіма європейськими країнами.

Таким чином, держава не лише має забезпечити свою присутність у мережевому просторі, а, насамперед, досягати спільних (для влади і суспільства) цілей: зміцнювати і розширювати форми комунікації та співпраці між суспільством і державою; більш ефективно здійснювати економічний і соціальний розвиток суспільства; підвищувати ефективність реагування влади на соціальні проблеми; зменшувати вартість послуг населенню; підвищувати прозорість публічного управління [303, с. 412-422].

Електронна Європа -2010 об'єднує в собі всю політику, ініціативу і дії Європейського Союзу, які направлені на стимулювання розробки й використання цифрових технологій у повсякденному, робочому й особистому житті, і формулює ключові цілі. Згідно з цією стратегією, першочерговими завданнями, що постають перед державами-членами Європейського Союзу у процесі становлення єдиного європейського кіберпростору, є: введення єдиних

стандартів, узгодження програмних платформ та забезпечення сумісності комунікаційних технологій; підвищення швидкості доступу до широкосмугових мереж зв'язку в Європі; розробка нових та збагачення змістової наповненості існуючих спільних інформаційних ресурсів; охорона інформаційних ресурсів від кіберзлочинів, шкідливого змістового наповнення і невдалих технологій; модернізація правової основи для аудіовізуальних послуг; усунення «цифрового розриву». На сучасному етапі розвитку е-урядування в ЄС найбільш вагомими напрямками є програми: «Електронна митниця» (eCustoms), «Електронний паспорт» (ePassport), «Електронне голосування» (eVoting) тощо<sup>42</sup>.]

Кабінет Міністрів Ради Європи визначає такі елементи е-уряду: портал державних послуг; мережева інфраструктура та центри обробки даних; інфраструктура інтеграції та пересилання електронних повідомлень; Інфраструктура ідентифікації та авторизації; стандарти та архітектура в сфері електронного уряду та інформаційні системи, що забезпечують їх функціонування; системи, орієнтовані на підвищення ефективності роботи відомств: електронні архіви та управління документами, управління знаннями, національні облікові системи, реєстри, кадастри тощо; електронні закупівлі; інформаційні системи, створювані на національному рівні в інтересах регіональних та місцевих органів влади; інформаційні системи в галузі бюджетних (публічних) послуг: освіта, охорона здоров'я, охорона правопорядку.

Всі держави-члени ЄС в тій чи іншій мірі розвивають е-урядування. Варіативність і політична спрямованість програм у різних країнах, обумовлена низкою чинників, як-то - культура організації та культура управління, культура праці, прийняті норми поширення та використання інформації, особливостями використання частот, ступенем використання різними аудиторіями для різних видів технологій, особливостями національного законодавства, темпами становлення інформаційної (інтелектуальної) економіки тощо.

Одним із флагманів електронного урядування стала Естонія, яка хоча й розпочала далеко не першою – у 2003 р., проте шлях розвитку є дуже інтенсивним. Переважна більшість існуючих інформаційних систем органів влади

---

<sup>42</sup> Основні програми електронного урядування в ЄС.

і багатьох недержавних установ об'єднані в єдину систему. Наприклад, через інтернет-банкінг проводиться 98 % банківських операцій країни [258]. Громадяни Естонії можуть брати участь у виборах за допомогою інформаційних технологій як на території, так і з поза меж держави.

При цьому Естонія чітко визначила для себе сфери втручання держави: модернізація законодавства; підтримка потенціалу приватного сектору в використовувати потенціал ІКТ; зміцнення взаємодії між державою та громадяни; підвищення обізнаності щодо переваг та ризиків в інформаційному суспільстві. А таких, власне, є немало, зокрема, недоліки безпеки ID-карт. Картки використовуються для доступу до широкого спектру цифрових послуг, від підписання документів до подання податкової декларації та перевірки медичних документів, а також іноземцями, які є резидентами в країні. 30 серпня 2017 р. міжнародна група дослідників поінформувала Адміністрацію Естонської інформаційної системи про вразливість, яка потенційно впливає на цифрове використання ідентифікаційних карток Естонії, ймовірна кількість ідентифікаційних карток, що є вразливими, близько 750 000, випущених з жовтня 2014 р., включаючи картки, що випускаються для електронних резидентів [638].

Десять років тому, досвідчивши кібернетичну атаку, яка призвела до знищення таких систем як інтернет-банкінг, Естонія створила єдине агентство, відповідальне за захист кібербезпеки, і визначило підхід «колективного розуму» до широкого обміну інформацією про цифрові атаки та загрози. Вона створила окрему кіберкоманду у своїх збройних силах, а також підрозділ кіберзахисту в добровільній оборонній лізі.

Система електронного уряду в Естонії, зокрема, та в ЄС в цілому, розглядається як один із інструментів демократичного розвитку. Тому наступними кроками вбачаються реалізація е-демократії через врахування впливу ІКТ на основні права, підвищення участі громадян у прийнятті рішень, зокрема, шляхом публічного обговорення рішень, що приймаються органами публічної влади, та можливості впливати на них; підтримку участі у політичному житті як шляхом традиційних форм участі, так і через новітні інструменти, наприклад,

соціальні мережі та новітні медіа, е-петиції, соціальні мережеві платформи, платформи для публічного обговорення, краудсорсінг, а також бюджети участі.

Водночас, європейські країни постійно дбають про співвідношення транспарентності<sup>43</sup> інформаційної політики і забезпечення інформаційної безпеки. Політика транспарентності є багатовіковою традицією організації системи державного управління, що заснована на ліберально-демократичних цінностях. Перші нормативні акти, що мали на меті її забезпечення датуються ще 18 сторіччям і повстали власне у Європі - 2 грудня 1766 р. було видано Милостивий указ Його Величності, короля Швеції, про свободу письма й друку, яким визначено зокрема, що є відкритою інформацією, а що - таємною (в інтересах держави) [183].

Сучасна політика транспарентності ЄС спрямована на три ключові області: збільшення фінансової звітності; зміцнення особистої недоторканності і незалежності інститутів; введення більш суворого контролю на лобіювання.

Європейський підхід відображає зацікавленість всіх учасників в полегшенні доступу до інформації державних органів: задля забезпечення прозорості діяльності вищих органів влади, підвищенні довіри до владних структур і через розуміння правильності й доцільності прийнятих рішень, можливість розбудови сервісів і послуг комерційними структурами на основі відкритих даних, спрощення доступу до державних послуг, зменшення державних витрат шляхом скорочення бюрократії; розвиток загальноєвропейського ринку інформаційних послуг.

Як стратегічний напрям комунікаційної політики ЄС розглядається забезпечення необхідного балансу транспарентності та інформаційної безпеки.

Досвід європейських країн свідчить про те, що в них давно законодавчо визначаються обмеження щодо запровадження принципу транспарентності на окремі категорії інформації. Ці обмеження стосуються інформації про захист національної безпеки і міжнародних відносин, захисту приватного життя, комерційної конфіденційності, правоохоронної діяльності і забезпечення громадського порядку, інформації, отриманої конфіденційно [463, с.22-28].

---

<sup>43</sup> Транспарентність - забезпечення прозорості та відкритості в оприлюдненні інформації

На національному та на пан'європейському рівнях визначаються види інформації, які повинні і які не повинні розкриватися, а також строки через які мають розкриватись документи, доступ до яких є закритий протягом певного часу (в Ірландії цей строк, наприклад, становить десять років) [564]. Сформульовані кілька основних принципів розкриття інформації: діяльність у рамках спільної інформаційної політики безпеки і практики; розкриття інформації при наявності відповідного мандата, коли розкриття необхідно у зв'язку з правовими або нормативними вимогами; формування адекватної архітектури безпеки, коли повинні бути розкриті деталі безпеки, які можуть або сприяти або перешкоджати забезпечення безпеки; управління. Також принципи, при яких розкриття не рекомендується: не посилювати ризики, не розкривати нічого, що може створити ризик для центрів обробки даних або цілісності даних, що зберігаються в центрі обробки даних; не нашкодь: слід уникати розкриття інформації, якщо це може створити потенційну шкоду для клієнтів або партнера; управління відповідальністю, що вимагає уникнення розкриття інформації у випадку створення невинуватеної відповідальності; утримання від розкриття інформації при наявності відповідного мандата (якщо розкриття призвело б до порушення юридичних чи нормативних вимог, його слід уникати)[534].

Важливим аспектом транспарентизації інформаційної безпеки професор Тихомирова Є.Б. називає підвищення поінформованості та розуміння проблеми безпеки, а також базових знань у цій області, що може бути пов'язано з процесом масового просвітництва та формуванням культури транспарентності та інформаційної безпеки [463, с.22-28]. Аналітики RAND Corporation зазначають про залежність балансу між свободою, конфіденційністю і безпекою від співвідношення проблеми громадянських свобод та громадської безпеки. Результати досліджень свідчать, що люди готові відмовитися від деяких свобод і недоторканності приватного життя [577].

Проте, власне захисту приватності і персональних даних з кожним роком присвячується все більше уваги як в законодавчому регулюванні, так і наукових дослідженнях. І не останню роль у цьому відграє судова практика національних судів, Суду ЄС та Європейського Суду з прав людини.

Правове регулювання персональних даних в ЄС є широко досліджуваною темою в українській науці, зокрема, цим питанням приділяли увагу в своїх працях О. Баранов, В. Брижко, К. Мельник, Т. Обуховська, А. Пазюк, О. Рогова, а також перекладений українською «Посібник з європейського права у сфері захисту персональних даних», що був підготовлений Агентством Європейського Союзу із основоположних прав (FRA) та Радою Європи спільно з Секретаріатом Європейського суду з прав людини [321]. Тому ми звернемо увагу лише на основні акти і загальні тенденції.

Формування сучасного європейського законодавства про захист персональних даних розпочалось прийняттям в 70-80 роках ХХ століття окремими європейськими країнами національних законів про захист персональних даних. Наприкінці тисячоліття сформувався масив основних документів ЄС у галузі захисту персональних даних: Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних»; Директива 95/46/ЄС від 24.10.1995 р. «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних»; Директива 97/66/ЄС від 15.12.1997 р. «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі»; Директива 2002/58/ЄС від 12.07.2002 р. про обробку персональних даних та захист сектору електронних комунікацій; Регламент Європейського парламенту та Ради ЄС № 45/2001 від 18.12.2001 р. про захист фізичних осіб, що стосується обробки персональних даних установами і органами ЄС і щодо вільного переміщення таких даних; Директива 2005/28/ЄС від 08.04.2005 р., що встановлювала принципи та детальні настанови належної клінічної практики, які стосуються досліджуваних лікарських засобів для вживання людиною, а також вимог надання дозволу на виготовлення або імпорт таких продуктів; Рішення та рекомендації створеної згідно зі ст. 29 Директиви 95/46/ЄС в 1996 р. постійно діючої Робочої групи з метою гармонізації європейського права в сфері захисту персональних

даних та консультацій, а також рішення та рекомендації наглядових органів країн — учасниць ЄС.

З метою створення дієвого механізму контролю за діяльністю національних інституцій у 2000 р. було запроваджено незалежний інститут Європейського уповноваженого з захисту даних. Функції цього інституту подібні до функцій омбудсмена, але більш вузько спеціалізовані в межах захисту персональних даних. Головним критерієм діяльності Європейського уповноваженого з захисту даних є його незалежність від інших інституцій ЄС, що забезпечується спеціальним механізмом, закладеним в Регламенті [399,с.619-625].

Важливим кроком стосовно розвитку гарантій захисту персональних даних стало також впровадження норми Директиви, яка зобов'язує членів ЄС створювати спеціальні незалежні інституції, які повинні слідкувати за дотриманням принципів захисту персональних даних в кожній з держав-членів ЄС, а також розглядати та приймати рішення щодо скарг від своїх громадян з приводу порушення їх прав у сфері захисту персональних даних. На сьогодні фактично кожна держава-член ЄС має подібні інституції. Цей досвід є надзвичайно цінним, і на нашу думку, має бути вивченим і впровадженим в нашої державі.

Держави-члени ЄС при формуванні національного законодавства про захист персональних даних, хоча й зобов'язані були опиратись на стандарти вищезначених актів, але способи реалізації були різні: 1) шляхом створення єдиного акту про захист персональних даних; 2) шляхом створення спеціальних законів для різних сфер використання персональних даних.

Активний розвиток правового регулювання захисту персональних даних спостерігається в ЄС постійно. Сьогодні існує більш ніж 100 міжнародно-правових актів – Конвенцій, Протоколів, Директив, Рекомендацій Ради Європи та Європейського Союзу, які прямо або побічно відносяться до правового регулювання захисту персональних даних [63,с.45-57].

Проте навіть наявність такого обсягу не знімає всіх протиріч, що існують у цій сфері. У 2010 р. у своєму Повідомленні про “Комплексний підхід до захисту персональних даних у Європейському Союзі” Європейська Комісія дійшла

висновку про те, що Європейський Союз потребує більш комплексної та послідовної політики щодо основоположного права на захист персональних даних. В повідомленні особливо підкреслювалась роль технологічного прогресу та процесу глобалізації в створенні нових викликів у сфері захисту персональних даних. Окрім масового розповсюдження соціальних мереж, користувачами яких на сьогодні є більш ніж 300 млн. європейців, в якості прикладу незахищеності даних громадян в повідомленні також згадується так зване “хмарне зберігання даних”. При даній моделі зберігання інформації використовуються великі віддалені в мережі сервери, що надаються в користування клієнтам третьою особою. Інформація користувачів зберігається та обробляється, як правило, на одному віртуальному сервері. При цьому, маючи певні переваги, дана модель зберігання може нести в собі потенційну загрозу безпеці даних, особливо конфіденційним даним про особу[549,с.55-61].

З 2010 р. розпочато тривалу реформу, основні вимоги якої набирають чинності у 2018 р.. Пакет захисту даних становить три основних документи: Регламент (ЄС) 2016/679 від 27.04.16 р. “Про захист фізичних осіб у зв’язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальні Положення про захист даних)[628]”; Директива (ЄС) 2016/680 Європейського Парламенту і Ради від 27.04.16 р. “Про захист фізичних осіб у зв’язку з обробкою персональних даних компетентними органами в цілях запобігання, розслідування, виявлення або переслідування злочинця злочину або виконання кримінальних покарань, а також про вільне переміщення таких даних, і скасування Рамкового рішення Ради 2008/977/ПВД”[627]; Директива (ЄС) 2016/681 Європейського Парламенту і Ради від 27.04.16 р. “Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину”[627].

Серед головних цілей нового регулювання є приведення законодавства у сфері захисту персональних даних у відповідність до первинного права ЄС; посилення прав особи, а також поглиблення єдиного ринку ЄС. При цьому, аналіз документів свідчить про прагнення ЄС до запровадженні єдиних наднаціональних



стандартів захисту персональних даних. Регламент, відповідно до базових угод ЄС, має безпосередньо виконуватись державами-членами після його прийняття, (на відміну від Директиви, яку держава-член починає виконувати її положення лише після їх імплементації до національного законодавства). Регламентом передбачено ряд організаційних змін у забезпеченні захисту персональних даних. Зокрема, ним пропонується створити посади службовців з захисту персональних даних ("контролер" и "процесор"), які обов'язково мають бути у компаніях, де кількість персоналу перевищує 250 осіб, а також у державних установах. Вони будуть здійснювати спостереження за виконанням положень Регламенту на рівні компаній та забезпечуватимуть досягнення необхідних результатів. Нові правила застосовуються до обробки даних фізичних осіб у компаніях, підприємствах тощо, які розміщуються не тільки на європейській території, але і здійснюють свою діяльність за межами ЄС і пов'язані з обробкою персональних даних в рамках ЄС.

Змінюється також і регулювання транскордонної передачі даних. Компанії матимуть право передавати особисті дані до третіх країн, лише якщо в них створено такий же рівень захисту даних, як і в ЄС. Суд Європейського Союзу в жовтні 2016 р. оголосив недійсною угоду між США та країнами ЄС, відому під назвою "SafeHarbor" ("Безпечна гавань"), яка загалом дозволяла передачу даних і їх зберігання в США. ЄС і США ведуть перемовини про нову угоду. Нова угода про захист даних передбачає, що держави, в яких органи влади мають неспіврозмірний доступ до даних і здійснюють масове стеження за ними, більше не зможуть вважатися "безпечними гаванями" для даних. Компанії в Європі не мають права передавати дані безпосередньо органам влади в США чи ще де. Для цього в кожному конкретному випадку необхідна угода про правову допомогу між ЄС та третіми країнами. Крім того, особам має бути забезпечено можливість судового захисту у випадку неправомірного використання даних в третій країні.

Таким чином, масштабна робота здійснюється з одного боку в урядах держав-членів, з іншого – європейських інститутів. Подальший розвиток буде відбуватись в напрямках, визначених вже згадуваним Цифровим порядком

денним для Європи: створення єдиного цифрового ринку; розвиток інтероперабельності (експлуатаційної сумісності) і стандартів; розвиток довіри і безпеки користувачів онлайн-транзакцій; розвиток швидкісного інтернету; розвиток наукових досліджень та інновацій; підвищення навичок користувачів; використання ІКТ для вирішення соціальних проблем[562].

Ще одну сферу забезпечення, на яку хотілося б звернути увагу в аналізі інформаційної безпеки людини в країнах ЄС, становить боротьба з дезінформацією. У березні 2015 р. Європейська Рада доручила Верховному Представнику ЄС у співпраці з інституціями ЄС та країнами-членами ЄС представити план дій зі стратегічних комунікацій. Як наслідок, була створена оперативна робоча група для протидії кампанії з дезінформації з боку Росії.

Група займається розробкою комунікаційних матеріалів і кампаній, покликаних роз'яснити політику ЄС в регіоні Східного партнерства, в тому числі реалізує: попереджувальні кампанії зі стратегічних комунікацій, в основі яких лежить предметний аналіз, який роз'яснює ключові сфери політики ЄС і створює позитивний наратив ЄС; ситуативні комунікації з актуальних і значущих питань політики ЄС; аналіз дезінформаційних трендів, пояснення дезінформаційних наративів і спростування міфів.

Крім того, робоча група, в тісній співпраці з іншими акторами ЄС, надає підтримку зусиллям ЄС, спрямованим на зміцнення медіасередовища в регіоні Східного партнерства. Робоча група взаємодіє з інститутами ЄС, представництвами ЄС, країнами-членами і цілим рядом інших партнерів - як державних, так і недержавних - всередині ЄС і в країнах Східного партнерства. Мета цього широкого міжнародного співробітництва - обмін передовим досвідом у сфері стратегічних комунікацій та доступ до об'єктивної інформації в регіоні Східного партнерства, а також забезпечення підтримки незалежних ЗМІ в регіоні.

Одним з прикладів діяльності комісії є спростування міфів щодо нацизму в Україні. «Значна частина дезінформації, свідками якої ми стали за останні два тижні (вересень 2017 р.), зосереджена на все тій же меті - Україна. Ми побачили кілька звичайних сюжетів: «Україна - не держава», «Європа кинула Україну», «Україна позбавлена незалежності». Однак найчастіше повторюють ту частину

дезінформації, яка пов'язує Україну з нацистами. Так, країну звинуватили в тому, що вона стала неонацистських чудовиськом, створеним Заходом, і в тому, що її окупували нацисти, які йдуть слідами Геббельса. Ніхто особливо не згадав справжню окупацію деяких районів України»[538].

У зв'язку з тим, що Міністр закордонних справ Німеччини Габріель привітав Україну з Днем незалежності і використав в Твітері вираз «Слава Україні», щодо нього також було декілька дезінформаційних публікацій. У цьому вислові, нібито, приховано поширений нацистський слоган часів Другої світової війни. Хоча, насправді вислів «Слава Україні» використовується, як мінімум, з 1919 р. і знову став популярним після подій на Майдані в 2013-2014 рр.

Крім того, в деяких виданнях Україна змальовували жертвою «підступного Заходу», і почали повторювати це в цілях дезінформації. Група хакерів КіберБеркут заявила, що має докази того, що Україна є лишу випробувальним полігоном секретних експериментів США. Жодного доказу існування не неводилось, проте інформація була багаторазово про дубльована у виданнях Вірменії, Чехії, Грузії і Росії. На статтю «The Guardian» послався В. Соловйов в телепередачі «Недільний вечір», зі словами: «Було опубліковано інтерв'ю, в якому стали говорити: це правда, неправда». У традиційній манері прокремлівського дезінформування пізніше він припустив, що сьогодні практично неможливо дізнатися, як все було насправді»[538].

#### **4.3. Досвід правового регулювання відносин у сфері інформаційної безпеки людини у країнах Східного партнерства ЄС**

Політика Європейського Союзу, що мала на меті зміцнення стосунків зі східними сусідами ЄС і продовженням східного напрямку існуючої Європейської політики сусідства під назвою «Східне партнерство» була відкрита Європейським Союзом у 2009 р. Вона стосується шести країн пострадянського простору - України, Білорусі, Молдови, Вірменії, Грузії та Азербайджану. Хоча останнім часом точиться значна кількість дискусій щодо перспектив, так, глава МЗС Польщі В. Ващиковський, коментуючи перспективи «Східного партнерства» заявив, що «програма відводила згаданим державам лише роль буферної зони між

Росією та ЄС» [533]. Проте, власне ці два фактори – (1) проєвропейська політична спрямованість, а отже і спроби адаптації до законодавства і стандартів ЄС, а також (2) геополітична ситуація, що обумовлена значним впливом Російської Федерації, і визначили вибір цих країн задля дослідження соціально-правових питань інформаційної безпеки людини.

На сьогодні простежується тенденції певної диференціації в рамках "Східного партнерства", коли три країни - Україна, Грузія і Молдова – більш інтенсивно рухаються в напрямку ЄС, оскільки всі вони підписали Угоду про асоціацію з ЄС, а також отримали безвізовий режим.

У Молдові розроблений значний масив законодавчих актів в інформаційній сфері, до яких належать: Конституція, (ст. 32 Свобода думок і вираження; ст. 34 - Право на інформацію); Закон про свободу вираження поглядів (2010); Закон про пресу (1994); Закон про доступ до інформації (2000); Закон про прозорість процесу прийняття рішень (2008); Закон про захист персональних даних (2007, та нова редакція 2011); Закон про народного адвоката - омбудсмена (2014 р.); Закон про електронні комунікації (2007); Кодекс телебачення і радіо Республіки Молдова (2006); Закон про запобігання та боротьбу з кіберзлочинністю (2010).

Поруч із певними позитивними напрацюваннями мають місце загрозливі тенденції, втому числі пов'язані з проблемами реалізації положень законодавства. Зокрема, на думку експертів, мають місце випадки, коли положення Закону «Про захист персональних даних», а також Закону «Про державну таємницю» використовується владою, щоб обмежити публічний доступ до інформації.

Починаючи з 2010 р. в Молдові розробляється електронне урядування. У 2010 р. створений Урядом Республіки Молдова Центр електронного урядування ([www.egov.md](http://www.egov.md)), діяльність якого спрямована на забезпечення громадян країни публічною інформацією та послугами в режимі «нон-стоп», а також прозорості діяльності органів державного управління шляхом використання та просування інформаційних технологій в публічному секторі. За цей час реалізовано низку ініціатив для громадян, бізнесу, уряду, зокрема, введено в дію спрямовані на громадян сервіси: «Платформа відкритих даних», «Єдина платформа для публічних послуг», «Мобільний підпис», «Е-довідка про несудимість», «Реєстр

місцевих актів». Зокрема, завдяки Платформі відкритих даних ([www.date.gov.md](http://www.date.gov.md)) уряд забезпечує доступ громадян та підприємств і організацій до пакетів даних публічного характеру, а єдина платформа публічних послуг (<https://servicii.gov.md/>) фактично є каталогом публічних послуг органів державної влади. Розроблена і впроваджена послуга «мобільний підпис», що дозволяє за допомогою мобільного телефону отримувати дозволяючи при цьому ідентифікувати та підтверджувати особу у віртуальному просторі. За допомогою послуги «мобільний підпис» громадяни мають доступ до електронних послуг - засвідчення документів, електронна звітність, декларування тощо. Портал «Реєстр місцевих актів» ([www.actelocale.md](http://www.actelocale.md)) дозволяє громадянам та бізнесу мати доступ до централізованої бази актів органів публічної влади Молдови. Цінними для бізнесу є послуги «Е-ліцензування», «Швидка декларація», «Електронна декларація». Для органів державної влади введено сервіси: «Реєстр персональних даних», «Particip.gov.md», «M-pass». Упровадження платформи «Particip.gov.md» достосовано до потреб партисипативної демократії, яка проваджується в Молдові з метою подолання недоліків представницької демократії. Використовується платформа у консультаціях з громадянами щодо проектів нормативних актів, для розсилки новин, а також генерування спеціального коду, що спрощує процедуру інформування про появу проектів актів, що становлять публічний інтерес. Ця платформа позиціонується як елемент Програми «Національна стратегія розвитку «Молдова 2020». Послуга «M-pass» через мобільний підпис, цифровий сертифікат або пароль забезпечує ідентифікацію осіб, що звертаються за електронними послугами.

Проте системи е-демократії є вразливими з точки зору інформаційної безпеки. Хакери атакували урядову автоматизовану інформаційну систему «Вибори» під час референдуму 2010 р.. Референдум стосувався змін Конституції, і проведені атаки призвели до дублювання даних в системі. Хакери, як з'ясувалося, домагалися, щоб референдум був визнаний недійсним, але результати їх дій виявилися незначними і лише відклали оголошення підсумків референдуму, а не скасували їх [273].

У Молдові вчиняється значна кількість кіберзлочинів, в основному це: порушення таємниці листування, порушення авторських прав, розголошення таємниці, поширення дитячої порнографії і несанкціонований доступ до мереж і телекомунікаційних послуг. Окрім того, правоохоронні органи розслідують все більше кіберзлочинів, пов'язаних з порушенням недоторканності приватного життя. Відділ інформаційних технологій та розслідувань кіберзлочинів Генеральної прокуратури зайнятий питаннями, пов'язаними з фальсифікацією особистих облікових записів в соціальних мережах, незаконним видаленням особистого листування з електронної пошти і SMS, а також захопленням офіційних облікових записів з метою відправки фішинг-повідомлень. з метою охорони права інтелектуальної власності було розпочато розслідування файлообмінного сайту [Torrentsmd.com](http://Torrentsmd.com).

Нестійка економіка Молдови створює сприятливі умови для фінансових кіберзлочинів. Часто, фінансові злочини вчиняються у змові з громадянами інших країн СНД. Наприклад, група з 37 осіб переважно з Росії та Молдови була притягнута до відповідальності за ретельно опрацьовану схему по відмиванню грошей та хакінгу. Фізичні особи в Молдові і Росії зламували комп'ютери дрібного і середнього бізнесу і заражали їх троянської програмою Zeus, яка поставляла паролі іноземцям, котрі перебувають в США на підставі студентських віз, які по ним знімали гроші і відправляли їх своїм ватажкам. Так кіберзлочинці здійснили крадіжку понад 70 мільйонів доларів [273].

Злочинність зі звичного середовища має своє продовження в інтернет. Молдова, що відноситься до країн 2-го рівня відповідно до звіту Держдепартаменту США по боротьбі з торгівлею людьми, має проблему щодо ліквідації торгівлі людьми. Нові технології означають, що «традиційні» злочини переходять в онлайн-простір; викрадачі використовують смартфони, комп'ютери та інтернет, щоб вимагати гроші і перевозити жертв через кордони. Зокрема, спостерігається значний підйом використання інтернету для рекрутингу та експлуатації жертв. У Молдові був створений спеціальний відділ по боротьбі зі злочинністю, що спеціалізується на злочинах сексуального характеру проти дітей [273]. Молдова, як і раніше залишається притулком для піратства і порушень

авторських прав - надзвичайно високий рівень поширення піратського програмного забезпечення; за приблизною оцінкою 90 % всього програмного забезпечення в країні поширюється незаконно. Ситуацію погіршує той факт, що більшість таких справ закриваються без суду і винесення вироку.

Мають місце і порушення інформаційних прав громадян. Молдова має багатоцільову централізовану базу даних по всіх громадянах під назвою «Registru». У «Registru» агрегована інформація, зібрана державними органами. Урядові установи і організації можуть отримати доступ до бази даних на підставі спеціальної угоди, в якому вказані їх допуски і обмеження. Організації з захисту прав людини постійно звертають увагу на занадто розширене призначення цієї бази даних, і те, що їй не вистачає контролю, що може привести до безпрецедентного рівня державного нагляду. Незважаючи на стурбованість щодо приватної інформації «Registru» надалі функціонує.

Онлайн-нагляд в Молдові не так розвинений, як в інших країнах СНД, проте правове поле розвивається повільно. У грудні 2012 р. увійшов в силу новий Закон про спеціальну розшукову діяльність з поправками щодо законного перехоплення повідомлень, а також змін обов'язків і функціоналу відповідних інстанцій. Винятковим правом законного перехоплення повідомлень як і раніше володіє Національна служба інформації і безпеки, яка в цих цілях співпрацює з провайдерами мережевих послуг і послуг електронного зв'язку. Крім того, в 2012 р. прийнято поправки до кримінально-процесуального кодексу, які ввели процедуру законного перехоплення електронного зв'язку і даних, зібраних провайдерами послуг. Закон накладає ряд обов'язків на власників комп'ютерних систем, доступ до яких заборонений або обмежений для деяких категорій користувачів. Вони зобов'язані попередити користувачів про правові умови доступу та користування, а також про юридичні наслідки несанкціонованого доступу до цих комп'ютерних систем. Попередження повинне бути доступно для кожного користувача.

У той же час ряд зобов'язань накладається на постачальників послуг. Вони ведуть облік користувачів і повідомляють компетентним органам дані про інформаційні потоки, в тому числі про нелегальний доступ до інформації з

комп'ютерних систем, спробах впровадження незаконних програм. Провайдери зобов'язані повідомляти про порушення відповідальними особами правил збору, обробки, зберігання, поширення і розподілу інформації або правил захисту комп'ютерної системи, якщо ці дії спричинили серйозні наслідки, наприклад, сприяли присвоєнню, перетворенню або знищення інформації, порушили роботу комп'ютерних систем.

У зв'язку з тенденціями інформаційних впливів, зараз у Молдові розглядаються відразу кілька законодавчих ініціатив, пов'язаних з регулюванням блокування інтернет-ресурсів, повноважень правоохоронних органів і покладених на провайдерів зобов'язань.

У 2016 р. була розроблена нова концепція інформаційної безпеки [615]. У драфті проекту два ключових елементи: (1) кібер-безпека - захист критичної інфраструктури, захист від кібер-атак, збереження цілісності даних тощо, (2) інформаційна безпека - все що стосується інформаційних воєн, пропаганди і дезінформації. Прийняття цієї концепції може стати важливим кроком, проте в проекті спостерігається проблема, типова також і для України, - кібербезпека ототожнюється з інформаційною безпекою, відсутній визначений понятійний апарат, а також стратегічний підхід до вирішення проблеми.

Гарантом громадських інтересів в сфері телебачення і радіомовлення покликана бути Аудіовізуальна Координаційна Рада. Рада задекларована як незалежний інститут, але часто ця "незалежність" викликає сумніви. Вона наділена недостатньою кількістю інструментів для того, щоб ефективно регулювати медійний ринок і карати порушників. Найчастіше мають місце публічне попередження, штраф, призупинення права на трансляцію реклами на певний період, про призупинення ліцензії на мовлення протягом певного періоду або (вкрай рідко і зазвичай політично мотивовано) анулювання ліцензії.

Після зміни влади в 2009 р. на "про-європейську" значно покращилась ситуація з цензурою. Раніше державні ресурси використовувалися з метою тиску на вільні ЗМІ і політичних опонентів. Проте, на сьогодні, має місце монополізація інформаційного ринку, зокрема ЗМІ. А вже згадана Аудіовізуальна координаційна Рада не має достатніх важелів впливати ні на внутрішній інформаційні війни (між



політичними гравцями), ні на зовнішні інформаційні впливи (як з боку Росії, так і зі сторони Румунії). У 2014 Рада заборонила ретрансляцію Росія-24, але цим справа і обмежилось. Триває розробка проекту нового Кодексу телебачення і радіо Республіки Молдова, який, ймовірно, міститиме норми про заборону російських інформаційних каналів. Хоча щодо цього питання триває політичне протистояння, оскільки у авторів, окрім завзяття боротися з пропагандою, є також і власні фінансові та політичні інтереси.

Також з 2013 р. правоохоронні органи все пробують «проштовхнути» низку законопроектів для боротьби з дитячою порнографією. Для цього хочуть змінити ряд законів: Кримінальний кодекс, Закон про електронні комунікації, Закон про попередження та боротьбу зі злочинністю сфері комп'ютерної інформації і т.д. Поки що це лише ініціативи, які не підтримав парламент.

**Грузія** вирізняється серед інших колишніх радянських республік як найбільш прозахідна, за винятком країн Прибалтики. Нормативно-правове регулювання країни, в тому числі в сфері інформаційній сфері, змінювалося, з метою наближення до вимог членства Світової організації торгівлі та участі в програмі Східного партнерства Європейського союзу (ЄС), а в перспективі також і вимогам вступу в ЄС і НАТО.

Організація «Freedom House» окреслила ситуацію в сфері засобів масової інформації як найбільш ліберальну і плюралістичну в регіоні в 2013 р., проте наголошується зростаюче занепокоєння з приводу політичного впливу на основні канали мовлення. Медійне середовище відрізняється різноманітністю, але при цьому поляризованим характером.

Наслідки російсько-грузинської війни 2008 р., в ході якої відбулася одна з перших кібератак в умовах міждержавного конфлікту, показали вразливість Тбілісі в інформаційному та кіберпросторі. Як наслідок, уряд Грузії посилив інформаційну політику, в тому числі підтримку вільного інтернету і запобігання цензурі.

В цілому можна говорити про ліберальність телекомунікаційної галузі. Інформаційно-комунікаційні технології щораз більше інтегруються в економіку, суспільне життя і політику країни. Відомості про контроль і нагляд нечисленні,

урядові заходи блокування онлайн-контенту відсутні. При цьому все-таки спостерігається деякий брак прозорості телекомунікаційної сфери. Склад власників медіакампаній зачасто приховується за фіктивними фірмами і компаніями в офшорних зонах.

Конституція Грузії визначає, що «особисте життя кожної людини, його робоче місце, особисті записи, листування, переговори по телефону або з використанням інших технічних засобів, а також отримані за допомогою технічних засобів повідомлення недоторканні» (ст.20). Також, стаття 24 Конституції захищає право кожного громадянина «вільно отримувати та поширювати інформацію, висловлювати і поширювати свої думки в усній, письмовій чи іншій формі. Засоби масової інформації є вільними. Цензура забороняється». Конституційні засади втілені в нормах галузевого законодавства, зокрема, Законами «Про електронні комунікації», «Про інтелектуальну власність», «Про інформаційну безпеку», «Про мовлення» та інші.

Закон «Про електронні комунікації» встановлює принципи розвитку конкурентного середовища в сфері комунікацій, регламентує права і обов'язки учасників правовідносин, визначає засади передачі персональних даних, а також визначає сферу компетенції національного органу регулювання зв'язку - Національної комісії Грузії з комунікацій. Національна комісія наділена двома основними механізмами забезпечення дотримання встановлених норм: відкликання ліцензій на роботу і накладення штрафів за недотримання, до 3 % доходу оператора після третього порушення. Штрафи та відкликання ліцензій не вимагають санкціонування судом, але в суд можна подати апеляцію, і протягом цього часу санкції будуть продовжувати діяти.

Серед соціальних мереж за кількістю користувачів в Грузії лідирує Facebook. Хоча в інтернет-просторі Грузії широко використовується російська мова. Російськомовна блогосфера в Грузії більше політизована, ніж англо- або грузино-мовний інформаційний простір. Певною мірою це обумовлено бажанням спілкування блогерів з колегами на пострадянському (а отже російськомовному) просторі.

Інтернет посідає друге за важливістю місце серед джерел новин та інформації після телебачення. Результати опитування показали, що 6 % респондентів дізнаються новини політики онлайн, а ще 12 % вважають інтернет в цілому важливим джерелом інформації [272]. Для онлайн-джерел новин не встановлено вимоги ліцензування, вихід на цей ринок відрізняється мінімальними перешкодами і низькою собівартістю. Онлайн-журналістика в Грузії характеризується високою якістю і виграє від здорового рівня плюралізму. На відміну від телевізійних станцій онлайн-ресурси меншою мірою залежать від політичного тиску. Доступ до всіх можливостей електронного врядування відкритий на одному сайті: <http://e-government.gov.ge>, серед доступних послуг, наприклад, можливості: перевірити виписані на громадянина штрафи на сайті поліції; замовити закордонний паспорт на сайті громадянського реєстру он-лайн, так само - отримати будь-яку довідку; поспілкуватися з відеоконсультантом на сайті міністерства фінансів і з'ясувати, які податки потрібно сплатити у тому чи іншому випадку, в тому числі, прямо на сайті розрахувати вартість розмитнення авто; підготуватися до здачі тестів на водійські права; перевірити дійсність будь-якого завіреного нотаріусом документа у банку нотаріальних даних та інші [131].

Для Грузії, як і для України, суттєве значення має інтеграція з ЄС. Отримання безвізового режиму та підписання асоціації продемонстрували грузинським громадянам відчутну вигоду від проведених в країні реформ. Хоча демократичний розвиток Грузії переживає значні труднощі, як з огляду на складну геополітичну ситуацію, так і враховуючи слабкі опозиційні сили всередині держави [588]. Це ще одна причина, яка робить цінним вивчення досвіду Грузії у сфері безпеки, зокрема, інформаційної.

**Білорусь.** Інформаційна політика Республіці Білорусь є досить суперечливою. Республіка входить в число «Країн під наглядом», відповідно до рейтингу «Репортерів без кордонів», і раніше навіть вважалась «Ворогом інтернету». Але з технічної точки зору приватне використання інтернету здійснюється без значних обмежень. Швидкість з'єднання, легкість доступу і тарифи досить конкурентоспроможні, навіть в порівнянні з розвиненими країнами.

Конституція Білорусі [205] закріплює такі права в інформаційній сфері: ст. 28 (право на недоторканність приватного життя); ст. 33 (право на свободу думок); ст. 34 (право на загальнодоступну інформацію). Положення Конституції заклали основу для регулювання інформаційної сфери: Закон «Про інформацію, інформатизацію і захист інформації» (2008) [281] містить положення щодо права на інформацію; загальнодоступної інформації та її класифікація; інформації, поширення і (або) надання якої обмежено, та її класифікація; права на захист інформації про приватне життя фізичної особи та персональних даних; службової інформації, а також регулює контент щодо широкого спектру питань, від безпеки даних до політики управління.

Існує ряд спеціальних законів, які конкретизують права, закріплені в Конституції і Законі «Про інформацію»: «Про архівну справу та діловодство» [285] визначає право на доступ до архівних документів; «Про засоби масової інформації» - право на інформацію і свободу думок, «Аб бібліотечної справе»[1]; «Про електронний документ і електронний цифровий підпис», «Про авторське право і суміжні права» [284]. Регулювання інформації, поширення і (або) надання якої обмежено, здійснюється Законами: «Про державні секрети»[280]; «Про комерційну таємницю»; «Про охорону здоров'я» (норми, що визначають лікарську таємницю); Банківський кодекс (банківська таємниця) [23] та ін.

З 2010 р. Білорусь активно розробляє національну політику в сфері ІКТ, на що частково впливає зростання соціальних мереж і їх вплив на білоруське суспільство. Регулювання інтернету переважно здійснюється на рівні президентських указів. Головним виконавчим органом в секторі телекомунікації є Міністерство зв'язку та інформатизації і йому підпорядковано тринадцять організацій. Структурним підрозділом Міністерства є Республіканське унітарне підприємство з нагляду за електрозв'язком “БелГІЭ”, і наділене широкими повноваженнями щодо інтернету, а саме контролює сектор електронних комунікацій, здебільшого щодо технічних стандартів, таких, як радіочастоти, накладає санкції на операторів або ініціює відкликання ліцензії провайдера-порушника; здійснює управління Центром реєстрації цифрових сертифікатів,

надає послуги організаціям і приватним особам, а також адмініструє «чорний список» сайтів з обмеженим доступом в державних організаціях.

Оперативно-аналітичний центр при адміністрації президента Республіки Білорусь, спочатку був підрозділом спецслужб (КДБ), а з 2010 функціонує як спеціалізований орган, безпосередньо підпорядкований президенту. Він контролює роботу провайдерів інтернет-послуг і управляє головним доменом республіки Білорусь (.by). Повноваження і обов'язки центру були розширені в 2011 р. і тепер включають криптографію, випущені державою електронні підписи і взаємодію між ІТ-системами державних інститутів.

Вже згаданий Указ № 60 також вимагає, щоб провайдери інтернет-послуг блокували доступ до певної інформації в державних організаціях або за запитом конкретних користувачів.

У секторі онлайн-новин домінують два політично нейтральних і незалежних ресурси: TUT.BY і Onliner.by. У топ-50 найбільш часто відвідуваних веб-сайтів Білорусі є лише один абсолютно опозиційний ресурс - Charter97.org, який забезпечується командою з Польщі і Литви. Традиційні ЗМІ повністю контролюються державою. В країні немає незалежних місцевих новинних видань, а друковані ЗМІ залежать від економічних санкцій, які можуть негативно вплинути на тираж. Онлайн-платформи представляють собою єдиний відносно відкритий простір для вираження опозиційних або незалежних ідей, але вони можуть піддавати ризику тих, хто використовує їх для політичної пропаганди.

У Білорусі немає спеціальних законів щодо кіберзлочинності, але деякі аспекти регулюються Кримінальним кодексом і нормативними актами, що регулюють інтернет. Відповідно до офіційної статистики, понад 90% кіберзлочинності в Білорусі мають фінансовий характер, а також мають місце: несанкціонований доступ до даних; диверсійні акти; незаконне отримання електронних даних; порушення правил використання комп'ютерних систем; а також створення, використання або розповсюдження шкідливого програмного забезпечення або комп'ютерних пристроїв. Створення і розповсюдження порнографії, включаючи дитячу порнографію, є серйозною проблемою в Білорусі,

особливо з огляду на тенденцію швидко поширюватися по соцмережах, зокрема, в мережі вКонтакте.

Інститут персональних даних також переживає етап становлення: відсутній відповідний закон, немає уповноваженого органу, а регулювання відбувається фрагментарно. Республіка Білорусь не приєдналася до Конвенції Ради Європи 108, яка визначає міжнародні стандарти в сфері захисту персональних даних. Основу політики щодо персональних даних складають закони «Про інформації, інформатизації та захисту інформації», «Про реєстр населення», «Про перепис населення».

Відсутнє у республіці і законодавче визначення особливо чутливих/вразливих видів інформації, адекватного захисту їм не надається. Навіть в коментарях до закону про реєстр населення, які запропоновані Національним центром законотворчої діяльності термін «чутливі/вразливі дані» не вживається. «У реєстрі не буде ніяких даних, які можуть бути використані для будь-якого тиску на людину: про расу, національність і колір шкіри; про світогляд, політичних або релігійних переконаннях; щодо будь-яких захворювань; щодо сексуальної орієнтації; про усиновлення і багато інших»[19].

При цьому, у Білорусі нагляд за населенням здійснюється на національному рівні. Влада здійснює активний моніторинг протестів за допомогою обладнання для моніторингу російського виробництва, що використовується телекомунікаційними компаніями.

Законодавство **Вірменії** в інформаційній сфері останні роки спрямоване на свободу, безпеку, а також економічного ефекту для всіх сфер (держави, суспільства, бізнесу та особистості). Нормативно-правова база у Вірменії розвивається з урахуванням стандартів та норм ЄС. Телекомунікаційний сектор Вірменії одночасно ліберальний і відкритий бізнесу. Хоча спостерігається залишкова тенденція до надмірного регулювання кіберпростору.

Норми інформаційного права містять Конституція Республіки Арменії (зокрема, ст. 33. Свобода і таємниця обміну повідомленнями, ст. 34. Захист персональних даних, ст. 41. Свобода думки, совісти і релігії, ст. 42. Свобода вираження поглядів, ст. 51. Право на отримання інформації, ст. 53. Право на

подачу петицій), Кримінальний кодекс (містить норми щодо відповідальності за злочини проти безпеки комп'ютерної інформації), Цивільний Кодекс, а також закони Республіки Вірменії «Про свободу інформації», «Про електронну комунікацію», «Про державне сприяння сфері інформаційних технологій», «Про захист персональних даних» та інші.

Дуже розвиненим, в тому числі на рівні міжнародних домовленостей, є законодавче регулювання у сфері інтелектуальної власності, зокрема, Закони «Про авторське право і суміжні права», «Про правову охорону топологій інтегральних мікросхем» та інші.

Інформаційній безпеці на законодавчому рівні окремого акта не присвячено, в 2009 р. Радою національної безпеки було схвалено Концепцію інформаційної безпеки. Окремі положення містяться в Стратегії національної безпеки, Стратегії оборони та інших актах. Повноваження щодо забезпечення інформаційної безпеки також має низка органів, зокрема органи національної безпеки, міністерства оборони, поліція.

Особливістю вірменської системи інформаційної безпеки є спрямованість на вирішення інформаційних проблем не тільки Вірменії, але і всього вірменства [282]. При цьому, як першочергові завдання цієї сфери виділяють: (1) інвентаризація наявних і формування нових інформаційних ресурсів, розробка системи їх ефективного співробітництва і безпечної діяльності; (2) концептуальна розробка методів внутрішньої і зовнішньої пропаганди/контрпропаганди і їх практична реалізація; (3) створення взаємодоповнюючих брендів вірменства і Вірменії, впровадження цих брендів - як елементи свідомості - у вірменському середовищі і в інших спільнотах; (4) розробка і реалізація суспільно-політичних, наукових, навчальних та інших загальнонаціональних проектів; (5) широке застосування сучасних технологій інформаційної політики для вирішення політичних, історичних, культурних, економічних і інших проблем вірменства; (6) концептуальна розробка національної «ноополітики» - мережевоцентричної системи, і формування на цій базі єдиного інформаційного і організаційного простору вірменства [282].

Інформаційна політика Вірменії пережила значних змін. Обмеження роботи ЗМІ під час президентських виборів 2008 р., яке вплинуло на інтернет-ресурси новин і сайти опозиції, сприяло розвитку блогів і соцмереж. Висвітлення парламентських виборів 2012 р. було значно більш різнобічним, проте на сьогодні прояви жорстокості і погрози на адресу журналістів сприяють самоцензурі.

Як платформа для комунікації і координації політики в ІКТ і нормативно-правовій сферах у Вірменії створена Рада з підтримки розвитку сектора ІКТ, консультативна група, яка складається з представників приватного сектора, чиновників і представників громадянського суспільства, і очолює його прем'єр-міністр. Рада сприяє змінам політики та законодавства, у напрямку розвитку кіберпростору Вірменії та лібералізації радіочастотного спектру. Рада істотно спростила елементи процесу мережевого ліцензування.

У Вірменії практикується ліберальний підхід щодо управління інтернетом. В країні проголосували проти поправок до Регламенту міжнародного електрозв'язку, запропонованих Росією і підтриманих державами-однодумцями на Всесвітній конференції з міжнародного електрозв'язку в грудні 2012. Ці поправки були спрямовані на передачу контролю над управлінням глобальною мережею Організації об'єднаних націй і, в результаті, на зонування кіберпростору.

Вірменія була однією з перших пострадянських держав, в якому пройшла приватизація телекомунікаційної індустрії. Провайдери телекомунікаційних послуг значною мірою зосереджені в руках іноземних компаній. Уряд Вірменії ще в 2001 р. сформулював план розвитку сектора ІКТ. Паралельно був схвалений пакет поправок в законодавство, які звільняли ІТ компанії з персоналом до 15 осіб від прибуткового податку (20%) на три роки з моменту заснування. Законопроект також передбачав пільгову ставку прибуткового податку для працівників ІКТ-стартапів на рівні 10 % замість загальнодержавного мінімуму, що становить в даний час 24,4% [271]. Уряд і міністерство економіки продовжують просувати розвиток сектора ІКТ, одночасно працюючи над розвитком електронного уряду в Вірменії і підвищуючи якість послуг зв'язку.

Телебачення залишається основним джерелом інформації. Однак стрімко розвивається взаємодія через соціальні мережі. Лідирують Однокласники,



Facebook на другому місці, але існує також і кілька локальних платформ соціальної взаємодії, найбільш популярна - це Hayland, що нараховує 156 000 зареєстрованих користувачів. У 2013 р. платформа отримала фінансові вливання і була оновлена, щоб краще відображати «етнічні і психологічні характеристики Вірменського народу». Проте, соцмережі Facebook і Однокласники, також доступні на вірменській мові і підривають конкурентоспроможність локальних соціальних мереж. Ці сайти не тільки володіють високим проникненням, але вони також дозволяють отримати кращий доступ до членів вірменської діаспори, що є важливим для внутрішньої і зовнішньої політики Вірменії.

Соцмережі мають все значніший вплив на політичне життя. В ході парламентських виборів 2012 р., Facebook виступив як важлива платформа діалогу і ведення передвиборної кампанії, більшість політиків і їхніх партій вже були присутні в мережі. На думку Т. Кочаряна, блогера і експерта з інформаційної безпеки, політики все більше усвідомлюють, що інтернет, платформи соціальної взаємодії і блоги є важливими джерелами інформації для молоді, не в останню чергу через недовіру останніх до телебачення і газет [271].

Вірмени активно використовують простір інтернету для просування локальних громадських ініціатив. При цьому аудиторія, на яку розраховані ініціативи, знаходиться не лише всередині країни, а й і за кордоном. Члени діаспори, особливо що знаходяться в Каліфорнії, беруть помітну участь у політичній і фінансовій життя Вірменії. З цієї причини основна частина контенту генерується вірменською та англійською мовами.

В ой же час, мають місце злочини в мережевому просторі, за оцінкою поліції 80% кіберзлочинів в Вірменії відбуваються в соціальних мережах, серед яких найбільш поширені - розкрадання персональних даних та вимагання. Порушники часто створюють підроблені аккаунти і розміщують компрометуючі фото, наклепницькі заяви або пропонують сексуальні послуги від імені сфальсифікованих акаунтів з викраденими даними. Найчастіше злочинці дають реальні телефонні номери жертви, а компрометуючі матеріали видаляють тільки після отримання грошей.

Кіберзлочини в Вірменії часто пов'язані з невирішеним конфліктом з Азербайджаном через Нагірний Карабах. Експерти оцінюють це протистояння як інформаційну війну другого покоління. Конфлікт супроводжується втручанням третіх сторін, зокрема, свої інтереси в інформаційнішому протистоянні мають країни регіону – Турція, Іран, Грузія, а також глобальні гравці – РФ, США і ЄС. При цьому використовуються широко методи інформаційного впливу (пропаганда), а також кібератаки. Атаки на сайти загострюються в певні періоди р., часто в місяць здійснюється від 50 до 100 атак на вірменські сайти. За даними фонду «Нораванк»[271], вірменського аналітичного центру, який вивчає проблеми інформаційної безпеки, вірменські сайти часто атакують під час національних свят.

**Азербайджану** в останні роки була властива багатовекторна зовнішньополітична модель, хоча ситуація з демократизацією суспільства та правами людини і надалі залишається проблемною, про що свідчить аналітика незалежних експертів багатьох міжнародних організацій – Amnesty, Reporters sans frontières, Freedom House.

Інформаційну політику характеризує комбінація цензури, електронного нагляду і фізичного впливу на громадян-дисидентів і незалежні засоби масової інформації. В країні відсутня свобода слова, всі провідні ЗМІ залишаються під контролем уряду, держава є власником 80 % газет в країні. Відомі випадки юридичного тиску, наприклад, у вигляді судових позовів за наклеп і дискредитацію, також при першій-ліпшій можливості застосовується до незалежних ЗМІ. Інтернет часто виявляється єдиним альтернативним простором для вільного самовираження, але й інтернет все більше зазнає тиску

Нормативно-правова база Азербайджану є продовженням законодавства радянського періоду. Держава реалізує свій вплив на сектор ІКТ шляхом підтримки тісних зв'язків з головним оператором країни, компанією «Delta Telecom» - найбільшим оптовим інтернет-провайдером, який контролює основну частину міжнародних з'єднань і керує єдиною точкою обміну трафіком інтернет. Міністерство зв'язку та високих технологій Азербайджану наділено значними владними повноваженнями, що дозволяє обмежувати, модифікувати і

здійснювати моніторинг інтернету в країні. З урахуванням відносин між інтернет-провайдерами та органами влади, офіційний Баку забезпечений неофіційними і неконтрольованими інструментами здійснення контролю над сектором ІКТ.

Нафтозалежна економіка Азербайджану останні роки суттєво постраждала від падіння цін на нафту та зниження курсу її валюти, манату, на половину вартості. Тому нова концепція розвитку, під назвою «Азербайджан 2020: бачення майбутнього», робить акцент на економіці, заснованій на знаннях, і на проникненні ІКТ в усі сфери суспільства. Доступ до ІКТ і інфраструктура сконцентровані в містах, де знаходиться 80 % усіх стаціонарних мереж. Більш того, поширення стаціонарних мереж дещо зросло протягом останніх кількох років, досягнувши 18 %. Азербайджанці добре представлені в соцмережах і дуже активні в місцевій блогосфері. Переважає Facebook, де зареєстровано близько одного мільйона аккаунтів. Приблизно 35% усіх інтернет-користувачів посилаються на Facebook як на ресурс, яким вони активно і регулярно користуються. Другий за поширеністю онлайн-ресурс - YouTube; російські соціальні мережі Однокласники і вКонтакте займають 6-е і 11-е місця відповідно [270].

Доступ до інтернету дозволив онлайн-активістам творити альтернативне контрольованому урядом медіа середовище в країні. Досвід Арабської Весни спонукала азербайджанських активістів організувати власну Бакинську Весну в 2011 р., вимагаючи демократичної реформи і поваги до людських прав. Спочатку задумана як виключно онлайн-захід, учасники якого могли повідомляти про свою підтримку, поставивши 'Like' (що вже було для Азербайджану досить сміливим політичним кроком), акція трансформувалася в живий протест, призначений на 11 березня 2011 р.. У відповідь на Бакинську Весну розпочались арешти, кількість затриманих учасників в протестах, організованих за допомогою соціальних мереж, становили сотні.

Проте використання інструментів Web 2.0 азербайджанськими активістами не лише не припинився, а й набув нових форм. Так, наприклад, на початку 2013 р. в Баку за допомогою Facebook були організовані протести у відповідь на смерть призовника Д. Губадова, який, очевидно, загинув від поранень, отриманих під час

жорстокого конфлікту, пов'язаного з «дідівщиною». Сторінка в мережі Facebook «Зупиніть загибель солдатів», закликала приєднатися до протесту, призначеного на 12 січня. Протягом декількох днів "like" на сторінці поставили понад 17 тисяч користувачів, і близько 3000 взяли участь в акції протесту. Після участі в заході від 22 активістів вимагали заплатити штраф в розмірі зарплати за 1-2 місяці. У Facebook була запущена кампанія під назвою «5 qerik», з метою допомогти активістам виплатити штрафи; суть кампанії полягала в тому, щоб кожен «донор» пожертвував всього п'ять центів. Через п'ять днів вдалося зібрати більше 10 тисяч доларів, чого цілком вистачило для виплати штрафу.

Декілька разів уряд робив спроби обмеження доступу до мережі інтернет. В 2013 р. члени уряду були стурбовані підвищенням активності в соцмережах і можливими у зв'язку з цим протестами перед виборами намагалися зробити це шляхом закриття інтернет-кафе регіонах в Ісмаил та Нахічеван.

Іншим способом обмеження онлайн-активізму є обмеження вільного потоку інформації, блокуючи доступ до веб-ресурсів. У дні, що передували протестам 12 січня 2013 р., в зв'язку з загибеллю Д. Губадова, кілька веб-сайтів, які критикують уряд, включаючи [azadliq.az](http://azadliq.az), [azadliq.org](http://azadliq.org), [musavat.com](http://musavat.com), [qafqazinfo.az](http://qafqazinfo.az), повідомили про успішні DDoS- атаки на них.

З законодавчої точки зору в Азербайджані, онлайн-контент відноситься до ЗМІ. Весь створюваний користувачами контент, від блогів до постів в мережі Facebook, відповідно підлягає законодавчому регулюванню як ЗМІ. Це звужує простір для політичної онлайн-активності та обмежує свободу слова і самовираження в віртуальному просторі. Має місце посилення контролю над цифровим простором і паралельне посилення урядового втручання в діяльність традиційних та нових ЗМІ.

Важливою рисою азербайджанського інформаційного і мережевого просторів є націоналізм. Політична криза в стосунках з Вірменією в зв'язку з невирішеним Нагірно-карабахським конфліктом провокує конфлікти між хакерами обох сторін. Націоналісти з обох сторін періодично завдають кібератаки на сайти супротивників і обмінюються один з одним образами в Мережі. Мають місце кібератаки на урядові сайти, ресурси ЗМІ, що критикують існуючий режим. Окрім

того, у цьому конфлікті задіяні ще декілька країн, які також мають свої інтереси в інформаційному та кіберпросторі. Наприклад, у січні 2012 р. Азербайджанська Кіберармія, група, ймовірно пов'язана з Іраном, атакувала приблизно 40 державних структур в знак протесту проти тісних відносин Баку і Тель-Авіва. Встановлено, що 24 з 25 були здійснені з Ірану, а одна - з Нідерландів.

Значною проблемою також залишається онлайн-нагляд за громадянами, що здійснюється в інтересах влади Азербайджану. Вираз незгоди чи критика державних осіб в мережі часто призводить до відстеження автора. У повсякденному житті азербайджанці перебувають під враженням, що за їх діяльністю в інтернеті постійно спостерігають. Це призводить до значної самоцензури і страху, а отже виключає можливість демократичних процесів з використанням новітніх технологій, як-то участь в онлайн-дискусіях на «гарячі» політичні теми.

В 2013 р., в підтримку комплексного плану дій щодо запобігання випадків помилкової інформації про тероризм, була введена мобільна реєстрація. Всі мобільні пристрої повинні бути зареєстровані відповідно до свого ідентифікаційним кодом IMEI, SIM-картою та номером мобільного мережі з реєстрацією центру мобільних пристроїв.

Органи безпеки мають доступ як до даних операторів мобільного зв'язку, так і до інтернет-провайдерів. Програма «Uppdrag Granskning» («Місія - розслідувати»), шведське телешоу, яке займається розслідуваннями, в 2012 р. документальний фільм про телекомунікаційної компанії «Teliasonera», фінсько-шведської фірми й основному акціонерів в «Azercell». У цьому документальному фільмі стверджувалося, що «Teliasonera» дозволила встановити «чорні ящики» в своєму обладнанні, зробивши можливим моніторинг в реальному часі за допомогою всіх форм комунікації в своїх мережах, включаючи геолокацію. Один абонент «Teliasonera» в ході інтерв'ю заявив, що його допитували органи безпеки після того, як він проголосував за Вірменію в конкурсі пісень «Євробачення» в 2011 р.[270].

Про рівень правозастосування говорить також і той факт, що перше в історії Азербайджану рішення про застосування законодавчого регулювання в сфері

захисту авторських прав на програмне забезпечення було прийняте у вересні 2017 р.. Бакинський адміністративно-економічний суд №1 зобов'язав компанію ABC Telecom, яка продавала комп'ютери з встановленим неліцензійним програмним забезпеченням Microsoft, відшкодувати збитки компанії Microsoft [7].

#### **Висновки до розділу 4**

Інформаційна безпека в системі міжнародної безпеки пройшла різні етапи становлення. В другій половині XX сторіччя міжнародні домовленості здебільшого стосувались забезпечення існування та розвиток інформаційного середовища бізнесу. На межі тисячоліть відбулися значні трансформаційні процеси в геополітиці і внаслідок подвійної трансгранично-національної природи кіберпростору[128,с.28] національна політика держав щодо інформаційної безпеки стає значимою у вимірі зовнішньої політики, оскільки пов'язана з розбудовою інфраструктури.

І, очевидним є, що опрацювання міжнародних домовленостей в сфері інформаційної безпеки в цілому, і людини зокрема, значною мірою залежить від політичної волі держав, які мають та/чи змагаються за визначальний геополітичний вплив. На сьогодні, до таких держав, насамперед, належать США, Російська Федерація, КНР та ЄС.

На сьогодні у світі сформувалось два основних підходи щодо змісту міжнародної інформаційної безпеки. Перша група країн демонструє підхід до проблематики міжнародної інформаційної безпеки в широкому розумінні, в основу якої мають бути покладені принципи неподільності безпеки та відповідальності держав за свій інформаційний простір. Друга група країн звужує питання міжнародної інформаційної безпеки до міжнародної кібербезпеки і такий підхід зосереджується на боротьбі із злочинами у сфері інформаційно-комунікаційних технологій, в т.ч. боротьбу із кібертероризмом. Як наслідок, при цих підходах простежується різне розуміння місця інформаційної безпеки людини в складній системі інформаційної безпеки як на міжнародному, так і на національному рівнях. Перший підхід, на нашу думку, передбачає узаконення значного простору для обмеження інформаційних прав і свобод людини на

користь гарантування інформаційного безпеки міжнародної спільноти і окремих держав. При цьому, прихильниками такого розвитку міжнародної політики виступають здебільшого держави, що мають значні проблеми щодо реалізації конституційних засад демократії, або ж взагалі не визнають демократичних цінностей.

Другий підхід визначається значно більшим соціальним і економічним спрямуванням, передбачає встановлення міжнародних стандартів для інформаційних прав та свобод людини (особливо пов'язаних з використанням мережі) на достатньо високому рівні. При цьому не передбачає втручання в питання інформаційного суверенітету, ведення інформаційних воєн та деякі інші аспекти політичної і військової сфери.

Безперечною вбачається цінність напрацювання міжнародних стандартів як орієнтирів для підвищення рівня захисту прав і свобод людини в інформаційній сфері. Водночас, як свідчить аналіз становлення інституту прав людини у складі міжнародного права, їх значення здебільшого є прогностичним і полягає у виконанні таких функцій як: визначають перелік прав та свобод, які відносяться до категорії основних та обов'язкових для всіх держав-учасниць відповідних міжнародних угод або конвенцій; формулюють головні риси змісту прав та свобод, які повинні втілюватись у відповідних конституційних та інших нормативних положеннях окремих держав; встановлюють зобов'язання держав щодо визнання та забезпечення проголошених прав та свобод, а також встановлення на міжнародному рівні гарантій, необхідних для реалізації і захисту прав та свобод; фіксують умови щодо застосування прав та свобод людини, одночасно із законними обмеженнями цих прав та свобод [256,с.359].

Як свідчить досвід країн з розвиненою демократією, інформаційна безпека людини не повинна протиставлятися інформаційній безпеці держави та суспільства. Адже саме людина визнається основною цінністю кожного суспільства і забезпечення її прав і свобод є кінцевою метою реалізації функцій держави. Проте, реалії інформаційного суспільства обумовлюють необхідність обмеження прав та законних інтересів людини з метою захисту національних інтересів держав, попередження міжнародних конфліктів чи/та терористичних

актів, а також забезпечення безпеки національних інформаційних ресурсів. Таким чином, має місце конфлікт інтересів різних об'єктів інформаційної безпеки. Вирішення цього конфлікту демократичним шляхом є однією з первинних задач при створенні відповідних правових норм.

Як бачимо, підходи США і ЄС до вирішення цього питання суттєво відрізняються. Про це свідчить як аналіз законодавства, так і правозастосування. США декларує високі стандарти прав і свобод людини в інформаційній сфері, але при виникненні протиріч між гарантуванням дотримання цих стандартів і інтересами національної безпеки перевага віддається саме інформаційній безпеці держави.

Країни ЄС, в свою чергу, демонструють більш послідовну політику щодо гарантування і дотримання прав і свобод людини в інформаційній сфері. Про це свідчать, зокрема, останні зміни в законодавстві щодо захисту персональних даних. Окрім того, політика ЄС у інформаційній сфері характеризується узгодженістю і забезпечується дієвими механізмами реалізації.

Значну роль нормотворчості відграють міжнародні судові органи, зокрема суд ЄС та ЄСПЛ, які шляхом правозастосування конкретизують розуміння змісту правових норм на основі суспільної практики, а часом і формують нове розуміння з огляду на зміни, що відбуваються в суспільстві. Зокрема, про це свідчить аналіз рішень у справах ЄСПЛ щодо права на доступ до інформації, який відображає зміну розуміння цього права, а також його співвідношення з іншими інформаційними правами, зокрема правом на захист персональних даних, свободою вираження поглядів тощо.

Україна, обравши шлях євроінтеграції і підписавши угоду про асоціацію з ЄС взяла на себе зобов'язання щодо адаптації законодавства з відповідними нормами ЄС. Відповідно, значні зусилля спрямовуються власне на приведення у відповідність вже існуючого законодавства. Проте самих змін в законах не достатньо. Правове регулювання має відображати бажані соціальні зміни і їх стимулювати.

Як вже неодноразово звертали увагу, загрози інформаційній безпеці людини значною мірою узалежнені від геополітики. Аналіз ситуації в країнах Східного



партнерства, зокрема досвід Грузії, Вірменії і Молдови в сфері інформаційної безпеки людини є цінним для України з огляду на:

- (1) проєвропейську політичну спрямованість, а отже і спроби адаптації до законодавства і стандартів ЄС;
- (2) геополітичну ситуацію, що пов'язана зі значним впливом (в т.ч. інформаційним) зі сторони Російської Федерації;
- (3) наявність територій, що не підконтрольні уряду, і використання конфліктів в цілях підірвання суверенності державної влади;
- (4) нестійку політичну і економічну ситуацію в середині держави.

На пострадянському просторі сьогодні простежується виокремлення двох груп країн, що різко відрізняються принципами формування політики у інформаційній сфері. Про це свідчать також результати опитування 50 експертів ІКТ, які відображені в дослідженні «Ціна свободи і безпеки. Індекс ІКТ-законодавств Євразії за 2016 р. », виконаному DR Analytica на замовлення Digital.Report.[497]

У першій групі опинилися Вірменія, Грузія і Молдова: націленість влади цих країн на збільшення свободи у всіх сферах, а також облік економічного ефекту від вжитих заходів дозволяє проводити збалансовану політику, одночасно приводить до збільшення безпеки. Так, зокрема, в Молдові прийняті в 2016 р. правові акти збільшували як свободу, так і безпеку в усіх сферах.

Друга група країн, до якої входять Білорусь, Азербайджан, Росія, Казахстан і Киргизстан, в інформаційній політиці віддає пріоритет інтересам безпеки, переважно - державної. Така політика веде до обмеження свободи інформації для особистості і суспільства. Ці країни також беруть за основу реалізовані в Росії законодавчі ініціативи, зокрема, ті закони, що пов'язані з моральною стороною інтернет-контенту, а також з інформаційною безпекою держави.

Проблемним питанням в країнах пострадянського простору залишається боротьба з кіберзлочинністю. Хоча в більшості країн ратифікована Конвенція про кіберзлочинність та прийняті відповідні закони по боротьбі з кіберзлочинністю, реалізація їх положень зачасти є малоефективною, зокрема

через те, що влада не вважає кіберзлочинність реальною загрозою, якщо вона не загрожує безпосередньо їх режиму або економічним інтересам.

Для країн Східного партнерства актуальною проблемою залишається домінування Російської Федерації в інформаційному просторі. Російська Федерація довгий час домінувала в культурній, політичній та економічній сферах в Євразії, в тому числі в сфері розвитку ІКТ. Останні роки Грузія, Молдова і Україна докладають багато зусиль, щоб дистанціюватися від Росії, проте інші держави Східного партнерства залишаються під суттєвим впливом її геополітичного впливу. Такий вплив обумовлений цілою низкою чинників – економічними зв'язками, енергетичною залежністю, значною насиченістю мережі російськомовним контентом, а також тим, що російські комунікаційні компанії відіграють помітну роль в країнах регіону.

Зокрема, російські соціальні мережі «Вконтакте», «Однокласники» і «Мой Мир» входять до п'ятірки найбільш відвідуваних соціальних мереж у багатьох державах пострадянського простору. Держави по різному реагують на цю загрозу. Від повного ігнорування (Білорусь, Казахстан, Азербайджан) до спроб створити чи посилити вплив власних альтернативних ресурсів (Вірменія, Грузія) або заборони окремих ресурсів російського виробництва (Молдова).

Таким чином, міжнародний досвід свідчить про дихотомію проблеми міжнародної інформаційної безпеки, та інформаційної безпеки людини як складової інституту прав людини в міжнародному праві. Узгодження основних питань є необхідним з огляду на економічні інтереси держав, демократичні цінності та глобалізаційні процеси, і, водночас, практично неможливим з огляду на розбіжності в інтересах основних геополітичних гравців. При цьому закладення правових основ інформаційної безпеки людини лише на національному рівні є недостатнім з огляду на глобалізацію, інтенсивні транскордонні інформаційні процеси, трудову міграцію, е-комерцію, втрату ідентичності та ще цілу низку соціальних процесів, що виникають у зв'язку зі становленням глобального інформаційного суспільства.

## РОЗДІЛ 5

### ПРІОРИТЕТИ РОЗВИТКУ ПРАВОВИХ ОСНОВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ В УКРАЇНІ

#### 5.1. Державна політика щодо інформаційної безпеки людини в Україні

Ст. 3 Конституції України визначила людиноцентризм як пріоритетний напрямок державної політики — «Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави» [207]. Окрім того, в ст. 17 було закріплено забезпечення інформаційної безпеки як одну з найважливіших функцій держави і справу всього Українського народу. Відповідальність за забезпечення державного суверенітету, в тому числі інформаційного, здійснення внутрішньої і зовнішньої політики держави, виконання Конституції і законів України, актів Президента України статтею покладено на Кабінет Міністрів України. При цьому рішення, які приймаються суб'єктами державного управління, повинні відповідати положенням державної політики, а державна політика за жодних обставин не повинна виходити за межі законодавства. Проте, в умовах правової соціальної держави передбачається активне державне втручання в процес юридичного регулювання суспільних відносин, гарантування соціальних свобод, оскільки беруться до уваги так звані «неспроможності ринку», до яких традиційно відносять: суспільні блага, зовнішні ефекти, природні монополії та інформаційну асиметрію. В той же час слід зважати на обмеження державного втручання, так звані неспроможності влади. Це передусім проблеми, які є властивими прямій демократії: парадокс голосування, інтенсивність вподобань і пакетування позицій; представницькій владі: вплив організованих інтересів, географічні виборчі округи, обмежені часові горизонти, породжені виборчими циклами, позування перед громадськістю; бюрократичному

забезпеченню: проблеми державних інститутів, труднощі оцінювання наданих послуг, обмежена конкуренція, захист прав державних службовців, бюрократичні ігри з державно-політичними рішеннями; децентралізації: розмиті повноваження, фінансові зовнішні ефекти [ 71, с. 53-54]. В глобалізованому сучасному суспільстві слід також зважати на взаємозв'язок і взаємопроникнення комерційних інтересів великих корпорацій і політичних сил.

Підходи до розуміння інформаційної безпеки України та світу за цей час зазнали суттєвих трансформацій, зокрема, сформувались політичні уявлення про місце цієї сфери в суспільному житті, роль держави в її регулюванні, розуміння мети і змісту державного управління інформаційною безпекою, механізмів державного впливу на інформаційні процеси та відносини. Відповідним чином змінювалося законодавство, структура та функції суб'єктів цієї політики.

За формальну основу дослідження державної політики інформаційної безпеки людини в Україні було взято періодизацію новітньої історії державного управління забезпеченням інформаційної безпеки України, яку здійснив Зозуля О.С. з урахуванням таких трьох критеріїв: 1) розвитку національного законодавства як правової основи державного управління; 2) структури та змісту діяльності суб'єктів забезпечення інформаційної безпеки в контексті еволюції теорії державного управління; 3) основних змін об'єкта управління (власне інформаційної безпеки). Хоча, здійснення державної політики інформаційної безпеки як окремого напрямку, на нашу думку, не може розглядатись на перших трьох етапах. І лише починаючи з 2014 р. можна простежити тенденції до формування цього напрямку. Нижче зміст окремих етапів державної політики у сфері інформаційної безпеки людини з урахування предмета нашого дослідження, а також з огляду на здійснене в розділі 2 дослідження становлення нормативно-правового забезпечення інформаційної безпеки людини в Україні.

На першому етапі (1991-1997 рр.) пріоритетним завдання було формування сукупності інститутів державної влади, що забезпечуватимуть прямий державний контроль та різновекторний вплив на інформаційний простір України, а "інформаційна безпека" як окрема самостійна категорія ніде не визначалася. Від СРСР Українська держава успадкувала модель адміністративно-державного

управління, відома у англомовному середовищі як “Old Public Management”. Її особливостями, насамперед, є: ієрархічний, вертикально інтегрований спосіб організації системи управління, з чітким розмежуванням повноважень, субординацією для різних рівнів органів і посадових осіб; прямий (адміністративний) державний контроль за всіма сферами життєдіяльності; відокремленість і закритість влади від суспільства.[ 156, с.90]

Окрім того, створена ще за радянських часів політична система гальмувала суспільний розвиток, вступала в суперечність з економічним базисом, особливо з інститутом приватної власності, а також Радянська концепція прав людини суттєво відрізнялась від концепції прав і свобод людини, яка була покладена в основу Хартії прав людини. Радянська держава і комуністична ідеологія розглядалися як джерело прав людини, а правова система СРСР використовувала право і закон як важелі політики, а суди як органи виконавчої влади. Свобода інформації та похідні від неї права суперечили ідеї комунізму, тому в правовому полі знайшлося місце категоріям «цензура», «атеїзм»<sup>44</sup>, «репресії», «терор», «інакомисліє» та іншим. Диктатура пролетаріату повинна була придушити опір інших класів, які марксизм розглядав антагоністичними до класу пролетаріату. Поширеним явищем було втручання державних органів, особливо КДБ, в особисте і сімейне життя громадян. Наприклад, громадянка Макклеллан, що перебувала у шлюбі з громадянином США, у листі до Президента США Картера описує становище своєї сім'ї, що підтверджує недотримання прав людини в СРСР. «Тут, коли я працювала в школі вчителем англійської мови, а моя дочка вчилася в цій же школі, ми піддавалися усіляким репресіям з боку дирекції та вчителів школи. Тепер, коли моя дочка хвора на виразку, радянська влада не віддає ліки, які чоловік вислав з США. Ми живемо в комунальній квартирі, і сусіди виконують роботу по стеженню за нами, покладену на них органами КДБ, тероризують нас, ображають з приводу шлюбу з американцем. Час від часу я піддаюся переслідувань на вулицях міста. Життя моє абсолютно ненормальне» [337].

---

<sup>44</sup> При чому, Патріарх Московський і всієї Русі належав до номенклатури Секретаріату ЦК КПРС, і по суті залишався маріонеткою в руках партійної верхівки.

Окремі напрями науки, в тому числі кібернетика і порівняльне мовознавство, на певних етапах було засуджено як «буржуазні лженауки», що суттєво стримувало їх розвиток, отже і формування передумов інформаційного суспільства.

Одним із найболючіших питань радянської спадщини для України стало національне, хоча на той момент воно не стояло так гостро. Більшовики, проголошуючи на словах дружбу народів, інтернаціоналізм і вільний розвиток усіх націй і народностей, дотримувалися на практиці відомої марксистської тези про те, що пролетарі не мають національності, наслідками такої політики були голодомори, масові депортації та русифікація. Національна політика використовувалась задля «окозамилування» - про що свідчить створення не тільки союзних, а й автономних республік, національних країв і областей, а також збереження аж до 1991 р. графі про національність у радянських паспортах і наявність в офіційній радянській статистиці даних про національний склад населення СРСР і окремих союзних республік.

В Україні, на відміну від країн Прибалтики та східноєвропейських держав, які раніше входили у так звану соціалістичну співдружність, не відбулося осмислення і, як наслідок, відторгнення радянської спадщини. Тому формування усіх напрямів державної політики пострадянського періоду розпочалось радянською партійно-номенклатурною «елітою» на звичним їм засадам. Після розпаду СРСР Україна фактично залишилась сам-на-сам зі своєю самостійністю - без будь-якого державного апарату. У новій державі не було власної законодавчої гілки влади, розвинутого апарату судової влади, а апарат четвертої влади, тобто засобів масової інформації, був дуже слабенький. Найрозвинутішим виявився апарат виконавчої влади - Кабінету Міністрів, кадри якого досить швидко зорієнтувалися і проникли у нові сегменти інших гілок влади. Вони зосередилися в апараті законодавчої і судової гілок влади, а також підпорядкували інформаційне середовище.

Тим не менш, важливими подіями цього етапу є створення Ради національної безпеки України в 1992 р. [382] і прийняття Закону України «Про інформацію» [365], який визначив засади інформаційного суверенітету України,

хоча сама категорія не визначалась. Натомість, в ст. 6 тогочасної редакції закону вперше для незалежної України було визначено поняття державної інформаційної політики як сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації. Головними її напрямками і способами визначались забезпечення доступу громадян до інформації; створення національних систем і мереж інформації зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності; забезпечення ефективного використання інформації; сприяння постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів; створення загальної системи охорони інформації; сприяння міжнародному співробітництву в галузі інформації і гарантування інформаційного суверенітету України.

На його основі в наступні роки було закладено правові основи державної політики у сфері ЗМІ шляхом прийняття законів "Про друковані засоби масової інформації (пресу) в Україні", "Про систему Суспільного телебачення і радіомовлення України", "Про Національну раду України з питань телебачення і радіомовлення», "Про державну підтримку засобів масової інформації та соціальний захист журналістів" та інші.

Указом Президента України в 1994 р. на базі Державного комітету України у справах видавництв, поліграфії та книгорозповсюдження й Державного комітету України з охорони державних таємниць у пресі та інших ЗМІ було створено Міністерство України у справах преси та інформації [380], з доволі широким колом повноважень щодо державного управління в сфері забезпечення інформаційної безпеки України.

В цей же період в Концепції (основи державної політики) національної безпеки вперше в українському законодавстві було задекларовано, що загроза інформаційної експансії іноземних держав є однією з основних загроз національній безпеці України в інформаційній сфері [367].

Згодом з'ясувалося, що такі підходи призвели до загрозливих деформацій вітчизняного інформаційного простору, оскільки переважна більшість новостворених телерадіоканалів, газет, журналів, а також неурядові аналітичні

центри не підконтрольні державі, бо фінансуються фондів міжнародних донорських агенцій. Саме їх зусиллями в українське суспільство вносились непритаманні для вітчизняної цивілізаційної моделі ідеологія й цінності, організаційні моделі, просувалися певні ідеологеми, що негативно впливають на суспільну думку щодо проблем внутрішньої та зовнішньої політики тощо [154].

Знаковими на цьому етапі було ще дві події - Конституційним Судом України під час розгляду справи щодо офіційного тлумачення ст. 3; 23; 31; 47; 48 Закону України "Про інформацію" було винесено рішення, що в Україні поняття "інформаційна безпека" законодавчо не визначено [405], а також створення Комісії з питань інформаційної безпеки [366].

Важливим для цього етапу було також усвідомлення існування різних моделей розробки державної політики. Типова для радянського періоду модель "зверху - вниз", яка передбачала, що державні рішення приймаються на вищих рівнях державного управління, а низові рівні є пасивним виконавцями політики, перестає бути єдино можливою. Хоча, на нашу думку, на цьому етапі ще зарано говорити про закладення основ моделі "знизу - вгору", яка передбачає, що формування державної політики починається з низових структур управління при активному залученні громадян, громадських інститутів. Адже для політичної системи України того періоду були притаманні застиглість і обмежена спроможність до трансформацій, монополія з боку кланової бюрократії, продажність і корупція, відсторонення від політичного життя широких верств населення, контрольованість засобів масової інформації, тотальна цензура, висування на керівні політичні посади осіб, професійно не підготовлених, схильних до хабарництва, але відданих тому хто їх фінансує і, зачасти, пов'язаних з ним сімейними зв'язками, бізнесовими, а часом і злочинними інтересами.

Неможливо переоцінити значення закріплення в Конституції України інформаційних прав, а також проголошення забезпечення інформаційної безпеки України "справою всього українського народу". Таким чином, інформаційна безпека з вузькоспеціалізованого кола вжитку фахівців прикладного характеру була піднесена до правового закріплення на рівні Основного Закону. Як можна



простежити, в науковій думці того періоду спостерігалось значне ототожнення понять «інформаційна безпека», «безпека інформації», «захист інформації», що й досі має місце в багатьох країнах [683, с. 363].

Для питання, що досліджується, має значення п. 5 ст. 92 Конституції України, де закріплено, що виключно законом встановлюються засади організації транспорту та зв'язку, а також основи національної безпеки, складовою якої слід вважати інформаційну безпеку. Забігаючи наперед, слід звернути увагу, що все ще не прийнято закону, який би визначав концепцію державної інформаційної політики України. Хоча відбулося декілька спроб ухвалити концепцію державної інформаційної політики на законодавчому рівні – 2002, 2009, 2010 та 2011 рр.

Поруч із закріпленням інформаційної безпеки як складової національної безпеки, Конституція України окреслила повноваження суб'єктів, що відповідають за формування і реалізацію відповідної державної політики - Президент України; Рада національної безпеки і оборони України; Верховна Рада України; Кабінет Міністрів України та інших.

Початок **другого етапу** (1998-2005 рр.) автор пов'язує з прийняттям 4 лютого 1998 р. Закону України “Про Концепцію Національної програми інформатизації” [368], в якому “інформаційна безпека”, визначена як невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки. Насамперед йшлося про політику інформатизації, про яку Арістова І.В. зазначає, «Те, що називали “політикою інформатизації” означало таку політику, що орієнтована на створення техніко-технологічної бази переходу країни до інформаційного суспільства (“залізо”, “кабелі”, будинки і т.ін., тобто взагалі — предмети матеріальні). У політиці не було місця для вирішення проблем інформаційних прав особистості, узгодження інтересів людини — суспільства — держави. Можна говорити про те, що ця політика прагнула “уникнути” соціальних проблем, зокрема, впливу інформації на громадську свідомість, демократизацію суспільства.»[15] Проте, як зазначає професор, ця політика прагнула “уникнути” соціальних проблем, зокрема, впливу інформації на громадську свідомість, демократизацію суспільства. Як вже зазначалось в 2 розділі ці роки ознаменувались прийняттям низки правових актів задля

врегулювання інформаційної сфери, і ще більшою кількістю спроб законодавчо визначити поняття “інформаційний суверенітет” і “інформаційна безпека”, жодна з яких так і не було легалізовано.

Разом з тим Рада національної безпеки і оборони України у рішенні “Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України”[363], звертала увагу на незадовільний стан забезпеченні інформаційної безпеки України і поставила низку завдань відповідним міністерствам і відомствам у сфері забезпечення інформаційної безпеки України, тм самим визначивши по суті систему органів, що здійснюють забезпечення інформаційної безпеки. Кабінету Міністрів України було доручено: розробити проект Концепції національної інформаційної політики та інформаційної безпеки України; розробити заходи щодо оптимізації системи державних органів, які реалізують інформаційну політику, забезпечивши чітке розмежування повноважень і налагодження їх взаємодії та координації; створити організаційну структуру системи забезпечення інформаційної безпеки; визначити механізм реалізації повноважень Генерального штабу Збройних Сил України щодо участі в організації і контролі за інформаційним простором держави та його здійснення в особливий період; Службі безпеки України – подати пропозиції щодо вдосконалення роботи з протидії інформаційним агресіям та спеціальним інформаційно-пропагандистським операціям, здійснюваним проти України іноземними спецслужбами; новоствореній Міжвідомчій комісії з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України – координація виконання заходів щодо забезпечення формування і захисту національного інформаційного простору, безпеки у цій сфері, розроблення і підготовка проектів відповідних нормативно-правових актів.

Абсолютно новим для України кроком щодо захисту власного інформаційного простору та гідного представлення у міжнародному інформаційному просторі стало затвердження “Державної програми забезпечення позитивного міжнародного іміджу України на 2003-2006 роки” 15.10.2003 р., якою передбачалось вироблення єдиного комплексного підходу до формування та здійснення інформаційно-пропагандистської політики держави, яка б охоплювала

різноманітні сторони її життя [357].

Однією з найважливіших подій цього етапу стало прийняття у 2003 р. Закону України “Про основи національної безпеки України”, що визначив загальну структуру суб’єктів та об’єктів національної безпеки, встановив основні напрями розвитку політики державної безпеки [376].

Ще однією інституцією, що повстала на цьому етапі є Національна експертна комісія України з питань захисту суспільної моралі, як постійно діючий державний позавідомчий експертним і контролюючим органом, який діє відповідно до Закону України „Про захист суспільної моралі” № 1296-IV від 20 листопада 2003 р. та Положення про Національну експертну комісію України з питань захисту суспільної моралі, затвердженого постановою Кабінету міністрів України №1550 від 17 листопада 2004 р.. Вона проіснувала до 2015 р.. Основними завданнями були: проведення експертизи продукції, видовищних заходів сексуального чи еротичного характеру та продукції, що містить елементи або пропаганду культу насильства, жорстокості, порнографії; аналіз процесів і тенденцій, що відбуваються у сфері захисту суспільної моралі, розроблення для органів державної влади та органів місцевого самоврядування рекомендацій з їх правового регулювання; контроль за дотриманням законодавства у сфері захисту суспільної моралі; участь у розробці міжнародних договорів України з питань захисту суспільної моралі.

Діяльність Національної експертної комісії мала бути спрямована на піднесення культури та духовності українського народу, всіх національностей, що проживають на Україні, утвердження здорового способу життя та належного стану моральності в суспільстві, виховання майбутніх поколінь українців на основі традиційних духовних і культурних цінностей, уявлень про добро, честь, гідність, громадський обов’язок, совість, справедливість, на засадах народних традицій, українських звичаїв, етичних норм і правил поведінки, що склалася у суспільстві. Для реалізації цих завдань комісії було надано повноваження щодо проведення у межах своєї компетенції перевірок діяльності засобів масової інформації, юридичних осіб усіх форм власності, що займаються організацією видовищних заходів та діяльністю з обігу продукції сексуального чи еротичного

характеру або такої, що містить елементи насильства і жорстокості. Рішення Національної експертної комісії, ухвалені в межах її повноважень, були обов'язковими для розгляду центральними і місцевими органами влади, засобами масової інформації всіх форм власності, а також фізичними та юридичними особами.

В цей період було здійснено спробу дебюрократизації управлінської системи та впровадження нових підходів до організації процесу державного управління з високим ступенем орієнтації на ефективність та результативність. В результаті такою інновацією стала модель “Нового державного управління” (New Public Management). Основний зміст нової моделі полягає у зміні принципів формування організаційної структури державного управління; підвищенні гнучкості прийняття рішень у державному апараті, зменшенні його ієрархічності, делегування повноважень на нижчий рівень прийняття рішень та посилення механізмів зворотного зв'язку між державою та громадянами [11, 271].

**3-й етап** (2006-2013 рр.) Зозуля характеризує як етап кардинальних змін у державному управлінні інформаційною безпекою, інтенсивною роботою з визначення концептуальних засад системи забезпечення інформаційної безпеки в Україні, які мали базуватися на постулатах та цінностях громадянського суспільства, відповідати сучасним європейським нормам, упровадження яких розглядається як безпосередній обов'язок держави [156]. Ця позиція, на нашу думку, категорично не відповідає дійсності. Хоча, як наслідок участі у Всесвітньому Самміті Інформаційного Суспільства в січні 2007 р. і було прийнято Закон України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007- 2015 роки”, де законодавчо закріплено поняття “інформаційна безпека” [378]. Проте, його реалізація так і не стала пріоритетом в державній політиці. Про це свідчить і той факт, що Закон на 2007-2015 роки досі залишається чинним, наступної його редакції не існує і, наскільки нам відомо, не передбачається її створення найближчим часом.

Про неадекватність реальним умовам, декларативність і неефективність, а подекуди – невідповідність політики інформаційної безпеки цього періоду національним інтересам держави і суспільства свідчить також інформаційне

протиставлення та реальні військові дії на території України, якими увінчалась така політика.

Хоча, мали місце певні поодинокі спроби. У 2009 р. підготовлена і затверджена Указом Президента України від 08.07.2009 р. № 514/2009 Доктрина інформаційної безпеки країни [121]. Доктрина окреслювала основні засади інформаційної безпеки України, визначила місце інформаційної безпеки в системі забезпечення національної безпеки України, називала реальні та потенційні загрози інформаційній безпеці України, визначала напрями державної політики у сфері інформаційної безпеки держави. Слід згадати також Хартію про партнерство заради інформаційних прав і свобод та захисту суспільної моралі, підписану у 2009 р. [496]. Хартія за своєю формою і змістом є суспільним договором, що укладений суб'єктами інформаційного процесу та представниками державних органів України з метою запровадження саморегулювання в дотриманні суб'єктами інформаційної діяльності законодавства про захист суспільної моралі, яка є не тільки конституційним обов'язком Української держави, але й однією із найважливіших складових національної безпеки України. Наступним кроком стало схвалення у 2010 р. Концепції проекту Закону України «Про основні засади державної комунікативної політики» метою якої є визначення шляхів законодавчого врегулювання питання забезпечення взаємодії між органами державної влади, органами місцевого самоврядування, засобами масової комунікації і громадськістю на засадах рівноправного партнерства, що сприятиме зміцненню демократії, становленню громадянського та інформаційного суспільства [388].

В травні 2011 р. набула чинності нова редакція Закону України «Про інформацію», в ст. 3 якого серед основних напрямів державної інформаційної політики з'явилися: «створення умов для формування в Україні інформаційного суспільства; забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень; створення інформаційних систем і мереж інформації, розвиток електронного урядування; забезпечення інформаційної безпеки України та інші. Таким чином, забезпечення інформаційної безпеки було віднесено до напрямів реалізації державної інформаційної політики. При тому, що норма щодо її

розробки і здійснення залишилась без змін - органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції, тобто, по факту, всі і ніхто конкретно.

Важливим кроком щодо забезпечення інформаційної безпеки людини були ратифікація в 2010 р. Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї, як наслідок - прийняття Закону України «Про захист персональних даних» і створення Державної служби України з питань захисту персональних даних. Останній було надано широкі повноваження щодо реалізації державної політики у сфері захисту персональних даних, зокрема, контроль за додержанням вимог законодавства про захист персональних даних; реєстрація бази персональних даних та ведення Державного реєстру баз персональних даних; здійснення державного нагляду та контролю за додержанням законодавства про захист персональних даних та інші, всього понад 30 повноважень. Цей Закон, як і діяльність Служби зазнали суттєвої критики, що призвело до того, що в 2013 р. Верховна Рада України прийняла Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», яким з метою забезпечення незалежності уповноваженого органу з питань захисту персональних даних, повноваження щодо контролю за додержанням законодавства про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини.

У 2011 р. набули чинності Закон України «Про доступ до публічної інформації» та нова редакція Закону України «Про інформацію», які стали важливою сходинкою до забезпечення не лише свободи інформації, а й демократизації суспільства. Законом «Про доступ до публічної інформації» було визначено : 1) порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації; 2) гарантії та принципи забезпечення права на доступ до публічної інформації; 3) суб'єктів відповідних відносин, їх права та обов'язки тощо. Окрім того, нова редакція Закону «Про інформацію» передбачає «право кожного на інформацію», визначивши при цьому одним із основних

напрямів державної інформаційної політики «забезпечення доступу кожного до інформації». У ст. 20 цього ж Закону було закріплено важливий принцип максимальної відкритості, згідно з яким «будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом», та інші положення, важливі для реалізації права на доступ до інформації, а саме: дозвіл на поширення інформації з обмеженим доступом, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від поширення (ч. 1. ст. 29); визначення невичерпного переліку інформації, що становить предмет суспільного інтересу (ч. 2 ст. 29); звільнення від відповідальності за розголошення інформації з обмеженим доступом, якщо суд встановить, що ця інформація є суспільно необхідною (ч. 3 ст. 30). Таким чином, ці два закони демонстрували відмову від хибної концепції права власності на інформацію загалом і власності держави на інформацію зокрема. Вони закріпили підхід, що ґрунтується на Конституції України, Цивільному кодексі України та міжнародних стандартах і передбачає, що інформація є об'єктом особистих немайнових прав, об'єктом особистих прав фізичної чи юридичної особи.

В 2013 р. було схвалено Стратегію розвитку інформаційного суспільства в Україні, що визначила мету, базові принципи, стратегічні цілі розвитку інформаційного суспільства в Україні [388]. В Стратегії зазначається, що забезпечення інформаційної безпеки у процесі використання інформаційно-комунікаційних технологій є однією з найважливіших умов успішного розвитку інформаційного суспільства. Суттєвим недоліком цього документа, було акцентуація уваги на заходах по технічному забезпеченню інформаційної безпеки (захист інформації, забезпечення безпеки інформаційних мереж, тощо).

**4-й етап** (починаючи з 2014 р. – по теперішній час) в історичній динаміці становлення і розвитку системи забезпечення інформаційної безпеки України запропонованій Зозулею С.В. співпадає з періодизацією розвитку правового забезпечення інформаційної безпеки, що здійснена нами у 2 розділі. Кардинальна трансформація взаємодії між державою і громадянським суспільством призвела до запровадження нових способів і механізмів державного управління з метою

забезпечення ефективного управління суспільними процесами в сучасних умовах.

Окрім того, проєвропейський вектор зовнішньої політики і підписання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (далі Угоди про асоціацію) [477] в державному управлінні намітився курс на запровадження європейської моделі належного (доброго) управління<sup>45</sup>.

Першою реакцією на ситуацію, що склалась в Україні, стало Рішення Ради національної безпеки і оборони України “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України” [363], а також було скасовано чинність низки актів РНБО затверджених Президентом України, в тому числі Доктрина інформаційної безпеки України, що була затверджена в 2009 р. [121].

На цьому етапі спостерігається суттєва інтенсифікація наукового опрацювання, публічної дискусії та нормотворчої роботи щодо питань забезпечення інформаційної безпеки. В 2014 р. до Верховної Ради України був поданий Проект Закону “Про засади інформаційної безпеки України” (реєстраційний № 4949 від 28.05.2014 р.) [354], Державним комітетом телебачення і радіомовлення України розроблено проект нової Доктрини інформаційної безпеки України і проект Стратегії розвитку інформаційного простору України на період до 2020 р. [394, 396].

В 2015 р. Верховна Рада України суттєво доопрацювала законодавство щодо доступу до публічної інформації, особливо слід виділити чотири закони. Перший стосувався внесення змін до деяких законів України щодо доступу до публічної інформації у формі відкритих даних. Закон передбачив створення єдиного державного веб-порталу відкритих даних, а також встановив, що оприлюднена на такому веб-порталі інформація є публічною інформацією у формі відкритих даних

---

<sup>45</sup> “Good Governance”. Концепція “Good Governance” наповнює державне управління гуманітарною та соціальною складовою, формує новий підхід до розуміння врядування, яке має тепер відповідати не лише вимогам ефективності, але й бути відкритим, доступним, підзвітним і підконтрольним, а отже, чутливим до вимог громадян, їхніх потреб і запитів. Тобто це спосіб реалізації публічної влади, завдяки якому досягаються реальна участь громадян у виробленні та реалізації публічної політики; об’єднання потенціалу всіх трьох секторів (влада, бізнес, громадськість); постійний контроль різними інститутами громадянського суспільства за публічною владою [156]



та є дозволеною для її наступного вільного використання та поширення [77]. Беручи до уваги можливості, які відкриває цей закон перед громадськістю, значення його прийняття для подальшого розвитку українського суспільства і для кожної людини зокрема, важко недооцінити.

Другий Закон України «Про внесення змін до статті 28 Бюджетного кодексу України щодо доступу до інформації про бюджетні показники у формі відкритих даних» передбачає оприлюднення бюджетних запитів, квартальної та річної звітності про виконання Державного бюджету України, паспортів бюджетних програм та звітів про виконання паспортів бюджетних програм, рішень про місцеві бюджети, інформації про виконання Державного бюджету України та місцевих бюджетів (крім бюджетів сіл і селищ)[304].

Прийнятий Закон України «Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917-1991 років» має за мету врегулювання основних засад, принципів, гарантій, шляхів реалізації державної політики щодо забезпечення доступу до архівної інформації репресивних органів. А Закон України «Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції» запроваджував механізм подання індивідуальних та колективних звернень в електронній формі[342].

В 2015 р. було затверджено нову Стратегію національної безпеки України [379], в якій пріоритетами забезпечення інформаційної безпеки визначені: забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії; створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності; створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики держав - членів НАТО;

удосконалення професійної підготовки у сфері інформаційної безпеки.

Як зазначає Зозуля О.С. на сьогодні жоден з існуючих центральних органів виконавчої влади не в змозі самостійно здійснювати весь комплекс заходів із забезпечення інформаційної безпеки[154, с.150].

Хоча в січні 2015 р. було утворено Міністерство інформаційної політики України, як головний орган у системі центральних органів виконавчої влади у сфері забезпечення інформаційного суверенітету України [311], проте інформаційний суверенітет України на законодавчому рівні не визначений. Була спроба ще в 1999 р. прийняти відповідний закон [361], але і досі це питання не вирішено.

В 2015 р. було підписано “Дорожню карту програми Партнерства зі стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО” [124]. Програма Партнерства спрямована на здійснення комплексної підтримки України у сфері стратегічних комунікацій, зокрема протидії російській пропаганді та інформуванні громадськості про події в Україні. В 2016 р. було визначено принципи, пріоритети та напрями забезпечення кібербезпеки України в Стратегії кібербезпеки України[443].

І лише на межі 2016 і 2017 років держава нарешті отримала Доктрину інформаційної безпеки України [121], яка визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері, і спрямована на уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни.

Складно на даний момент оцінити вплив цього документу на українські реалії інформаційної сфери. Передбачено, що основними суб'єктами повноважень згідно неї мають стати Кабінет міністрів, Міністерство інформаційної політики, Міністерство закордонних справ, Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, Служба безпеки України, розвідувальні органи, Державна служба спеціального зв'язку та

захисту інформації, Національний інститут стратегічних досліджень; а також РНБО як орган, що здійснює координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері. Суттєво посилені і конкретизовані повноваження Міністерства інформаційної політики.

Таким чином, можна констатувати, що чинне законодавство не дає цілісного і системного закріплення офіційних поглядів, принципів, напрямів діяльності, спрямованих на реалізацію державної політики інформаційної безпеки людини.

Водночас, аналіз правових основ державної політики дозволяє зробити висновок, що як окремий напрям державна політика інформаційної безпеки (і в цілому, і людини, зокрема) не виділяється, хоча в науковій думці існує такий підхід (Олійник О.В., Зозуля О.С., Ліпкан В.М., Кормич Б.А).

Б. Кормич відзначав, що як за суб'єктним складом, так і за компетенцією механізм інформаційної безпеки повинен дещо відрізнятися від традиційного механізму державного управління, що інституціональний механізм інформаційної безпеки являє собою сукупність інститутів публічної влади та інститутів громадянського суспільства, до компетенції яких входить вирішення питань щодо забезпечення умов функціонування і розвитку інформаційної сфери [208, с.8]. При цьому основні напрями забезпечення інформаційної безпеки він суттєво звужував, розглядаючи їх лише через сферу обігу інформації, тобто її одержання, зберігання, використання, поширення та захисту [там же, с.214-363]. Його критикує Олійник О.В. і гостро ставить питання про необхідність відмовитися від подальшої примітивізації інформаційної безпеки як складової національної безпеки лише в інформаційній сфері, тобто сфері обігу інформації. Погоджуючись з його аргументацією, вважаємо доцільним концептуальний підхід до визначення інформаційної безпеки як складової національної безпеки у сфері інформаційної діяльності. Інформаційна безпека має бути важливою основою інформаційних складових усіх сфер забезпечення національної безпеки [288, с. 67].

Якщо ж говорити про інформаційну безпеку людини, то політика щодо неї знаходиться на перетині декількох пріоритетних напрямів державної політики – насамперед, інформаційної політики, політики національної безпеки та політики з прав людини, але також і правової політики, соціальної політики, політики у

галузі освіти і науки, і, навіть, зовнішньої політики. При цьому, за кожним напрямом має враховуватись єдиний підхід до забезпечення інформаційної безпеки людини – створення умов для своєчасного виявлення потенційних і реальних загроз; розробки і впровадження заходів і засобів попередження і протидії викликам; нейтралізації або послаблення дії небезпек. Тому вбачається доцільним визначити на рівні незалежного органу держави закріпити інститут Уповноваженого з інформаційної безпеки людини, як аналог прийнятого в ЄС інституту інформаційного комісара. Його діяльність має бути спрямована на реалізацію політики держави щодо забезпечення інформаційної безпеки людини, в тому числі захист прав і свобод людини в інформаційній сфері, зокрема, права на доступ до публічної інформації та захист персональних даних. Уповноваженому необхідно надати достатні важелі впливу, з однієї сторони, на формування інформаційного законодавства, наприклад, шляхом обов'язкової експертизи нормативних актів що зачіпають відповідні права людини, з іншої – повноваження щодо припинення правопорушень та відновлення порушених прав.

Окрім того, ефективність політики держави щодо інформаційної безпеки людини значною мірою залежить від системного розуміння проблеми розбудови приязного для людини інформаційного суспільства, а отже вимагає визначення єдиного органу відповідального за її здійснення. З цією метою та з урахуванням позитивного досвіду європейських країн, пропонується зосередити повноваження по реалізації політики держави щодо розбудови інформаційного суспільства в єдиному центральному органі виконавчої влади. При цьому, на законодавчому рівні має бути визначено відповідальність держави і зобов'язання щодо реалізації інформаційної політики у основних сферах життєдіяльності суспільства – обороні, захисті прав людини, економіці, освіті, охороні здоров'я, екології, демократизації та децентралізації тощо. Особливими сферами відповідальності такого органу мають стати: координація розбудови інформаційної інфраструктури держави; забезпечення умов для реалізації інтересів людини, суспільства і держави в інформаційному (в т.ч. кібер) просторі; координація діяльності інших державних органів в інформаційній сфері, забезпечення безвідмовної роботи об'єктів критичної інформаційної інфраструктури, створення умов для

формування належного рівня інформаційної культури населення, в тому числі, професійної підготовки населення в умовах розбудови інформаційного суспільства, сприяння розвитку ІТ галузі, забезпечення відкритості та прозорості діяльності влади, а також сприяння формуванню позитивного іміджу України як в середині держави, так і за її межами.

## **5.2. Механізм правового регулювання відносин у сфері інформаційної безпеки людини**

Механізм правового регулювання як сукупність правових засобів, за допомогою яких держава здійснює правовий вплив на суспільні відносини, насамперед, має на меті досягнути бажаний для держави і суспільства результат. Таким чином, він по суті відображає пріоритети політики держави в означеній сфері правового регулювання.

Теоретичні основи механізму правового регулювання закладені в працях С.С. Алексєєва, зокрема, його монографіях "Механізм правового регулювання в соціалістичній державі" і "Теорія права", де категорія "механізм правового регулювання" визначалась через правовий вплив. Однак поняття механізму правового регулювання вужче, ніж поняття механізму правового впливу.

Не кожні суспільні відносини урегульовано правом. Зокрема, не завжди підлягають правовому регулюванню процеси виробництва інформаційного продукту, хоча щораз частіше мають місце техніко-юридичні норми; за загальним правилом поза межі правового регулювання виведено особисте життя і релігійні відносини тощо. Сфера правового регулювання може об'єднувати лише відносини, що піддаються правовому регулюванню - конкретні, значимі відносини, що усвідомлюються людиною, і щодо яких може бути прийняте вольове рішення. Так, відносини, що на сьогодні становлять суттєву загрозу інформаційній безпеці і пов'язані із негативним інформаційним впливом на її психіку, часто складно включити в перелік тих, що усвідомлюються і піддаються правовому регулюванню. Проте, власне визначення механізму правового регулювання покликане встановити межі необхідного і можливого втручання

держави у суспільні відносини, що виникають у зв'язку з інформаційною безпекою людини.

Оскільки інформаційна безпека є невід'ємною властивістю її об'єктів, то говорити про регулювання інформаційної безпеки немає підстав. Це також одна з суперечностей, що має місце при визначенні самої інформаційної безпеки як стану, адже стани не регулюються правом. В такому випадку правове регулювання може розглядатись лише як складова забезпечення інформаційної безпеки. Подібний підхід можна зустріти в роботах багатьох українських і зарубіжних науковців.

Істотне значення для розуміння правового регулювання має його предмет чи сфера правового регулювання. Інформатизація та інші етапи становлення інформаційного суспільства обумовили формування категорії «інформаційна сфера» як предмету правового регулювання.

Російська класик інформаційного права І.Бачило, предметом, що формує спеціальну галузь відносин, умовно званих інформаційними, визначала сукупність реально існуючих матеріалізованих результатів творчості і праці, втілених: 1) в інформації, при різноманітності форм її прояву, і сформованих на її основі інформаційних ресурсах, 2) засоби і технології роботи з інформацією (інформаційних технологіях); 3) засоби і технології комунікації інформації по мережах зв'язку. На базі цієї тріади предметів формується нова галузь суспільних відносин, яка в системі права виділяється як самостійна галузь правового регулювання [35, с.26].

Глибокий і комплексний аналіз цієї категорії було здійснено українським вченим Барановим О.А. в монографії «Правове забезпечення інформаційної сфери: теорія, методологія і практика» [24]. Проаналізувавши доктринальні і нормативні визначення інформаційної сфери, вчений сформулював авторське визначення інформаційної сфери як сукупності інформації та інформаційних ресурсів, інформаційної інфраструктури, суб'єктів, що здійснюють оборот інформації, тобто її створення, поширення (передавання), зберігання, використання та знищення, та забезпечують цей оборот, суспільних відносин, які

при цьому виникають, системи її правового забезпечення, а також інституційної системи державного управління та регулювання цієї сферою [24, с.22].

Проте, суспільні відносини, що виникають у зв'язку з інформаційною безпекою людини не обмежуються лише інформаційною сферою. Інформаційна безпека людини, як вже визначалось раніше, є складовою будь-якого виду інформаційної безпеки – чи то держави, чи суспільства, чи міжнародного співтовариства, а також має місце у складі інших сфер безпеки – продовольчої, екологічної, економічної, соціальної тощо. Таким чином, недоцільно визначати предмет її правового регулювання виключно в межах інформаційної сфери. Він є значно ширшим, комплексним за своєю суттю, охоплює декілька предметних сфер.

Слід також враховувати, що у світі склалось дві тенденції правового регулювання правовідносин у інформаційній сфері: використовувати за аналогією законодавство, що існує, при цьому створюючи нові норми лише щодо дійсностей, що повстають у зв'язку з всеосяжною інформатизацією; або творити нове комплексне інформаційне законодавство. Україна, як відомо пішла першим шляхом, що призвело до виникнення суттєвим дисбалансів у питаннях інформаційної безпеки і проблем як при нормотворчій діяльності, так і на стадії правозастосування.

Як приклад, можна розглядати ситуацію з правовим регулюванням суспільних відносин, що реалізуються за допомогою інтернету. На думку, М. Дворового, експерта Центру демократії та верховенства права, впродовж тривалого часу інтернет в Україні перебував поза межами правового регулювання [107]. У рейтингу Freedom on the Net, що створює міжнародна правозахисна організація Freedom House, до 2013 р. включно Україна вважалася країною з вільним інтернетом. Після Революції Гідності рейтинг свободи інтернету в Україні погіршився, країна перейшла із групи “вільних” до групи “частково вільних” країн.

Починаючи з 2014 р. на обговоренні у владних структурах почастишали проекти актів, спрямовані на врегулювання відносин, що реалізуються за допомогою мережі, які, водночас, подекуди містять норми, спрямовані на

обмеження прав користувачів інтернету<sup>46</sup>. Так, в жовтні 2017 р. було прийнято два Закони, що мають суттєве значення як для інформаційної сфери в цілому, так і для інформаційної безпеки людини, зокрема, це «Про основні засади забезпечення кібербезпеки України» та Закон «Про електронні довірчі послуги». Станом на кінець 2017 р. на розгляді парламенту перебувало ще три законопроекти, які можуть суттєво вплинути на стан свободи інтернету в Україні: проект Закону про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю (№ 2133а від 19.06.2015); проект Закону про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері (№ 6688 від 12.07.2017); проект Закону про внесення змін до Закону України «Про захист прав споживачів» та деяких законодавчих актів України щодо заходів детінізації діяльності суб'єктів електронної комерції (№ 6754 від 17.07.2017).

Як обґрунтування ініціатив наводились необхідність забезпечити інформаційну безпеку України в умовах війни та посилити захищеність авторського та суміжних прав. Проте, такий підхід продовжує усувати «точкові» недоліки за відсутності загальної концепції регулювання інформаційної сфери. Таким чином, посилюється дисбаланс між забезпеченням інформаційної безпеки і свободою інформації, яка є основою демократії.

При цьому, сценарії які розглядаються для врегулювання інформаційної сфери, сприймаються по-різному в наукових, урядових, бізнесових колах, а також серед представників інститутів громадянського суспільства. Останні насамперед пильнують свободу слова і там, де це можливо, наполягають на саморегулюванні. Ділові кола, а це ІТ-компанії та медіа бізнес, зацікавлені в правовому забезпечення ринкових умов для їх діяльності. Влада, затиснута поміж реальністю інформаційної війни та бойових дій на сході України, задекларованим процесом євроінтеграції та зовнішнім тиском, політичними лобістськими інтересами, а подекуди і корупційними схемами, в черговий раз демонструє

---

<sup>46</sup> При цьому в аналітиці громадських діячів ці права здебільшого називають «цифровими», ми ж не погоджуємось з таким підходом, що обґрунтовано в розділі 3 цього дослідження.



невиваженість державної інформаційної політики. Щодо науковців – останні 3 роки спостерігається певна дихотомія. З одного боку, кількість наукових досліджень цієї проблематики постійно зростає, з іншого – академічна наука, в цілому, є під загрозою. Проте, це питання виходить за межі предмету дослідження.

Необхідним вбачається наукове осмислення, громадське обговорення і подальше нормативне закріплення прийнятного і обумовленого реаліями українського суспільства і держави принципів правового регулювання інформаційної сфери з метою забезпечення інформаційної безпеки людини. Власне виходячи з цих основоположних засад може бути розмежовано відносини щодо інформаційної безпеки людини, які: 1) обґрунтовано і ефективно регулюються правом, 2) не регулюються правом, але в цьому є суспільна необхідність; 3) не регулюються і регулювання не вбачається доцільним та/або можливим.

Принципи правового регулювання мають відображати його основну мету - забезпечення безперешкодного руху інтересів суб'єктів до цінностей, тобто гарантованість справедливого задоволення інформаційних потреб людини, в умовах її захищеності від шкоди або інших небажаних результатів для її гідності та вільного розвитку.

В правовій системі діє ієрархія принципів, які можна уявити як взаємодію різних видів по вертикалі. Бачило І. виділяє такі групи принципів, як: 1) загальнонаукові; 2) конституційні принципи організації суспільства і державної системи; 3) загальні принципи правового регулювання; 4) принципи правового регулювання в конкретній галузі; 5) принципи правозастосування. В цілях цього дослідження хочемо звернути увагу на дві останні категорії.

Зважаючи на те, що системоутворюючим законом в інформаційній сфері є Закон України «Про інформацію», то слід звернути увагу на принципи інформаційних відносин, які визначені ст. 3: «гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту

інформації; захищеність особи від втручання в її особисте та сімейне життя» [360].

В Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», який досі залишається чинним, було визначено, що «при створенні інформаційного законодавства слід керуватися загальними принципами Конституції України, а також базуватися на принципах свободи створення, отримання, використання та розповсюдження інформації; об'єктивності, достовірності, повноти і точності інформації; гармонізації інтересів людини, суспільства та держави в інформаційній діяльності; обов'язковості публікації інформації, яка має важливе суспільне значення; обмеження доступу до інформації виключно на підставі закону; мінімізації негативного інформаційного впливу та негативних наслідків функціонування ІКТ; недопущення незаконного розповсюдження, використання і порушення цілісності інформації; гармонізації інформаційного законодавства та всієї системи вітчизняного законодавства»[374]. Запропонований підхід базується на дослідженнях російських теоретиків інформаційного права Копилова В.А. і Бачило І.Л. Доцінюючи їх внесок в розвиток науки інформаційного права, вважаємо доцільним і необхідним їх переосмислення з огляду на сучасний розвиток інформаційної сфери суспільства, а також на інформаційне протистояння і обумовлені ним загрози інформаційній безпеці людини, демократичного суспільства і української держави.

Л. П. Коваленко, зазначає, що правове регулювання інформаційних відносин ґрунтується на принципах інформаційного права, під якими розуміють основні вихідні положення, що юридично пояснюють і закріплюють об'єктивні закономірності суспільних відносин, що проявляються в інформаційній сфері [195, с. 190] І до них відносить наступні – пріоритету прав особи; вільного створення й поширення будь-якої інформації, не обмеженої українським законом (принцип свободи творчості й волевиявлення); заборони створення й поширення інформації, шкідливої й небезпечної для розвитку особистості, суспільства, держави; вільного доступу (відкритості) інформації, не обмеженої національним законом (право знати), або принцип гласності; повноти опрацювання й оперативності надання інформації; законності; інформаційно-правового

регулювання; вилучення «відчуження» інформації в її власника, відповідальності за неправомірне використання інформації (її сутності); обігу інформації; двоєдності інформації і її носія; поширення інформації; організаційної форми та принцип екземплярності інформації. Як на нашу думку, такий перелік є надмірно деталізований і поєднує в собі не лише спеціальні, а й загально правові принципи.

Вважаємо обґрунтованою думку Баранова О.А., що незважаючи на те, що всі дослідники відзначають важливість формування принципів інформаційного права, дотепер не сформульована єдина, стала точка зору на їх зміст [25, с. 7].

В якості базового принципу інформаційного права вчений пропонує використовувати принцип забезпечення інформаційної безпеки з урахуванням того, що забезпечення інформаційної безпеки є одним з основних атрибутивних властивостей систем, у тому числі соціальних. Цей принцип знайшов відображення в ст. 17 Конституції України: “Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу”. Наступні принципи Баранов О.А. вважає похідними від цього базового принципу і до них відносить такі: 1. Свободи одержання і поширення інформації. 2. Об'єктивності, вірогідності, повноти і точності інформації. 3. Гармонізації інтересів особи, суспільства і держави в інформаційній діяльності. 4. Мінімізації негативного інформаційного впливу. 5. Мінімізації негативних наслідків функціонування інформаційних технологій. 6. Недопущення несанкціонованого поширення, використання і знищення інформації 7. Інформація виступає в якості об'єкту цивільних правовідносин. 8. Невідторгаємість інформації. 9. Єдність і різниця інформації і носія інформації. 10. Об'єктність надання інформації. 11. Первинність створення інформації. 12. Обмеження доступу до інформації. 13. Обов'язковість опублікування. 14. Взаємна гармонізація інформаційного права і всієї системи вітчизняного законодавства. 15. Гармонізація українського інформаційного законодавства з міжнародним законодавством і законодавством інших країн [25, с. 7].

Слід зважати, що сформульовані 2006 р. принципи інформаційного права України О.А. Баранов пропонував використовувати, насамперед, у процесі

формування власне інформаційного законодавства, а також у процесі правозастосування існуючих правових норм, що регулюють інформаційні відносини. Також звертав увагу на те, що сформована система принципів інформаційного права не є остаточною, тому що в діалектичному процесі створення конкретних правових норм інформаційного законодавства і розвитку загальної системи права держави, правосвідомості в Україні принципи можуть піддаватися відповідним змінам, як по кількості, так і по змісту.

Погоджуючись в основному з запропонованим підходом, зробимо спробу співставити запропоновану систему принципів з принципами правового регулювання у сфері інформаційної безпеки. О.В. Олійник вважає, вихідними положеннями формування і функціонування системи інформаційної безпеки як системоутворюючого фактору всіх складових національної безпеки, норм і правил поведінки громадян, державних і суспільних інститутів України у цій сфері, є наступні: пріоритет прав, свобод і законних інтересів людини і громадянина; верховенство права, рівність усіх суб'єктів правовідносин перед законом; відповідальність держави перед людиною за свою діяльність; комплексний підхід до вирішення завдань забезпечення інформаційної безпеки; єдність і взаємозв'язок напрямів забезпечення інформаційної безпеки; розмежування сфер відповідальності й повноважень державних органів і органів місцевого самоврядування з питань забезпечення інформаційної безпеки; участь у міжнародних і регіональних системах інформаційної безпеки; оперативність, своєчасність, превентивність і адекватність заходів щодо попередження і захисту від зовнішніх інформаційних загроз та нейтралізації джерел внутрішніх інформаційних загроз [290, с.72]

Як свідчить досвід країн з розвиненою демократією, інформаційна безпека людини не повинна протиставлятися інформаційній безпеці держави та суспільства. Адже саме людина визнається основною цінністю кожного суспільства і забезпечення її прав і свобод є кінцевою метою реалізації функцій держави. Проте, реалії інформаційного суспільства обумовлюють необхідність обмеження прав та законних інтересів людини з метою захисту національних інтересів держав, попередження міжнародних конфліктів чи/та терористичних

актів, а також забезпечення безпеки національних інформаційних ресурсів. Таким чином, має місце конфлікт інтересів різних об'єктів інформаційної безпеки. Вирішення цього конфлікту демократичним шляхом є однією з первинних задач при створенні відповідних правових норм.

Як було зазначено в розділі 4, підходи США і ЄС до вирішення цього питання суттєво відрізняються. Про це свідчить як аналіз законодавства, так і правозастосування. США декларує високі стандарти прав і свобод людини в інформаційній сфері, але при виникненні протиріч між гарантуванням дотримання цих стандартів і інтересами національної безпеки перевага віддається саме інформаційній безпеці держави.

Країни ЄС, в свою чергу, демонструють більш послідовну політику щодо гарантування і дотримання прав і свобод людини в інформаційній сфері. Про це свідчать, зокрема, останні зміни в законодавстві щодо захисту персональних даних. Окрім того, значну роль у нормотворчості відграють міжнародні судові органи, зокрема суд ЄС та ЄСПЛ, які шляхом правозастосування конкретизують розуміння змісту правових норм на основі суспільної практики, а часом і формують нове розуміння з огляду на зміни, що відбуваються в суспільстві.

Натомість, Радзієвська О.Г. зазначає, що норми міжнародного права і законодавства ЄС, а також досвід іноземних держав свідчить про існування двох моделей забезпечення інформаційної безпеки: людиноцентричну (країни Європейського Союзу, США) та державоцентричну (РФ, КНР) [396, с.225]. Частково не поділяємо поглядів автора щодо моделі забезпечення інформаційної безпеки США, адже хоча безперечно, США закріплено конституційно принцип пріоритету прав, свобод і законних інтересів людини і громадянина. Проте, аналіз законодавства США у сфері інформаційної безпеки свідчить про пріоритетність окремих напрямів забезпечення національної кібербезпеки США, зокрема, захист критично важливих об'єктів інфраструктури.

При визначенні принципів правового регулювання відносин, що виникають з приводу інформаційної безпеки людини, вважаємо, що вони мають базуватись на основних засадах (1) правового регулювання інформаційної сфери; (2) правового

регулювання у сфері інформаційної безпеки та (3) правового регулювання прав і свобод людини.

Таким чином, до основних принципів правового регулювання відносин у сфері інформаційної безпеки людини пропонується віднести:

- принцип пріоритету прав, свобод і законних інтересів людини і громадянина;
- принцип свободи інформації і обмеження доступу до інформації виключно у випадках передбачених законом;
- принцип розвитку сприятливого для людини інформаційного суспільства;
- принцип відповідальності держави перед людиною та суспільством за реалізацію державної політики інформаційної безпеки;
- принцип мінімізації негативного інформаційного впливу на людину, в т.ч. шляхом формування інформаційної культури людини і суспільства;
- принцип участі громадянського суспільства у розробці та контролі за реалізацією заходів щодо попередження та захисту від загроз інформаційній безпеці людини;
- принцип гармонізації інформаційного законодавства України із законодавством ЄС та положеннями міжнародного права у сфері інформаційної безпеки.

Базуючись на запропонованих принципах, механізм правового регулювання має включати систему правових засобів, організованих найбільш послідовним чином з метою попередження, нейтралізації, обмеження та подолання загроз інформаційній безпеці людини.

В теорії права відсутнє єдине бачення визначення елементів механізму правового регулювання. Скакун О.Ф., як елементи механізму правового регулювання визначає: 1) ті, що діють на відповідних стадіях регулювання - норми права; нормативно-правові акти; юридичні факти; правовідносини; акти безпосередньої реалізації суб'єктивних юридичних прав і обов'язків; 2) ті, що діють протягом усього регулювання - суб'єкти, що здійснюють правове регулювання чи правову діяльність; правова законність, правосвідомість, правова культура, 3) ті, що мають факультативний характер - інтерпретаційно-правові

акти, акти застосування норм права [428, с. 115]. Онищенко і Зайчук вважають, що сучасна юридична наука характеризується наявністю двох підходів до визначення елементів механізму правового регулювання [456, с.123]. Перший, широкий підхід, передбачає наявність сукупності елементів, які беруть участь у процесі впорядкування суспільних відносин, а саме: норми права,; нормативно-правового акту; юридичних фактів; правовідносин; тлумачення і реалізація права; законність; правосвідомість і правову культуру; правову поведінку та юридична відповідальність.

Досліджуючи проблеми правового регулювання у сфері інформаційної безпеки людини під таким кутом, поруч з категорією правова культура необхідно звернути увагу на інформаційну культуру, яка втілюється в культурі формування інформаційних потреб, впровадження і використання інформаційних технологій, удосконалення інформаційної діяльності, відповідних правовідносин тощо і є чинником інформаційної цивілізації. Беляков К.І., Шопіна І.М. і Онопрієнко С.Г., досліджуючи феномен інформаційної культури, зазначають, що істотні інформаційно-глобалістичні перетворення в соціумі зумовлюють постійний розвиток і видозміну форм суспільної комунікації, виникнення новітніх суспільних відносин, що не може не позначитися на правовій системі, а отже, на правосвідомості і правовій культурі, правовому вимірі в цілому [45, с. 68]. Вони визначають перелік основних нових загроз, зокрема правового характеру, подолання яких є одним із пріоритетів держави і суспільства на шляху подальшого розвитку. По-перше, це нові деформації правосвідомості. Уявний "віртуальний світ" негативно впливає, передусім, на молодь, свідомість якої перебуває на стадії формування, зменшуючи потреби і здатності людини в реальних соціальних контактах. Це негативно позначається на правовій активності та викликає проблеми соціалізації. По-друге, швидкість розвитку інформаційних відносин значно перевищують темпи правового розвитку, що зумовлює певне відставання наявних правових механізмів від реальних соціальних потреб у правовому впорядкуванні інформаційної сфери. По-третє, інформаційні технології стали новим простором і знаряддям для вчинення правопорушень. Зокрема, як приклад, вони наводять саме технології негативного

інформаційного впливу на свідомість людини. Швидкість, анонімність, латентність, транскордонність таких правопорушень вимагають суттєвого удосконалення національного законодавства, діяльності судової і правоохоронної систем, а також запровадження додаткових напрямів освіти, спеціальної підготовки і перепідготовки представників юридичної професії з метою формування відповідного рівня інформаційної культури. По-четверте, глобалізація розмиває соціокультурні межі суспільств різних країн. Відбувається інтеграція правових систем, вироблення універсальних правових форм і процедур, глобальних важелів управління. Надмірна уніфікація правового життя світового суспільства може спричинити втрату ідентичності національних правових систем, інформаційного суверенітету та їхнього культурного розмаїття, що також є глобальною загрозою [45, с.72].

Не відкидаючи цінність широкого підходу, який дозволяє розглядати механізм правового регулювання в єдності з важливими елементами правової дійсності – правовою культурою та правосвідомістю, все ж автор більш схильний до другого, вузького, підходу, який включає лише елементи, які складають основу регулятивної функції права, наприклад в [456, с.142]. Серед них виділяють: норми права і принципи права, об'єктивовані в законах та підзаконних нормативно-правових актах, акти тлумачення права (інтерпретаційні акти), акти застосування норм права (правозастосовчі акти), правовідносини, суб'єктивні права та юридичні обов'язки суб'єктів правовідносин. Кожен з елементів даної системи виконує специфічну функцію у задоволенні інтересів суб'єктів, в регулюванні суспільних відносин, у досягненні ефективності правового регулювання.

Норма права є основою механізму правового регулювання. Вона встановлює можливий варіант поведінки (активної чи пасивної), визначає суб'єктивні права та можливості реалізувати охоронюваний законом інтерес, так і необхідний варіант поведінки – юридичні обов'язки. Завдання норми права в механізмі правового регулювання полягає в тому, щоб: а) визначити загальне коло учасників правовідносин (взагалі, у конкретних правовідносинах зокрема); б) встановити зміст суспільних відносин (зміст поведінки суб'єкта), а також об'єкти правовідносин; в) визначити гіпотезу чи обставини, за яких слід керуватися даним



правилом поведінки; г) розкрити саме правило поведінки (диспозиція) вказівкою на права і обов'язки (зміст) учасників відносин, що регулюються, характер їх зв'язку між собою, а також державно-примусові заході, що можуть бути застосовані при невиконанні юридичних обов'язків [516, с. 300].

Якість правового регулювання значною мірою залежить від того, наскільки норми права враховують закономірності суспільних відносин, що регулюються, а також від рівня правової культури як законотворців зокрема, так і суспільства в цілому. Тому, правове регулювання відносин, що виникають з зв'язку інформаційною безпекою людини є можливим і ефективним лише у випадку розуміння як першими, так і другими інформаційної безпеки людини як необхідної умови її існування і розвитку в інформаційному суспільстві.

Нормам інформаційного права властиві як загальні ознаки - державно-владна природа, загальнообов'язковість, формальна визначеність і структурованість, так і специфічні ознаки, обумовлені насамперед комплексним характером цієї галузі законодавства. До таких специфічних ознак Ковленко Л.П. віднесла: вираження державного інтересу; переважно імперативний характер, їх реалізація підкріплюється можливістю застосування засобів державного примусу; є регулятором інформаційних відносин; пов'язані з реалізацією інформаційних прав і свобод; наявність специфічних способів реалізації інформаційних норм [198, с.86].

Слід зазначити, що норми інформаційного права на сьогодні є розпорошені в великій кількості нормативних актів, що суттєво знижує ефективність правового регулювання всієї інформаційної сфери. Тому підтримуємо позицію багатьох вчених (Белякова К.І., Баранова О.А., Цимбалюка К.І., Пилипчука В.Г. та інших), які вже понад 10 років звертають увагу на необхідність систематизації норм у цій сфері шляхом прийняття Інформаційного кодексу. Так, абсолютно переконливою вважаємо позицію Баранова О.А., що систематизація норм інформаційного права повинна забезпечити: створення єдиної і не суперечливої системи класифікації норм і нормативно-правових актів; стабілізацію інформаційного законодавства; внутрішню єдність інформаційного права та інформаційного законодавства за рахунок групування правових норм згідно з прийнятим алгоритмом; аналіз

поточного стану інформаційного законодавства та усунення наявних прогалин і суперечностей; виключення дублюючих правових норм; єдине використання основних термінів; ефективність пошуку необхідних правових норм; підвищення ефективності правотворчої та правозастосовної діяльності у галузі інформаційного права тощо [24, с.201].

Також підтримуємо позицію вченого, що офіційна структура інформаційного законодавства в державі не відповідає структурі інформаційного права, що є однією із причин його нерозвиненості та недосконалості, а також відставання від вимог сучасності в частині розвитку інформаційного суспільства [24, с.202]. Окрім того, така невідповідність негативно впливає на нормотворчу та правозастосовну діяльність, оскільки аналіз і тлумачення несистемних і часто суперечливих норм вимагає глибокого розуміння правової природи інформаційних відносин, що не завжди має місце на практиці.

Нормативно-правові акти обслуговують нормативну основу механізму правового регулювання. До нормативно-правових актів (законів, підзаконних актів) приєднуються акти, в яких дається їх офіційне роз'яснення, тлумачення. Вони не містять нових правових положень, лише є засобом, який забезпечує однакове розуміння і застосування чинних нормативних актів. Чіткість і ефективність механізму правового регулювання залежать від правильного тлумачення норм права. В Україні основним видом інтерпретаційних актів є акти Конституційного Суду України. А.О. Селіванов та А.А. Стрижак зазначають, що Конституційний Суд України дає офіційне тлумачення Конституції України і порівнюваних з нею законів, інших нормативних правових актів, їх окремих положень, що містить певну нормативність; Конституційний Суд України визначає їх відповідність або невідповідність Основному Закону країни, що є спірним стосовно їх нормативності; рішення Конституційного Суду України є підставою для приведення актів (норм) законодавства (у тому числі трудового) у відповідність з Конституцією України для вдосконалення права [415, с. 113].

Відповідно, рішення та висновки Конституційного Суду забезпечують реалізацію принципу законності та верховенства права, а також є важливим важелем розвитку інформаційного законодавства. Слід відзначити, значну

кількість Рішень Конституційного Суду України, які стосуються теми дослідження, зокрема Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (щодо медичної інформації)), Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України (щодо конфіденційної інформації) та інші.

Водночас, слушно зауважують В.Я. Тацій і Ю.М. Тодика на тому, що помилкові рішення Конституційний Суд України може приймати і під тиском політичних обставин, політичної та іншої кон'юнктури тощо. З'являються нові чинники, які необхідно враховувати, щоб правова позиція єдиного органу конституційної юрисдикції не ставала дестабілізуючим фактором [454, с. 63]. Так, суттєвої критики зі сторони правозахисників зазнало Рішення Конституційного Суду від 20.01.2012 щодо офіційного тлумачення конфіденційної інформації, коли Конституційний Суд України встановив, що збирання, зберігання, використання і поширення конфіденційної інформації про особу без її згоди є втручанням в особисте життя і допускається винятково у випадках, визначених законом, і тільки в інтересах національної безпеки, економічного добробуту і прав людини. Хоча досі Конституційний Суд послідовно демонстрував позицію захисту особистого життя людини, але прийняття такого рішення було спрямовано на захист вищих посадових осіб, а не пересічних громадян.

Тим не менш, діяльність Конституційного Суду України, його рішення забезпечують вищу юридичну силу Конституції України, зміцнюють правопорядок і законність у країні, що визначає нормативність для правозастосування; рішення Конституційного Суду України належать до сфери конституційного права; водночас його висновки про оцінку конституційності актів (норм) законодавства, правові позиції, що стосуються регулювання суспільних відносин, тісно пов'язані з правом; вони не належать до нього безпосередньо, є джерелом удосконалення і розвитку галузей права [415, с. 212].

Важливо, що згідно ст.46 Конвенції про захист прав людини і основоположних свобод та ст.2 Закону України «Про виконання рішень та застосування практики Європейського суду з прав людини» передбачено обов'язковість виконання рішень Європейського суду з прав людини, що на жаль не робить їх джерелами законодавства, як в більшості європейських держав, де вони є актами прямої дії.

Таким чином, на законодавчому рівні закріплено статус рішень Європейського суду з прав людини як джерела права, але керуватись цими рішеннями при розгляді справ чи ні, вирішують саме національні суди. І, на жаль, аналіз правозастосування і постійне зростання кількості звернень від громадян України, що були задовільнені ЄСПЛ, свідчать про небажання керуватися судовою практикою Європейського суду при розгляді справ і, як наслідок, запобігати подальшим аналогічним порушенням на стадії використання національних засобів правового захисту прав людини.

Наступним необхідним елементом механізму правового регулювання є правовідносини, які індивідуалізують положення відповідної правової норми, конкретизують суб'єктивні юридичні права і обов'язки певних суб'єктів, їх повноваження і юридичну відповідальність.

Питання інформаційних правовідносин досліджувались в працях Баранова О.А., Белєвцевої В.В., Белякова К.І., Брижка В.М., Кормича Б.А., Кохановської О.В., Маріц Д.О., Марущака А.І., Коваленко Л.П., Цимбалюка В.С., та інших. Проте, незважаючи на значний науковий інтерес, відсутній єдиний загальноприйнятий підхід до їх природи і структури. В інформаційній концепції права мається на увазі інформаційна складова будь-яких правовідносин. Проте, переважна більшість науковців визначають інформаційні правовідносини відштовхуючись від права на інформацію, тобто процесів створення, поширення, зберігання, використання та знищення інформації. Особливості прав, обов'язків, повноважень і відповідальності значною мірою обумовлені від регулюючого впливу норм права, у результаті якого складаються різні види правовідносин.

Отже, правовідносини в механізмі правового регулювання утворюють певну систему і таким чином забезпечують переведення загальних розпоряджень норм

права в суб'єктивні юридичні права і суб'єктивні юридичні обов'язки, повноваження і юридичну відповідальність для конкретних осіб, дозволяють досягти виконання їх волі, задоволення інтересів.

Особливої уваги, на нашу думку, заслуговує позиція Баранова О.А., який описуючи інформаційні відносини, звертає увагу на їх зв'язок із: «особливостями життєвого циклу існування (функціонування) суб'єктів інформаційної інфраструктури як юридичних осіб; наданням інформаційних послуг і виконанням інформаційних робіт у процесі створення, поширення (передачі), зберігання, використання та знищення (утилізації) інформації; виробництвом і використанням інформаційних технологій і ресурсів, зокрема із використанням обмежених ресурсів; забезпеченням інформаційної безпеки» [24, с.65]. На основі ґрунтовного аналізу вчений дає наступне визначення інформаційних правовідносин - «суспільні відносини, що регулюються нормами інформаційного права і виникають у процесі обороту інформації, тобто в процесі її створення, поширення (передачі), зберігання, використання та знищення (утилізації), а також у процесі забезпечення обороту інформації між суб'єктами, які мають суб'єктивні права та юридичні обов'язки, що реалізуються методами правого регулювання приватного і публічного права».

В механізмі правового регулювання правовідносини виконують наступні функції: окреслюють коло осіб, на яких поширюється дія норми права; закріплюють можливу або необхідну поведінку учасників правовідносин; обумовлюють можливість реалізації спеціальних юридичних засобів з метою забезпечення суб'єктивних прав, обов'язків, відповідальності.

Основу правовідносин становить правосуб'єктність, яка складається з правоздатності та дієздатності. Як нами вже зазначалось, формування інформаційного суспільства обумовило не лише значення існуючих і появу нових інформаційних прав людини, а й змінило змістовне наповнення усіх прав і свобод людини, а також її обов'язків, в напрямку формування інформаційної складової кожного з них. Таким чином, актуалізація інформаційних правовідносин обумовлює формування інформаційної правосуб'єктності людини та інформаційно-правового статусу як нового галузевого правового статусу людини.

Наступним важливим елементом механізму правового регулювання є акти безпосередньої реалізації прав і обов'язків, які можуть відбуватись в два способи: активний - вчинення дій, що дозволяються (наприклад, використання права на доступ до публічної інформації); пасивний - утримування від заборонених дій (наприклад, нерозголошення інформації з обмеженим доступом).

Використання правових норм передбачає реалізацію прав і свобод шляхом виконання активних дій. І в умовах становлення інформаційного суспільства актуалізації великої кількості інформаційних загроз саме використання інформаційних правових норм є бажаною поведінкою суб'єктів інформаційної безпеки. Адже стрімкий і багатовекторний розвиток інформаційного середовища відбувається значно швидшими темпами ніж розвиток інформаційного законодавства, отже встановлення обов'язкової моделі поведінки. В той же час, свідома і проактивна позиція людини, що базується на використанні наданих законом можливостей дозволяє їй самостійно уникати небезпек.

Реалізація обов'язків активними діями свідчить про виконання правових норм. Насамперед, це є очікувана поведінка від органів публічної влади. Адже саме вони уповноважені розробляти та реалізовувати заходи щодо попередження, нейтралізації та усунення реальних та потенційних загроз інформаційній безпеці людини.

Утримуванні від вчинення дій, що забороні, свідчить про додержання норм права. Тобто, норми, що встановлюють адміністративну чи кримінальну відповідальність за розголошення інформації з обмеженим доступом, наприклад, реалізуються тоді, коли особа не вчиняє протиправних дій.

Отже, акти безпосередньої реалізації у формах використання наданих нормами права можливостей, виконання зобов'язуючого правового розпорядження, додержання правових заборон фактично є кінцевою метою механізму правового регулювання.

У процесі правового регулювання стадія застосування норм права є факультативною і полягає у виданні державно-владного акта. Якщо суб'єкти права не є спроможні самостійно реалізувати суб'єктивні права і юридичні обов'язки, держава в особі компетентних органів здійснює застосування норм

права (наприклад, блокування доступу до інформаційних ресурсів, винесення обов'язкових приписів, здійснення правосуддя).

Акти застосування норм права мають форму рішень, розпоряджень, наказів, вироків тощо. У них персоніфікуються загальні права і обов'язки, а також, за необхідністю, індивідуалізуються санкції. Специфікою акта застосування норм права є можливість його примусового виконання.

Акти застосування норм права у механізмі правового регулювання використовуються в таких випадках: коли самі норми права передбачають, що індивідуалізація прав і обов'язків здійснюється органами держави, посадовими особами, а не учасниками відноси; коли суб'єкти відносин, що регулюються, поведуться протиправно: порушують права, не виконують обов'язки. У цьому разі актом застосування норм права індивідуалізується юридична відповідальність, передбачена нормами права за їх порушення, тобто встановлюється персональна відповідальність правопорушників.

У досліджуваній сфері здебільшого має місце другий випадок. Розглянемо, наприклад, акти застосування, що видає Уповноважений Верховної Ради з прав людини у випадках порушення інформаційних прав людини. Свою щорічну доповідь про стан дотримання прав людини та основоположних свобод у 2016 р. відкривали 3 теми, які є визначальними при реалізації європейського вектора розвитку країни, – доступ до публічної інформації, захист персональних даних, боротьба з усіма формами дискримінації.

З дня набрання чинності Закону України «Про доступ до публічної інформації» Уповноважений з прав людини здійснює парламентський контроль за дотриманням права людини на доступ до інформації. державним органом контролю за додержанням права на доступ до інформації. Так, 26.10.2014 р., тобто з дати набрання чинності окремими положеннями Закону України «Про прокуратуру» від 14.10.2014 р., уповноваженим особам Секретаріату Уповноваженого Верховної Ради України з прав людини були передані повноваження щодо складання протоколів про адміністративні правопорушення, зокрема, за порушення Закону № 2939 (ст. 212-3 Кодексу України про адміністративні правопорушення. З прийняттям вказаного Закону України «Про

прокуратуру» до сфери повноважень працівників Секретаріату було передано не тільки складення протоколів про адміністративне правопорушення у сфері доступу до публічної інформації. Відповідно до п. 8-1 ст. 255 КУпАП уповноважені особи Секретаріату Уповноваженого з прав людини набули повноважень складати протоколи щодо адміністративних правопорушень, передбачених статтею 212-3 (крім порушень права на інформацію відповідно до Закону України «Про адвокатуру та адвокатську діяльність»). Станом на 26.10.2014 р. стаття 212-3 КУпАП, крім порушень права на інформацію відповідно до Закону України «Про адвокатуру та адвокатську діяльність», передбачала такі правопорушення: неоприлюднення інформації, обов'язкове оприлюднення якої передбачено законами України «Про доступ до публічної інформації» та «Про засади запобігання і протидії корупції»; порушення Закону України «Про доступ до публічної інформації», а саме: необґрунтоване віднесення інформації до інформації з обмеженим доступом, ненадання відповіді на запит на інформацію, ненадання інформації, неправомірна відмова в наданні інформації, несвоєчасне або неповне надання інформації, надання недостовірної інформації; обмеження доступу до інформації або віднесення інформації до інформації з обмеженим доступом, якщо це прямо заборонено законом; ненадання доступу до судового рішення або матеріалів справи за заявою особи, а також інше порушення «Про доступ до публічної інформації»; незаконна відмова у прийнятті та розгляді звернення, інше порушення «Про звернення громадян»; повторне протягом р. вчинення будь-якого з порушень, передбачених чч. 1-6 цієї статті, за яке особу вже було піддано адміністративному стягненню [320]. Протягом 2015 р. перелік адміністративних правопорушень, які передбачені цією статтею та за якими складають адміністративні протоколи виключно уповноважені працівники Секретаріату Уповноваженого з прав людини, значно розширено. Відтак, повноваження було збільшено щодо нових трьох видів адміністративних правопорушень: неоприлюднення інформації, обов'язкове оприлюднення якої передбачено Законами України «Про особливості доступу до інформації у сферах постачання електричної енергії, природного газу, теплопостачання, централізованого постачання гарячої води, централізованого питного



водопостачання та водовідведення"; "Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917-1991 рр.", "Про відкритість використання публічних коштів"; "Про відкритість використання публічних коштів". А також сім нових адміністративних правопорушень у сфері порушення вимог Закону України "Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917-1991 рр.": необґрунтоване віднесення інформації до інформації з обмеженим доступом; ненадання відповіді на запит на інформацію; ненадання інформації, неправомірна відмова у наданні інформації; неповне надання інформації; неповідомлення про подовження строку розгляду запиту; відстрочення розгляду запиту, крім випадків, визначених законом [320].

Таке передання повноважень мало на меті підсилити ефективність парламентського контролю за дотриманням права на доступ до публічної інформації, забезпечення належної практики застосування Закону № 2939 та запобігання порушенням у цій сфері. Однак його без забезпечення належного ресурсу для виконання цих функцій, реалізація покладених повноважень не є можливою.

Подібною є ситуація у сфері захисту персональних даних, контрольні функції щодо яких було передано у тому ж 2014 р. Уповноваженому Верховної Ради України з прав людини. При цьому поклавши функції, чинним законодавством не передбачено достатній обсяг повноважень для їх виконання.

Завершення правового регулювання відбувається через безпосередню або опосередковану реалізацію прав і обов'язків учасниками правовідносин. Таким чином, положення юридичних норм втілюються у фактичній реальній поведінці учасників суспільних відносин, на які було спрямовано правове регулювання.

Ще одним важливим елементом механізму правового регулювання є метод. У теорії правового регулювання прийнято виділяти два методи правового впливу:

- метод децентралізованого регулювання, побудований на координації цілей і інтересів у суспільних відносинах і який застосовується у сфері галузей приватно-правового характеру;

- метод централізованого, імперативного регулювання, що базується на відносинах субординації між учасниками суспільних відносин і що використовується у публічно - правових галузях.

Метод інформаційного права, як нової комплексної галузі права, є питанням, що інтенсивно досліджується. Аналізуючи методи інформаційного права, Баранов О.А. слушно зауважує, що сучасні процеси розвитку суспільства в Україні призводять до того, що зміст конкретних суспільних відносин, які вимагають правового врегулювання, та правосвідомість можуть змінюватися, а в деяких аспектах навіть кардинально. З цього випливає дуже важливий висновок – методи конкретної галузі права, особливо такого, що зароджується, зокрема інформаційного права, знаходяться в діалектичному розвитку, тому можуть змінюватися як за складом, так за змістом. З врахуванням цього процес дослідження проблематики методів інформаційного права повинен носити постійний характер [29, с. 11].

В той же час, автори першого в Україні підручника з інформаційного права в 2004 р. визначали, що провідним методом інформаційного права метод комплексного застосування методів конституційного, адміністративного, цивільного, трудового та кримінального права [294].

Коваленко Л.П. під методом інформаційного права пропонувала розуміти сукупність зафіксованих у нормах цієї галузі прийомів (засобів) впливу на суспільні відносини, що складають її предмет, застосування яких дозволяє створити належні умови для реалізації і захисту прав громадян, в інформаційній сфері нормального функціонування інформаційного суспільства [198, с. 85].

Правове регулювання відносин у сфері інформаційна безпеки здавана здійснювалось переважно імперативними публічно-правовими методами. Проте, розвиток інформаційної сфери і набуття інформацією ознак товару у вигляді інформаційного продукту, з однієї сторони, а також становлення інформаційних прав людини і їх реалізація як особистих немайнових прав людини, з іншої, обумовили також використання цивільно-правового методу.

Окрім того, єдиний механізм правового регулювання згідно стадіям правового регулювання підрозділяється на три компоненти: механізм

правотворчості, механізм реалізації норм права і механізм державного примусу. Кожен механізм діє на своїй стадії правового регулювання - правотворчості, правореалізації і застосуванні юридичної відповідальності – і характеризується специфічними, тільки йому властивими правовими засобами.

Кожен спосіб правового регулювання реалізуються через суб'єктивні права. Суб'єктивне право утворює зміст дозволеного. При зобов'язувані та забороні – іншим особам передається право вимоги, що спрямовано на виконання активного або пасивного юридичного обов'язку. З цим, насамперед, пов'язана проблематичність закріплення права людини на безпечне інформаційне середовище. Адже його реалізація буде реальною лише за наявності обов'язків в інших суб'єктів задовольняти потреби, що виникли у цьому зв'язку в уповноваженого суб'єкта. А визначення таких кореспондуючих обов'язків і коло суб'єктів, що взаємодіють в інформаційному середовищі в умовах глобалізації, вбачається неможливим.

Отже, розуміння механізму правового регулювання суспільних відносин, що виникають у зв'язку з інформаційною безпекою людини, дозволяє: узагальнити явища правової дійсності, що спрямовані на досягнення мети правового регулювання – правопорядку і законності; виявити специфічні функції, що виконують юридичні явища в правовій системі, показати їхній зв'язок між собою і взаємодію; визначити ефективність їх взаємодії, виявити прогалини та окреслити можливі шляхи їх усунення.

Механізм правового регулювання є динамічною частиною правової системи суспільства, оскільки його результативність обумовлена ефективністю взаємодії всіх компонентів. Але вивчення його структури на рівні складових не є неповним. Тому, щоб оцінити спроможність механізму правового регулювання варто розглядати його компоненти у взаємозв'язку і взаємодії. Проте, це вимагає більш ґрунтового дослідження, тому визначається нами як перспективний напрямок досліджень.

### **5.3. Актуальні напрями вдосконалення правових основ інформаційної безпеки людини**

Вироблення правових основ інформаційної безпеки людини вимагає переосмислення підходів до низки напрямів правового регулювання і державної політики. Зокрема, в умовах інтернаціоналізації всіх сфер суспільного життя розвиток законодавства не може відбуватись без врахування глобалізаційних процесів. При цьому, законотворчі органи окремих держав вимушені враховувати стандарти міжнародного права, а також тенденції до зближення правових систем. Як правило, такі інтеграційні процеси обумовлені геополітичним становищем держави, економічними чинниками, історичними передумовами, а також національною правовою культурою і традиціями державотворення.

Гармонізація і уніфікація відбувається за двома напрямками. По перше, шляхом творення міжнародних актів, укладання міждержавних договорів, а також нормотворчої діяльності міжнародних організацій, які визначають пріоритети, орієнтири, а часом і рамки для розвитку національного законодавства у визначених сферах. Другий напрям стосується національного нормотворення, коли держави самостійно сприймають і закріплюють в національному законодавстві досвід правового регулювання інших держав чи міжнародно-правові тенденції.

Інформаційна безпека, як сфера правового регулювання, апріорі не може розвиватись без врахування міжнародного правового поля та досвіду зарубіжних країн. Це обумовлено самою істотою інформаційної сфери, яку складно обмежити національними кордонами в демократичній державі.

При цьому важливо, що правове регулювання має відповідати не лише обраному політичному курсу, а й базуватись на існуючій суспільній практиці, відповідати нагальним інтересам громадян і запитам суспільства. Становлення правового забезпечення інформаційної безпеки людини відбувається в конкретних історичних умовах та невіддільне від правового статусу людини в державі, ступеня розвитку демократичних процесів та правової культури суспільства.

Інформаційна безпека в системі міжнародної безпеки пройшла різні етапи становлення. В другій половині XX сторіччя міжнародні домовленості здебільшого стосувались забезпечення існування та розвиток інформаційного середовища бізнесу. На межі тисячоліть відбулися значні трансформаційні процеси в геополітиці і внаслідок подвійної трансгранично-національної природи кіберпростору [128,с.28] національна політика держав щодо інформаційної безпеки стає значимою у вимірі зовнішньої політики, оскільки пов'язана з розбудовою інфраструктури. Дубов Д.В. наводить як приклад, що цілком внутрішні питання освітньої сфери (наприклад, щодо підготовки фахівців ІТ-сфери) робить це питання частиною зовнішньої політики держави [128, с.29]. Тим більше значимим в міжнародному аспекті є правове забезпечення інформаційного простору держави, інформаційних прав і свобод людини, режимів доступу до інформації, зокрема в глобальній мережі, гарантування принципу міжнародного нейтралітету, електронної демократії та інші.

І, очевидним є, що опрацювання міжнародних домовленостей в сфері інформаційної безпеки в цілому, і людини зокрема, значною мірою залежить від політичної волі держав, які мають та/чи змагаються за визначальний геополітичний вплив. На сьогодні, до таких держав, насамперед, належать США, Російська Федерація, КНР та ЄС.

На сьогодні у світі сформувалось два основних підходи щодо змісту міжнародної інформаційної безпеки. Перша група країн демонструє підхід до проблематики міжнародної інформаційної безпеки в широкому розумінні, в основу якої мають бути покладені принципи неподільності безпеки та відповідальності держав за свій інформаційний простір. Друга група країн звужує питання міжнародної інформаційної безпеки до міжнародної кібербезпеки і такий підхід зосереджується на боротьбі із злочинами у сфері інформаційно-комунікаційних технологій, в т.ч. боротьбу із кібертероризмом. Як наслідок, при цих підходах простежується різне розуміння місця інформаційної безпеки людини в складній системі інформаційної безпеки як на міжнародному, так і на національному рівнях. Перший підхід, на нашу думку, передбачає узаконення значного простору для обмеження інформаційних прав і свобод людини на

користь гарантування інформаційного безпеки міжнародної спільноти і окремих держав. При цьому, прихильниками такого розвитку міжнародної політики виступають здебільшого держави, що мають значні проблеми щодо реалізації конституційних засад демократії, або ж взагалі не визнають демократичних цінностей.

Другий підхід визначається значно більшим соціальним і економічним спрямуванням, передбачає встановлення міжнародних стандартів для інформаційних прав та свобод людини (особливо пов'язаних з використанням мережі) на достатньо високому рівні. При цьому не передбачає втручання в питання інформаційного суверенітету, ведення інформаційних воєн та деякі інші аспекти політичної і військової сфери.

Безперечною вбачається цінність напрацювання міжнародних стандартів як орієнтирів для підвищення рівня захисту прав і свобод людини в інформаційній сфері. Водночас, як свідчить аналіз становлення інституту прав людини у складі міжнародного права, їх значення здебільшого є прогностичним і полягає у виконанні таких функцій як: визначають перелік прав та свобод, які відносяться до категорії основних та обов'язкових для всіх держав-учасниць відповідних міжнародних угод або конвенцій; формулюють головні риси змісту прав та свобод, які повинні втілюватись у відповідних конституційних та інших нормативних положеннях окремих держав; встановлюють зобов'язання держав щодо визнання та забезпечення проголошених прав та свобод, а також встановлення на міжнародному рівні гарантій, необхідних для реалізації і захисту прав та свобод; фіксують умови щодо застосування прав та свобод людини, одночасно із законними обмеженнями цих прав та свобод [256, с.359].

Проте, інформація та інформаційні технології у сучасному світі є одночасно і основним ресурсом, поруч з енергією і матерією, водночас є джерелом загроз, що вимагає інших підходів до етичної оцінки та правового регулювання питань, пов'язаних з технологіями. Тому стандарти прав і свобод людини в інформаційному суспільстві визначається не лише особливостями національного співтовариства людей, а й розвитком людської цивілізації в цілому, рівнем

інтегрованості міжнародного співтовариства, а також з огляду на реальні та потенційні загрози інформаційній безпеці.

Для прикладу, 1 жовтня 2017 р. набув чинності Закон про захист мереж, який раніше називався "Законом про Facebook", нормами якого передбачено обов'язок соціально-медійних компаній в Німеччині вилучати підроблені новини або повідомлення, що містять мову ненависті протягом 24 годин. Насамперед, це стосуватиметься Facebook, Twitter, YouTube та інших сайтів з більш ніж 2 мільйонами користувачів у Німеччині. Покарання застосовуватимуться лише у межах Німеччини, але міністр юстиції Німеччини Хайко Маас, ініціатор закону, заявив, що буде наполягати на подібних заходах у всьому Європейському Союзі [584].

Подібні ініціативи вже довгий час обговорюються в ЄС, і зустрічають як підтримку, з огляду на значну кількість дипломатичних, викликаних фейковими новинами, так і критику захисників вільного мовлення. В Україні відсутнє ефективне правове регулювання питань як щодо мови ворожнечі (ненависті), так і з питань дезінформації. При цьому, в умовах постійного інформаційного протистояння, вважаємо, що це одне з першочергових питань, що мало би вирішуватись як на рівні законодавства, так і шляхом відповідних організаційних заходів, які б дозволили не лише зменшити деструктивний вплив дезінформації і мови ненависті на населення, а й відновити порушені права осіб чи навіть соціальних груп.

Важливо зауважити, що рішення ЄСПЛ на сьогодні не визнаються в Україні джерелами законодавства, що не виключає можливість їх використання як джерел права. Отже, на нашу думку, врахування аналізу практики ЄСПЛ щодо справ, для вдосконалення національного законодавства в напрямку зближення до міжнародних стандартів, а також усунування недоліків національного законодавства, які спричинили порушення, що стали предметом розгляду.

Як свідчить досвід країн з розвинутою демократією, інформаційна безпека людини не повинна протиставлятися інформаційній безпеці держави та суспільства. Адже саме людина визнається основною цінністю кожного суспільства і забезпечення її прав і свобод є кінцевою метою реалізації функцій

держави. Проте, реалії інформаційного суспільства обумовлюють необхідність обмеження прав та законних інтересів людини з метою захисту національних інтересів держав, попередження міжнародних конфліктів чи/та терористичних актів, а також забезпечення безпеки національних інформаційних ресурсів. Таким чином, має місце конфлікт інтересів різних об'єктів інформаційної безпеки. Вирішення цього конфлікту демократичним шляхом є однією з первинних задач при створенні відповідних правових норм. Тому, нагальною потребою вбачаємо необхідність розробки і прийняття базового закону для досліджуваної сфери - «Про інформаційну безпеку», в основу якого може бути покладено запропоновані нами в попередньому підрозділі принципи, а також досвід іноземних держав.

Як бачимо, підходи США і ЄС до вирішення цього питання суттєво відрізняються. Про це свідчить як аналіз законодавства, так і правозастосування. США декларує високі стандарти прав і свобод людини в інформаційній сфері, але при виникненні протиріч між гарантуванням дотримання цих стандартів і інтересами національної безпеки перевага віддається саме інформаційній безпеці держави.

Країни ЄС, в свою чергу, демонструють більш послідовну політику щодо гарантування і дотримання прав і свобод людини в інформаційній сфері. Про це свідчать, зокрема, останні зміни в законодавстві щодо захисту персональних даних. Окрім того, політика ЄС у інформаційній сфері характеризується узгодженістю і забезпечується дієвими механізмами реалізації.

Значну роль нормотворчості відграють міжнародні судові органи, зокрема, суд ЄС та ЄСПЛ, які шляхом правозастосування конкретизують розуміння змісту правових норм на основі суспільної практики, а часом і формують нове розуміння з огляду на зміни, що відбуваються в суспільстві. Зокрема, про це свідчить аналіз рішень у справах ЄСПЛ щодо права на доступ до інформації, який відображає зміну розуміння цього права, а також його співвідношення з іншими інформаційними правами, зокрема правом на захист персональних даних, свободою вираження поглядів тощо.

Україна, обравши шлях євроінтеграції і підписавши угоду про асоціацію з ЄС взяла на себе зобов'язання щодо адаптації законодавства з відповідними нормами



ЄС. Відповідно, значні зусилля спрямовуються власне на приведення у відповідність вже існуючого законодавства. Проте самих змін в законах не достатньо. Правове регулювання має відображати бажані соціальні зміни і їх стимулювати.

Великим викликом для українського суспільства є нерозуміння доцільності окремих змін в правовому регулюванні інформаційної сфери. Для прикладу, спостерігається брак підтримки з боку державних органів та органів місцевого самоврядування оприлюднення публічної інформації у вигляді відкритих даних. В свідомості багатьох чиновників все ще має місце «радянське» мислення - інформація належить державі, в особі її уповноважених органів. В демократичному ж суспільстві інформація накопичена публічними органами є власністю громадянського суспільства, яке вільне використовувати її на власний розсуд (або не використовувати). Про це також говориться в Рекомендації ЮНЕСКО з використання та розвитку багатомовності та загального доступу до всесвітнього електронного простору, де надане визначення інформації, що є суспільним надбанням: «Інформацією, що є суспільним надбанням, вважається доступна для населення інформація, використання якої не порушує жодних передбачених законом прав або зобов'язань щодо дотримання конфіденційності». Одним з пріоритетів демократичного суспільства є надання права всім членам на доступ до інформації і знань і на їх використання на виконання однієї з основних громадянських свобод - свободи вираження та свободи участі у культурному житті і науковому прогресі. Для досягнення цієї мети державними органами створюється значні обсяги інформації, істотна частина якої має бути відкритою для вільного розповсюдження через інтернет, бібліотеки та інші пункти публічного доступу, а також за допомогою таких інструментів розвитку суспільства, як бізнес і освіта. Оскільки законодавство і політика більшості країн в основному орієнтовані саме на захист інформації, на яку поширюються права власності, роль і значимість інформації, що є суспільним надбанням, особливо інформації, створюваної державними установами, часто недооцінюється.

В Керівних принципах ЮНЕСКО в політиці вдосконалення державної інформації [632], що є суспільним надбанням, метою було визначено сприяння

вдосконаленню інформації, що є суспільним надбанням, на урядовому рівні, причому особлива увага приділена поширенню інформації в електронному форматі.

Іноземний та міжнародний досвід свідчить, що створення самого лише правового поля в цій сфері виявляється недостатнім для досягнення мети – демократизації суспільства і забезпечення реалізації інформаційних прав громадян, проте дозволяє розширити можливості для їх використання в інтересах людини і суспільства. Так, у Сполученому Королівстві відкриті дані є не лише відповіддю на суспільний запит, але при ефективному використанні приносять 2-5% ВВП. В Великобританії понад 70% комерційних організацій користується відкритими даними. При цьому доступні і належним чином викладені відкриті дані є сигналом для потенційних інвесторів. Держава не спроможна самотійно розбудовувати сервіси на основі цих масивів інформації, якими володіє. Створення належної правової бази означає вирішення таких питань – визначання процедури розкриття даних, яка б не залежала від бажання посадових осіб розпорядників інформації, забезпечення належної форми оприлюднення таких даних, визначення механізмів захисту прав на доступ до таких даних.

Закон про доступ публічної інформації містить окремі положення щодо відкритих даних, проте ним не передбачено шляхів забезпечення виконання цих положень і органів, що мали би здійснювати відповідний нагляд. Що стосується відкритих даних, що не належать державі, то їх системне правове регулювання відсутнє. Відсутнє на рівні законодавства і визначення відкритих даних, порядок надання такого статусу і його зміст. На нашу думку, має бути закріплено на нормативно-правовому рівні, що інформація (дані) є відкритою, якщо будь-хто має до нього вільний доступ, може вільно використовувати та ділитися нею.

Ще одним важливим кроком у напрямку підвищення стандартів захисту інформаційної безпеки людини вбачається створення інституту на зразок інформаційного комісара – як незалежного органу, діяльність якого спрямована на захист прав і свобод людини в інформаційній сфері. Інституція Інформаційного комісара нині існує в Туреччині, Словаччині, Великобританії, Португалії та Словенії.

Досвід цих країн свідчить, що така незалежна інституція займається питаннями захисту прав громадян, журналістів та громадських активістів у справах з доступу до інформації, а також має набір повноважень щодо забезпечення захисту персональних даних. Створити єдиний орган інформаційного комісара, у компетенції якого була б робота з двома правами: доступ до публічної інформації та захист персональних даних, також рекомендують експерти Ради Європи. Зокрема, голова офісу Ради Європи в Україні М. Енберг назвав її «ключовою рекомендацією Ради Європи щодо аналізу та розподілу повноважень держустанов у сфері інформаційної політики та медіа в Україні» [395].

Суспільна думка та позиції політикуму щодо цього питання суттєво змінились за останні 10 років. В 2008 р. дослідження діяльності омбудсмана по здійсненню контролю за додержанням права на доступ до інформації, дозволяло стверджувати, що – Уповноважений Верховної Ради з прав людини не приділяє належної уваги цій проблемі. Зокрема, висвітлюючи в щорічних доповідях стан забезпечення в Україні інформаційних прав, уповноважений розглядав лише проблеми пов'язані зі свободою інформації та свободою ЗМІ. В доповідях не аналізувалась ситуація щодо забезпечення доступу до інформації в Україні й лише опосередковано згадувалась проблема неправомірного застосування органами виконавчої влади грифів, що не визначені жодним нормативним актом: «для службового користування», «не для друку», «опублікуванню не підлягає». У зв'язку з тим, що кількість звернень на адресу Уповноваженого з прав людини про порушення органами державної влади права громадян на доступ до інформації, становила за рік у середньому від 0,1 до 0,3 відсотка загальної кількості звернень, Уповноважений Верховної Ради з прав людини вважав не актуальним запровадження посади спеціалізованого омбудсмана з питань інформації [275].

Проте, вже в 2017 р. діючий Уповноважений Верховної Ради з прав людини, на якого покладені відповідні повноваження, провадить чітку політику підтримки створення такого незалежного інституту, зокрема на рівні законодавчих ініціатив. Під час міжнародної конференції «Відзначення 250-ї річниці права на інформацію

та подальше зміцнення всіх національних систем країн Східного партнерства», Валерія Лутковська зазначила про необхідність створення інституції Інформаційного комісара: «Ми маємо низку проблемних питань у цьому зв'язку. По-перше, рекомендації Уповноваженого з прав людини, як і в більшості країнах-членах Ради Європи, не є обов'язковими до виконання, а це в свою чергу, знижує ефективність захисту права на інформацію. По-друге, функція покарання не є притаманною для національної інституції з прав людини. Крім того, функції контролю за доступом до інформації йдуть урозріз з так званими «паризькими принципами» діяльності національної інституції з прав людини» [181].

Нами пропонується впровадження інституції Уповноваженого з інформаційної безпеки людини, для чого є необхідність внесення змін до Конституції України, а також створення правових засад діяльності такого органу, які б надавали достатню кількість інструментів впливу на правопорушників не лише з метою притягнення їх до відповідальності, а й задля відновлення порушеного права, а також запобіганню подальших незаконних обмежено реалізації інформаційних прав і свобод людини.

Оскільки не можливо надати вичерпний перелік інформаційних загроз людині, бо вони модифікуються з розвитком інформаційних технологій і самого суспільства, то необхідним вбачається надання відповідних повноважень щодо моніторингу інформаційних загроз людині і суспільству.

Прикладом може бути ситуація, що склалася з приводу прийняття Закону «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» [348]. Ще до набрання ним чинності точилася публічна дискусія щодо його суперечливого характеру і загрози правам і свободам людини. Зокрема, Українська гельсінська спілка з прав людини ще на етапі законопроекту звертала увагу на надмірно розширений перелік цілей з якими створюється реєстр, а також недоцільність в умовах сучасної України, «збирати таку низку персональних даних про особу в єдиному реєстрі, а з метою більшого забезпечення права особи на приватність, рекомендовано мати декілька реєстрів, причому з заборобою об'єднувати

інформацію з різних реєстрів без згоди особи»[440]. Окрім того, Закон не розрізняє загальні і вразливі дані.

Критиці з боку правозахисників Закон піддавався і після прийняття [137]. Певна кількість недоліків була усунена, проте все ще залишається відкритими значна кількість питань – які суб'єкти (крім самої фізичної особи, дані якої обробляються, та розпорядника Реєстру), за яких обставин, на якій підставі та за якою процедурою можуть мати доступ до інформації, яка зберігається в Реєстрі, не визначено строків зберігання та обробки інформації в Реєстрі, відсутня процедура знищення персональних даних, необхідність зберігання яких у Реєстрі більше не існує та інші.

Важливим питанням також залишається етичність впровадження єдиного незмінного реєстраційного номеру особи. Українська гельсінська спілка з прав людини ґрунтує заперечення на декількох підставах: «По-перше, заперечення морального характеру. Призначення особі незмінного реєстраційного номеру, який проставлятиметься на всіх документах принижує гідність особи, ототожнює особу з набором цифр, який отримується за допомогою невідомого алгоритму. Більше того, така практика призначення державою номера замість імені характерна для тоталітарних держав, перш за все в концтаборах. Нагадаємо, що під час Нюрнберзького процесу Міжнародний воєнний трибунал визнав практику присвоєння особам знеособлюючих номерів і клейміння осіб ними злочином проти людяності. Можна сказати, що ототожнення особи з певним кодом не лише посягає на право особи на ім'я, але й нав'язує особі відчуття власної незначущості. На жаль, історія існування Української держави свідчить про те, що цій державі громадянин майже ніколи не може беззастережно довіряти, тож невідомо з якою метою буде насправді використано зібрану інформацію. По-друге, як показало впровадження податкового ідентифікаційного коду, для низки громадян поставлення коду у відповідність імені є неприйнятним з релігійних міркувань. По-третє, запровадження єдиного реєстраційного номеру особи становить фундаментальну загрозу праву особи на приватне життя (на приватність). Це значною мірою пов'язане з відсутністю в Україні ефективної системи захисту персональних даних, а гарантії захисту персональних даних,

передбачені цим законопроектом, не можна вважати адекватними, тим більше з огляду на практику контролю приватного життя в СРСР і історичну пам'ять про це державних чиновників. Неприйнятним видається і вимога розміщення реєстраційного номеру на всіх документах Реєстру, до яких віднесено низку галузевих документів: права водія, учнівський квиток тощо. Таке положення створить умови для тотального контролю за особою і, відповідно, до порушення права особи на приватність. Крім того вважаємо за доцільне знизити кількість документів реєстру власне до ідентифікаційних документів»[440].

Питання існування реєстрів і їх взаємодії є взагалі дуже чутливим як зі сторони інформаційної безпеки людини, так і з огляду на права та свободи людини в демократичному суспільстві. Норми, що передбачають існування єдиних та державних реєстрів, а також порядок зберігання, реєстрації та надання інформації персонального характеру не завжди визначаються нормами законів. Закріплення подібних норм на підзаконному рівні суперечить п.1 ст. 92 Конституції, який передбачає, що виключно законами України визначаються «права і свободи людини і громадянина, гарантії цих прав і свобод; основні обов'язки громадянина».

А реєстри, що порядок ведення реєстрів в установах, підприємствах і організаціях, взагалі часто не відповідає нормам визначеним законом, а особи, що здійснюють ведення таких реєстрів, уявлення не мають про законодавство щодо персональних даних і поведуться з ними неналежним чином. Це призводить до порушення не лише інформаційних прав і свобод людини, а й може становити загрозу її життю і здоров'ю. Для прикладу, персональні дані, що вносяться до реєстрів в медичних установах, у тому числі інформація про стан здоров'я, належать до так званої «чутливої» інформації, тому мають бути ретельно захищені. Розголошення певних видів такої інформації, наприклад, щодо захворювання на онкологічні, неврологічні захворювання тощо, може призвести до соціальної стигматизації [65].

Величезну загрозу для безпеки фізичних осіб може бути створено у зв'язку з внесенням змін до законодавства щодо трансплантації органів та інших анатомічних матеріалів людини. В законопроекті 2386(а-1), що був прийнятий в

першому читанні 21.04.2016 передбачається створення Єдиної державної інформаційної системи трансплантації, яка буде містити інформацію щодо потенційних донорів. При цьому у законопроекті відсутні гарантії забезпечення конфіденційності такої інформації, не визначений механізм захисту та відповідальні суб'єкти забезпечення. Окрім того, відсутній правовий механізм забезпечення доступу реципієнтів до інформації про наявність донорських органів та інших анатомічних матеріалів людини.

В умовах, коли країна знаходиться фактично у стані війни, а окрім того має складну криміногенну ситуацію, розголошення персональних даних особи можуть стати підставою для зазіхань на її життя зловмисниками. Тому питання створення будь-яких реєстрів, що містять чутливу інформацію, мають чітко і однозначно регулюватись на законодавчому рівні і відразу визначати суб'єктів, що відповідальні за забезпечення захисту такої інформації та відповідальність у випадку порушення інформаційних прав людини.

В той же час, не слід залишати поза увагою, особливості національного інформаційного простору. В умовах гібридної війни, невід'ємною складовою якої є інформаційна, стоїть нагальна потреба ефективного моніторингу ситуації із дотриманням прав всіх суб'єктів інформаційних правовідносин, а також виявлення системних проблем як на рівні правового забезпечення, так і в правозастосовчій діяльності.

Інформаційна війна – це завжди атака інформаційної функції, незалежно від засобів, які застосовуються. При цьому ціллю враження є дуже широке коло суб'єктів – від пересічних громадян, членів окремих суспільних груп – етнічних, релігійних, територіальних тощо, до політичних діячів, посадових осіб, від яких залежить прийняття доленосних рішень для всієї держави.

Як вже неодноразово звертали увагу, загрози інформаційній безпеці людини значною мірою узалежнені від геополітики. Аналіз ситуації в країнах Східного партнерства, зокрема досвід Грузії, Вірменії і Молдови в сфері інформаційної безпеки людини є цінним для України з огляду на: (1) проєвропейську політичну спрямованість, а отже і спроби адаптації до законодавства і стандартів ЄС; (2) геополітичну ситуацію, що пов'язана зі значним впливом (в т.ч. інформаційним)

зі сторони Російської Федерації; (3) наявність територій, що не підконтрольні уряду, і використання конфліктів в цілях підривання суверенності державної влади; (4) нестійку політичну і економічну ситуацію в середині держави.

На пострадянському просторі сьогодні простежується виокремлення двох груп країн, що різко відрізняються принципами формування політики у інформаційній сфері. Про це свідчать також результати опитування 50 експертів ІКТ, які відображені в дослідженні «Ціна свободи і безпеки. Індекс ІКТ-законодавств Євразії за 2016 р. », виконаному DR Analytica на замовлення Digital.Report [497].

У першій групі опинилися Вірменія, Грузія і Молдова: націленість влади цих країн на збільшення свободи у всіх сферах, а також облік економічного ефекту від вжитих заходів дозволяє проводити збалансовану політику, одночасно приводить до збільшення безпеки. Так, зокрема, в Молдові прийняті в 2016 р. правові акти збільшували як свободу, так і безпеку в усіх сферах.

Друга група країн, до якої входять Білорусь, Азербайджан, Росія, Казахстан і Киргизстан, в інформаційній політиці віддає пріоритет інтересам безпеки, переважно - державної. Така політика веде до обмеження свободи інформації для особистості і суспільства. Ці країни також беруть за основу реалізовані в Росії законодавчі ініціативи, зокрема, ті закони, що пов'язані з моральною стороною інтернет-контенту, а також з інформаційною безпекою держави.

Проблемним питанням в країнах пострадянського простору залишається боротьба з кіберзлочинністю. Хоча в більшості країн ратифікована Конвенція про кіберзлочинність та прийняті відповідні закони по боротьбі з кіберзлочинністю, реалізація їх положень зачасти є малоефективною, зокрема через те, що влада не вважає кіберзлочинність реальною загрозою, якщо вона не загрожує безпосередньо їх режиму або економічним інтересам.

Для країн Східного партнерства актуальною проблемою залишається домінування Російської Федерації в інформаційному просторі. Російська Федерація довгий час домінувала в культурній, політичній та економічній сферах в Євразії, в тому числі в сфері розвитку ІКТ. Останні роки Грузія, Молдова і Україна докладають багато зусиль, щоб дистанціюватися від Росії, проте інші



держави Східного партнерства залишаються під суттєвим впливом її геополітичного впливу. Такий вплив обумовлений цілою низкою чинників – економічними зв'язками, енергетичною залежністю, значною насиченістю мережі російськомовним контентом, а також тим, що російські комунікаційні компанії відіграють помітну роль в країнах регіону.

Зокрема, російські соціальні мережі «Вконтакте», «Однокласники» і «Мой Мир» входять до п'ятірки найбільш відвідуваних соціальних мереж у багатьох державах пострадянського простору. Держави по різному реагують на цю загрозу. Від повного ігнорування (Білорусь, Казахстан, Азербайджан) до спроб створити чи посилити вплив власних альтернативних ресурсів (Вірменія, Грузія) або заборони окремих ресурсів російського виробництва (Молдова).

Україна вже має досвід щодо намагання обмежити доступ до російських інформаційних і комунікаційних ресурсів шляхом зобов'язання провайдерів зробити їх технологічно недоступними. Указ Президента від 15 травня 2017 р. № 133/2017 щодо затвердження рішення Ради національної безпеки і оборони України «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» від 28 квітня 2017 р. викликав бурхливу реакцію громадськості і поставив низку питань щодо його законності, правомірності, допустимості в демократичному суспільстві, а також результативності.

Щодо законності цього рішення слід звернутись Конституції України, де ст. 92 встановлює, що «виключно законами України визначаються: права і свободи людини і громадянина, правові засади і гарантії підприємництва, основи національної безпеки...», а ст. 107 - «Рада національної безпеки і оборони України координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони». Стаття 10 закону «Про Раду національної безпеки і оборони України» говорить: «Рішення Ради національної безпеки і оборони України, введені в дію указами Президента України, є обов'язковими до виконання органами виконавчої влади», тобто рішення РНБО не поширюються на приватних осіб і приватні компанії. Укази президента сили закону не мають. Таким чином, цей акт не може бути визнаний конституційним.

Викликають сумніви і правомірність та допустимість в демократичному суспільстві такого рішення. Хоча, Указ президента і рішення Ради національної безпеки і оборони України про введення санкцій за своєю суттю є "адресними", тобто зачіпають тільки юридичних та фізичних осіб, зазначених в цих документах, а також покладають обов'язки щодо реалізації положень рішення на деякі держоргани – Національний банк України, Кабінет міністрів та Службу безпеки України. Проте, фактично цим Указом встановлюється обов'язок провайдерів обмежити доступ до певних ресурсів, що опосередковано визначає неможливість доступу до них окремих громадян. В сучасному суспільстві доступ до інтернету та його ресурсів пов'язаний з реалізацією низки конституційних прав і свобод людини і громадянина, зокрема: прав на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31), недоторканність особистого і сімейного життя (ст. 32), свободу думки і слова, на вільне вираження своїх поглядів і переконань (ст. 34), свободу світогляду і віросповідання (ст. 35), на мирне зібрання (ст. 39), право власності, у тому числі інтелектуальної (ст. 41), на підприємницьку діяльність (ст. 42), на працю (ст. 43), на освіту (ст. 53), на свободу літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, їхніх авторських прав, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності (ст. 54).[300]

Рекомендація Комітету міністрів державам-членам Ради Європи щодо свободи в інтернеті від 13 квітня 2016 р. звертає увагу, що право на доступ до інформації є правом інструментальним, тобто необхідне для реалізації інших прав і свобод людини. А його обмеження має бути необхідним в демократичному суспільстві і пропорційним визначеній законній меті.

Наостанок, виникає питання, яку саме мету переслідували творці цього рішення. Якщо ж йшлося про виведення з українського ринку окремих інформаційних технологій російського виробництва, то ця мета досягнута майже цілком. Проте підприємці змушені були понести додаткові витрати на заміну відповідних технологій, а також у зв'язку з обмеженням доступу до відповідних

ресурсів. Викликає обґрунтовані сумніви допустимість такого розв'язання у демократичному суспільстві.

Якщо йдеться про обмеження негативного інформаційного впливу на користувачів, то ця мета частково досягнута. Проте залишається можливим використання доступу до заборонених ресурсів через VPN, а також з-за меж України. А суспільний резонанс цього рішення відрізняється від крайнє радикальної підтримки («давно пора було це зробити») до критики як змісту, так і форми реалізації рішення. При цьому, має місце також і нігілістичне ставлення, що виявляється у ігноруванні обмежень і використання технологій для їх обходу і доступу до заборонених ресурсів. Абсолютно логічною в цих умовах є позиція О. Гелетканича: «Інтернет створювався як місце свободи, тому повністю обмежити або заблокувати доступ до ресурсу фактично неможливо через саму природу мережі» [523].

Таким чином, безсистемність і відсутність єдиного концептуального підходу до правових основ інформаційної безпеки людини призвели до появи значних проблем у правозастосовній діяльності. Зокрема, єдиним легальним способом блокування інтернет-ресурсів, що здійснюють незаконну діяльність на сьогодні є судовий. В той же час, протягом останніх років мали місце неодноразові спроби внесення до національного законодавства змін, які б встановлювали нові позасудові механізми блокування інтернет-ресурсів, що суперечить свободі інформації. В той же час, чинне законодавство не визначає порядку витребування інформації (даних) від операторів мереж передачі даних, а також відповідальності за невиконання обов'язку щодо розміщення реальної інформації щодо власників інтернет-ресурсів.

Аналізу правозастосовної діяльності та судової практики свідчить про відсутність належного правового регулювання порядку фіксації об'єктів в інтернеті для пред'явлення їх в суді та інших органах. Забезпечення збору та фіксації доказів в інтернеті є проблемою насамперед, для захисту авторських прав, але також і у інших випадках – наприклад, передвиборча агітація в день виборів, шахрайство, захист честі, гідності та ділової репутації, втручання в особисте життя тощо. З моменту порушення і до моменту судового розгляду

інформація, що розміщена на певній веб-сторінці, може бути неодноразово змінена, більше того така веб-сторінка взагалі може зникнути.

Крім того, аналіз норм законодавства, правозастосовної практики та наукових поглядів свідчить про існування кількох способів фіксації змісту веб-сторінки. Таку фіксацію можуть здійснювати особи, чиї права порушуються; треті особи (наприклад, в РФ це нотаріуси); суд або правоохоронні органи. При цьому така фіксація може бути здійснена як візуальним так технологічним способом. К.О. Зеров пропонує до візуальних способів фіксації слід віднести: 1) Роздруківка веб-сторінки (Web-скріншот); 2) Фіксація особою контенту, що міститься на веб-сайті, шляхом його збереження на відповідних носіях (CD, DVD, магнітні диски, тощо); 3) Протокол огляду веб-сторінки нотаріусом; 4) Огляд доказів судом за їх місцезнаходженням; 5) Проведення відеозапису процесу дослідження будь-якою заінтересованою особою; 6) Проведення протоколу огляду веб-сайту адвокатом на підставі його професійного права на збирання відомостей про факти, що можуть бути використані як докази відповідно до п. 7 ч. 1 ст. 20 ЗУ «Про адвокатуру та адвокатську діяльність»; а до технологічних способів фіксації (тобто таких, що приділяють увагу технічним аспектам функціонування веб-сторінок) слід віднести: 1) Довідки, отримані від провайдерів (log-файли); 2) Миттєву фіксацію веб-сторінок за допомогою приватних онлайн-сервісів; 3) Використання сервісу InternetArchive. WaybackMachine; 4) Проведення експертного дослідження за експертизою 10.17 – дослідження телекомунікаційних систем (обладнання) та засобів. засобів [192]. Водночас, слід звернути увагу, що візуальні способи фіксації не передбачають аналізу вихідного коду веб-сторінки, що вбачається недостатнім для встановлення особи правопорушника. Жодний з візуальних способів фіксації змісту веб-сторінок не в змозі дати належне і достовірне уявлення про те, що ж насправді розміщується (і чи розміщується) на даній веб-сторінці і чи не була вона модифікована, оскільки такий спосіб є лише відтворенням (останнім етапом використання твору в інтернеті), яке подається на пристрій виведення інформації, а не дослідженням її внутрішньої структури (що здатне довести правомочності відтворення та надання твору до загального відома публіки)[192]. Слід звернути увагу, що жоден з цих способів не має однозначного

закріплення в процесуальному законодавстві. Така прогалина законодавства є порушенням конституційного права людини на захист, оскільки в більшості випадків унеможлиблює надання доказів, що пов'язані з порушенням інформаційної безпеки та прав людини за допомогою інтернету.

Зазначені приклади вказують на системну проблему, що має місце у правовому забезпеченні інформаційної сфери в цілому, і інформаційної безпеки людини зокрема. Стан українського законодавства у інформаційній сфері свідчить про його невідповідність, неузгодженість та безсистемність. Окрім того, слід зазначити, що на сьогодні інформаційна сфера розглядається і як відносно самостійна сфера, і як складова інших видів діяльності. Другий підхід свідчить про те, що інформаційна сфера обслуговує практично всі аспекти суспільного життя – державотворення, безпеку, оборону, економіку, фінансову та грошову системи, соціальну сферу, екологію, науку, освіту і культуру, міжнародне співробітництво. Відповідно, інформаційна безпека виступає і як самостійна сфера регулювання, і, відповідно, є складовою всіх інших – національної, екологічної, економічної, військової та інших. Таким чином, законотворення у сфері інформаційної безпеки не може відбуватись відокремлено від розвитку системи права частиною якого воно є.

Розвиток законодавства у цій сфері вимагає ефективної співпраці органів державної влади, інститутів громадянського суспільства, комерційних структур і наукового потенціалу держави. Розробка законодавства щодо інформаційної безпеки людини вимагає створення ефективних механізмів активної участі у законотворчій діяльності її суб'єктів - належний доступ до проектів нормативних актів у цих сферах, реальні публічні обговорення, а також врахування їх результатів. Цінним в цьому аспекті є досвід держав з напрацьованими інструментами е-демократії – наприклад, Сполученого Королівства, Естонії.

Актуальною проблемою залишається необхідність вироблення єдиних техніко-юридичних та мовно-термінологічних вимог до підготовки проектів законів у інформаційній сфері. Оскільки ця сфера відносно нова, надзвичайно динамічна і наукоємна, то й вимагає використання наукового потенціалу при

розробці законопроектів у цій сфері, а також проведення експертного оцінювання ефективності вже існуючого законодавства.

Цінним з цих позицій вбачається досвід США та окремих країн ЄС. Для прикладу, в США, крім офіційних, практикуються експертизи законопроектів з відомими та авторитетними недержавними інститутами, які володіють достатнім авторитетом і довірою парламенту, виконують цю функцію професійно та відповідально. В Швейцарії оцінка законодавства входить в обов'язки парламенту, в багатьох законах і підзаконних актах містяться статті щодо подальшої періодичної оцінки їх дієвості.

Важливо зауважити, що рішення ЄСПЛ на сьогодні не визнаються в Україні джерелами законодавства, що не виключає можливість їх використання як джерел права. Отже, на нашу думку, врахування аналізу практики ЄСПЛ щодо справ, для вдосконалення національного законодавства в напрямку зближення до міжнародних стандартів, а також усунування недоліків національного законодавства, які спричинили порушення, що стали предметом розгляду.

Цінною є участь представників громадянського суспільства, комерційної діяльності і науковців з огляду також на використання професійного досвіду, порівняльних досліджень та зарубіжного досвіду в законотворчому процесі. А питання інформаційної безпеки, як вже згадувались є надзвичайно динамічними і потребують значного обсягу професійних знань для розуміння не лише їх технологічної сторони, а й соціальних наслідків.

Особливою уваги заслуговує питання правової культури та громадянської свідомості членів суспільства. Інструменти, що надає у руки громадянам, інститутам громадянського суспільства і державним органам матимуть вплив за умови їх осмисленого використання усіма учасниками правовідносин. Електронна демократія і електронне урядування означає не лише оцифровування окремих документів та зміна каналів отримання інформації. Має відбутись переосмислення всіх процесів і цінностей в демократичному суспільстві.

Таким чином, міжнародний досвід свідчить про дихотомію проблеми міжнародної інформаційної безпеки, та інформаційної безпеки людини як складової інституту прав людини в міжнародному праві. Узгодження основних

питань є необхідним з огляду на економічні інтереси держав, демократичні цінності та глобалізаційні процеси, і, водночас, практично неможливим з огляду на розбіжності в інтересах основних геополітичних гравців. При цьому правове та організаційне забезпечення інформаційної безпеки людини лише на національному рівні є недостатнім з огляду на глобалізацію, інтенсивні транскордонні інформаційні процеси, трудову міграцію, е-комерцію, втрату ідентичності та ще цілу низку соціальних процесів, що виникають у зв'язку зі становленням інформаційного суспільства.

Український законодавець вже визначився з основним вектором зовнішньої політики, а, отже, законодавство в інформаційній сфері має відповідати цьому вектору. Враховуючи, що інформаційне законодавство України формувалось безсистемно і під впливом різних моделей правового регулювання інформаційної сфери, на сьогодні, важливим є опрацювання Інформаційного кодексу, який би відображав основні пріоритети, визначав систему і структуру інформаційного законодавства, залишаючи простір для реагування на динамічні процеси в інформаційній сфері.

З огляду на це, перспективними напрямками наукової розробки у досліджуваній предметній сфері вбачаються: захист прав людини на безпечне інформаційне середовище; правове забезпечення інформаційного суверенітету держави і суспільства; правове забезпечення освіти і науки в умовах глобалізації та розбудови інформаційного суспільства; правові засади захисту персональних даних з урахуванням змін в законодавстві ЄС; процесуальні проблеми правозастосовчої і правореалізаційної діяльності в інформаційній сфері; правове регулювання діяльності в сфері ІТ; правове регулювання діяльності суб'єктів системи забезпечення інформаційної безпеки, правові основи інформаційно-психологічної безпеки людини; правове регулювання надання інформаційно-психологічних послуг та психотерапевтичної допомоги; питання правового забезпечення інформаційної безпеки людини у зв'язку з використанням електронних реєстрів; правове регулювання використання генетичної інформації; правове забезпечення інформаційної безпеки людини в умовах використання інтернету речей, хмарних технологій, технології обробки великих даних,

нейронних мереж, штучного інтелекту та робототехніки; юридична відповідальність за інформаційні делікти.

### **Висновки до розділу 5**

Підходи до розуміння інформаційної безпеки людини в Україні та світі за роки зазнали суттєвих трансформацій, зокрема, сформувались політичні уявлення про місце цієї сфери в суспільному житті, роль держави в її регулюванні, розуміння мети і змісту державного управління інформаційною безпекою, механізмів державного впливу на інформаційні процеси та відносини. Відповідним чином змінювалося законодавство, структура та функції суб'єктів цієї політики.

Аналіз державної політики щодо інформаційної безпеки людини в Україні дозволив визначити, що інформаційна безпека людини є істотною частиною державної політики в переважній більшості напрямів, зокрема, зовнішньої політики, соціальної політики і політики в галузі прав людини, у сфері національної безпеки, у сфері охорони здоров'я і екологічної політики тощо. Таким чином, можна констатувати, що чинне законодавство не дає цілісного і системного закріплення офіційних поглядів, принципів, напрямів діяльності, спрямованих на реалізацію державної політики інформаційної безпеки людини.

Водночас, аналіз правових основ державної політики дозволяє зробити висновок, що як окремий напрям державна політика інформаційної безпеки (в цілому, і людини, зокрема) не виділяється, хоча в науковій думці існує такий підхід.

З метою вдосконалення системи організаційного забезпечення та правового регулювання відносин у сфері інформаційної безпеки людини, які повинні базуватись на комплексному і системному підходах, запропоновано створити центральний орган виконавчої влади, що буде реалізовувати політику держави щодо розбудови приязного для людини інформаційного суспільства в Україні. До сфери відповідальності такого органу мають бути віднесені: координація розбудови інформаційної інфраструктури держави; забезпечення умов для



реалізації інтересів людини, суспільства і держави в інформаційному просторі; координація діяльності інших державних органів в інформаційній сфері.

Встановлення сутнісних ознак механізму правового регулювання відносин у сфері інформаційної безпеки людини, вбачається необхідним для визначення засад, на яких мають базуватись підходи щодо розробки та здійснення ефективного правового регулювання відносин у цій сфері. Оскільки інформаційна безпека є не лише самостійною сферою регулювання, а й невід'ємною складовою всіх інших – національної, екологічної, економічної, військової та інших, то її регулювання вимагає застосування єдиного системного підходу. В його основу має бути покладено принцип найвищої цінності людини, гарантування її прав, свобод і законних інтересів. Окреслено загальну систему принципів правового регулювання інформаційних відносин, а також виокремлено специфічні принципи, що є визначальним для правових основ інформаційної безпеки людини, до яких запропоновано віднести:

- принцип пріоритету прав, свобод і законних інтересів людини і громадянина;
- принцип свободи інформації і обмеження доступу до інформації виключно у випадках передбачених законом;
- принцип розвитку сприятливого для людини інформаційного суспільства;
- принцип відповідальності держави перед людиною та суспільством за реалізацію державної політики інформаційної безпеки;
- принцип мінімізації негативного інформаційного впливу на людину, в т.ч. шляхом формування інформаційної культури людини і суспільства;
- принцип участі громадянського суспільства у розробці та контролі за реалізацією заходів щодо попередження та захисту від загроз інформаційній безпеці людини;
- принцип гармонізації інформаційного законодавства України із законодавством ЄС та положеннями міжнародного права у сфері інформаційної безпеки.

Здійснено аналіз окремих видів актів застосування норм права у механізмі правового регулювання у сфері інформаційної безпеки людини. На його основі

запропоновано уповноваженому із захисту прав людини, а в перспективі – Уповноваженому з інформаційної безпеки людини - надати відповідні повноваження щодо застосування норм права з метою припинення правопорушень та відновлення порушених прав.

Також на основі аналізу судової практики у справах, що стосуються порушення прав людини на доступ до інформації, захисту персональних даних та інших інформаційних прав, обґрунтовано необхідність створення Вищого інформаційного суду.

Пропозиції щодо вдосконалення українського законодавства у інформаційній сфері, насамперед, щодо інформаційної безпеки людини, сформовані на основі аналізу його розвитку, сучасного стану, досвіду іноземних держав та наукових досліджень. Сучасний стан інформаційного законодавства характеризується невпорядкованістю, неузгодженістю та безсистемністю. Інформаційна сфера обслуговує практично всі аспекти суспільного життя – державотворення, безпеку, оборону, економіку, фінансову та грошову системи, соціальну сферу, екологію, науку, освіту і культуру, міжнародне співробітництво. Отже, інформаційна безпека виступає і як самостійна сфера регулювання, і є складовою всіх інших – національної, екологічної, економічної, військової та інших. Таким чином, законотворення у сфері інформаційної безпеки не може відбуватись відокремлено від розвитку системи права, частиною якого воно є. Розвиток законодавства у цій сфері вимагає ефективної співпраці органів державної влади, інститутів громадянського суспільства, комерційних структур і наукового потенціалу держави. Розробка законодавства щодо інформаційної безпеки людини вимагає створення ефективних механізмів активної участі у законотворчій діяльності її суб'єктів – належний доступ до проектів нормативних актів у цих сферах, реальні публічні обговорення, а також врахування їх результатів.

Актуальною проблемою залишається необхідність вироблення єдиних техніко-юридичних та мовно-термінологічних вимог до підготовки проектів законів у інформаційній сфері. Оскільки ця сфера відносно нова, надзвичайно динамічна і наукоємна, то й вимагає використання наукового потенціалу при

розробці законопроектів у цій сфері, а також проведення експертного оцінювання ефективності вже існуючого законодавства.

Особливої уваги заслуговує питання правової культури та громадянської свідомості членів суспільства. Нові інструменти, що надаються громадянам, інститутам громадянського суспільства і державним органам, матимуть вплив за умови їх осмисленого використання усіма учасниками правовідносин. Електронна демократія і електронне урядування означає не лише оцифровування окремих документів та зміну каналів отримання інформації, вони вимагають переосмислення всіх процесів і цінностей в демократичному суспільстві.

Враховуючи, що інформаційне законодавство України формувалось безсистемно і під впливом різних моделей правового регулювання інформаційної сфери, на сьогодні, важливим є опрацювання базового закону – Інформаційного кодексу, який би відображав основні пріоритети, визначав систему і структуру інформаційного законодавства, водночас, залишаючи простір для реагування на динамічні процеси в інформаційній сфері.

Врегулювання вимагає низка питань, що щільно пов'язані з інформаційною безпекою людини, які мають різний ступінь наукового опрацювання і сприйняття суспільством. Особливої уваги при нормотворенні вимагають ті, що не мають сформованої однозначної етичної оцінки, і тому значно складніше інтегруються у суспільну свідомість, отже, і в правову культуру. Зокрема, йдеться про правове регулювання відносин, пов'язаних із використанням штучного інтелекту та робототехніки, технологій аналізу великих даних, політтехнологій, пропаганди та маніпуляцій суспільною свідомістю, використання генетичної інформації тощо. Вони безпосередньо пов'язані не лише з інформаційною безпекою людини, а й з безпекою людини в цілому, як фізичної особи і як члена суспільства.

## ВИСНОВКИ

У результаті проведеного дослідження на основі здобутків вітчизняної та зарубіжної правової науки, положень чинного національного і зарубіжного законодавства та норм міжнародного права і практики їх реалізації, вирішено наукову проблему, що полягає у з'ясуванні правової природи, сутнісних ознак та особливостей інформаційної безпеки людини, визначенні її місця в системі інформаційної і національної безпеки, визначенні реальних та потенційних загроз інформаційній безпеці людини в Україні, а також сформульовано авторське бачення концептуальних засад державної політики інформаційної безпеки людини і запропоновано низку положень і висновків, спрямованих на удосконалення правових основ інформаційної безпеки людини, зокрема:

1. Виявлено, що правова і доктринальна основа інформаційної безпеки в Україні розвивались симптоматично і безсистемно. Певною мірою це обумовлено тим, що сучасні методи дослідження базуються на різних світоглядних позиціях, по-різному вирішують дослідницькі завдання, а також використовують відмінні стратегії досліджень. Окрім того, первинно інформаційна безпека розглядалась, насамперед, як інформаційна безпека держави. Згодом інтенсифікація процесів інформатизації в усіх сферах, а особливо, зростання значення технічного захисту інформації зумовило становлення правового забезпечення захисту інформації як невід'ємної складової безпеки підприємств, установ та організацій, а також окремих галузей господарства. На межі тисячоліть гостро повстало питання про міжнародну інформаційну безпеку, а також кібербезпеки у складі інформаційної безпеки. Проаналізовано етапи становлення українського законодавства у інформаційній сфері в цілому, та щодо інформаційної безпеки, зокрема, і з'ясовано, що на кожному з цих етапів інформаційна безпека людини залишалась вторинним питанням.

2. На основі історико-правового аналізу інформаційної безпеки людини як соціально-правового явища встановлено, що кожна історична епоха поглиблювала розуміння соціальних структур і в історичній генезі людина переживала зміну свого соціально-правового статусу. В сучасному українському

суспільстві, яке декларує себе як правове, демократичне і інформаційне, можливості і необхідність правового впливу на суспільні відносини знаходяться в прямій залежності від визначення правового статусу людини як суб'єкта і об'єкта соціальних відносин. Насичення інформаційними відносинами усіх сфер суспільного життя і суттєве узалежнення якості життя людини від інформаційних ресурсів та інформаційних технологій дає підстави говорити про формування інформаційної правосуб'єктності людини та інформаційно-правовий статус як новий галузевий правовий статус людини.

3. Проаналізувавши доктринальні підходи, норми міжнародного права та національного законодавства, вважаємо, що слід розрізняти дві різні категорії: інформаційні права і свободи людини, а також права і свободи людини в інформаційному суспільстві. При чому перша категорія є складовою другої.

Під інформаційними правами і свободами пропонується розуміти комплекс прав, похідних від свободи інформації, як фундаментального права людини, а саме: 1) Інформаційні права, що пов'язані з особою (особистістю) людини – право на захист персональних даних, право визначати конфіденційність інформації та розпоряджатися нею; 2) Право власності на інформацію; 3) Право на доступ до інформації – в широкому розумінні, тобто доступ до публічної, екологічної, правової, наукової та інших видів інформації, в тому числі необхідної для реалізації інших прав та свобод – політичних прав, право на освіту, право на безпечне для життя та здоров'я довкілля, трудових та інших прав; 4) Свобода поширення інформації будь-яким законним способом, яка є необхідною умовою повноцінного життя людини в демократичній державі, а також існування самого громадянського суспільства, її реалізація пов'язана з свободою думки і слова, правом на вільне вираження своїх поглядів і переконань; 5) право на безпечне інформаційне середовище.

Водночас, важливо зважати на те, що формування інформаційного суспільства обумовило не лише значення існуючих і появу нових інформаційних прав людини, а й змінило змістовне наповнення усіх прав і свобод людини, а також її обов'язків, в напрямку формування інформаційної складової кожного з них.

4. Доведено, що інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, а також спрямована реалізацію прав і законних інтересів людини в кожній сфері його життєдіяльності. Встановлено, що не дивлячись на активні наукові дослідження в сфері інформаційної безпеки відсутній єдиний підхід до інформаційної безпеки в цілому, інформаційної безпеки людини, зокрема. Зміст і складність цієї концепції є також атрибутивною властивістю відносин у сучасному інформаційному суспільстві. Аналіз різних підходів до визначення категорії інформаційної безпеки дозволяє зробити висновок про недоцільність суворого дотримання однієї позиції. Найбільш відповідним, на нашу думку, є комплексний підхід, згідно з яким інформаційна безпека визначається через її істотні риси, основні функції, беручи до уваги постійну динаміку інформаційних і соціальних систем.

Таким чином, онтологічне розуміння інформаційної безпеки опирається на ціннісному вимірі об'єкта безпеки; тобто при інформаційній безпеці людини йдеться про її потреби, можливість реалізації яких в правовому полі закріплюється через права і свободи. Гносеологічно зміст інформаційної безпеки зводиться, з однієї сторони, до небезпек і загроз, що виникають і впливають на існування об'єкта, а з іншої – до діяльнісної складової – можливостей суб'єктів щодо створення безпечних умов існування об'єкта інформаційної безпеки. Логічний зміст інформаційної безпеки має особливе значення в правовій площині, адже нормативне закріплення як правової категорії робить його основоположним для системи правового забезпечення. Визначеність логічного змісту інформаційної безпеки залежить від розвитку наукового пізнання, а також від розбудови механізму державного управління. Розуміння інформаційної безпеки людини як правової категорії повинне ґрунтуватися на розумінні комплексності її як соціального явища, а також враховувати інформаційні права і свободи людини як змістовне наповнення, що визначає сутність даної категорії.

5. Проаналізовані доктринальні праці щодо розуміння інформаційної безпеки людини дозволили окреслити два основні підходи, базуючись на яких сформульовано авторське бачення структури інформаційної безпеки людини як сукупності інформаційно-психологічної, інформаційно-технологічної (елементом

якої є кібербезпека людини) та інформаційно-правової складових. Остання визначається закріпленням на національному та міжнародному рівнях інформаційно-правовим статусом людини, тобто обсягом прав і свобод в інформаційній сфері, а також гарантіями їх реалізації.

6. Обґрунтовано, що інформаційна безпека людини, водночас, є і станом, і процесом, оскільки виступає невід'ємною частиною життя, в якому людина постійно перебуває під дією конкретних інформаційних впливів. Тому значимим з позицій забезпечення інформаційної безпеки людини вбачається врахування особливостей конкретної особистості на основі співвідношення в них біологічного та соціального, а також середовища в якому вона знаходиться. При цьому різні категорії осіб знаходяться у неоднакових умовах щодо можливості реалізації своїх прав і свобод в інформаційній сфері, що визначає їх ступінь захищеності в інформаційному суспільстві, види і інтенсивність небезпек, що їм загрожують.

Запропонована типологізація категорії осіб, що характеризуються наявністю спільних інформаційних загроз їх безпеці, дозволила звернути увагу на особливу уразливість цих категорій осіб в умовах інформаційного суспільства. Так, інтегрованість в сучасному суспільстві значною мірою залежить від можливості використання інформаційних технологій. При цьому, обмежені фізичні можливості (вади зору, слуху, координації) досить часто в українських реаліях стають причиною порушення прав людини у зв'язку з неможливістю повноцінно використовувати інформаційні технології. Такі обмеження стосуються не лише інформаційних прав, а в умовах інформаційного суспільства – політичних, соціальних, трудових та інших прав людини. Окрім того, особливо гострою залишається проблема доступу до інформації осіб із інтелектуальною та психосоціальною формою інвалідності.

7. Запропоноване власне бачення системи інформаційної безпеки, елементами якої вбачаються: 1) правова та наукова (доктринальна) основа; 2) об'єктно-суб'єктний склад, тобто об'єкти інформаційної безпеки, а також система органів (підрозділів), що здійснюють забезпечення; 3) політика інформаційної безпеки; 4) засоби і способи забезпечення інформаційної безпеки. Системний

підхід є необхідною умовою для визначення загроз, а також пошуку оптимальних шляхів їх нейтралізації.

8. Дослідження існуючого законодавства та зарубіжного досвіду регулювання інформаційної безпеки вказує на системну проблему, що має місце у правовому забезпеченні інформаційної сфери України в цілому, і інформаційної безпеки людини зокрема – відсутність єдиного системного підходу до регулювання сфери інформаційної безпеки, в основу якого має бути покладено принцип найвищої цінності людини, гарантування її прав, свобод і законних інтересів.

Оскільки, інформаційна безпека виступає і як самостійна сфера регулювання, і, відповідно, є складовою всіх інших, то законотворення у цій сфері не може відбуватись відокремлено від розвитку системи права, частиною якого воно є. Розвиток законодавства у цій сфері вимагає ефективної співпраці органів державної влади, інститутів громадянського суспільства, комерційних структур і наукового потенціалу держави. Розробка законодавства щодо інформаційної безпеки людини вимагає створення ефективних механізмів активної участі у законотворчій діяльності її суб'єктів – належний доступ до проектів нормативних актів у цих сферах, реальні публічні обговорення, а також врахування їх результатів.

9. В умовах, коли на території держави відбувається збройний конфлікт, а фактично все населення держави є об'єктом негативних інформаційних впливів, ситуація ускладнена також низкою соціальних, політичних, економічних, історичних передумов, правове забезпечення інформаційної безпеки людини має здійснюватись виходячи не від загроз і небезпек – як це є на сьогодні, а з позицій створення ефективної системи забезпечення основних інформаційних прав і свобод людини. Визначено, що державна політика у сфері інформаційної безпеки людини реалізується, насамперед, у складі державної інформаційної політики і політики національної безпеки, але не обмежується ними.

Проте, відсутність скоординованої діяльності органів державної влади та громадянського суспільства у інформаційній сфері створюють умови для реалізації потенційних та появи нових загроз інформаційній безпеці на всіх



рівнях. З огляду на це, вбачаються необхідність інституційних змін на рівні державної влади.

По-перше, необхідним є концентрація повноважень по реалізації політики держави щодо розбудови приязного для людини інформаційного суспільства в Україні, в єдиному центрального органу виконавчої влади. При цьому, на законодавчому рівні має бути визначено відповідальність держави і зобов'язання щодо реалізації інформаційної політики у основних сферах життєдіяльності суспільства – обороні, захисті прав людини, економіці, освіті, охороні здоров'я, екології, демократизації та децентралізації тощо. Особливими сферами відповідальності такого органу мають стати: координація розбудови інформаційної інфраструктури держави; забезпечення умов для реалізації інтересів людини, суспільства і держави в інформаційному (в т.ч. кібер) просторі; координація діяльності інших державних органів в інформаційній сфері, забезпечення безвідмовної роботи об'єктів критичної інформаційної інфраструктури, створення умов для формування належного рівня інформаційної культури населення, в тому числі, професійної підготовки населення в умовах розбудови інформаційного суспільства, сприяння розвитку ІТ галузі, забезпечення відкритості та прозорості діяльності влади, а також сприяння формуванню позитивного іміджу України як в середині держави, так і за її межами.

По-друге, нагальним є на рівні незалежного органу держави закріплення Уповноваженого з інформаційної безпеки людини, діяльність якого має бути спрямована на реалізацію політики держави щодо забезпечення інформаційної безпеки людини, в тому числі захист прав і свобод людини в інформаційній сфері, зокрема, права на доступ до публічної інформації та захист персональних даних.. Уповноваженому необхідно надати достатні важелі впливу, з однієї сторони, на формування інформаційного законодавства, наприклад, шляхом обов'язкової експертизи нормативних актів що зачіпають відповідні права людини, з іншої – повноваження щодо припинення правопорушень та відновлення порушених прав.

По-третє, враховуючи специфіку справ, що пов'язані з порушенням інформаційних прав і свобод громадян, вбачається доцільним створення спеціалізованого суду - Вищого інформаційного суду. До його підсудності мають

бути віднесені справи, що стосуються порушення прав людини на доступ до інформації, захисту персональних даних, дифамації, а також щодо реалізації прав громадян на участь у політичному житті, пов'язані з використанням інструментів електронної демократії.

10. Завдяки аналізу міжнародного досвіду виявлено дихотомію проблеми міжнародної інформаційної безпеки та інформаційної безпеки людини як складової інституту прав людини в міжнародному праві.

Узгодження основних питань є необхідним з огляду на економічні інтереси держав, демократичні цінності та глобалізаційні процеси, і, водночас, практично неможливим з огляду на розбіжності в інтересах основних геополітичних гравців. При цьому правове та організаційне забезпечення інформаційної безпеки людини лише на національному рівні є недостатнім з огляду на глобалізацію, інтенсивні транскордонні інформаційні процеси, трудову міграцію, "е-комерцію", втрату ідентичності та ще цілу низку соціальних процесів, що виникають у зв'язку зі становленням інформаційного суспільства.

11. В результаті аналізу моделей правового регулювання досліджуваної сфери правовідносин розмежовуються підходи до інформаційної безпеки людини в США і країнах ЄС. Аналіз федерального законодавства США щодо інформаційної безпеки свідчить про пріоритет національної безпеки перед дотриманням прав і свобод людини. В той час як спільна позиція країн Європейського Союзу щодо інформаційної безпеки та стандартів прав людини в інформаційній сфері базується на передумовах побудови інформаційного суспільства в країнах Європи – розвиненій економіці та соціальній спрямованості політики, і, насамперед, акцентує такі індивідуальні цінності людини як можливість самореалізації, вільний час, можливість спілкування, а також захищеність приватного життєвого простору. При чому інформаційна політика ЄС є динамічною і постійно зазнає переосмислення. Таким чином, Україна, як держава, що обрала європейський вектор розвитку, зобов'язана враховувати досвід країн ЄС, але, водночас, слід враховувати національні особливості формування інформаційного законодавства і стан демократизації суспільства.

12. Надання громадянам, інститутам громадянського суспільства і державним органам численних нових інструментів для реалізації безпосередньої та опосередкованої форм демократії, з однієї сторони, а також для ефективної публічно-сервісної діяльності держави вимагає високого рівня не лише правової культури та громадянської свідомості членів суспільства, а й інформаційної культури та інформаційної грамотності. Тому, необхідним є правове забезпечення формування таких компонентів інформаційної культури як світоглядний, ціннісний і комунікативний на всіх етапах соціалізації, а також урахування проблеми цифрового розриву і ціннісних відмінностей поколінь та окремих соціальних груп у сучасному українському суспільстві.

13. Вирішення на законодавчому рівні потребує низка питань, що щільно пов'язані з інформаційною безпекою людини, зокрема: створення правової основи для освіти протягом життя, як необхідної умови існування людини в інформаційному суспільстві; врегулювання питань щодо надання психологічної і психотерапевтичної допомоги, а також інших видів послуг, що використовують методи інформаційно-психологічного впливу; підвищення поінформованості громадян про свої права і свободи через формальні джерела інформації; ефективне регулювання ЗМІ, особливо нових медіа з метою забезпечення дотримання стандартів журналістської діяльності; створення умов для розвитку критичного мислення та оволодіння іншими інструментами, життєво необхідними в умовах формування інформаційного суспільства, особливо у вразливих категорій населення; подолання цифрової нерівності в географічному та демографічному (віковому) вимірі та інші.

14. Обґрунтовано, що необхідною умовою ефективної реалізації державної політики щодо інформаційної безпеки людини постає проведення фундаментальних та прикладних наукових досліджень. Поруч із вищезгаданими проблемами, які мають відносно добре наукове опрацювання і користуються суспільним схваленням, існують інші, що вимагають етичної оцінки, і тому значно складніше інтегруються у суспільну свідомість, отже і правосвідомість та правову культуру. Зокрема, осмислення на доктринальному рівні потребують питання, пов'язані із правовим забезпеченням використання штучного інтелекту

та робототехніки, технологій аналізу великих даних, використання генетичної інформації та ін.

Тому необхідним вбачається завершення процесу виокремлення інформаційного права (разом з правом інтелектуальної власності) в окрему наукову спеціальність.

15. Виявлено, що безсистемність і відсутність єдиного концептуального підходу до правового забезпечення інформаційної безпеки людини призвели до появи значних проблем у правозастосовній діяльності. Зокрема, проаналізовано, механізми блокування інтернет-ресурсів, що здійснюють незаконну діяльність, і встановлено, що єдиним легальним на сьогодні способом є судовий. В той же час, протягом останніх років мали місце неодноразові спроби внесення до національного законодавства змін, які б встановлювали нові позасудові механізми блокування інтернет-ресурсів, що суперечить свободі інформації як.

В той же час, запропоновано вдосконалити чинне законодавство в частині регуляції порядку витребування інформації (даних) від операторів мереж передачі даних, а також щодо встановлення відповідальності за невиконання обов'язку щодо розміщення реальної інформації щодо власників інтернет-ресурсів.

На основі аналізу правозастосовної діяльності та судової практики виявлено відсутність належного правового регулювання порядку фіксації об'єктів в інтернеті для пред'явлення їх в суді та інших органах. Така прогалина законодавства є порушенням конституційного права людини на захист, оскільки в більшості випадків унеможливорює надання доказів, що пов'язані з порушенням інформаційної безпеки та прав людини за допомогою інтернету.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аб бібліятечнай справе: Закон Рэспублікі Беларусь от 22.03.1995 г. № 3680-XII.  
URL: <http://rlst.org.by/metodist/laws-ntb/823.html>.
2. Аболіна Т. Г. Прикладна етика. Навч. посіб. / Аболіна Т. Г. та ін. / За наук. ред. Панченко В.І. К.: Центр учбової літератури, 2012. 392 с.
3. Абулмагд А. К. Преодолевающие барьеры. Диалог между цивилизациями: пер. с англ. /А. К. Абулмагд и др. под ред. С. П. Капицы; пер. Т.П. Вечернина. М.: Логос, 2002. 192 с.
4. Аврелій Августин. Сповідь. Л., Свічадо, 2008. 356 с.
5. Адміністративне право України: підр. Ю.П. Битяк, В.М. Гаращук, О.В. Дьяченко та ін.; за ред. Ю. П. Битяка. К.: Юрінком Інтер, 2007. 544 с.
6. Адылханов А.А., Казезов А.Н. Права человека в киберпространстве . Актуальные вопросы юридических наук: Мат. II междунар. науч. конф. (г. Челябинск, февраль 2015 г.). Челябинск: Два комсомольца, 2015. URL: [moluch.ru/authors/10704/](http://moluch.ru/authors/10704/) (дата звернення: 02.10.2017)
7. Азербайджан: Суд впервые запретил компании использовать нелицензионное ПО. URL: <https://digital.report/azerbaydzhan-sud-vpervyie-zapretil-kompaniiispolzovat-nelitsenzionnoe-po/> (дата звернення: 19.10.2017)
8. Акопов В.И., Маслов Е.Н. Право в медицине. М. : Книга-сервис, 2002. 352 с.
9. Алещенко В.І., Сербін В.Г. Проблеми захисту від негативного інформаційнопсихологічного впливу противника. Мат. машини і системи. 2010. № 1. С. 77-86.
10. Американская компания уже в августе вживит чипы сотрудникам URL: <http://datification.org/article/amerikanskaya-kompaniya-vzhivit-chipy-svoim-sotrudnikam/> (дата звернення: 29.07.2017)
11. Амосов О.Ю. Моделі публічного адміністрування (архетипова парадигма) . *Публічне управління: теорія та практика. Спец. випуск.* 2013. С. 6–13.

12. Анализ законодательства в Российской Федерации в контексте права человека на информацию. URL: [http://www.medialaw.ru/publications/books/inf\\_right](http://www.medialaw.ru/publications/books/inf_right). (дата звернення: 20. 08.2017)
13. Ананьев Б.Г. Психология чувственного познания. М.: Наука, 2001. 279 с.
14. Андрущенко В. Філософія: Підр. Харків: Консум, 2000. 672 с.
15. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти: Моногр. / За заг. ред Бандурки О.М. Х.: Вид-во Ун-ту внутр. справ, 2000. 368 с.
16. Арістова І.В. Розбудова правової держави в Україні: правовий механізм забезпечення права на доступ до інформації в суспільстві знань. Правова інформатика. 2010. №1(25). С. 3-13.
17. Артамонова Я.С. Информационная безопасность российского общества: теоретические основания и практика политического обеспечения: дис. ... доктора политических наук / Московский государственный областной университет. М., 2014. 359 с.
18. Архипова Є. О. Інформаційна безпека: соціально-філософський вимір : дис. ... кандидата філософ. наук : 09.00.03 / НТУ України «Київський політехнічний інститут». К., 2012. 199 с.
19. Аскерко А. Комментарий к Закону Республики Беларусь «О регистре населения.» URL: <http://www.center.gov.by/article61.html> (дата звернення: 02.10.2017)
20. Астрахан В.И., Гусев В.В., Павлов В.В., Чернявский Б.Г. Становление и развитие правительственной связи в России. Орел: ВИПС, 1996. с. 10.
21. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. М. : КДУ, 2013. 736 с.
22. Балалыкина Э.А. Метаморфозы русского слова: учебное пособие. М.: Флинта. Наука, 2012. 524 с.
23. Банковский кодекс: Кодекс Республики Беларусь от 25.10.2000 г. № 441-З. URL: <http://kodeksy.by/static/bankovskiy-kodeks.pdf>
24. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика монографія Київ: Едельвейс, 2014. 434 с.

25. Баранов О. Система принципів інформаційного права. *Правова інформатика*. 2006. № 2(10) с.5-11
26. Баранов О.А. Право власності на інформацію. *Правова інформатика*. 2008. № 1(17). С.15-19.
27. Баранов О.А. Інформаційна безпека і економічні перетворення. Поглиблення ринкових реформ та стратегія економічного розвитку України до 2010 р.: Мат.міжнародної конференції. К., 1999. Ч. 2, т. 1. 168 с.
28. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи Київ: СофтПрес, 2005. 316 с.
29. Баранов О.А. Методи інформаційного права. *Правова інформатика* 2007. № 4(16). с.8-12.
30. Баранов О.А. Правове забезпечення інформаційної сфери: теорія, методологія і практика: Моногр. Київ: Едельвейс, 2014. 434 с.
31. Баранов О.А. Правові проблеми “електронної демократії”. *Інформація і право*. 2017. № 1(20). с.28-38.
32. Бауман З. Глобалізація. Наслідки для людини і суспільства / пер. з англ. І. Андрущенко. К.: Вид. дім "Києво-Могилянська академія", 2008. 109 с.
33. Бачило И.Л. Гражданское общество в зеркале Интернета. Массовая информация в Интернете: науч.-практ. конф. Москва, 12-13 октября 2007 г. URL: [http://www.igpran.ru/about/subjects/center2/Konf/conference\\_abstracts.doc](http://www.igpran.ru/about/subjects/center2/Konf/conference_abstracts.doc) (дата звернення: 11.08.2016)
34. Бачило И.Л. Информационное право. Основы практической информатики: Учеб.пособ. М.: Юринформцентр, 2001. 352 с.
35. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учеб. СПб.: Юрид. центр Пресс, 2001. 789 с.
36. Беззубов Д.О. Суспільна безпека: (організаційно-правові засади забезпечення): Моногр. К.: МП Леся, 2013. 451 с.
37. Безпека дітей в Інтернеті: відомості для батьків і вчителів URL: <https://support.office.com/uk-ua/article> (дата звернення: 02.10.2017)

- 38.Безпека дітей в Інтернеті URL:  
<http://mon.gov.ua/ua/activity/education/59/196/korinfl9/bezditvinet/> (дата звернення: 02.10.2017)
- 39.Безпека інформації URL: <http://jrn1.nau.edu.ua/index.php/Infosecurity> (дата звернення: 10.09.2017)
- 40.Белл Д. Социальные рамки информационного общества. Новая технократическая волна на Западе. М.: Прогресс, 1986. С. 330–342.
- 41.Беляева Е. В. Метаморфозы нравственности: динамика исторических систем нравственности. Минск: Экономпресс, 2007. 464 с.
- 42.Бергсон А. Творческая эволюция / пер. с фр. В. Флеровой. М.: Академический проект, 2015. 318 с.
- 43.Беркмен О. Зникла межа між віртуальним і матеріальним світами. URL:  
<http://osvita.telekritika.ua/print/material/2099>. (дата звернення: 24.11.2016)
- 44.Бехтерев В.М. Внушение и его роль в общественной жизни. СПб.: Питер, 2001. 256 с.
- 45.Беляков К.І., Онопрієнко С.Г., Шопіна І.М. Інформаційна культура в Україні: правовий вимір. Монографія. К.: КВІЦ, 2018. 169 с.
- 46.Беляков К.І. Інформаційна безпека. Внутрішня безпека України та шляхи її забезпе-зпечення: наукове видання. К.: Міжвідомчий наук. дослід. центр, 2005. С. 26–32.
- 47.Беляков К.І., Ярмиш О.Н. Національна безпека України в інформаційній сфері: проблеми організаційного та правового забезпечення Безпекотворення: питання теорії і практики та правові аспекти : зб. наук.-практ. конф. (Київ, 16 лют.2007 р.): у 2 ч. Ч. 2 . К. : Вид-во Європ. ун-ту, 2007. С. 8–15.
- 48.Беляков К., Ланде Д., Ніконова В. Інформаційне законодавство: новели 2013 р.. Юридчний Вісник України. № 52 (965). 28 грудня 2013 р. – 3 січня 2014 р.. с.14-15
- 49.Беляков К.І. Знання про безпеку: проблеми визначення та методології. Боротьба з організованою злочинністю і корупцією (теорія і практика). К.: Міжвідомчий наук. дослід. центр, 2008. № 18. С.153-159.



- 50.Беляков К.І. Інформація в праві: теорія і практика: Моногр. К.: КВІЦ, 2006. 118 с.
- 51.Беляков К.І. Понятійні та методологічні основи регулювання нових типів інфор-маційних відносин : «віртуальні правовідносини». «Lex Portus». Одеса, Національний університет «Одеська юридична академія», 2016. № 2-2016. С. 47-63.
- 52.Більше половини жителів сіл в Україні вже користуються інтернетом  
URL:<http://watcher.com.ua/2017/04/13/bilshe-polovyny-zhyteliv-sil-v-ukrayini-vzhekorystuyutsya-internetom/> (дата звернення: 04.10.2017)
- 53.Битяк Ю.П., Яковюк І.В. Проект «Міжмор'я» як відображення геополітичних інтересів країн Східної Європи // Політичні та правові дисонанси в сучасних українських реаліях: зб. наук. статей (за матеріалами XXX Харків. політол. читан., 16 червня 2017 р.). Х., 2017. С. 7–13.
- 54.Битяк Ю.П., Яковюк І.В. Стратегія національної безпеки України: на шляху до оновлення // Воркшоп: «Інформаційна безпека як часть національної безпеки у Східній Європі». Х.: Право, 2016.С.86–93
- 55.Богуш В., Юдін О. Інформаційна безпека держави. К.: «МК-Прес», 2005. 432 с.
- 56.Боднар І. Інформаційне право країн західної Європи. Підприємництво, господарство і право. № 6. 2011. С. 34-38.
- 57.Боднар І.Р. Державна політика та інформаційна безпека України: післякризові виклики. Актуальні проблеми післякризового відновлення економіки України:Зб. мат. наук.-прак. конференції викладацького складу і аспірантів навчально-наукового комплексу "Академія". Л., 2013.
- 58.Бодрук О.С. Структура воєнної безпеки: національний та міжнародний аспекти: Моногор. К.: НІПМБ, 2001. 300 с.
- 59.Большая Советская Энциклопедия (цитаты). Наука и образование: школьникам, студентам, научным работникам. Новости науки и техники. URL: <http://oval.ru/enc/66129.html>. (дата звернення: 04.08.2017)
- 60.Бостром Н. Искусственный интеллект. Этапы. Угрозы. Стратегии / пер. с англ. С. Филина. М.: Манн, Иванов и Фербер, 2016. с.496.413

61. Бот — друг или враг юриста? URL: <https://delo.ua/tech/kak-ispolzovat-chat-botovv-ecommerce-330479/> (дата звернення: 06.11.2017)
62. Брижко В. До питання сучасної інформаційної політики. Вісн. Академії управління МВС. 2009. № 2. С. 32–36.
63. Брижко В. Сучасні основи захисту персональних даних в європейських правових актах. Інформація і право. 2016. № 3(18). С. 45-57.
64. Брижко В.М. Захист персональних даних: реалії та практика сучасності. *Інформація і право*. 2013. № 3 (9). С. 31 – 49.
65. Булеца С. Персональні дані пацієнта розголошу не підлягають URL: [http://yurincom.com/ua/legal\\_practice/analitichna\\_yurysprudentsiia/personalni\\_dani\\_patsiienta\\_rozgholosu\\_ne\\_pidliagaiut-publication/](http://yurincom.com/ua/legal_practice/analitichna_yurysprudentsiia/personalni_dani_patsiienta_rozgholosu_ne_pidliagaiut-publication/) (дата звернення: 11.10.2017)
66. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підр. / Бурячок В.Л. та ін.; за заг. ред. д.т.н., проф. В.Б. Толубка. К.: ДУТ, 2015. 288 с.
67. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України URL: [http://nbuviap.gov.ua/index.php?option=com\\_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannyata-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350](http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannyata-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350) (дата звернення: 15.08.2017)
68. В ЛНР издали детский журнал Вежливые человечки URL: <http://korrespondent.net/ukraine/3630876-v-lnr-izdaly-detskyi-zhurnal-vezhlyvye-chelovechky> (дата звернення: 12.03.2016)
69. Вагнер Е.А., Росновский А.А. О самовоспитании врача. Пермь : Пермское книжное издательство, 1976. 157 с.
70. Василенко В.О. Антикризове управління підприємством: Навч. посібник. К.: Центр навч. л-ри, 2005. 504 с.
71. Веймер, Л. Девід, Вайнінг, Р. Ейден Аналіз політики: концепції, практика / Пер. з англ. І.Дзюб, А.Олійник; наук. ред. О.Кілієвич. К., Основи, 1998. 654с.
72. Великий тлумачний словник сучасної української мови / Уклад. і голов. ред. В.Т.Бусел. Київ, Ірпінь: ВТФ “Перун”, 2005. 1728 с.

- 73.Вернадский В. Несколько слов о ноосфере. URL: [https://www.e-reading.club/bookreader.php/11180/Vernadskiii\\_-\\_Neskol%27ko\\_slov\\_o\\_noosfere.html](https://www.e-reading.club/bookreader.php/11180/Vernadskiii_-_Neskol%27ko_slov_o_noosfere.html) (дата звернення: 01.02.2015)
- 74.Веселуха В. Значення віктимологічної профілактики в системі запобігання злочинам. Право України. 1999. № 10. С. 67–73.
- 75.Винокуров И., Гуртовой Г. Психотронная война: От мифов — к реалиям, М.:Мистерия, 1993. 366 с.
- 76.Висновок на проект Закону України «Про внесення змін до деяких законів України щодо доступу до публічної інформації у формі відкритих даних» (реєстр. № 2171 від 19.02.2015 р.) URL: <http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=54100&pf35401=330839>
- 77.Витяг з протоколу засідань Комісії при Президенті України по підготовці пропозицій про статус, порядок діяльності і структуру Ради національної безпеки 10 лютого 1992 р. № 31/92-пп URL: <http://zakon3.rada.gov.ua/laws/show/31/92-%D1%80%D0%BF>
- 78.Виявлено порушення права на доступ до публічної інформації у Головному управлінні Національної поліції в Івано-Франківській області URL:<http://www.ombudsman.gov.ua/ua/all-news/all-activity/4116-lm-viyavleno-porushennya-pravana-dostup-do-publichnoii-informatsiii-u-g/> (дата звернення: 04.09.2017)
- 79.Віртуальний світ – це вже реальність. Секонд лайф. (Новини ТСН, 17.06.07). URL:[www.pokrovka.2bb.ru/viewtopic.php?id=15](http://www.pokrovka.2bb.ru/viewtopic.php?id=15)]. (дата звернення: 04.03.2015)
- 80.Войтович П. П. Проблеми міжнародно-правового регулювання інформаційної безпеки. Міжнародні читання з міжнародного права пам'яті проф. П.Є. Казанського: Матер. третьої міжнар. наук. конф. Одеса, 2–3 листопада 2012 р. Одеса :Фенікс, 2012. С. 42-44.
- 81.Волошина Н.М. Поняття «безпека інформації» та «інформаційна безпека» в сучасному науковому просторі. Сучасні інформаційні технології у сфері безпеки та оборони. 2010. № 2. С. 53-56.

- 82.Гарантувати безпеку/ Мова – ДНК нації. URL: <https://ukr-mova.in.ua/library/inshe/garantuvati-bezpeku> (дата звернення: 04.03.2017)
- 83.Герасимова И. А. Диалог культур и когнитивная эволюция. Эволюция. Мышление. Сознание. М.: Канон, 2004. С. 169 -227.
- 84.Гиппократ. Избранные книги URL: <http://lechebnik.info/423/11.htm>.
- 85.Гілевич Л. Соцмережі під захистом ЄС: роботодавцям прикривають доступ до особистої інформації URL: [https://www.eurointegration.com.ua/experts/2017/07/24/7068910/view\\_print/](https://www.eurointegration.com.ua/experts/2017/07/24/7068910/view_print/) (дата звернення: 11.10.2017)
- 86.Глобальний звіт про розвиток інформаційних технологій-2015 URL: <http://edclub.com.ua/analitika/riven-rozvytku-informaciy-no-komunikaciy-nyh-tehnologiyv-ukrayini-ta-sviti> (дата звернення: 24.09.2016)
- 87.Голіна В.В. Запобігання злочинності (теорія і практика): навч. посіб. Х.: Нац. юрид. акад. України, 2011. 120 с.
- 88.Головатий С. Верховенство права: Моногр. у 3-х кн. Київ: Вид-во «Фенікс», 2006. 1747 с.
- 89.Головенко Р. Право засобів масової інформації на поширення інформації як складова свободи слова. URL: <http://ru.telekritika.ua/daidzhest/print/8620> (дата звернення: 10.05.2017)
- 90.Головенко Р.Б., Котляр Д.М., Слизьконіс Д.М. Доступ до публічної інформації: посібник із застосування «трискладового тесту». К.: ЦПСА, 2014. 152 с.
- 91.Головченко В. Правові механізми формування правосвідомості студентів. Право України. 2006. № 9. С. 100-103.
- 92.Голубев С.А. К 150-летию Государственного банка России (историко-правовой аспект. *Деньги и кредит*. 2010. № 6. С. 3-14.
- 93.Гольев Ю.И., Ларин Д.А., Тришин А.Е., Шанкин Г.П. Криптография: страницы истории тайных операций. М.: Гелиос АРВ, 2008. 288 с.
- 94.Горбань О.М., Бахрушин В.Є. Основи теорії систем та системного аналізу. Запоріжжя: ГУ ЗІДМУ, 2004. 204 с.

95. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. Вісник Національної академії державного управління при Президентові України. 2015. № 1. С. 136-141.
96. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. Вісник Київського університету імені Т. Шевченка. 1999. Вип.14: Міжнародні відносини. С. 46-48.
97. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу URL:[https://dt.ua/internal/gibridna-viyna-yak-klyuchoviy-instrumentrosiyskoyi-geostrategiyi-revanshu-\\_html](https://dt.ua/internal/gibridna-viyna-yak-klyuchoviy-instrumentrosiyskoyi-geostrategiyi-revanshu-_html) (дата звернення: 04.03.2017)
98. Городенко Л.М. Цифрова та інформаційна нерівність у мережевій комунікації.
99. Государственные стратегии кибербезопасности URL:  
<http://www.bezpeka.com/ru/lib/sec/gen/government-cybersecurity-strategy.html>  
(дата звернення: 04.03.2017)
100. Грачев Г.В. Мельник И.К. Манипулирование личностью: Организация, способы и технологии информационно-психологического воздействия. М.: Алгоритм, 2002. 228 с.
101. Губерський Л. Філософія: Навч. посіб. для студ. і аспір. вищих навч. закл. К.:Вікар, 2005. 516 с.
102. Гурковський В.І. Деякі організаційно-правові питання взаємовідносин органів державної влади в сфері інформаційної безпеки. Правове, нормативне та метро-логічне забезпечення системи захисту інформації в Україні. 2002. Вип. 5. С. 87.
103. Гурковський В.І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: автореф. дис. ... канд. юрид.наук: 25.00.02 / Національна академія державного управління при Президентові України. Київ, 2004. 22 с.
104. Гуцу С. Ф. Правові основи інформаційної діяльності: Навч. посібник Х.: Нац. Аерокосм. Ун-т «Харк. авіац. ін. -т», 2009. 48 с.
105. Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: сутність, структура та напрямки реалізації. Х. : ФОЛІО, 2002. 285 с
106. Давидов С. А. Социология: консп. лекций. М., Изд-во: Эксмо; 2008. 160 с.

107. Дворовий М. Як регулюватиметься Інтернет в Україні в 2017-2019 роках? Оцінка ризиків та рекомендації URL: <http://netfreedom.org.ua/jak-reguliuvatymetsia-internet-v-ukraini/>
108. Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» від 12.12.2003. URL: [http://zakon2.rada.gov.ua/laws/show/995\\_c57](http://zakon2.rada.gov.ua/laws/show/995_c57)
109. Дем'яненко М. Електронне декларування: суспільний резонанс і політичні прогнози. Україна: події, факти, коментарі. 2016. № 21. С. 7–15.
110. Дембо Л.И., Вальтер Ф.А. Врачебная тайна. Л., 1926. 36 с.
111. Денисенко вважає, що був прийняти «дуже» сирий «закон», який може мати негативні наслідки. URL: <https://ua.112.ua/polityka/nardep-denysenko-vvazhaieshcho-e-deklaratsii-mozhut-staty-priamoiu-navodkoiu-dlia-zlochyntsiiv-334219.html>(дата звернення: 11.09.2016)
112. Державна інформаційна політика URL:[http : // merega. org. ua / law / projects / derzh polityka](http://merega.org.ua/law/projects/derzh-polityka). (дата звернення: 15.11.2016)
113. Державно-правові проблеми інформаційної безпеки людини і суспільства в умовах інтеграції України у світовий інформаційний простір: Звіт про науково-дослідну роботу НДПП НАПрН України. Київ, 2016. 364 с.
114. Деякі рекомендації по відродженню інтересу української громадськості до Відкритих даних. URL: <https://www.prostir.ua/?blogs=deyaki-rekomendatsiji-povidrodzhennyu-interesu-ukrajinskoji-hromadskosti-do-vidkrytyh-danyh> (дата звернення: 04.03.2017)
115. Дзьобань О.П. Соціокультурні аспекти інформаційної безпеки Зовнішня торгівля: економіка, фінанси, право. 2013. № 2. С. 171-176.
116. Дзьобань О.П., Пилипчук В.Г. Інформаційне насильство та безпека: світоглядно-правові аспекти: Моногр. Х.: Майдан, 2011. 244 с.
117. Довгань О. Д. Теоретико-правові основи забезпечення інформаційної безпеки України: автореферат... д-ра юрид. наук, спец.: 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право / Ін-т законодавства ВР України.К., 2016. 44 с.

118. Довгань О.Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти: моногр. К.: НАПрН України, НДПП, НАН України, Нац. б-ка України ім. В.І. Вернадського, 2015. 388 с.
119. Доктрина інформаційної безпеки України – це лише декларація  
URL: <http://www.radiosvoboda.org/a/28336852.html> (дата звернення: 29.05.2017)
120. Доктрина інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 514/2009. URL: <http://www.president.gov.ua/documents/9570.html>
121. Доктрина інформаційної безпеки України, затв. Указом Президента України від 25 лютого 2017 р. № 47/2017 URL:  
<http://www.president.gov.ua/documents/472017-21374>
122. Домарєв В.В., Швець В.А., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом: Навч. пос. К.: НАУ, 2006. 108 с.
123. Донбас Медіа Форум: інформаційний простір та інформаційна політика в умовах війни URL: <http://www.isdpa.org.ua/news/donbas-media-forum-informaciyniuyprostir-tainformaciyna-politika-v-umovah-viyni> (дата звернення: 26.08.2017)
124. Дорожня карта Партнерства у сфері стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО URL: [http://mfa.gov.ua/mediafiles/sites/nato/files/Roadmap\\_Ukr.pdf](http://mfa.gov.ua/mediafiles/sites/nato/files/Roadmap_Ukr.pdf)
125. Дослідження проведене соціологічною службою Центру Разумкова з 21 по 26 квітня 2017 р.. URL: [https://dt.ua/POLITICS/prezidentu-ukrayini-doviryayut-22-gromadyan-uryadu-13-radi-9-242814\\_.html](https://dt.ua/POLITICS/prezidentu-ukrayini-doviryayut-22-gromadyan-uryadu-13-radi-9-242814_.html) (дата звернення: 04.08.2017)
126. Доступность Интернета для людей с ограниченными возможностями URL: <https://www.internetsociety.org/sites/default/files/bp-accessibilitypaper-20121105-ru.pdf> (дата звернення: 04.09.2017)
127. Дубенко Л. Соціальні мережі : реальні загрози віртуального світу. URL: [www.ogo.ua/articles/toprint/2011-02-23/26490.html](http://www.ogo.ua/articles/toprint/2011-02-23/26490.html)
128. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: моногр. К.: НІСД, 2014. 328 с.
129. Европейский центр борьбы с киберпреступностью отчитался за первый год работы URL: <http://www.interfax.ru/world/357250> (дата звернення: 22.07.2017)

130. Ежевская Т.И. Психологическое воздействие информационной среды на современного человека. Психопедагогика в правоохранительных органах. 2012. No3(27) URL: <https://cyberleninka.ru/article/n/psihologicheskoe-vozdeystvieinformatsionnoy-sredy-na-sovremennogo-cheloveka> (дата звернення: 11.03.2015)
131. Електронне врядування в Грузії. URL: <http://gurt.org.ua/news/recent/7822/> (дата звернення: 04.08.2017)
132. Елементи для створення глобальної культури кібербезпеки, затв. Резолюцією 57/239 ГА ООН від 20.12.2002 URL: [http://zakon2.rada.gov.ua/laws/show/en/995\\_b42](http://zakon2.rada.gov.ua/laws/show/en/995_b42) (дата звернення: 04.03.2015)
133. Енциклопедичний словник. Том XXXП-А. СПб: Брокгауз-Ефрон, 1901, с.493.
134. Еріксен Т.Г. Тиранія моменту. Швидкий і повільний час в інформаційну добу /пер. з англ. В. Дмитрука. Л.: Кальварія, 2004. 196 с.
135. Етимологічний словник української мови : у 7 т. Т. 1. К.: Наукова думка. 1982.632 с.
136. Євдоченко Л. О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації: автореф. дис. канд. наук з держ. упр.: 25.00.01 / Львівський регіональний інститут державного управління Національної академії державного управління при Президентові України. Львів, 2011. 24 с.
137. Єдиний демографічний реєстр порушує права людини і принципи верховенства права. URL: <http://pravo.org.ua/ua/news/4960-> (дата звернення: 23.07.2017)
138. Єленський В. Глобальні тенденції релігійного розвитку у XXI столітті URL:[https://risu.org.ua/ua/index/studios/studies\\_of\\_religions/32037/](https://risu.org.ua/ua/index/studios/studies_of_religions/32037/) (дата звернення:04.03.2017)
139. Єсімов С. Право на доступ до інформації – ключовий елемент громадського контролю . Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки : зб. наук. праць. 2016. № 855. С. 63–72



140. Єсімов С.С. Телекомунікаційне право як одна з частин інформаційного права .Наук. записки Львівського ун-ту бізнесу та права. 2013. Вип. 10. С. 171-174.
141. Жарков Я. Небезпеки особистості в інформаційному просторі. Юридичний журнал. 2007. №2. URL: <http://www.justinian.com.ua/article.php?id=2554> (дата звернення: 09.10.2015)
142. Живайкина А.А., Кузнецова М.Н. Интеракция больных с нарушениями психи-ческого здоровья на платформе Интернета. Бюллетень медицинских Интернет-конференций. 2016. Т. 6. №1. С.184-187.
143. Забара І.М. Міжнародна інформаційна безпека: сучасні концепції в міжнародному праві. Теорія і практика правознавства. 2013. Вип. 2. URL: [http://nbuv.gov.ua/UJRN/tipp\\_2013\\_2\\_77](http://nbuv.gov.ua/UJRN/tipp_2013_2_77) (дата звернення: 15.09.2017)
144. Забара І.М. Міжнародне інформаційне право: актуальні проблеми: Наук. доп.Київ, 2011. 23с.
145. Загальна декларація прав людини, прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 р.  
URL:[http://zakon5.rada.gov.ua/laws/show/995\\_015](http://zakon5.rada.gov.ua/laws/show/995_015)
146. Закликаємо припинити переслідування журналістів у Криму URL:  
URL:<https://docs.google.com/document/d/1krMs7UCaB5MTp5hRGbg9jZwaqOV3pdoInTjaPXsgpuY/edit> (дата звернення: 04.08.2017)
147. Запорожець О.Ю. Політика Європейського Союзу в сфері інформаційної безпеки. Актуальні проблеми міжнародних відносин : зб. наук. пр. / Київський нац.ун-т ім. Тараса Шевченка, Ін-т міжнар. відносин. Київ, 2009. Вип.87. Ч.2. С.36-45.
148. Захист інформаційних ресурсів в інформаційно-телекомунікаційних системах: матеріали круглого столу. Київ: [б. в.], 2001. 212 с.
149. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. Видання офіційне. Київ, Держстандарт України, 1996.
150. Захист інформації. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. Видання офіційне. Київ, Держстандарт України, 1997.

151. Згуровський М.З. Шлях до інформаційного суспільства – від Женеви до Тунісу. Тернистий шлях до відродження. К.: Генеза, 2010. 368 с.
152. Зеров К. О. Фіксація змісту веб-сторінки в мережі Інтернет як елемент здійснення права на захист авторських прав на твори, розміщені в мережі Інтернет. Юридичний Інтернет ресурс Протокол URL: [http://protokol.com.ua/ua/fiksatsiya\\_zmistu\\_veb\\_storinki\\_v\\_meregi\\_internet\\_yak\\_element\\_zdiysnennya\\_prava\\_na\\_zahist\\_avtorskih\\_prav\\_na\\_tvori\\_rozmishcheni\\_v\\_meregi\\_internet/](http://protokol.com.ua/ua/fiksatsiya_zmistu_veb_storinki_v_meregi_internet_yak_element_zdiysnennya_prava_na_zahist_avtorskih_prav_na_tvori_rozmishcheni_v_meregi_internet/) (дата звернення: 09.02.2018)
153. Зозуля О. С. Зарубіжний досвід державного управління забезпеченням інформаційної безпеки в умовах інформаційно-психологічного протистояння. *Науково-інформаційний вісник Академії національної безпеки*. 2016.- № 1-2. С. 28-36.
154. Зозуля О.С. Інституційна система державного управління інформаційною безпекою України: сучасний стан та шляхи удосконалення. *Інвестиції: практика та досвід*. К., 2015. №6. С. 147-153
155. Зозуля О.С. Основи публічного управління інформаційною безпекою України в умовах соціальних трансформацій. Публічне управління: шляхи розвитку: мат. наук.-практ. конф. (Київ, 26 лист. 2014 р.). К.: НАДУ, 2014. Т. 1. С. 110-111.
156. Зозуля О. С. Державне управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протистояння. дис. ... канд. наук з держ. упр.: 25.00.01 / Національна академія державного управління при Президентові України. Київ, 2017. 251 с.
157. Золотар О. Информационная безопасность человека: доктринальные подходы к определению категории. SCI-ARTICLE.RU: науч. период. электрон. журн. 2017. № 52 (декабрь). URL: <http://sci-article.ru/stat.php?i=1513689444>.
158. Золотар О.О. Віртуальна реальність. Моделі колективної безпеки: інформаційний вимір: Зб. мат. / Упоряди. Ланде Д.В. К.: НДЦП НАПрН України, 2011 С. 63-66.
159. Золотар О.О. Генеза охорони і захисту інформації в Україні: історико-правовий аспект. Державна політика цивільної авіації ХХІ ст.: економічні і

- стратегічні можливості України: Мат. наук.-прак. конференції, Київ, 19-20 лютого 2009 р. К.: Вид-во Європ. Ун-ту, 2009. С. 118-129
160. Золотар О.О. Генеза суспільних відносин щодо інформаційної безпеки людини. *Інформація і право*. 2018. №1(24). С. 139-148.
  161. Золотар О.О. Досвід правового забезпечення інформаційної безпеки в країнах Східного Партнерства ЄС (Молдова, Грузія). *Lex Portus*. 2017. №3 (5) С.70-80.
  162. Золотар О.О. Електронна демократія і цифрова диктатура. *Інформація і право*. 2017. №4(23). С. 16-25.
  163. Золотар О.О. Загрози інформаційній безпеці людини. *Правова інформатика*. 2014. № 2(42). С. 80-89.
  164. Золотар О.О. Інформаційні революції: соціально-правове значення. *Публічне право*. 2017. № 2(26). С. 40-46.
  165. Золотар О.О. Критичне мислення як необхідна умова безпеки людини в інформацій-ному суспільстві: соціально-правовий аналіз. *Інформаційна безпека людини, суспільства, держави*. 2018. № 3(23).
  166. Золотар О.О. Обмеження доступу до інформації: інформаційно-правовий аспект *Інформаційна безпека людини, суспільства, держави*. 2012. № 1(8). С. 74-80.
  167. Золотар О.О. Особливості інформаційної безпеки людини в умовах гібридної війни. *Інформація і право*. 2017. № 3(22). С. 124-131.
  168. Золотар О.О. Правова охорона як складова інформаційної безпеки: монографія. К.: ТОВ «ПанТот», 2011. 100 с.
  169. Золотар О.О. Правове регулювання знищення інформації. *Правова інформатика*. 2012. № 1(33). С. 39-44.
  170. Золотар О.О. Правовий статус людини в інформаційному суспільстві. *Юридичний науковий електронний журнал*. 2018. № 1. URL: [http://lsey.org.ua/1\\_2018/25.pdf](http://lsey.org.ua/1_2018/25.pdf)
  171. Золотар О.О. Про поняття “інформаційний шум” у правовідносинах. *Інформація і право*. 2012. № 1(4). С. 70-74.

172. Золотар О.О. Свобода інформації в контексті концепції природного права.  
*Правова інформатика*. 2011. № 1(29). С. 12-16.
173. Золотар О.О., Трубін І.О. Класифікація загроз інформаційній безпеці.  
*Інформація і право*. 2013. № 3(9). С. 105-114.
174. Измозик В.С. Черный кабинет. К истории перлюстрации в России. *Родина*. 2000. № 10. С. 48–54. Федотов Н.Н. Тайна связи против технических средств защиты информации в Интернете URL:<http://forensics.ru/zi-ts.html>
175. Информационная безопасность (2-я книга социально-политического проекта. «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009. 456с.
176. Інтернет-залежність. URL: <http://megasite.in.ua/5168-internet-zalezhnistspravzhnisinka-narkotichna-prihilnist.html> (дата звернення: 04.11.2016)
177. Інформаційна безпека (соціально-правові аспекти): Підр. / Остроухов В.В., Петрик В.М. та ін.; за ред. Є. Д. Скулиша. – Київ : КНТ, 2010. 776 с.
178. Інформаційна безпека України в умовах євроінтеграції: Навч. посіб. / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський. К.: КНТ, 2006. 280 с.
179. Інформаційне суспільство. К., 2012. Вип. 16. 64 с.
180. Інформаційний вплив: теорія і практика прогнозування : Моногр. / За ред. П.Д.Фролова. К.: Міленіум, 2011. 304 с.
181. Інформаційний комісар: хто захищатиме доступ до інформації .  
URL:<https://dostup.pravda.com.ua/stories/publications/informatsiinyi-komisar-khtozakhyshchatyme-dostup-do-informatsii> (дата звернення: 04.03.2017)
182. Інформаційні виклики гібридної війни: контент, канали, механізми протидії :аналіт. доп. / за заг. ред. А. Баровської. К.: НІСД, 2016. 109 с.
183. Історія доступу по-шведськи: королівський указ про свободу друку 1766 р..  
URL: <https://dostup.pravda.com.ua/stories/publications/istoriia-dostupupo-shvedsky-korolivskyi-ukaz-pro-svobodu-druku-1766-roku> (дата звернення:04.11.2017)
184. Історія становлення інституту доступу до інформації у світі та міжнародні стандарти. *Доступ до публічної інформації: від А до Я*. URL: <https://courses.prometheus.org.ua/>

185. Калюжний К.Р. Сутність інформаційних прав людини в науці інформаційного права. *Юридичний вісник*. 2012. № 4(25). С. 55–58.
186. Калюжний Р.А., Баєв О.О. Нормативно-правове забезпечення інформаційної безпеки України. *Правова інформатика*. 2009. № 4(24). С. 5-11.
187. Кант І. Критика практичного розуму. К.: «Юніверс», 2004. 240 с.
188. Капліна О., Маринів В. Правові стандарти Європейського суду з прав людини. *Вісник пр.ратури*. 2007. № 8. С. 65-70.
189. Кастельс М. Галактика Інтернет: Размышления об Интернете, бизнесе и обществе. Екатеринбург: У-Фактория, 2004. 328 с.
190. Кастельс М. Информационная эпоха: экономика, общество и культура. / Пер.с англ. под науч. ред. О.И. Шкаратана. М.: ГУ ВШЭ, 2000. 608 с.
191. Кафтя А.А. Інформаційне законодавство України: стан та тенденції розвитку URL: <http://goal-int.org/informacijne-zakonodavstvo-ukraini-stan-ta-tendenciirozvitku/>(дата звернення: 21.05.2016)
192. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи. К., ІПНБ, НА СБУ, 2004. 472 с.
193. Кібер-буллінг: небезпечне віртуальне «бикування» URL: [http://osvita.mediasapiens.ua/mediaprosvita/research/kiberbullin\\_nebezpechne\\_virtualne\\_bikuvannya/](http://osvita.mediasapiens.ua/mediaprosvita/research/kiberbullin_nebezpechne_virtualne_bikuvannya/) (дата звернення: 09.10.2017)
194. Ковалев Г.А. О системе психологического воздействия (к определению понятия). *Психология воздействия (проблемы теории и практики)* : Сб. науч. тр. / под ред. А.А. Бодалева, Г.А. Ковалева. М.: Наука, 1989. С. 4–5.
195. Коваленко Л.П. Принципи інформаційного права. *Державне будівництво та місцеве самоврядування*. 2012 . № 22. с. 185 – 195.
196. Коваленко І.І., Бідюк П.І., Гожий О.П. Вступ до системного аналізу: Навч. посіб. Миколаїв: МДГУ ім. Петра Могили, 2004. 148 с.
197. Коваленко І.П. Правова соціалізація особистості як процес формування правової культури. *Культура України*. 2011. № 32. С.110-118
198. Коваленко Л. П. Предмет і методи інформаційного права України . *Вісник Харківського національного університету імені В. Н. Каразіна. Серія : Право*. 2014. № 1137, вип. 18. С. 83-86.

199. Кодекс суддівської етики, затв. XI черговим з'їздом суддів України 22.02 2013 р. URL: [http://court.gov.ua/userfiles/Kodex%20sud%20etiki\(1\).pdf](http://court.gov.ua/userfiles/Kodex%20sud%20etiki(1).pdf)
200. Коновалова В. О., Шепітько В. Ю. Юридична психологія: Підр. 2-ге вид., перероб. і доп. Х.: Право, 2008. 240 с.
201. Конвенция об обеспечении международной информационной безопасности від 18.12.1979 № 995\_207. URL: [http://www.mid.ru/foreign\\_policy/official\\_documents/-/asset\\_publisher/CptICkB6BZ29/content/id/191666?p\\_p\\_id=101\\_INSTANCE\\_CptICkB6BZ29&\\_101\\_INSTANCE\\_CptICkB6BZ29\\_languageId=ru\\_RU](http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=ru_RU)
202. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28.12.1981 р. № 994\_326 . URL: [http://zakon0.rada.gov.ua/laws/show/994\\_326](http://zakon0.rada.gov.ua/laws/show/994_326)
203. Конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.2001 № 994\_575. Офіційний вісник України. 2007, 10 вересня. № 65. Ст. 2535.
204. Конвенція про ліквідацію всіх форм дискримінації щодо жінок: Конвенція ООН від 18.12.1979 № 995\_207. URL: [http://www.apc.org/sites/default/files/APC\\_charter\\_RU\\_1\\_2.pdf](http://www.apc.org/sites/default/files/APC_charter_RU_1_2.pdf)
205. Конституція Республики Беларусь. URL: <http://pravo.by/pravovaya-informatsiya/normativnye-dokumenty/konstitutsiya-respubliki-belarus/>
206. Конституція України від 28.06.96 р. № 254/96 ВР: Відомості Верховної Ради (ВВР) України. 1996. № 30. Ст. 141.
207. Копылов В.А. Информационное право. М.: Юристъ, 2002. 512 с.
208. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посіб. К.: Кондор, 2004. 382 с.
209. Кормич Б.А. Інформаційне право: Підр. Х.: БУРУН і К., 2011. 334 с.
210. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: автореф. дис. ...д-ра юр. наук: 12.00.07 / Нац. ун-т внутр. справ. Харків, 2004. 43 с.
211. Косиця О.О. Інституціональний механізм системи інформаційної безпеки Порів-няльно-аналітичне право. 2016. № 4. URL: [http://www.par.in.ua/4\\_2016/45.pdf](http://www.par.in.ua/4_2016/45.pdf). (дата звернення: 25.06.2017)

212. Костецька Т.А. Конституційно-правове регулювання інформаційних прав: деякі термінологічні аспекти. Часопис Київського університету права. 2013. № 2. С. 114-117.
213. Котляр Д. Інформація не може бути об'єктом право власності URL: <https://www.youtube.com/watch?v=nTKYEI-5P0M> (дата звернення: 08.12.2017)
214. Кохановська О.В. Втілення та реалізація ідей розробників ЦК України щодо нормативного закріплення поняття та видів об'єктів цивільних прав. Актуальні проблеми приватного права: зб. стат. до ювілею д.ю.н., проф.. Н.С. Кузнецової /Відп. ред. : Р.А. Майданик та О.В. Кохановська. К.: ПрАТ «Юридична практика», 2014. С. 247–271.
215. Кохановська О.В. Цивільно-правові проблеми інформаційних відносин в Україні. Дис. ... д-ра юрид.наук: 12.00.03. Київ, 2006
216. Кравець Є. А. Інформаційна безпека держави. Юридична енциклопедія: в 6 т. К.:Укр. енцикл., 1992. С. 744.
217. Красноступ Г.М. Організаційно-правові аспекти необхідності реформування су-часного інформаційного законодавства. Право України. 2005. № 9. С. 81—83.
218. Кримінальний кодекс України: кодекс України від 05.04.2001 № 2341-III. ВВР України. 2001. № 25-26. Ст.131.
219. Кримінально-процесуальний кодекс України: кодекс України від 13.04.2012 № 4651-VI. ВВР України. 2013. № 9-10. № 11-13. Ст.88.
220. Крутских А.В., Сафонова И.Л.. Международное сотрудничество в области ин-формационной безопасности. URL: <http://www.ict.edu.ruft002472intcoop.pdf>.pdf (дата звернення: 11.08.2017)
221. Крымов Г. Всемирная сеть мошенников. Жертвой киберпреступников может стать каждый URL: [http://cripo.com.ua/?sect\\_id=6&aid=115837](http://cripo.com.ua/?sect_id=6&aid=115837) (дата звернення: 10.06.2015)
222. Криницький І. Дотримання податкової таємниці як спеціальний принцип податково-процесуального права. Підприємництво, господарство і право. 2007. № 11 (143). С.19-22.

223. Кубі Г.: накидання «гендерної рівності» – це культурне перепрограмування суспільства. URL: <http://credo.pro/2013/05/83148> (дата звернення: 09.10.2017)
224. Лазоренко О.А. Інформаційний складник гібридної війни Російської Федерації проти України: тенденції розвитку. Стратегічні пріоритети. 2015. № 3. С. 124-133.
225. Левицька М.Б. Теоретико-правові аспекти забезпечення національної безпеки органами внутрішніх справ України : дис. ... канд. юрид. наук : 12.00.01/ Київський нац. ун-т внутр. справ. К., 2002. 206 с.
226. Левченко О.В. Проблеми і шляхи формування системи інформаційної безпеки держави. Зб. наук. праць Харків. ун-ту Повітряних Сил. 2014. Вип. 2(39). С. 166-168.
227. Леон П. Хроника Перу. Ч. 2. Владычество Инков.  
URL:<http://kuprienko.info/pedro-cieza-de-leon-cronica-del-peru-parte-segunda-al-ruso/>
228. Лещенко М.П., Тимчук Л.І. Підходи до стандартизації сформованості інформаційно-комунікаційної компетентності учнів: польський досвід. Інформаційні технології і засоби навчання. 2014. Т. 42. № 4. С. 33-46.
229. Линник Г.М. Адміністративно-правове регулювання інформаційної безпеки України : автореф. дис. ... канд. юрид. наук : 12.00.07 / Нац. ун-т біоресурсів і природо-користування України. Київ, 2011. 20 с.
230. Лист НАПрН України в МОН України від 28.11.14 р. № 1226, цит. за Пилипчук В.Г., Беланюк М.В.: Історичні аспекти розробки і впровадження наукової спеціальності 12.00.13 – “інформаційне право; право інтелектуальної власності” Інформація і право. 2016. № 2(17). с.5-17.
231. Лист представника Уповноваженого Верховної Ради України з прав людини від 19.04.2016 р. № 11/15-263366.16-1/НД-107 URL:  
<https://uteka.ua/ua/publication/Oshtrafax-za-neobnarodovanie-publichnoj-informacii-v-forme-otkrytyx-danny> (дата звернення: 09.10.2017)
232. Литвиненко О. Інформація і безпека. Нова політика. 1998. № 1. С. 47-49.
233. Литвиненко О. Проблема інформаційної безпеки в контексті міграційних процесів. URL:



- [http://www.nbuu.gov.ua/portal/soc\\_gum/Ukrain/2012\\_7/lytvynenko.pdf](http://www.nbuu.gov.ua/portal/soc_gum/Ukrain/2012_7/lytvynenko.pdf) (дата звернення: 04.03.2015)
234. Литовченко І. Діти в Інтернеті: як навчити безпеці у віртуальному світі: посібник для батьків / І. Литовченко, С. Максименко, С. Болтівець та ін. К.: Вид. будинок «Аванпост-Прим», 2010. 48 с.
235. Лицевая идентификация может помогать преступникам URL: [http://www.infox.ru/hi-tech/tech/2011/08/02/Licyevaya\\_idyentifik\\_print.phtml](http://www.infox.ru/hi-tech/tech/2011/08/02/Licyevaya_idyentifik_print.phtml) (дата звернення: 19.10.2017)
236. Ліпкан В.А. Національна безпека України: навч. посіб. К.: КНТ, 2009. 576 с.
237. Ліщинська О.А. Культова психічна залежність особистості: передумови, чинники, механізми: монографія. Київ: Легко інк, 2008. 266 с.
238. Логінов О. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: дис. ... кан. юр. наук за спец-тю 12.00.07 / Нац. акад. внутр. справ України. К., 2005. 192 с.
239. Логінов О.В. Гносеологічний аспект управління інформаційною безпекою України . Наук. вісн. Юридичної академії МВС України. 2004. № 2. С. 153-161.
240. Логінова Н.І. Аналіз співвідношення інформаційної та кібернетичної безпеки. Використання сучасних інформаційних технологій в підготовці та професійній діяльності правознавців: мат. І наукової Інтернет-конференції «Нац. ун-ту«Одеська юридична академія» URL: <http://conf.inf.od.ua/doklady-konferentsii> (дата звернення: 10.06.2016)
241. Лоренц К. Агрессия (так называемое «зло») URL: <http://lib.ru/PSIHO/LORENC/agressiya.txt> (дата звернення: 19.10.2017)
242. Лукашевич М.П., Мигович І.І. Теорія і методи соціальної роботи: Навч. посіб. К.: МАУП, 2003. 168 с
243. Лызь Н.А. Развитие безопасной личности в образовательном процессе вуза: Моногр. Таганрог: Изд-во ТРТУ, 2005. 305 с.
244. Магда Є.В. Гібридна війна: вижити і перемогти. Х.: Віват, 2015. 304с.
245. Макаренко Є.А. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст. Актуальні проблеми міжнародних відносин. 2011. Вип.102(1). С. 51-62 .

246. Максименко Т. Мобильник под запретом. Ущемление прав человека или “закон есть закон”? URL: [www.mobiset.ru/articles/text/?id=3280&printer=ok](http://www.mobiset.ru/articles/text/?id=3280&printer=ok).  
(дата звернення: 19.10.2017)
247. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: автореф. дис... канд. юрид. наук: 12.00.01 / Київ. нац. ун-т внутр.справ. Київ, 2007. 20 с.
248. Малик Я.Й. Інформаційна безпека України: стан та перспективи розвитку. Ефек-тивність державного управління: Зб. наук. праць. 2015. Вип. 44. С. 13-20.
249. Маритен Ж. От Бергсона к Фоме Аквинскому. Очерки метафизики и этики: Моногр. Серия: Bibliotheca Ignatiana, Ин-т философии, теологии и истории св. Фомы, 2006, 216 с.
250. Марущак А. І. Інформаційне право України: Підр. К.: Дакор, 2011. 456 с.
251. Марущак А.І. Визначення поняття “інформаційні права людини”. Інформація і право. 2011. № 2(2). С. 21 – 26.
252. Марущак А.І. Інформаційне право: Доступ до інформації: Навч. посіб. К.: КНТ, 2007. 532 с
253. Марценюк О.Г. Теоретико-методологічні засади інформаційного права України: реалізація права на інформацію: дис. ... канд. юрид. наук : 12.00.07. К., 2009. 266 с.
254. Марчукова С.М. Медицина в зеркале истории. М. : Европейский Дом, 2003. 272 с.
255. Матюхіна Н.П. Приватний сектор безпеки: нові реалії сучасного простору безпеки України / Матюхіна Наталія Петрівна // Приватний сектор безпеки: сучасний досвід та проблеми правового регулювання : зб. тез доп. І Міжнар. наук.-практ. конф. (м. Харків, 19 квіт. 2013 р.) / Нац. ун-т. «Юрид. акад. України ім. Ярослава Мудрого». Х. : Мадрид, 2013. С. 7–11.
256. Международное право: Учеб. для вузов / Отв. ред. проф. Г.В. Игнatenко и проф. О.И. Тиунов. М.: Изд. группа НОРМА-ИНФРА, 1999. 584 с., с. 359
257. Мельник К.С. Іноземний та вітчизняний досвід становлення інституту захисту персональних даних. Інформаційна безпека людини, суспільства, держави. 2013. № 2 (12). С. 97-103.

258. Мерило Я. Электронное государство: опыт Эстонии для Украины:  
URL:<http://forbes.ua/opinions/1374119-elektronnoe-gosudarstvo-opyt-estonii-dlya-ukrainy>.(дата звернення: 19.10.2017)
259. Мищериков А.А. Безопасность и свобода личности в информационном обществе: анализ проблемы. Теория и практика общественного развития. 2011.№ 1. URL: <http://cyberleninka.ru/article/n/bezopasnost-i-svoboda-lichnosti-v-informatsionnom-obschestve-analiz-problemy> (дата звернення: 02.02.2016)
260. Міжнародна інформаційна безпека: Сучасні виклики та загрози / Макаренко Є.А., Рижигов М.М. та ін. Київ: Центр вільної преси, 2006. 916 с.
261. Монтеск'є Ш.Л. О духе законов. М.: Мысль, 1999. 672 с.
262. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. Віче. 2007. №12. С. 23-25.
263. Мукомела І.В. Право на доступ до Інтернету: проблеми визначення та забезпечення. Вісник Національної академії правових наук України. – 2016. № 4. С. 77-85.
264. Мурашкевич О.А., Черних О.О. Освіта в сфері прав людини в Інтернеті: Метод.посіб. К.: ВАІТЕ, 2015. 70 с.
265. Нагнічук О.І. Співвідношення права на свободу вираження щодо публічних осіб та права на повагу до приватного та сімейного життя публічних осіб у практиці Європейського суду з прав людини URL: [http://ekmair.ukma.edu.ua/bitstream/handle/123456789/7831/Nahnichuk\\_Spivvidno-shennia\\_prava\\_na\\_svobodu.pdf](http://ekmair.ukma.edu.ua/bitstream/handle/123456789/7831/Nahnichuk_Spivvidno-shennia_prava_na_svobodu.pdf) (дата звернення: 06.09.2017)
266. Найдьонова Л.А. Кібер-булінг або агресія в інтернеті: способи розпізнання і захист дитини. Методичні рекомендації. Серія: На допомогу вчителю. 2011. Вип. 4. 34 с.
267. Наливайко Л.Р. Інформаційна безпека та інформаційна політика в Україні: кон-ституційно-правовий аспект. Вісник Запорізького державного університету.2003. №1. С. 60-65.
268. Настюк В.Я., Белєвцева В.В. Адміністративно-правовий захист інформації: проблеми та шляхи вирішення. Х.: Право, 2013. 128 с.

269. Науково-методичне забезпечення реалізації концепції New Public Management : наук. розробка. Ю.П. Шаров, І.А. Чикаренко, Т.В. Маматова, Е.О. Сергієнко. К.: НАДУ, 2013. 92 с.
270. Национальный ИКТ-профайл Азербайджана. Часть 7: Информационная приватность URL: <https://digital.report/azerbaydzhan-informatsionnaya-privatnost/> (дата звернення: 19.10.2017)
271. Национальный ИКТ-профайл Армении. Часть 6: Информационная безопасность и защита информации URL: <https://digital.report/armeniya-informatsionnayabezopasnost/> (дата звернення: 19.10.2017)
272. Национальный ИКТ-профайл Грузии. Часть 4: Доступ в интернет и интернет-услуги URL: <https://digital.report/gruziya-dostup-v-internet/> (дата звернення: 19.10.2017)
273. Национальный ИКТ-профайл Молдовы. Часть 6: Информационная безопасность и защита информации. URL: <https://digital.report/moldova-informatsionnayabezopasnost/> (дата звернення: 19.10.2017)
274. Некрасов Н.А. Полное собрание сочинений и писем в 15-ти томах. Том 1. Л.:Наука, 1981. 719 с.
275. Нестеренко О. Інформаційний омбудсман в механізмі забезпечення прав людини і основоположних свобод. Бюлетень «Права людини». 2008. № 17. URL: <http://khpg.org/index.php?id=1216383271> (дата звернення: 22.04.2015)
276. Нижник Н.Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): Навч. посіб. / Н.Р. Ситник, Г.П. Ситник, В.Т., В.Т. Білоус; за заг. ред. П.В. Мельника, Н.Р. Нижника. Ірпінь, 2000. 304с.
277. Німецькі поборники приватності угледіли загрозу в соціальній мережі Facebook, а точніше в улюбленій користувачами кнопці like. URL: <http://briz.if.ua/9590.htm> (дата звернення: 08.09.2017)
278. Новая философская энциклопедия: в 4 т. / Институт философии РАН; Национальный общественно-научный фонд; М.: Мысль, 2000—2001. URL: <http://iphlib.ru/greenstone3/library/collection/newphilenc/document/HASH131792c7772ffa4b7f4613> (дата звернення: 19.02.2015)

279. Новицька Н.Б. Правові аспекти зловживання правом на свободу слова та інформації Науковий вісник Нац. ун-ту держ. податкової служби України (економіка,право). 2013. № 4. С. 60-66.
280. О государственных секретах: Закон Республики Беларусь от 19.07.2010 р. № 170-3. URL: <http://www.kgb.by/ru/zakon170-3/printv>
281. О информации, информатизации и защите информации: Закон Республики Бела-русь от 10 ноября 2008 г. № 455-3. URL: <http://pravo.by/document/?guid=3871&p0=h10800455>
282. О некоторых проблемах информационной безопасности. Ереван: НОФ «Нораванк», 2009. 236с.
283. О принципах построения кредитной системы: Постановление ЦИК и СНК от 15.06.1927 г. Собр. законодательства СССР. 1927. № 35. Ст. 364.
284. Об авторском праве и смежных правах: Закон Республики Беларусь от 17.05.2011 р. №262-3. URL: [https://base.spinform.ru/show\\_doc.fwxrgn=43409](https://base.spinform.ru/show_doc.fwxrgn=43409)
285. Об архивном деле и делопроизводстве в Республике Беларусь: Закон Республики Беларусь от 25.11.2011 р. №323-3. URL: <http://pravo.newsby.org/belarus/zakon0/z194.htm>
286. Общая политика США в сфере информационной безопасности URL: <http://www.INTUIT.ru>. (дата звернення: 25.12.2016)
287. Окинавская хартия глобального информационного общества : рекомендации стран „восьмерки“ о принципах и направлениях развития информационного общества. Окинава, 22 июля 2000 г. Дипломатический вестник, 2000, № 8, с. 51-56.
288. Олійник О. В. Державна політика інформаційної безпеки України. *Юридичний вісник. Повітряне і космічне право*. 2012. № 4. С. 65-69.
289. Олійник О.В. Нормативно-правове забезпечення інформаційної безпеки в Україні. *Право і суспільство*. 2012. № 3. С. 132-137.
290. Олійник О.В. Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки України. Моногр. К., Вид. підпр-во «Український пріоритет», 2012. 400 с.

291. Опорний конспект лекцій з електронного урядування / Дзюба С.В., Жиляєв І.Б. та ін., за ред. А.І. Семенченка. К., [б.в.] 2012. 266 с.
292. Орбан-Лембрик Л. Б. Соціальна психологія: Навч. посіб. К.: Академвидав, 2005. 448 с.
293. Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посіб. Стоцький А.Б., Тимошенко О.І., Гуз А.М. та ін. К. : Європ. ун-т, 2006. 232 с.
294. Основи інформаційного права України: навч. посіб. / Цимбалюк В.С., Гавловський В.Д., Гриценко В.В. та ін.; За ред. М.Я. Швеця, Р.А. Калюжного та П.В.Мельника. К.: Знання, 2004. 274 с.
295. Основы немецкого торгового и хозяйственного права [Grundzüge des deutschen Handels- und Wirtschaftsrechts]. М.: БЕК, 1995. 288 с.
296. Осторожно: Кибербуллинг!  
URL:<http://darkermagazine.ru/page/ostorozhnokiberbulling> (дата звернення: 18.09.2017)
297. Панов М., Тихий В. Безпека як фундаментальна категорія в методології правознавства (до постановки проблеми). Вісник Академії правових наук України. Х. : Право, 2000. № 3(22). С. 10-16.
298. Пазюк А.В. Інтеграція України в Європейське інформаційне суспільство виклики та завдання. К.: ФОП Клименко, 2014. 212 с.
299. Пазюк А.В. Міжнародно-правовий режим кіберпростору в мирний час  
Право і суспільство. 2014. № 1.2. С. 313-315.
300. Пазюк А.В. Правовий аналіз Указу Президента щодо блокування доступу до ресурсів Інтернету . URL:<http://moe-pravo.com.ua/pravoviy-analiz-ukazu-prezidentashhodo-blokuvannya-dostupu-do-resursiv-internetu/> (дата звернення: 19.09.2017)
301. Парламент ухвалив два закони щодо доступу до відкритих даних  
<http://www.telekritika.ua/pravo/2015-04-09/105929> (дата звернення: 19.09.2016)
302. Пастернак-Таранушенко Г.А. Економічна безпека держави. Методологія забезпечення: Моногр. К.: Київ. екон. ін-т менедж., 2003. 320 с.

303. Пахнін М.Л. Особливості державної інформаційної політики в розвинених країнах світу. Теорія та практика державного управління. 2014. Вип. 4. С. 414-422.
304. Петрик В. Канарський Ю. Методи гібридної війни Росії проти України. Напрями протидії. Information Technology and Security. 2015. Vol. 3, № 1. С. 30-37.
305. Петрик В. М. Інформаційна безпека (соціально-правові аспекти): підруч. В.М.Петрик, В.В. Остроухов, М.М. Присяжнюк та ін. К.: КНТ, 2010. 771 с.
306. Петрик В.М. Забезпечення інформаційної безпеки держави: підручник; за заг.ред. О.А. Семченка та В.М. Петрика. Київ: ДНУ «Книжкова палата України», 2015. 672 с.
307. Петрицький А.Л. Інформаційне законодавство України: актуальні проблеми та шляхи їх вирішення. Вісник Маріупольського державного університету. Серія: право. 2013. Вип. 5. С. 64-68.
308. Петров В.П., Петров С.В. Информационная безопасность человека и общества: учеб. пособ. М.: ЭНАС, 2007. 334 с.
309. Петров Є.В. Інформація як об'єкт правовідносин . Вісник Національного Уні-верситету внутрішніх справ; Спецвипуск. 2001. С. 249–252.
310. Петрухин И.Л. Личные тайны (Человек и власть) М. : Институт государства и права РАН, 1998. 232 с.
311. Питання діяльності Міністерства інформаційної політики України: Постанова Кабінету Міністрів України від 14 січня 2015 р. № 2 URL: <http://zakon5.rada.gov.ua/laws/show/2-2015-%D0%BF> (дата звернення 07.01.2016 р.).
312. Плачинда С. Словник давньоукраїнської міфології. К.: Велес, 2007. С. 181–182.
313. Плешаков А. М. Банковская тайна: запрет, обязанность и порядок предоставленных сведений. *Деньги и кредит*. 1997. № 10. 65 с.
314. Погребняк А.В. Технології комп'ютерної безпеки: Моногр. Рівне: МЕГУ, 2011. 117 с.

315. Покровский И.А. Основные проблемы гражданского права: Монография. М.: Статут, 2001. 353 с.
316. Політанський В.С. Право на інформацію як фундаментальне право людини :Моногр. Х.: Право, 2017. 208 с.
317. Поощрение, защита и осуществление прав человека в Интернете URL: <https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/91/> (дата звернення: 08.06.2017)
318. Порухення прав людини під час конфлікту на Донбасі розглянуть в Раді ООН з прав людини. URL: <https://www.radiosvoboda.org/a/28403693.html> (дата звернення: 36.10.2017)
319. Порухення права на приватність в Україні. URL: <http://forbiddentoforbid.org.ua/uk/porushennya-prava-na-privatnist/> (дата звернення: 19.09.2017)
320. Порядок оформлення матеріалів про адміністративні правопорушення, затв. наказом Уповноваженого Верховної Ради України з прав людини від 16 лютого 2015 року № 3/02-15. URL: [https://hrliga.com/docs/Nakaz\\_3-02-15.htm](https://hrliga.com/docs/Nakaz_3-02-15.htm)
321. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С.,2015. 216 с.
322. Постанова у справі № 800/198/17 від 14.06.2017, Вищий адміністративний суд України. URL: <http://www.reyestr.court.gov.ua/Review/67196698> (дата звернення: 22.08.2017)
323. Потебня А.А. Эстетика и поэтика. М.,»Искусство», 1976. 614 с.
324. Почепцов Г. Гібридна війна: інформаційна складова. URL: [http://osvita.mediasapiens.ua/trends/1411978127/gibridna\\_viyna\\_informatsiyna\\_skladova/](http://osvita.mediasapiens.ua/trends/1411978127/gibridna_viyna_informatsiyna_skladova/) (дата звернення: 23.12.2017)
325. Права людей з інвалідністю. URL: <https://www.helsinki.org.ua/%2Fwp-content%2Fuploads%2F2016%2F02%2FPrava-lyudej-z-invalidnistyu-Mojisa.doc&usg=AFQjCNGslANQQivOhD7KsJh1JwTlgcWdgQ&sig2=w9fvh0rLbIib0-eB1VfJ8g> (дата звернення: 19.09.2017)
326. Права людини в Криму. «Крим SOS». URL: <http://crimeamap.krymsos.com/ru/map.html> (дата звернення: 19.11.2017)



327. Правдін І. Шевчук: потрібно запроваджувати фейсбук-ідентифікацію адвокатів .Вектор Ньюз «НОВИНИ», Політика та право від 11.12.2016 р. URL: <https://www.vectornews.net/news/politics/21456-oleksy-shevchuk-potrбно-zaprovadzhuvatifeysbuk-dentifikacyu-advokatv.html>. (дата звернення: 20.12.2016)
328. Правила адвокатської етики, затв. Звітно-виборним з'їздом адвокатів України 9.06.2017 р. URL: [http://unba.org.ua/assets/uploads/3ae9a115a40b9a5bc04f\\_file.pdf](http://unba.org.ua/assets/uploads/3ae9a115a40b9a5bc04f_file.pdf) (дата звернення: 19.08.2017)
329. Право на доступ до інформації: еволюція підходів Європейського суду з прав людини. URL: [http://cedem.org.ua/analytics/pravo-na-dostup-do-informatsiyevolyutsiya-pidhodiv-yevropejskogo-sudu-z-prav-lyudyny/#\\_ftn2](http://cedem.org.ua/analytics/pravo-na-dostup-do-informatsiyevolyutsiya-pidhodiv-yevropejskogo-sudu-z-prav-lyudyny/#_ftn2) (дата звернення: 19.02.2015)
330. Право на інформацію та реалізація інформаційних прав у сфері особистих не-майнових прав людини в Україні / Є.В. Дергачов, О.О. Одінцова. Вісник Нац. техн. ун-ту України «Київський політехнічний інститут». Політологія. Соціологія. Право. 2013. № 2. С. 85-90.
331. Право природы в концепции римских юристов и Цицерона. Древнее право. IVS ANTIQVVM. 2009. № 1 (23).
332. Правова доктрина України (у 5 томах). Том 2 Публічно-правова доктрина України. За заг. ред. Ю. П. Битяка. 864 с.
333. Правозахисники опублікували звіт про порушення прав людини у Криму. URL: <http://www.pravda.com.ua/news/2017/07/30/7150877/> (дата звернення: 05.08.2017)
334. Президент США Дж. Картер и права человека в СССР / НИПЦ «Мемориал» URL: [http://memo.ru/history/diss/carter\\_index.htm](http://memo.ru/history/diss/carter_index.htm)
335. Про авторське право і суміжні права: Закон України від 23 грудня 1993 р. № 3792-12. ВВР України. 1994. № 13. Ст.64.
336. Про бібліотеки і бібліотечну справу: Закон України від 27 січня 1995 р. № 383-18. ВВР України. 2014. № 14. Ст.252.
337. Про внесення змін до деяких законів України щодо доступу до публічної інформації в формі відкритих даних: Закон України від 9.04.2015 р. № 319-VIII. ВВР України. 2015. № 25. Ст.192.

338. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних: Закон України від 03.07.2013 № 383-VII. ВВР України. 2014. № 14. Ст.252.
339. Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції»: Закон України від 02.07.2015 № 577-VIII URL: <http://zakon4.rada.gov.ua/laws/show/577-19>
340. Про внесення змін до Закону України «Про інформацію»: Закон України від 13.01.11 р. Офіційний вісник України. 2011. № 10. Ст. 2.
341. Про державну підтримку засобів масової інформації та соціальний захист журналістів: Закон України від 23.09.1997 р. № 540/97-вр. ВВР України. 1997. № 50. Ст. 302
342. Про державну таємницю: Закон України від 21.01.1994 р. ВВР України. 1994. № 16. Ст.93.
343. Про доступ до публічної інформації від 13.01.2011 № 2939-VI. ВВР України. 2011. № 32. Ст. 314.
344. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.1992 р. № 2782-XII. ВВР України. 1993. № 1. Ст. 1.
345. Про електронний цифровий підпис: Закон України від 22.05.2003 р. № 852-IV. ВВР України. 2003. № 36. Ст.276.
346. Про електронні довірчі послуги: Закон України від 5.10.2017 р. № 2155-VIII. ВВР України. 2017. № 45. Ст.400.
347. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. ВВР України. 2003. № 36. Ст.275.
348. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 р. № 5492-VI. Відомості ВВР України. 2013. № 51. Ст.716.
349. Про запобігання корупції: Закон України від 14 жовтня 2014 р., № 1700-VII. ВВР України. 2014. № 49. Ст.2056.

350. Про засади інформаційної безпеки України: проект Закону № 4949 від 28.05.2014 р. URL: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=51123](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123) (дата звернення 07.01.2016 р)
351. Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій): Рішення Ради національної безпеки і оборони України, введено в дію Указом Президента України від 15.05.2017 р. № 133/2017. URL: <http://zakon2.rada.gov.ua/laws/show/n0004525-174>
352. Про затвердження Державної програми забезпечення позитивного міжнародного іміджу України на 2003-2006 роки: Постанова Кабінету Міністрів України від 15 жовтня 2003 р. № 1609 URL: <http://zakon5.rada.gov.ua/laws/show/1609-2003-%D0%BF> (дата звернення 07.01.2016 р.)
353. Про затвердження Переліку наукових спеціальностей: Наказ Міністерства освіти і науки, молоді та спорту України від 14.11.11 р. № 1057. Освіта України, спецвипуск газети. № 10(22). 2014, жовтень. С. 3.
354. Про затвердження Положення про набори даних, що підлягають опублікуванню в формі відкритих даних: Постанова Кабінету Міністрів України від 21.10.2015 р. № 835. URL: <http://zakon2.rada.gov.ua/laws/show/835-2015-%D0%BF/page2>
355. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29.03.2006 р. № 373. Офіційний вісник України. 2006. № 13.
356. Про захист дітей від інформації, що завдає шкоду їх здоров'ю та розвитку: Мо-дельний закон від 03.12. 2009 р. № 33-15. URL: <http://jurconsult.net.ua/zakonystran-sng>.
357. Про захист інформації в автоматизованих системах: Закон України від 05.07.1994 р. №81/94-ВР; (зі змінами 2013 р. Про захист інформації в інформаційно-телеко-мунікаційних системах). ВВР України. 1994. № 31. Ст.286.

358. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Рішення РНБО, введено в дію Указом Президента № 449/2014 від 01.05.2014. URL:  
<http://zakon0.rada.gov.ua/laws/show/n0004525-14>
359. Про зв'язок: Закон України (втратив чинність) від 16.05.1995 р. №160/95-вр. ВВР України. 1995. № 20. Ст.143.
360. Про інформацію: Закон України від 02.10.92 р. № 2657-12. ВВР України. 1992. № 48. Ст. 650.
361. Про інформаційний суверенітет та інформаційну безпеку України: проект закону № 1207-д від 12.08.1999 р. URL: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=6670](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=6670)
362. Про Комісію з питань інформаційної безпеки: Указ Президента України від 03 лютого 1998 р. № 76/98 URL: <http://zakon3.rada.gov.ua/laws/show/76/98>.
363. Про Концепцію (основи державної політики) національної безпеки України: Постанова Верховної Ради України від 16 січня 1997 рок URL: <http://old.niss.gov.ua/book/otch/roz23.htm>
364. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. № 75/98. ВВР України. 1998. № 27-28. Ст.182.
365. Про науково-технічну інформацію: Закон України від 25.06.1993 р. № 3322-XII. ВВР України. 1993. № 33. Ст.345.
366. Про національний архівний фонд і архівні установи: Закон України від 24.12.1993 р. №3814-XII. ВВР України. 1994. № 15. Ст.86.
367. Про Національну програму інформатизації: Закон України від 4.02.1998 р. № 74/98. ВВР України. 1998. № 27-28. Ст.181.
368. Про Національну раду України з питань телебачення і радіомовлення: Закон України від 23.09.1997 р. № 538/97. ВВР України. 1997. № 48. Ст. 296.
369. Про невідкладні заходи щодо забезпечення інформаційної безпеки України: Рішення, затв. Указом Президента від 23.04.2008 р. № 377/2008. URL:  
<http://zakon3.rada.gov.ua/laws/show/377/2008>
370. Про освіту: Закон України від 05.09.2017 р. № 2145-19. ВВР України. 2017. № 38-39. Ст. 380.

371. Про основи державної політики у сфері науки і науково-технічної діяльності: Закон України від 13.12.1991 р. № 1977-XI. ВВР України, 1992, № 12, ст.165.
372. Про основи національної безпеки України: Закон України : від 19.06.2003 р. № 964-IV. ВВР України. 2003. № 39.
373. Про основні засади забезпечення кібербезпеки України: Закон України від 5.10.2017 р. № 2163-VIII. ВВР України. 2017. № 45. Ст.403.
374. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 9.01.2007 р. № 537-V. ВВР України. 2007. № 12. Ст. 102.
375. Про охорону прав на винаходи і корисні моделі: Закон України від 15.12.1993 р. ВВР України. 1994. № 7. ст. 32.
376. Про Положення про Міністерство України у справах преси та інформації: Указ Президента України від 02 січня 1995 р. N 9/95 URL: <http://zakon5.rada.gov.ua/laws/show/9/95>.
377. Про радіочастотний ресурс України: Закон України від 1.06.2000 р. № 1770-III. Офіційний вісник України. 2000. № 26. Ст. 1079.
378. Про Раду національної безпеки України: Указ Президента України від 01 липня 1992 р. № 357/92 URL: [http://search.ligazakon.ua/l\\_doc2.nsf/link1/U357\\_92.html](http://search.ligazakon.ua/l_doc2.nsf/link1/U357_92.html).
379. Про рекламу: Закон України від 3.07.1996 р. № 270/96-ВР. ВВР України. 1996. № 39. Ст. 181.
380. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 р. № 287/2015 . Офіційний вісник України. 2015. № 43. с. 14. Ст. 1353.
381. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. № 96/2016 URL: <http://zakon5.rada.gov.ua/laws/show/96/2016>
382. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про Доктрину інформаційної безпеки України»: Указ Президента

України від 25 лютого 2017 р. № 47/2017. URL:

<http://www.president.gov.ua/documents/472017-21374>

383. Про Суспільне телебачення і радіомовлення України: Закон України від 17.04.2014 р. № 1227-VII. Відомості Верховної Ради. 2014. № 27. Ст. 904.

384. Про схвалення Концепції проекту Закону України “Про основні засади державної комунікативної політики”: Розпорядження Кабінету Міністрів України від 13 січня 2010 р. № 85-р URL:

<http://zakon0.rada.gov.ua/laws/show/85-2010-%D1%80>.

385. Про схвалення Концепції проекту Закону України “Про основні засади державної комунікативної політики”: Розпорядження Кабінету Міністрів України від 13 січня 2010 р. № 85-р URL::

<http://zakon0.rada.gov.ua/laws/show/85-2010-%D1%80>.

386. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386-р. URL: <http://zakon5.rada.gov.ua/laws/show/386-2013-%D1%80> (дата звернення 07.01.2016 р.)

387. Про телебачення і радіомовлення: Закон України від 21.12.1993 р. ВВР України. 1994. № 10. ст. 43

388. Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV. ВВР України. 2004. № 12. Ст.155.

389. Проект Доктрини інформаційної безпеки, розроблений Державним комітетом телебачення і радіомовлення України URL:

[http://comin.kmu.gov.ua/control/publish/article/main?art\\_id=114348&cat\\_id=32820](http://comin.kmu.gov.ua/control/publish/article/main?art_id=114348&cat_id=32820)

390. Проект Закону про внесення доповнень до Цивільного кодексу України (щодо рантування права фізичної особи на доступ до Інтернету) URL:

[http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=50669](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=50669). (дата звернення: 19.08.2017)

391. Проект Стратегії розвитку інформаційного простору України на період до 2020, розроблений Державним комітетом телебачення і радіомовлення України. URL:

[http://comin.kmu.gov.ua/control/uk/publish/article?art\\_id=113102&cat\\_id=61025](http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113102&cat_id=61025)  
(дата звернення 07.01.2016 р.)

392. Протиправне використання персональних даних, що містяться у соціальних мережах як загроза інформаційній та національній безпеці України / Березовська І. Вісн. Львівського ун-ту. 2014. Вип. 60. С. 185-191.
393. Процик І. Як “витягнути” дитину з віртуального світу URL: <http://www.vn.20minut.ua/news/158911> (дата звернення: 19.06.2017)
394. Рабінович П.М. Межі здійснення прав людини (загальнотеоретичний аспект). Вісник академії правових наук України. 1996. № 6. С. 124–130.
395. Рада Європи рекомендує створити офіс інформаційного комісара в Україні. URL: <http://www.eurointegration.com.ua/news/2017/03/1/7062377/>
396. Радзієвська О.Г. Правові засади протидії негативним інформаційним впливам на дітей в Україні: дис. ... канд. юрид. наук: 12.00.07 / НДІ інформатики і права НАПрН України. Київ, 2018. 260 с.
397. Рекомендація CM/Rec(2014)6 Комітету міністрів Ради Європи державам-членам щодо посібника з прав людини для Інтернет-користувачів та пояснювальний ме-морандум. URL: <https://rm.coe.int/16802e3e96> (дата звернення: 19.10.2015)
398. Рівень розвитку інформаційно-комунікаційних технологій в Україні та світі. URL: <http://edclub.com.ua/analitika/riven-rozvytku-informaciyno-komunikaciynyhtehnologiy-v-ukrayini-ta-sviti> (дата звернення: 23.10.2017)
399. Різак В.М. Правовий статус уповноваженого органу з питань захисту персональних даних: досвід зарубіжних країн. Форум права. 2012. №3. С. 619-625.
400. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України “Про інформацію” та статті 12 Закону України “Про пр.ратуру” (справа К.Г. Устименка)” від 30 жовтня 1997 р. № 5-зп URL: <http://zakon5.rada.gov.ua/laws/show/v005p710-97> (дата звернення 07.01.2016 р.).
401. Рішення Верховного Суду штату Джорджія у справі «Павесіч vs. Нью Ігланд Лайф Іншуранс Ко» від 1905 р. (цит. за Pavesich vs. New England Life

- Ins. Co., 50 S.E. 68 (Ga. 1905)) // Information privacy law : Textbook / D.J. Solove, M. Rotenberg. New York : Aspen Publishers, 2003. 795 p.)
402. Рогожа М. Моральнісні засади сучасності. Людина в лабіринті перспектив. К.:Парапан, 2004. С.119-139
403. Розпізнавання осіб: сховатися від поліції буде все складніше. URL: <https://ukr.media/science/210350/> (дата звернення: 19.10.2017)
404. Романовский Г. Б. Банковская тайна как предмет правового регулирования. *Банковское право*. 2001. № 1. С. 38.
405. Російське іномовлення як інструмент маніпулювання громадською думкою у трансатлантичному просторі. Аналіт. записка Національний інститут стратегічних досліджень. URL: <http://www.niss.gov.ua/articles/1834> (дата звернення: 09.09.2017)
406. Руссо Ж.Ж. Об общественном договоре, М.:»КАНОН-пресс», «Кучково поле», 1998. 416 с.
407. Савінова Н.А. Стратегії соціальних комунікацій як спосіб зниження соціальної напруги на макро-, мезо- та макрорівнях. Актуальні проблеми управління ін-формаційною безпекою держави : зб. матер. наук.-практ. конф. у 2 ч., ч.2. Київ, 18.03.2016 р. К.: Нац. акад. СБУ, 2016. 164 с.
408. Сапожников Е. И. Общество потребления в странах Запада. Вопросы философии. 2007. №10. С. 53-63.
409. Світлична Г. О. Правові аспекти розкриття інформації, яка містить банківську таємницю, щодо юридичних та фізичних осіб . *Вісник Верховного Суду України*. 2007. № 11. С. 25-31.
410. Свобода інформації : навчальний посібник для державних службовців / пер.з англ. Р. Тополевського. К.: Тютюкін, 2010. 128 с.
411. Свобода інформації в Україні та світі. Теорія та практика / упоряд. О.М. Павліченко, Р.І. Стадник; ГО «Харківська правозахисна група». Х.: ТОВ «Видавництво права людини», 2015. 216 с.
412. Сегодня. Итоговая программа, 2 марта 2014 года URL: <http://www.ntv.ru/peredacha/itogovaya/m22900/o227537/> (дата звернення: 09.05.2014)



413. Сейд М. Концепция образования в исламе. Основы построения исламской фило-софии образования. / пер. с англ. под ред. Кямилева С.Х. М.: Типография МПГУ, 2000. 67 с.
414. Селіванов А.О. Право тлумачити закони та юридичні наслідки застосування офіційної інтерпретації . Вісник Верховного Суду України . 2006. № 7. С.2-6 .
415. Селіванов А.О., Стрижак А.А. Питання теорії конституційного правосуддя в Україні: актуальні питання сучасного розвитку конституційного правосуддя: [моногр. дослідж.] К.: Логос, 2010. 276 с.
416. Семикіна М.В. Удосконалення підготовки професійних кадрів промисловості на засадах соціального партнерства. Проблема ефективного використання та про-фесійно-технічної підготовки кадрів промислового сектору України: Доповіді міжнар. наук.-практ. конф., м. Київ, 28-29 листопада 2007р.: У 2 томах. К.: РВПС України НАН України, 2008. Т.2. С.76-88.
417. Сёмкин С.Н., Сёмкин А.Н.. Основы правового обеспечения защиты информации. Уч. пос. для вузов.: Горячая Линия - Телеком, 2008. 238 с.
418. Сепир Э. Коммуникация. Избранные труды по языкознанию и культурологии. М.: Прогресс, 1993. 656 с.
419. Сергій Жадан: Мова ненависті — це мова слабаків URL: [http://osvita.mediasapiens.ua/ethics/standards/sergiy\\_zhadan\\_mova\\_nenavisti\\_tse\\_mova\\_slabakiv/](http://osvita.mediasapiens.ua/ethics/standards/sergiy_zhadan_mova_nenavisti_tse_mova_slabakiv/) (дата звернення: 03.10.2017)
420. Сидоренко Е.В. Личностное влияние и противостояние чужому влиянию. Пси-хологические проблемы самореализации личности. СПб. : СПбГУ, 1997. С. 123–142.
421. Сидоренко Л.І. Філософське осмислення культури і цивілізаційних процесів. Навчальні матеріали для студентів та аспірантів природничих факультетів. URL:<http://www.philsci.univ.kiev.ua/biblio/sid-culture.htm> (дата звернення: 19.10.2017)
422. Система. URL: <https://uk.wikipedia.org/wiki/система> (дата звернення: 13.01.2017)

423. Ситник Г. Безпека як інтегральна характеристика розвитку соціальних систем. Державне управління в Україні: реалії та перспективи: зб. наук. праць. К., 2005. С. 278-282.
424. Ситник Г. Державне управління національною безпекою України. К.: Вид-во НАДУ, 2004. С. 69.
425. Сіденко В.Р. Нові глобальні виклики та їх вплив на формування суспільних цінностей. Український соціум. 2014. №1(48). С. 7-21.
426. Сіленко А. Цифрова нерівність як глобальна соціально-політична проблема. Політичний менеджмент. 2006. № 3. С. 51-62.
427. Сімончук О. Як видання регулюють поведінку журналістів у соцмережах. Те-лекритика. URL: <http://ua.telekritika.ua/society/kak-izdaniya-reguliruyut-povedeniezhurnalistov-v-sotssetyah> (дата звернення: 10.08.2017)
428. Скакун О. Ф. Теорія права і держави: Підр. К.: Алерта; ЦУП, 2011. 524 с.
429. Скалецький Ю.М., Бірюков Д.С., Кондратов С.І. Європейський досвід розбудови системи захисту критичної інфраструктури: уроки для України: Аналіт. записка. Нац. ін-т страт. досліджень/ URL: [http://www.niss.gov.ua/articles/1371/#\\_ftn2](http://www.niss.gov.ua/articles/1371/#_ftn2)(дата звернення: 04.09.2017)
430. Складенко А., Ковалевський В. Хто виховує наших дітей? URL: [//www.unk.org.ua/publ/informacijna\\_bezpeka/khto\\_vikhovue\\_nashikh\\_ditej/34-1-0-251](http://www.unk.org.ua/publ/informacijna_bezpeka/khto_vikhovue_nashikh_ditej/34-1-0-251) (дата звернення: 11.04.2015)
431. Словник синонімів української мови URL: [http://synonyms\\_uk.enacademic.com/](http://synonyms_uk.enacademic.com/) (дата звернення: 22.10.2017)
432. Сляднева Г. О. Правова природа комерційної таємниці та генезис законодавства про захист комерційної таємниці. *Актуальні проблеми держави і права*. С.270-274.
433. Собків Я. Класифікація інформаційних прав і свобод людини та громадянина. URL: <http://goal-int.org/klasifikaciya-informacijnix-prav-i-svobod-lyudini-tagromadyanina/> (дата звернення: 05.08.2017)
434. Соболева Т.А. История шифровального дела в России. - М.: ОЛМА-ПРЕСС-Образование, 2002, 512 с.

435. Солодка О.М. Щодо окремих організаційно-правових питань забезпечення інформаційної безпеки України URL: <http://stratcom.co.ua/shhodo-okremihorganizatsijno-pravovih-pitan-zabezpechennya-informatsijnoyi-bezpeki-ukrayini/>(дата звернення: 01.09.2017)
436. Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України : дис. на здоб. наук. ступеня доктора політ. наук : спец. 23.00.02. / Одес. нац. юрид. акад. О., 2005. 264 с.
437. Соціально-правові основи інформаційної безпеки: Навч. посіб./За ред. В. В.Остроухова. К.: Росава, 2007. 496 с.
438. Спам в марте 2014. URL: [//www.securelist.com/ru/analysis/208050840/Spam\\_v\\_marte\\_2014](http://www.securelist.com/ru/analysis/208050840/Spam_v_marte_2014) (дата звернення: 19.05.2015)
439. Спеціальні та галузеві соціології: Навч. посіб. 2–е вид. К.: Каравела,. 2004. 350 с.
440. Створення єдиного реєстру фізичних осіб – це можливість для тотального стеження за людиною URL: <https://helsinki.org.ua/articles/stvorenniya-jedynohorejestru-fizychnyh-osib-tse-mozhlyvist-dlya-totalnoho-stezhennya-zalyudynoyu/> (дата звернення: 19.11.2017)
441. Стеценко В. Екзистенціалізм як «філософія людини» XX сторіччя. Соціогуманітарні проблеми людини. 2010. Вип.4. С.44-54.
442. Столяренко О. Міжнародні трансфери персональних даних. URL: <http://uba.ua/documents/events/2017/20170407/Presentations/StoliarenkoOleksii.pdf> (дата звернення: 19.08.2017)
443. Стратегія кібернетичної безпеки України, затв.Указом Президента України від 15 березня 2016 р. № 96/2016. URL: <http://zakon3.rada.gov.ua/laws/show/96/2016>
444. Стратегія розвитку наукових досліджень Національної академії правових наук України на 2016-2020 роки URL: <http://www.aprnu.kharkiv.org/doc/strategiya.pdf> (дата звернення: 03.09.2017)
445. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы. М.: МЦМНО, 2002. 296 с.

446. Стрипко М.Я. Методологічні засади підготовки категоріально-понятійного апарату в нормотворчій діяльності органів державної влади України. Вісник Академії праці і соціальних відносин Федерації профспілок України. Серія: Право та державне управління. 2013. № 1. С. 29-35.
447. Сугестивні технології маніпулятивного впливу: Навч. посіб. / В.М.Петрик та ін.; за заг. ред. Є.Д. Скулиша. К.: Наук.-вид. відділ НА СБ України, 2010. 248 с.
448. Сунь-цзи. Мистецтво війни. К.: Арій, 2014. 128 с
449. Сухорольський П. Проблеми забезпечення та розвитку прав людини в умовах інформаційного суспільства. Український часопис міжнародного права. 2013. № 1. С. 21.
450. Талимончик В. П. Международно-правовое регулирование отношений инфор-мационного обмена. Спб. : Юридический центр-Пресс, 2011. 382 с.
451. Таран В. О., Зотов В. М., Резанова Н. О. Соціальна філософія: Навч. посіб. К.: Центр учбової літератури, 2009. 272 с
452. Тарнавська Т.В. Генеза поняття «система»: історичний огляд. Духовність особи-стості: методологія, теорія і практика. 2011. № 6 (47). С.130-139.
453. Татенко В.О. Соціальна психологія впливу: Моногр. К.: Міленіум, 2008. 216 с.
454. Тацій В., Тодика Ю. Межі тлумачення Конституційним Судом Конституції і законів України. *Вісник Конституційного Суду України*. 2002. № 2. С. 60–63.
455. Тема номер один для журналістської спільноти – фізична безпека журналістів –Томіленко. URL: <http://procherk.info/resonance/2-cherkassy-news/51677-temanomer-odin-dlja-zhurnalistskoyi-spilnoti-fizichna-bezpeka-zhurnalistiv-tomilenko> (дата звернення: 03.09.2017)
456. Теорія держави і права. Академічний курс: Підручник / За ред. О. В. Зайчука, Н. М. Оніщенко. К.: Юрінком Інтер, 2006. 688 с.
457. Тер-Акопов А.А. Безопасность человека: социальные и правовые основы. М.: НОРМА, 2005. 272 с.
458. Тертишник В.М. Кримінальний процес України. Загальна частина: Підруч. Акад. вид. К.: Алерта, 2014. 440 с.

459. Тихий В. П. Поняття безпеки людини і її правове забезпечення. Вісник Асоціації кримінального права України. 2016. № 1(6). С. 21-40.
460. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави : Моногр. / заг. ред. Р.А. Калюжний. К.: Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.
461. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави : дис. ... кандидата юрид. наук: 12.00.01 / Нац. акад. внутр. справ. К., 2011. 234 с.
462. Тихомиров О.О. Інформаційні права людини як цивільно-правова категорія. Юридичний вісник. Повітряне і космічне право. 2015. № 1. С. 104-109.
463. Тихомирова Є.Б. Комунікативна політика ЄС: інформаційна безпека vs транспарентність. Актуальні проблеми міжнародних відносин: зб. наук. пр. Вип. 102. Ч.1. К.: КНУ ім. Т. Шевченка, 2011. С. 22-28.
464. Толковый словарь Даля онлайн. Система / сайт Толковый словарь живого великорусского языка Владимира Даля. URL: <http://slovardalja.net/word.php?wordid=37673> (дата звернення: 15.09.2017)
465. Толковый словарь Ожегова. URL: <http://www.ozhegov-shvedova.ru/19-741515/СИСТЕМА> (дата звернення: 15.09.2017)
466. Толубко В.Б. Рось А.О. Складові інформаційної боротьби. Наука і оборона. 2002. № 2. С. 23 – 28.
467. Топалова Л. Д. Правовий режим банківської таємниці . *Науковий вісник Юридичної академії внутрішніх справ*. 2004. № 1. С. 386-395.
468. Тофтул М. Г. Фома Аквінський. Сучасний словник з етики. Житомир: Вид-во ЖДУ ім. І. Франка, 2014. 416 с.
469. Требін М. Інформаційне суспільство. Війни нової епохи. Віче. 2002. № 4. С. 64–68
470. Требін М. П. «Гібридна» війна як нова українська реальність. Український соціум. 2014. № 3. С. 113-127.
471. Труфанов С.Н. Классическая теория познания Вильгельма Гегеля. URL: <http://www.hegel.ru/trufanov1.html> (дата звернення: 03.08.2017).

472. У Донецьку заблокували 39 сайтів українських інтернет-видань URL:  
[http://zik.ua/ua/news/2015/06/09/u\\_donetsku\\_zablokuvaly\\_39\\_saytiv\\_ukrainskyh\\_internetvydan\\_597122](http://zik.ua/ua/news/2015/06/09/u_donetsku_zablokuvaly_39_saytiv_ukrainskyh_internetvydan_597122) (дата звернення: 19.10.2017)
473. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони URL:  
[http://zakon2.rada.gov.ua/laws/show/984\\_011/print](http://zakon2.rada.gov.ua/laws/show/984_011/print)
474. Удалова Л.Д., Кузьмічова-Кисленко Є.В. Лікарська таємниця в кримінальному процесі України: монографія. К. : Центр учбової літератури, 2015. 134 с.
475. Українська держава не оплачує мовлення в окупованому Криму — Муждабаєв /Перший український інформаційний. URL:  
<http://www.5.ua/okupaciyakrimy/Ukrainskaderzhava-ne-oplachuie-movlennia-v-okupovanomu-Krymu-Muzhdabaiev-107352.html> (дата звернення: 19.10.2017)
476. Урсул А.Д. Устойчивое развитие и проблема безопасности. Информационный сборник «Безопасность». 1995. № 9. С. 47-51.
477. Устав Государственного банка URL:  
<http://civil.consultant.ru/reprint/books/250/778.html>.
478. Фатьянов А.А. Тайна как социальное и правовое явление. Ее виды. Государство и право. 1998. № 6. С. 14–16.
479. Филипповский В. Сутність людини та її місце в сучасному світі URL:  
<http://h.ua/story/246400/> (дата звернення: 07.08.2017)
480. Философский энциклопедический словарь. М.:Сов. Энциклопедия, 1983. 840 с.
481. Фисун А.П., Белевская Ю.А. Различия и единство методологии теорий информатики, информационной безопасности социотехнических систем и теория права информационного общества: проблемы формирования информационной теории URL: <http://itnop.ostu.ru> (дата звернення: 03.08.2017)
482. Філософія. Навч. посіб. / За заг. ред. Ю.В. Осічнюка. К.: Атіка, 2003. 464 с.
483. Філософія: конспект лекцій: Зб. праць. К., 2012. 750 с.
484. Філософський словник / За ред. В. І. Шинкарука. К.: Голов. ред. УРЕ, 1986.

485. Фурашев В.М. Законодавче забезпечення інформаційної безпеки України Інформація і право. 2014. №1(10). С. 59-66.
486. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право. 2013. № 2(8). С. 113-119.
487. Халамендик В.Б. Інформаційна гігієна як фактор збереження психічного здоров'я людини. Гум. вісн. Запорізької державної інженерної академії. 2008. Вип. 35. С. 82-89.
488. Хамадун И. В поисках кибермира. URL: [https://www.itu.int/dms\\_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-R.pdf](https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-R.pdf) (дата звернення: 05.11.2016)
489. Хамзатов М.М. Влияние концепции сетецентрической войны на характер современных операций. Военная мысль. 2006. № 7. С. 13–17.
490. Ханін І. Г. Формування міжнародної системи інформаційної безпеки: економічні орієнтири для України URL: <http://www.m.nayka.com.ua/?op=1&j=efektyvnaekonomika&s=ua&z=4457> (дата звернення: 12.09.2017)
491. Хартия прав интернета / Ассоциация прогрессивных коммуникаций URL: [http://www.apc.org/sites/default/files/APC\\_charter\\_RU\\_1\\_2.pdf](http://www.apc.org/sites/default/files/APC_charter_RU_1_2.pdf) (дата звернення: 03.09.2017)
492. Хартія про партнерство заради інформаційних прав і свобод та захисту суспільної моралі від 19.03.2009 р. URL: <http://zakon2.rada.gov.ua/laws/show/n0001120-09>.
493. Хворост Х.Ю. Інформаційно-психологічний вплив у розрізі безпеки здоров'я. Наука і освіта. 2016. №2-3. с.184-191.
494. Химанен П., Кастелс М. Информационное общество и государство благосостояния. Финская модель М.: Логос, 2002. 224 с.
495. Хоффман Л.Дж. Современные методы защиты информации [пер. с англ.]. М: Советское радио, 1980. 57 с.
496. Хронологія розвитку засобів і методів захисту інформації URL: <http://kspu.kr.ua/index.php>

497. Цена свободы и безопасности – Индекс ИКТ-законодательств Евразии за 2016г. URL: <https://www.slideshare.net/VadimDryganov1/2016-73139338> (дата звернення: 03.09.2017)
498. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV. Офіційний Вісник України. 2003. № 11. Ст. 461.
499. Цимбалюк В. С. Безпека як інститут інформаційного права та його місце в структурі кодифікації інформаційного законодавства Моделювання колективної безпеки: інформаційний вимір: Мат. міжн. «круглого столу» (м. Київ, 27 квітня 2011 р.). К.: Вид-во «Академпрес», 2011. С. 28–32.
500. Цимбалюк В. С. Суспільна мораль як різновид інформаційної безпеки Правова інформатика. 2010. № 1(25). С. 23–29.
501. Цимбалюк В. Сутність інформаційної безпеки в умовах входження України до глобальної кіберцивілізації. Науковий вісник Нац. академії Держ. податк. служби України. 2004. № 4(26). С. 135–141.
502. Чевичалова Ж.В. Деякі аспекти становлення вітчизняного інституту «лікарської таємниці». *Медичне право України: правовий статус пацієнтів в Україні та його законодавче забезпечення* (генезис, розвиток, проблеми і перспективи вдосконалення) : мат. II Всеукр. наук.-прак. конф. 17–18.04.2008. Львів, 2008. С 348–352.
503. Черних О.О. Права людини в інтернеті як актуальний напрям роботи соціального педагога URL: <https://www.academia.edu/27680968> (дата звернення: 18.08.2017)
504. Чи є блокування інтернету «порушенням прав людини»? ООН вирішила, що так. URL: <http://ua.euronews.com/2016/07/05/un-denounces-disruption-of-internetaccess-as-human-rights-violation> (дата звернення: 18.08.2017)
505. Что такое система? Значение и толкование слова sistema, определение термина / Толковый словарь Ушакова. URL: <http://www.onlinedics.ru/slovar/ushakov/s/sistema.html>
506. Шапіро В.С. Адміністративно-правовий статус громадянина України як суб'єкта реалізації права на інформацію: дис. ... канд. юрид. наук: 12.00.07 / Сумський державний університет. Суми, 2013. 199 с.



507. Шапіро В.С. Права і свободи людини в галузі інформаційного права Права людини: історія, теорія, практика: мат. Міжнародної науково-практичної конференції, 9-10 грудня 2010 р.. Курськ : ЮЗГУ, 2010.
508. Шахбазян К. С. Міжнародно-правові основи регулювання відносин в мережі Інтернет: Автореф. дис. ... канд. юрид. наук: 12.00.11 / Київський наці. ун-т імені Тараса Шевченка. К., 2009. 19 с.
509. Швырёв В. С. Сциентизм. Новая философская энциклопедия / Ин-т философии РАН; Нац. обществ.-науч. фонд; Предс. научно-ред. совета В.С. Стёпин. М.: Мысль, 2000—2001.
510. Шевчук П. Інформаційно-психологічна війна Росії проти України: як їй протидіяти. Демокр. врядування. 2014. Вип. 13. URL: <http://lvivacademy.com/visnik13/zmist.html> (дата звернення: 03.05.2017)
511. Шевчук С. Судовий захист прав людини. Практика Європейського суду з прав людини у контексті західної правової традиції. К.: Реферат, 2006. С. 424.
512. Шевчук С.В. Загально-теоретичні проблеми нормативності актів судової влади: дис. ... доктора юрид. наук: 12.00.01 / Національна юридична академія України ім. Я. Мудрого. Харків, 2008. 434 с.
513. Шепітько В. Ю. Психологія судової діяльності: Навч. посібник. Х.: Право, 2006. 160 с.
514. Шершеневич Г.Ф. Курс торгового права. СПб., 1908. Т. 4. 624 с.
515. Широкова-Мурараш О.Г., Акчурін Ю.Р. Кіберзлочинність та кібертероризм як загроза інформаційній безпеці: міжнародно-правовий аспект. Інформація і право. 2011. № 1(1). С. 76-81.
516. Шишка Р.Б. Механізм правового регулювання правовідносин у сфері інтелектуальної власності *ІТ право: проблеми і перспективи розвитку в Україні*: зб. мат. наук.-прак. конф. (Львів, 18 лист. 2016 р.). Львів, 2016. С. 297-305.
517. Шлімакова І. І. Феноменологія категорії впливу у вітчизняній психології. Вісник Чернігівського національного педагогічного університету. Серія : Психологічні науки. 2014. Вип. 121(2). С. 203-206.

518. Шопіна І. М. Адміністративно-правове регулювання управління органами вну-трішніх справ України : дис. ... д-ра юрид. наук: 12.00.07 / ДНДІ МВС України. К., 2012. 514 с.
519. Шпенглер О. Закат Європы. Очерки морфологии мировой истории. Т. 1.: Гештальт и действительность. М.: Мысль, 1993. 663 с.
520. Щодня дивляться новини по телевізору 60% українців / Дослідження проводилося компанією R&B в період з 1-10 лютого 2017 р. серед 1800 осіб по всій території України за винятком Криму та ОРДЛО. URL: [https://dt.ua/UKRAINE/ukrayinci-doviryayut-televizoru-v-dva-razi-bilshe-nizh-internet-zmi-235601\\_.html](https://dt.ua/UKRAINE/ukrayinci-doviryayut-televizoru-v-dva-razi-bilshe-nizh-internet-zmi-235601_.html) (дата звернення: 16.10.2017)
521. Щодо інформаційно-психологічної складової агресії Російської Федерації проти України (за результатами подій 1-2 березня 2014 р.). Аналітична записка Національний інститут стратегічних досліджень URL: <http://www.niss.gov.ua/articles/1476/> (дата звернення: 28.03.2015)
522. Юридична психологія : Підруч. / Д.О. Александров та ін.; заг. ред. Л.І. Казміренко, Є.М. Моїсєєв. К.: КНТ, 2007. 359 с.
523. Юристи розглянули подробиці введення санкцій проти російських сайтів та соцмереж URL: <http://ukr.segodaya.ua/politics/society/yuristy-rassmotrelipodrobnosti-vvedeniya-sankciy-protiv-rossiyskih-saytov-i-socsetey-1021451.html>(дата звернення: 03.10.2017)
524. Як оскаржити порушення права на доступ до публічної інформації? практичний посібник URL: <http://cedem.org.ua/wp-content/uploads/2016/12/web.pdf> (дата звернення: 03.05.2017)
525. Ярочкин В.И. Информационная безопасность. М.: Междунар. отношения, 2000. 400 с.
526. Ярочкин В.И. Секьюритология – наука о безопасности жизнедеятельности. М.:Ось-89, 2000. 400 с.
527. Ященко В. А. Щуровський А. М. Національна та державна безпека : діалектика взаємозв'язку. Державна безпека України. 2004. № 1. С. 19-20.
528. «Е-декларації – «наводка» для грабіжників» – голова Ради суддів у Вінниці. URL: <http://www.judges.org.ua/dig11269.htm> (дата звернення: 13.10.2017)

529. «Інформаційний вибух» XXI століття, або Горе з розуму. URL: <http://for-ua.com/analytics/2012/11/26/084809.html> (дата звернення: 03.05.2017)
530. «Мова ворожнечі»: чи є протиріччя між професійним та громадянським обов'язком? URL: <http://detector.media/infospace/article/121803/2016-12-27-mova437vorozhnechi-chi-e-protirichchya-mizh-profesiinim-ta-gromadyanskim-obovyazkom/> (дата звернення: 03.09.2017)
531. «Мова ворожнечі»: як не абсолютизувати ані її уникання, ані правомірного вико-ристання під час війни? URL: <http://detector.media/infospace/article/122037/2017-01-08-mova-vorozhnechi-yak-ne-absolyutizuvati-ani-ii-unikannya-anipravomirnogo-vikoristannya-pid-chas-viini/> (дата звернення: 03.09.2017)
532. «Мова ненависті» — мова забороненої правди. URL: <http://credo.pro/2016/07/161637> (дата звернення: 03.09.2017)
533. «Східне партнерство» закінчилося катастрофою – глава МЗС Польщі URL: <http://www.eurointegration.com.ua/news/2016/01/29/7044114/> (дата звернення: 22.07.2017)
534. A comprehensive strategy on data protection in the European Union URL: [http://epic.org/privacy/intl/eu\\_data\\_protection\\_directive.html](http://epic.org/privacy/intl/eu_data_protection_directive.html). (Last accesed: 26.08.2017).
535. A Declaration on A Culture of Peace, UNESCO, A/Res/53/243. URL: [www.unesco.org/cpp/uk/declarations/2000.htm](http://www.unesco.org/cpp/uk/declarations/2000.htm).
536. An algorithm trained on emoji knows when you're being sarcastic on twitter URL: <http://www.businessinsider.com/this-algorithm-knows-when-youre-being-sarcasticon-twitter-2017-8> (Last accesed: 10.08.2017).
537. Analysis and Implications of Laws / Cyberbullying Research Center URL: <http://cyberbullying.org/cyberbullying-laws>
538. Back to basics. Disinformation Review. 2017, 7 September. URL: <https://euvsdisinfo.eu/> (Last accesed: 09.10.2017).
539. Becker K. Tactical Reality Dictionary, Cultural Intelligence and Social Control, Selene Verlag. Wien, New York: Autonomedia, 2002. URL: <http://world-information.org/trd> (Last accesed: 10.08.2017).

540. Benoist A. Etnobójcza ideologia Zachodu. Prawa człowieka i prawa narodów. *Eléments*. 2003. № 109. / cyt. za Obywatel. 2005. № 3. URL: [źródło: http://nowyobywatel.pl/kwartalnik/numery-archiwalne/](http://nowyobywatel.pl/kwartalnik/numery-archiwalne/) (Pobrano: 01.04.2015)
541. Buchanan L. Peter Drucker from A to Z. Inc. magazine. Retrieved 2012, 12 March.
542. Burke R. The Compelling dialogue of Freedom. *Human rights Quarterly: Human rights at the Bandung Conference*. 2006. Vol. 28. s.962.
543. Butlin J. Our common future. *Journal of International Development*. London, Oxford University Press, 1987. pp. 284–287.
544. Cassirer E. *An Essay on Man: An Introduction to a Philosophy of Human Culture*, Yale & New Haven, 1944. 294 p.
545. Castells M. *Sila tożsamosci*. Warszawa, Wydawnictwo Naukowe PWN, 2009. 464 s.
546. Castells M. *Społeczeństwo sieci*. Warszawa, Wydawnictwo Naukowe PWN, 2013. 556 s.
547. Colvin M. *Developing Key Privacy Rights*. Oxford, Portland, Oregon : Hart Publishing, 2002. 198 p.
548. Communication from the Commission on a European Programme for Critical Infrastructure Protection (COM/2006/786 final). URL: Режим доступу: <http://eurlex.europa.eu/> (Last accesed: 10.08.2017).
549. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the regions “A comprehensive approach on personal data protection in the European Union”, цит. за Мельник К. Правові механізми захисту персональних даних в Європейському Союзі. *Інформація і право*. 2013. № 4(40). с. 55-61.
550. Communication from the European Commission: «Network and Information Security: Proposal for a European Policy Approach». 2001, June 6. URL: – [http://ec.europa.eu/information\\_society/eeurope/2002/news\\_library/pdf\\_files/netsec\\_en.pdf](http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf) (Last accesed: 10.08.2017).

551. Compass: Manual For Human Rights Education With Young People URL:  
<http://www.coe.int/en/web/compass> (Last accessed: 07.06.2017)
552. Complak K. Uwagi o godności człowieka oraz jej ochrona w świetle nowej Konstytucji. Przegląd Sejmowy. 1998, № 5 (28). s. 43.
553. Council Decision 2008/0200 (CNS) on a Critical Infrastructure Warning Information Network (CIWIN), The Council of the EU. October 2008.
554. Council of Europe: Convention on the Access to Official Documents. URL:  
<http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta79/erec854.htm>.  
(Last accessed: 20.05.2017)
555. Council of Europe: Recommendation No. R(2002)2 of the. Committee of Ministers to member states on access to official documents. URL: <https://wcd.coe.int/ViewDoc.jsp?id=262135>. (Last accessed: 20.05.2017)
556. Cyberbezpieczeństwo: dyrektywa NIS przyjęta, firmy w UE muszą spełnić nowe wymagania. URL: [www.rp.pl/Bezpieczenstwo/307069909-Cyberbezpieczenstwodyrektywa-NIS-przyjeta-firmy-w-UE-musza-spelnic-nowe-wymogi.html#ap](http://www.rp.pl/Bezpieczenstwo/307069909-Cyberbezpieczenstwodyrektywa-NIS-przyjeta-firmy-w-UE-musza-spelnic-nowe-wymogi.html#ap) (Last accessed: 03.09.2017)
557. Cyberbullying Activity: Laws. URL: <http://cyberbullying.org/cyberbullying-laws>  
(Last accessed: 22.09.2017)
558. Data protection Eurobarometer URL: [http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet\\_data\\_protection\\_eurobarometer\\_240615\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf)  
(Last accessed: 10.08.2017).
559. Declaration on Human Rights and the Rule of Law in the Information Society. 2005, May 13. URL:  
[https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectID=09000016805da1a0](https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805da1a0)  
(Last accessed: 10.08.2017).
560. Declaration on Human Rights and the Rule of Law in the Information Society. 2005, May 13. URL:  
[https://coe.int/cm/Pages/result\\_details.aspx?ObjectID=09000016805da1a0](https://coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805da1a0)
561. Definition – What does Cyberlaw mean? URL:  
<https://www.techopedia.com/definition/25600/cyberlaw> (Last accessed: 10.08.2017).

562. Digital Agenda for Europe 2020 URL: [https://europa.eu/european-union/file/1497/download\\_en?token=KzfSz-C](https://europa.eu/european-union/file/1497/download_en?token=KzfSz-C) (Last accessed: 02.09.2017).
563. Digital freedom: the case for civil liberties on the Net URL: [http://news.bbc.co.uk/1/hi/special\\_report/1998/encryption/58154.stm](http://news.bbc.co.uk/1/hi/special_report/1998/encryption/58154.stm) (Last accessed: 10.08.2017).
564. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. URL: <http://eurolex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF> (Last accessed: 07.11.2016).
565. Discussion Draft of the Cybersecurity Information Sharing Act of 2014, 113<sup>th</sup> Congress, 2d Session, June 11, 2014. S. 2588.
566. Donahoe E. Human Rights in the Digital Age. URL: <https://www.hrw.org/about/people/eileen-donahoe> (Last accessed: 02.04.2017)
567. Drucker P. Landmarks of Tomorrow. New York: Harper & Row, 1957. 186 p.
568. Drucker P. Managing the Non-Profit Organization. New York: Harper Collins, 1990. 224 p.
569. Drucker P. The Five Most Important Questions You Will Ever Ask About your Organization. San Francisco: Jossey-Bass, 2008. p. 19.
570. Drucker P. The Future of Industrial Man. New York: The John Day Company, 1942. P. 205.
571. Drucker P. What Business Can Learn from Nonprofits. Harvard Business Review. 1989, July–August Is. URL: <https://hbr.org/1989/07/what-business-can-learn-fromnonprofits> (Last accessed: 05.08.2017)
572. Erice Declaration on Principles for Cyber Stability and Cyber Peace, World Federation of Scientists, Aug. 2009. URL: [www.ewi.info/system/files/Erice.pdf](http://www.ewi.info/system/files/Erice.pdf). (Last accessed: 02.04.2015)
573. Ethics and human rights in the information society. Proceedings, synthesis and recommendations/ Organized by the French Commission for UNESCO in cooperation with UNESCO and the Council of Europe. Strasbourg, 2007 September 13–14. P.11.

574. EU: eEurope 2002 – An Information Society For All. Action Plan. URL:  
[http://ec.europa.eu/information\\_society/eeurope/2002/documents/archiv\\_eEurope2002/actioplan\\_en.pdf39](http://ec.europa.eu/information_society/eeurope/2002/documents/archiv_eEurope2002/actioplan_en.pdf39)
575. EU: eEurope 2005 – An Information Society For All. Action Plan. URL:  
[http://ec.europa.eu/information\\_society/eeurope/2005/all\\_about/action\\_plan/index\\_en.htm](http://ec.europa.eu/information_society/eeurope/2005/all_about/action_plan/index_en.htm)
576. EU: i2010 eGovernment – Accelerating eGovernment in Europe for the Benefit of All. Action Plan. URL:  
[http://ec.europa.eu/information\\_society/activities/egovernment/docs/highlights/comm\\_pdf\\_com\\_2006\\_0173\\_f\\_en\\_acte.pdf](http://ec.europa.eu/information_society/activities/egovernment/docs/highlights/comm_pdf_com_2006_0173_f_en_acte.pdf)
577. Europe 2005 Security Policies in Brief [Электронный ресурс] – Режим доступа URL: :  
[http://ec.europa.eu/information\\_society/eeurope/2005/all\\_about/security/index\\_en.htm](http://ec.europa.eu/information_society/eeurope/2005/all_about/security/index_en.htm).
578. European Parliament legislative resolution C 184 E/174 on the proposal for a Council decision on a Critical Infrastructure Warning Information Network (CIWIN). The Official Journal of EU. 2009.
579. Evaristo, Adams & Curley. Information Load Revisited: A Theoretical Model URL: <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1061&context=icis1995> (Last accesed: 03.10.2015).
580. Facebook inwigiluje w sieci wszystkich. Nawet tych bez konta URL:  
<http://prawo.gazetaprawna.pl/artykuly/948121,facebook-inwigilacja-nawet-osob-bez-konta.html> (Pobrano: 15.10.2017).
581. Facebook отключил искусственный интеллект после «диалога» ботов на своем языке. URL: <http://www.dsnews.ua/future/facebook-otklyuchil-iskusstvennyyintellekt-posle-dialoga-botov-01082017132500> (Last accesed: 15.10.2017).
582. Factsheet on the «Right to Be Forgotten» ruling (C-131/12), European Commission, URL: [http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet\\_data\\_protection\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf)

583. Falling through the Net: A Survey of the «Have Nots» in Rural and Urban America. URL: <https://www.ntia.doc.gov/ntiahome/fallingthru.html> (Last accessed: 06.04.2015).
584. Figure of the Week: 50 million euros. URL: <https://euvdisinfo.eu/figure-of-the-week-50-million-euros/> (Last accessed: 05.03.2015).
585. Frank T. Catsouras v. Department of California Highway Patrol. Point of Law. 2010,
586. Garlicki L. Polskie prawo konstytucyjne. Warszawa 2003. S. 85.
587. General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) on 2016, 14 April. URL: <https://www.eugdpr.org/>
588. Georgia: Can Democracy Thrive Without Opposition? 2017, April 5. URL: <http://www.eurasianet.org/node/83116> (Last accessed: 15.10.2017).
589. Gibson A. Reframing Accessibility for the Web. Accessibility, Usability. № 413. 2015, February 03. URL: <https://alistapart.com/article/reframing-accessibility-for-the-web> (Last accessed: 15.03.2015).
590. Green Paper on a European Programme for Critical Infrastructure Protection, The European Commission. Brussels. 2005.
591. Green Paper. Living and Working in the Information Society: People First. European Comission. Brussels. 1996.
592. Gross B. M. The Managing of Organizations. The Administrative Struggle. 1964. Vol. 2. P. 856.
593. Guardchild: Protecting children in the digital age. URL: <https://www.guardchild.com/statistics/>
594. Hartmann F. H. The relations of nations. London: Macmillan, 1962. 710 p.
595. Hemp P. Death by information overload. Harvard Business Review. 2009. № 87(9). Pp. 83–89.
596. Henkin L. Human rights. New York, Foundation Press, 1999. P. 302-306.
597. Higher Education in the Twenty-First Century: Vision and Action. UNESCO on the World Conference on Higher Education (1998). URL: <http://perso.club-internet.fr/nicol/ciret/english/charten.htm> (Last accessed: 15.02.2016).



598. Hins W., Voorhoof D. Access to State-Held Information as a Fundamental Right under the European Convention on Human Rights.; European Constitutional Law Review. 2007, № 3. P. 124-125.
599. Hoffman F. G. Hybrid Warfare and Challenges / F.G.Hoffman // Joint Force Quarterly (JFQ). 2009. Vol. 52, Forth Quarter. – P. 34-39 [цит. за Косиєв ОА., Гриник Р.О Інфор-маційна агресія як невідємна складова ведення гібридної війни] URL:  
<https://sci.ldubgd.edu.ua/bitstream/handle/123456789/3198/8.pdf?sequence=1&isAll owed=y>.
600. How do children use the internet? We asked thousands of kids around the world. URL:<http://theconversation.com/how-do-children-use-the-internet-we-askedthousands-of-kids-around-the-world-67940> (Last accesed: 15.11.2016).
601. How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did URL:  
<http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teengirl-was-pregnant-before-her-father-did/#f13e1ad34c62>
602. Hybrid Warfare URL: <http://www.gao.gov/assets/100/97053.pdf> (Last accesed: 15.10.2017).
603. Ignatieff M. Human rights. The Midlife Crisis. The New York Review of Books. 1999, March 20. S.59.
604. INHOPE: the International Association of Internet Hotlines. URL:  
<http://www.inhope.org> (Last accesed: 15.10.2017).
605. International Organization for Standardization. URL: <http://www.iso.org> (Last accesed: 15.10.2017).
606. Internet Access Is Now A Basic Human Right. URL:  
<http://gizmodo.com/internetaccess-is-now-a-basic-human-right-1783081865> (Last accesed: 02.03.2017).
607. Izdebski H. Fundamenty współczesnych państw. Warszawa, 2007. S. 28.
608. Justynian. Instytucje. Warszawa, 1986. S. 17.
609. Kallas S. The Need for a European Transparency Initiative (Speech/05/130): The European Foundation for Management, Nottingham Business School, Nottingham. URL:

<http://europa.eu.int/rapid/pressReleasesAction.do?reference=SPEECH/05/130&format=HTML&aged=0&language=EN&guiLanguage=en>. (Last accessed: 03.03.2017).

610. Karvalics L. How to defend the original, multicriteria theories of Information Society? 3rd ICTs and Society Meeting; Paper Session — Theorizing the Internet; Paper 3. / Publication in «tripleC — Cognition, Communication and Co-operation» 2010. Vol. 8. No2.
611. Kowalski R, Limber S., Agatston P. Cyber bullying: bullying in the digital age. Oxford: Blackwell Publishing Ltd, 2008. 218 p.
612. Kuźniar R. Prawa człowieka, Warszawa, 2008. S. 22.
613. La notion des droits de l’homme est-elle un concept occidental? Diogène, 1982, p.88. (цит. за „La Revue du MAUSS”, 1 sem. 1999, ss. 211-235p.)
614. Le Bon G. Psychologia tłumy / tł. z fr. Bolesław Kaprocki. Kęty : ANTYK, 2004. 95 s.
615. Lege privind aprobarea Concepției securității informaționale a Republicii Moldova. URL:  
[http://www.sis.md/sites/default/files/transparenta/legea\\_privind\\_aprobarea\\_conceptiei\\_infosec\\_rm.pdf](http://www.sis.md/sites/default/files/transparenta/legea_privind_aprobarea_conceptiei_infosec_rm.pdf) (Last accessed: 15.10.2017).
616. Liderman K. Bezpieczeństwo informacyjne. Warszawa, Wydawnictwo Naukowe PWN, 2012. 216 s.
617. Liedel K. Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego. Torun: Wyd-wo Adam Marszałek, 2014. 96 s.
618. Linton S. Claiming Disability Knowledge and Identity. New York: New York University Press, 1998. P. 9.
619. Livingstone S. Young People and New Media: Childhood and the Changing Media Environment. London: Sage, 2002. 275 p.
620. Lucchi N. Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression. Cardozo Journal of International and Comparative Law. 2011. Vol. 19, No. 3. URL:  
[http://www.cjicl.com/uploads/2/9/5/9/2959791/cjicl\\_19.3\\_](http://www.cjicl.com/uploads/2/9/5/9/2959791/cjicl_19.3_)

621. Masuda Y. Computopia. Oxford, 1985. URL:  
<http://connection.ebscohost.com/c/articles/12608885/vision-computopia> (Last  
accessed: 15.10.2017).
622. Masuda Y. Hypothesis on the genesis of homo intelligens. Futures. Guilford,  
1985. Vol. 17. № 5. P. 479-494.
623. Masuda Y. The Information Society as Postindustrial Society. Wash.: World  
Future Soc., 1983. 320 p.
624. Mendel T. Freedom of information: A Comparative legal survey. Paris, UNESCO  
Publ., 2008. 176 p.
625. Networks for people and their communities: Making the most of the information  
society in the European Union: First Annual Report to the European Commission  
from the Information Society Forum, June 1996.
626. Obama's Remarks on Cyber-Security URL:  
<http://www.nytimes.com/2009/05/29/us/politics/29obama.text.html?mcubz=3> (Last  
accessed: 25.10.2017).
627. On the protection of natural persons with regard to the processing of personal  
data by competent authorities for the purposes of prevention, investigation, detection  
or prosecution of criminal offences or the execution of criminal penalties, and the  
free movement of such data and repealing Council Framework Decision  
2008/977/JHA: Directive (EU) 2016/680 of the European Parliament and of the  
Council, of 27 April 2016. URL: [https://eur-lex.europa.eu/legalcont](https://eur-lex.europa.eu/legalcontent/en/TXT/%3Furi%3DCELEX%253A32016L0680)  
[ent/en/TXT/%3Furi%3DCELEX%253A32016L0680](https://eur-lex.europa.eu/legalcontent/en/TXT/%3Furi%3DCELEX%253A32016L0680) &p rev=search
628. On the use of passenger name record (PNR) data for the prevention, detection,  
investigation and prosecution of terrorist offences and serious crime : Directive (EU)  
2016/681 of the European Parliament and of the Council, of 27 April 2016. URL:  
[https://consilium.europa.eu/en/press/press-releases/2016/04/21-council-adopts-](https://consilium.europa.eu/en/press/press-releases/2016/04/21-council-adopts-eupnr-directive/)  
[eupnr-directive/](https://consilium.europa.eu/en/press/press-releases/2016/04/21-council-adopts-eupnr-directive/)&prev=search
629. Osiatyński W. Historia i filozofia praw człowieka. URL:  
<http://www.hfhr.pl/publikacje/czym-sa-prawa-czlowieka/#sthash.yW2nvApZ.dpuf>  
(Pobrano: 22.03.2015)
630. Osiatyński W. Prawa człowieka i ich granice. Kraków: Znak, 2011. 371 s.

631. Pacem in Terris. URL:  
[http://www.opoka.org.pl/biblioteka/W/WP/jan\\_XXIII/encykliki/Pacem\\_In\\_Terris\\_11041963.html](http://www.opoka.org.pl/biblioteka/W/WP/jan_XXIII/encykliki/Pacem_In_Terris_11041963.html) (Pobrano: 02.04.2015)
632. Policy Guidelines for the Development and Promotion of Governmental Public Domain
633. Information; prep. by Paul F. Uhler. Paris: UNESCO, 2004. VIII, 39 p.
634. Pollitt and Bouckaert, Christopher and Geert. Public Management Reform. New York: Oxford University Press, 2011. p. 38.
635. Pyżalski J. Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży. Kraków, 2012, 318 s.
636. Rapaczynski A. Popular Sovereignty and the Concept of Representation. The Relevance of American Constitutionalism in Eastern Europe. International Journal of Sociology, Vol. 26. № 4. P. 7-16.
637. Recommendation Rec(2004)15 of the Committee of Ministers to member states on electronic governance ("e-governance") URL:  
[https://wcd.coe.int/ViewDoc.jsp?p=&Ref=Rec\(2004\)15&Language=lanEnglish&Ver=original&direct=true](https://wcd.coe.int/ViewDoc.jsp?p=&Ref=Rec(2004)15&Language=lanEnglish&Ver=original&direct=true)
638. Red faces in Estonia over ID card security flaw. URL:  
<https://www.ft.com/content/874359dc-925b-11e7-a9e6-11d2f0ebb7f0> (Last accessed: 05.11.2017)
639. Redefining Information Warfare Boundaries for an Army in a Wireless World URL:  
[http://www.rand.org/content/dam/rand/pubs/monographs//MG1100/MG1113/RAND\\_MG1113.pdf](http://www.rand.org/content/dam/rand/pubs/monographs//MG1100/MG1113/RAND_MG1113.pdf) (Last accessed: 15.10.2017)
640. Sartre J.-P. Being and Nothingness. N.Y., 1965., p. 529.
641. Security. English definition dictionary URL:  
<http://dictionary.reverso.net/englishdefinition/to%20provide%20security>
642. Sen A. Human Rights and Asian Values. New York, 1997. P. 171-193.
643. Shawn H. WCAG 2.0 is now also ISO/IEC 40500!. World Wide Web Consortium. 2012. October 15.

644. Solove D.J. Understanding Privacy. Cambridge: Harvard University Press, 2008. 272 p.
645. Stefan L. The GDPR Retention of Personal Data. URL: <https://www.linkedin.com/pulse/unacceptable-omission-gdpr-implementation-guides-data-stefan-mphil-?trk=hp-feed-article-title-publish> (Last accessed: 15.10.2017).
646. Stone L. Extracting Signal from Noise in Social Networking. – Режим доступа : <http://www.research.microsoft.com/en-us/um/redmond/events/scs2005>
647. Study: 80 percent of children under 5 use Internet weekly URL: <http://content.usatoday.com/communities/technologylive/post/2011/03/study-80-percent-ofchildren-under-5-use-internet-weekly/1> (Last accessed: 15.02.2014).
648. Sysiak P. AI Revolution 101. Our last invention, greatest nightmare, or pathway to utopia? URL: <https://medium.com/ai-revolution/ai-revolution-101-8dce1d9cb62d>(Last accessed: 05.08.2017)
649. The Blue Brain Project – A Swiss Brain Initiative URL: <http://bluebrain.epfl.ch/>(Last accessed: 08.10.2017).
650. The Cybersecurity Act of 2009. URL: <https://www.congress.gov/bill/111th-congress/senate-bill/773/summary/00> (Last accessed: 08.04.2017).
651. The Directive on security of network and information systems (NIS Directive) URL: <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nisdirective> (Last accessed: 08.10.2017).
652. The Global Information Infrastructure Commission URL: <http://giic.org/about/> (Last accessed: 02.04.2017).
653. The Open Data Economy. Unlocking Economic Value by Opening Government and Public Data. Capgemini Consulting. 2013. URL: [http://www.capgemini-consulting.com/resource-file-access/resource/pdf/opendata\\_pov\\_6feb.pdf](http://www.capgemini-consulting.com/resource-file-access/resource/pdf/opendata_pov_6feb.pdf) (Last accessed: 15.10.2017).
654. The Susan Mbarek Women’s International Peace Movement, The Cyber Peace Initiative. URL: <http://smwipm.cyberpeaceinitiative.org/> (Last accessed: 22.11.2017).

655. Thomae de Aquino. Summa theologiae, I, q. 76, a. 1. URL:  
<http://www.corpusthomicum.org/sth1075.html> (Last accessed: 22.10.2015).
656. Toffler A. Future Shock. USA, Random House, 1970. P. 576.
657. Toffler A. The Third Wave . N.Y.: William Morrow & Company, 1980. 544 p.
658. Toward knowledge societies, United Nations Educational, Scientific and Cultural Organization, 2005 URL:  
<http://unesdoc.unesco.org/images/0014/001418/141843e.pdf> (Last accessed: 17.10.2016).
659. U.S. Supreme Court GRISWOLD vs. CONNECTICUT, 381 U.S. 479 (1965)  
URL: <http://supreme.justia.com/cases/federal/us/381/479/case.html>
660. UN Chief proposes int'l accord to prevent cyber war 31 Jan. 2010. URL:  
[www.thepoc.net/breaking-news/world/3930-un-chief-proposes-intl-a](http://www.thepoc.net/breaking-news/world/3930-un-chief-proposes-intl-a). (Last accessed: 12.04.2016).
661. UN General Assembly Resolution 217 A (III) 10.12. 1948. Материалы ЮНЕСКО об информационном обществе. ЮНЕСКО, 2003.
662. Verdict in MySpace Suicide Case URL:  
<http://www.nytimes.com/2008/11/27/us/27myspace.html> (Last accessed: 02.10.2015).
663. Wallerstein I. Analiza systemów-światów. Wprowadzenie. Warszawa, 2007. 160 s.
664. Warren S., Brandeis L. The Right to Privacy. Harvard Law Review. Dec. 15, 1890. Vol. 4. № 5. P. 193-220.
665. Webster F. Theories of The Information Society. London and New York, 1995. P. 22.
666. Webster's Revised Unabridged Dictionary. The ARTFL Project. Chicago: The University of Chicago, 1913. p. 1465. URL:  
<http://machaut.uchicago.edu/?resource=Webster%27s&word=system&use1913=on> (Last accessed: 01.04.2015).
667. White Paper. The Challenges and Ways Forward into the 21s Century. Brussels, 1993.

668. Why most of Three Square Market's employees jumped at the chance to wear a microchip URL: <https://www.cnbc.com/2017/08/11/three-square-market-ceoexplains-its-employee-microchip-implant.html> (Last accessed: 05.08.2017).
669. Willard N. Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress. Champaign: Research Press, 2007. 311 p.
670. Wojtyła K. Miłość i odpowiedzialność. Seria Człowiek i moralność. Lublin, 1982. S. 42-43.
671. World Internet Users and Population Stats. URL: [www.internetworldstats.com/stats.htm](http://www.internetworldstats.com/stats.htm) (Last accessed: 15.10.2017).
672. Young K. Caught in the Net: How to Recognize the Signs of Internet Addiction and a Winning Strategy for Recovery. New York, John Wiley & Sons, 1998. 256 c.
673. Zięba R. Instytucjonalizacja Bezpieczeństwa europejskiego. Warszawa; Scholar, 2001. 406 s.
674. Zolotar O. Legal opposition of informational impact in hybrid warfare in Ukraine. International Journal of Economics and Society. 2017. Vol. 2. Is. 9. Pp. 93-96.
675. Zolotar O. System prawnej ochrony bezpieczeństwa informacyjnego Ukrainy/ Rocznik Towarzystwa Naukowego Płockiego. 2017. S. 687-702.
676. Zolotar O. The rights and safety of women in the informational society: informational gender inequality. International Journal of Economics and Society. 2016. Vol. 2. Is. 8.
677. Zolotar O. Tożsamość narodowa w epoce globalizacji. Teorie komunikacji i mediów. Vol.8. 2016. S. 111-119.
678. Zolotar O. Protection of human rights in the legal system of Ukraine. Studia nad Autorytaryzmem i Totalitaryzmem. 2014. № 36/3. S. 35-49.
679. Zolotar O. Human rights — from the enlightenment to the information society. Studia nad Autorytaryzmem i Totalitaryzmem. 2017. № 38/3. S. 7-20.
680. Zolotar O. Społeczeństwo informacyjne a bezpieczeństwo: kwestie teoretyczne i polityczno-prawne na przykładzie Polski, Ukrainy i Rosji. Wschodnioznawstwo. 2015. № 1. Ss. 361-374.

## ДОДАТКИ

## Додаток А

## Список публікацій здобувача

**Наукові праці, в яких опубліковані основні наукові результати дисертації:**

1. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. К.: «АртЕк», 2018. 446 с.
2. Золотар О.О. Правова охорона як складова інформаційної безпеки: монографія. К.: ТОВ «ПанТот», 2011. 100 с.
3. Золотар О.О. Генеза суспільних відносин щодо інформаційної безпеки людини. *Інформація і право*. 2018. №1(24). С. 139-148.
4. Золотар О.О. Критичне мислення як необхідна умова безпеки людини в інформаційному суспільстві: соціально-правовий аналіз. *Інформаційна безпека людини, суспільства, держави*. 2018. №1(23). С. 98-105
5. Золотар О.О. Правовий статус людини в інформаційному суспільстві. *Юридичний науковий електронний журнал*. 2018. № 1. С. 84-87.
6. Zolotar O. Legal opposition of informational impact in hybrid warfare in Ukraine /Правова протидія інформаційному впливу в умовах гібридної війни в Україні. *International Journal of Economics and Society*. 2017. Vol. 2. Is. 9. Pp. 93-96.
7. Zolotar O. System prawnej ochrony bezpieczeństwa informacyjnego Ukrainy / Система правової охорони інформаційної безпеки України. *Rocznik Towarzystwa Naukowego Płockiego*. 2017. S. 687-702.
8. Золотар О. Информационная безопасность человека: доктринальные подходы к определению категории. *SCI-ARTICLE.RU: науч. период. электрон. журн*. 2017. № 52. С. 260-269.
9. Досвід правового забезпечення інформаційної безпеки в країнах Східного Партнерства ЄС (Молдова, Грузія). *Lex Portus*. 2017. №3 (5) С.70-80.
10. Золотар О.О. Інформаційні революції: соціально-правове значення. *Публічне право*. 2017. № 2(26). С. 40-46.
11. Zolotar O. Права человека – от эпохи просвещения до информационного общества. *Studia nad Autorytaryzmem i Totalitaryzmem*. 2017. № 38(3). S. 7-20.



12. Золотар О.О. Електронна демократія і цифрова диктатура. *Інформація і право*. 2017. №4(23). С. 16-25.
13. Золотар О.О. Особливості інформаційної безпеки людини в умовах гібридної війни. *Інформація і право*. 2017. № 3(22). С. 124-131.
14. Zolotar O. Tożsamość narodowa w erze globalizacji / Національна ідентичність в епоху глобалізації. *Teorie komunikacji i mediów*. Vol.8. 2016. S. 111-119.
15. Zolotar O. The rights and safety of women in the informational society: informational gender inequality/ Права та безпека жінок в інформаційному суспільстві: інформаційна ген-дерна нерівність. *International Journal of Economics and Society*. 2016. Vol. 2. Is. 8. Pp. 118-124.
16. Zolotar O. Informacyjne społeczeństwo a bezpieczeństwo: kwestie teoretyczne i polityko-prawne (na przykładzie Polski, Ukrainy i Rosji) / Інформаційне суспільство і безпека: теоретичний і політико-правовий аспекти (на прикладі Польщі, України і Росії). *Wschodnioznawstwo*. 2015. S. 363-376.
17. Zolotar O. Охрана прав человека в правовой системе Украины. *Studia nad Autorytaryzmem i Totalitaryzmem*. 2014. № 36(3). S. 35-49.
18. Золотар О.О. Загрози інформаційній безпеці людини. *Правова інформатика*. 2014. № 2(42). С. 80-89.
19. Золотар О.О., Трубін І.О. Класифікація загроз інформаційній безпеці. *Інформація і право*. 2013. № 3(9). С. 105-114.
20. Золотар О.О. Про поняття “інформаційний шум” у правовідносинах. *Інформація і право*. 2012. № 1(4). С. 70-74.
21. Золотар О.О. Обмеження доступу до інформації: інформаційно-правовий аспект *Інформаційна безпека людини, суспільства, держави*. 2012. № 1(8). С. 74-80.
22. Золотар О.О. Правове регулювання знищення інформації. *Правова інформатика*. 2012. № 2(34). С. 39-44.
23. Золотар О.О. Свобода інформації в контексті концепції природного права. *Правова інформатика*. 2011. № 1(29). С. 12-16.

### **Наукові праці, які засвідчують апробацію матеріалів дисертації:**

24. Золотар О.О. Особливості інформаційної безпеки людей похилого віку. *ІТ право: проблеми і перспективи розвитку в Україні*: зб. мат. II міжн. наук.-прак. конф. (Львів, 17 лист. 2017 р.). Львів, 2017. С. 84-88.
25. Золотар О.О. Права і свободи людини: інформаційний вимір. *ІТ право: проблеми і перспективи розвитку в Україні*: зб. мат. наук.-прак. конф. (Львів, 18 лист. 2016 р.). Львів, 2016. С. 59-68.
26. Золотар О.О. Вища юридична освіта в Україні: камінь спотикання чи наріжний камінь? *Правові питання трансформації інформаційного суспільства в суспільство знань як основи інноваційного розвитку України*: мат. круглого столу (Київ, 27 квіт. 2016 р.). К., 2016. С. 107-117.
27. Золотар О.О. Особливості правової соціалізації особистості в інформаційному суспільстві: формування «інформаційного щита». *Філософські та суспільно-правові проблеми становлення і розвитку правового суспільства*: мат. круглого столу (Київ, 20 берез. 2013 р.). Ужгород, 2013. с. 194.
28. Золотар О.О. Віртуальна реальність. *Моделювання колективної безпеки: інформаційний вимір*: зб. мат. (Київ, 27 квіт. 2011 р.) К., 2011. С. 63-66.
29. Золотар О.О. Зміст інформаційного права в контексті концепції природного права. *Інформаційні стратегії в глобальному управлінні*: мат. міжн. наук.-практ. конф. (Київ, 29 жовт. 2011 р.). К., 2011. С. 51-57.

### **Наукові праці, які додатково відображають наукові результати дисертації:**

30. Золотар О.О. Інформаційна безпека як право людини. *Інформація та безпека*. 2011. №1-2 (5-6). С. 40-41.
31. Золотар О.О. Класифікація інформаційної безпеки. *Інформація і право*. 2011. № 2. С. 109-113.
32. Концепція кодифікації інформаційного законодавства України / авт. кол.: Баранов О.А., Брижко В.М., Золотар О.О. та ін. *Інформація і право*. 2012. № 1(4) С. 5-16. (Науковий твір зареєстр. Державною службою інтелектуальної власності України, свідоцтво № 44449 від 25.06.2012.)



**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ДЕРЖАВНА НАУКОВА УСТАНОВА  
«ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ»**

вул. Митрополита Василя Липківського, 36, м. Київ, 03035, тел./факс: (044) 248-25-13

16.04.2018 № 22.4/10-1091

На № \_\_\_\_\_ від \_\_\_\_\_

**Довідка**

**про впровадження результатів дисертаційного дослідження**

Результати дисертаційного дослідження кандидата юридичних наук, старшого наукового співробітника, Золотар Ольги Олексіївни на тему: «Правові основи інформаційної безпеки людини» на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 - адміністративне право і процес, фінансове право, інформаційне право, містить нові науково обґрунтовані результати, які можуть бути і, частково, були використані в діяльності Державної наукової установи «Інститут модернізації змісту освіти» з метою наукового і навчально-методичного забезпечення модернізації змісту освіти, процесу виховання, розвитку та соціалізації особистості та правового забезпечення впровадження сучасних інформаційно-комунікаційних технологій.

Заслужують на особливу увагу висновки автора стосовно необхідності удосконалення правового регулювання у сфері освіти, зокрема, що стосується:

- правового забезпечення інформаційної безпеки дитини;
- освіти протягом всього життя (Long Life Learning);
- компетенції критичного мислення як як обов'язкової складової на всіх етапах освітнього процесу;
- забезпечення реалізації права дитини на доступ до публічної інформації;
- подолання цифрового розриву за демографічними і географічними ознаками.

Заслужують на увагу пропозиції автора стосовно визначення понять «інформаційна безпека людини», «інформаційна культура», «загрози інформаційній безпеці людини», «інформаційна вразливість».

Окремі наукові результати Золотар О.О. знайшли своє відображення в практичній діяльності інституту, зокрема, для забезпечення нормативно-правового та інформаційного супроводу освітньої політики, розробки та впровадження електронних інформаційних ресурсів у сфері освіти.

Заступник директора

*Ю. М. Сафонов*

*начальник відділу кадрів*

Ю. М. Сафонов

*Г. В. Косар*

## Додаток В

## ЗАТВЕРДЖУЮ

Директор Науково-дослідного інституту інформатики і права Національної академії правових наук України,  
доктор юридичних наук, професор

В.Г. Пилипчук  
« 4 » березня 2018 року

## АКТ

впровадження результатів дисертаційного дослідження  
Золотар Ольги Олександрівни

## Комісія у складі:

першого заступника директора з наукової роботи, доктора юридичних наук, старшого наукового співробітника Довганя О.Д.; завідувача наукового відділу теорії, історії та філософії інформаційного права, доктора юридичних наук, професора Бесяков К.І.; завідувача наукового організаційного сектора, кандидата юридичних наук Беланюк М.В.,

склала цей акт про те, що результати дисертаційного дослідження на здобуття наукового ступеня доктора юридичних наук Золотар О.О. на тему «Правові основи інформаційної безпеки людини», яке проводилося в рамках планових дослідницьких тем Науково-дослідного інституту інформатики і права НАПрН України «Теоретико-правові основи формування і розвитку інформаційного суспільства» (номер державної реєстрації 0113U003154) та «Теоретико-правові основи захисту прав, свобод і безпеки людини в інформаційній сфері» (номер державної реєстрації 0117U007745), у частині розкриття теоретико-методологічного обґрунтування правових основ інформаційної безпеки людини, її місця в інформаційно-правових дослідженнях, визначення змісту інформаційних прав людини, а також формування інформаційно-правового статусу людини в інформаційному суспільстві, використані у науковій діяльності Інституту, при написанні монографічних видань, а також при підготовці пропозицій щодо удосконалення законодавства в інформаційній сфері.

## Члени комісії:

Доктор юридичних наук, с.н.с.

Доктор юридичних наук, професор

Кандидат юридичних наук

О.Д. Довгань

К.І. Бесяков

М.В. Беланюк

«ЗАТВЕРДЖУЮ»

Директор Інституту

підвищення кваліфікації керівних кадрів  
Національної академії державного управління  
при Президенті України

В.А.Гошовська

12 грудня 2014 р.

## АКТ

про впровадження результатів

дисертаційного дослідження Золотар Ольги Олексіївни, к.ю.н., с.н.с.,

на тему «Правові основи інформаційної безпеки людини»,

на здобуття наукового ступеня доктора юридичних наук за спеціальністю  
12.00.07 - адміністративне право і процес, фінансове право, інформаційне  
право,у діяльність Інституту підвищення кваліфікації керівних кадрів  
Національної академії державного управління при Президенті України

Комісія у складі:

Голова комісії – Ларіна Н. Б., перший заступник директора Інституту  
підвищення кваліфікації керівних кадрів Національної академії державного  
управління при Президенті України, к.пед.н., доцент;Члени комісії – Солоха М.Т. заступник директора Інституту підвищення  
кваліфікації керівних кадрів Національної академії державного управління при  
Президенті України;Пинюк І.І., заступник начальника відділу науково-методичного  
забезпечення системи підвищення кваліфікації публічних службовців Інституту  
підвищення кваліфікації керівних кадрів Національної академії державного  
управління при Президенті України

цим актом засвідчує, що результати дисертаційного дослідження Золотар Ольги Олексіївни використані в освітньому процесі і Інституту підвищення кваліфікації керівних кадрів Національної академії державного управління при Президенті України для навчання державних службовців 1-5 груп оплати праці та посадових осіб органів місцевого самоврядування для роботи на посадах I - IV категорій; а також в наданні методичної, інформаційної, консультативної допомоги регіональним і галузевим навчальним закладам, органам державної влади і органам місцевого самоврядування з питань підвищення кваліфікації державних службовців та посадових осіб місцевого самоврядування, зокрема, шляхом проведення тематичних семінарів «Загрози

інформаційній безпеці людини» (у 2014-2016 рр.), «Нові медіа: перспективи для держави і громадянського суспільства» (у 2016 р.), «Інформаційне суспільство: концепції і дійсність» (у 2017 р.).

Голова комісії



Ларіна Н. Б.

Члени комісії



Солоха М.Т.



Гинюк І.І.



СЕКРЕТАРІАТ  
КАБІНЕТУ МІНІСТРІВ  
УКРАЇНИ

вул. Грушевського, 12/2, Київ, 01008,  
тел.: (044) 252 7799, факс: (044) 256 7671

Департамент інформації та  
комунікацій з громадськістю

17-18/503 б.р. 27.02.19

#### ДОВІДКА

*про впровадження результатів дисертаційного дослідження  
Золотар Ольги Олексіївни на тему:  
«Правові основи інформаційної безпеки людини»  
на здобуття наукового ступеня доктора юридичних наук  
за спеціальністю 12.00.07- адміністративне право і процес;  
фінансове право; інформаційне право*

У січні 2018 року до Секретаріату Кабінету Міністрів України надійшли матеріали дисертаційного дослідження Золотар Ольги Олексіївни на тему: «Правові основи інформаційної безпеки людини». Надані матеріали було розглянуто в Департаменті інформації та комунікацій з громадськістю. Науково-теоретичні положення, висновки, пропозиції та практичні рекомендації, що містяться у дослідженні можуть бути використані у роботі Департаменту в частині, що стосується:

- концептуальних засад державної політики інформаційної безпеки в Україні;
- особливостей правового забезпечення прав і безпеки окремих категорій осіб в інформаційній сфері, зокрема права на доступ до публічної інформації;
- правового забезпечення інформаційної безпеки людини в умовах гібридної війни.

Впровадження зазначених матеріалів в діяльність Департаменту інформації та комунікацій з громадськістю Секретаріату Кабінету Міністрів України сприятиме використанню сучасних тенденцій розвитку науки інформаційного права з метою розвитку суспільних комунікацій та інформаційної сфери, сприяння створенню умов для розвитку громадянського суспільства та реалізації конституційних прав громадян на участь в управлінні державними справами.


В.о. директора

Р.І. Стадник



ЗАТВЕРДЖУЮ

Декан факультету соціології і права  
Національного технічного університету  
України «Київський політехнічний інститут  
імені Ігоря Сікорського»



Мельниченко А.А.  
«—» січня 2018 року

АКТ

**про впровадження результатів  
дисертаційного дослідження Золотар Ольги Олексіївни, к.ю.н., с.н.с.,  
на тему «Правові основи інформаційної безпеки людини»,  
на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 -  
адміністративне право і процес, фінансове право, інформаційне право**

*Комісія у складі:* завідувача кафедрою публічного права, кандидата юридичних наук, доцента Чепульченко Т.О., завідувача кафедрою інформаційного права та права інтелектуальної власності, кандидата юридичних наук, доцента Петряєва С.Ю., професора кафедри інформаційного права та права інтелектуальної власності, доктора юридичних наук, професора Лук'янчикова Є.Д., доцента кафедри інформаційного права та права інтелектуальної власності, доктора юридичних наук, доцента Гордієнко С.Г.,

*склала* цей акт про те, що результати дисертаційного дослідження на здобуття наукового ступеня доктора юридичних наук Золотар Ольги Олексіївни на тему: «Правові основи інформаційної безпеки людини», враховувалися під час розробки та впровадження програм навчальних дисциплін «Основи інформаційної безпеки», «Правові основи інформаційної безпеки», «Правові аспекти інформаційної безпеки», «Публічно-правова охорона інформаційної безпеки», «Проблеми інформаційного права».

Члени комісії:

Завідувач кафедрою публічного права к.ю.н., доц.



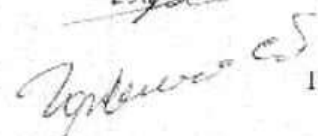
Чепульченко Т.О.

Завідувач кафедрою інформаційного права  
та права інтелектуальної власності к.ю.н., доц.


Петряєв С.Ю.

Професор кафедри інформаційного права  
та права інтелектуальної власності д.ю.н., проф.


Лук'янчиков Є.Д.

Доцент кафедри інформаційного права  
та права інтелектуальної власності д.ю.н., доц.


Гордієнко С.Г.





## АПАРАТ ВЕРХОВНОЇ РАДИ УКРАЇНИ

01008, м. Київ-8, вул. М. Грушевського, 5

№ 04-32/13-95

"13" 03 2018 р.

**Довідка**  
**про впровадження результатів**  
**дисертаційного дослідження Золотар Ольги Олексіївни, к.ю.н., с.н.с.,**  
**на тему «Правові основи інформаційної безпеки людини»,**  
**на здобуття наукового ступеня доктора юридичних наук**  
**за спеціальністю 12.00.07 - адміністративне право і процес,**  
**фінансове право, інформаційне право**

Результати дисертаційного дослідження к.ю.н., с.н.с. Золотар Ольги Олексіївни на тему «Правові основи інформаційної безпеки людини» використовувались Комітетом Верховної Ради України з питань свободи слова та інформаційної політики в процесі законотворчої роботи з питань інформаційної політики, інформаційних прав і свобод громадян, інформаційної безпеки людини та суспільства, а також при підготовці аналітичних матеріалів.

Керівник секретаріату Комітету  
Верховної Ради України з питань  
свободи слова та інформаційної політики

Микола Козлов

**ЗАТВЕРДЖУЮ**

Декан юридичного факультету  
Київського національного університету  
імені Тараса Шевченка  
доктор юридичних наук, професор

 С. Грищенко  
« 15 » 2018р.

**АКТ**

« 15 » 03 2018 р.

м. Київ

Про впровадження у навчальний процес юридичного факультету Київського національного університету імені Тараса Шевченка основних результатів дисертаційного дослідження к.ю.н., с.н.с. Золотар Ольги Олексіївни на тему «Правові основи інформаційної безпеки людини», поданого на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 - адміністративне право і процес, фінансове право, інформаційне право

Результати дисертаційного дослідження використовуються при викладанні на юридичному факультеті спецкурсів: «адміністративно-правове забезпечення інформаційної безпеки», «захист прав особи в інформаційному суспільстві», «інформаційне право України», «правовий режим обігу інформації в країнах Європейського Союзу», «теорія та практика деліктології в інформаційній сфері».

Окремі результати дисертаційного дослідження включені до лекцій з нормативних дисциплін «адміністративне право» та «Адміністративне процесуальне право» і використовуються у навчальному процесі юридичного факультету Київського національного університету імені Тараса Шевченка під час проведення практичних занять.

Наукові публікації О. О. Золотар внесені до списків рекомендованих джерел робочих навчальних програм та лекцій з навчальних дисциплін «Адміністративно-правове забезпечення інформаційної безпеки», «Захист прав особи в інформаційному суспільстві», «Інформаційне право України», «Правовий режим інформації з обмеженим доступом», «Правовий режим обігу інформації в країнах Європейського Союзу», «Теорія та практика деліктології в інформаційній сфері».

**Голова комісії**

**Члени комісії:**

Уклала комісія у складі:

Голови:

Членів комісії:



**П. В. Діхтієвський**

**А. І. Берlach**

**О. А. Заярний**

Професора кафедри адміністративного права, доктора юридичних наук, професора  
Діхтієвського Петра Васильовича ;

Професора кафедри адміністративного права, доктора юридичних наук, професора  
Берlach Анатолія Івановича

Доцента кафедри адміністративного права, кандидата юридичних наук,  
Заярного Олега Анатолійовича