

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

Ольга Золотар

**ІНФОРМАЦІЙНА БЕЗПЕКА ЛЮДИНИ:
ТЕОРІЯ І ПРАКТИКА**

монографія

Київ 2018

УДК 004.7.056:316.77]:342.738](477)(02)

З-80

*Рекомендовано до друку рішенням Вченої ради
Науково-дослідного інституту інформатики і права
Національної Академії правових наук України
24 січня 2018 року, протокол № 1*

Рецензенти :

- Калюженій Р.А.**, доктор юридичних наук, професор,
професор кафедри теорії та історії держави і права Юридичного Інституту
Національного авіаційного університету.
- Пазюк А.В.**, доктор юридичних наук, доцент,
доцент кафедри міжнародного права Інституту міжнародних відносин
Київського національного університету ім. Тараса Шевченка,
керівник лабораторії з управління Інтернетом Української асоціації між-
народного права

З-80 ЗОЛОТАР О.О.

Інформаційна безпека людини: теорія і практика : монографія. – Київ :
ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.

ISBN ISBN 978-617-7264-79-7

Монографія є комплексним теоретико-методологічним дослідженням проблем забезпечення інформаційної безпеки людини. Ґрунтуючись на комплексному аналізі міжнародного, національного та зарубіжного досвіду, автор досліджує проблеми прав і свобод людини в інформаційному суспільстві, загрози інформаційній безпеці людини, стан правового забезпечення цієї сфери та перспективи його розвитку.

Розраховано на фахівців в галузі права, безпеки, соціології, викладачів, студентів та слухачів як гуманітарних, так й технічних навчальних закладів, а також інших читачів, які цікавляться інформаційно-правовою проблематикою. Робота є науковим виданням і може використовуватися у навчальному процесі.

ISBN ISBN 978-617-7264-79-7

УДК 004.7.056:316.77]:342.738](477)(02)

© Науково-дослідний інститут інформатики і права
© Золотар О.О., 2018
© ТОВ «Видавничий дім «АртЕк»

ЗМІСТ

ВСТУП	4
РОЗДІЛ I. ЛЮДИНА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ	
1.1. Людина як суб’єкт суспільства і об’єкт суспільних відносин.....	8
1.2. Генеза прав і свобод людини: від античності до інформаційного суспільства.....	58
1.3. Правовий статус людини в інформаційному суспільстві.....	79
РОЗДІЛ II. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ТА ЗАКОНОДАВЧІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	
2.1. Онтологічний, гносеологічний і логічний зміст інформаційної безпеки.....	128
2.2. Інформаційна безпека як системне явище.....	147
2.3. Місце та роль інформаційної безпеки в інформаційно-правових дослідженнях.....	164
2.4. Правове забезпечення інформаційної безпеки в законодавстві України.....	179
РОЗДІЛ III. СУЧАСНИЙ СТАН ЗАХИЩЕНОСТІ ЛЮДИНИ ВІД ІНФОРМАЦІЙНИХ ЗАГРОЗ В УКРАЇНІ	
3.1. Реальні і потенційні виклики та загрози інформаційній безпеці людини.....	207
3.2. Особливості правового забезпечення прав і безпеки окремих категорій осіб у інформаційній сфері.....	253
3.3. Проблеми забезпечення інформаційної безпеки людини в умовах гібридної війни проти України.....	278
РОЗДІЛ IV. МІЖНАРОДНИЙ ТА ЗАРУБІЖНИЙ ДОСВІД ПРАВОВОГО РЕГУЛЮВАННЯ ВІДНОСИН У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ	
4.1. Інформаційна безпека людини в міжнародному праві.....	296
4.2. Правове регулювання відносин у сфері інформаційної безпеки людини в США, ЄС та країнах Східного партнерства.....	328
4.3. Перспективи використання іноземного досвіду для вдосконалення законодавства України у сфері інформаційної безпеки людини.....	381
ВИСНОВКИ	395
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	410

ВСТУП

Аналіз соціальних процесів, що відбуваються останні роки під натиском телекомунікаційної експансії у всіх сферах життя в Україні і світі, дозволяє говорити про наближення нашого суспільства до глобального інформаційного суспільства. При цьому, інформаційно-комунікаційне насичення суспільних відносин, одночасно створює можливість настання бажаних і загрозливих 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. Складно знайти сферу соціальної активності, що уникала б впливів нових технологій – економіка, медицина, освіта, культура, релігія і розваги – всюди існує величезний масив інформаційних впливів, що посилюється за допомогою ІКТ.

На початковому етапі правові дослідження інформаційних відносин були сконцентровані на вивченні особливостей суспільних відносин, що виникали у зв'язку з все більш активним використанням ІКТ, і намаганням врегулювати ці видозмінені правовідносини. При цьому, у світі склалось дві тенденції правового регулювання правовідносин у інформаційній сфері. Перша – використовувати за аналогією законодавство, що існує, при цьому створюючи нові правові норми лише щодо нових дійсностей, що повстають у зв'язку з всеосяжною інформатизацією. І друга – творити нове законодавство, спрямоване на врегулювання інформаційних відносин. При цьому про інформаційну безпеку людини замислювались лише в розрізі порушення її прав інтелектуальної власності, згодом – щодо права доступу до інформації та захистом персональних даних.

Проте, як показав час, лише врегулювання існуючих інформаційних суспільних відносин виявилось не достатнім. Законодавство не встигає за технологічним прогресом, що не лише породжує нові види суспільних відносин, які потребують регулювання, а й творить нові явища, що вимагають насамперед етичної, а вже потім правової, оцінки соціумом. При цьому окремих пересічний громадянин опиняється в такій же ситуації, як

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

Такий динамічний розвиток дійсності вимагає перегляду підходів до розуміння безпеки. 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. Сутність інформаційної безпеки людини як необхідної для існування і розвитку людини властивості, а отже бажаної для демократичного суспільства, має базуватись на розумінні ендогенних і екзогенних процесів, що виникають у зв’язку зі становленням інформаційного суспільства. Виокремлення і окреслення його функціональних і дисфункціональних рис має на меті сформулювати принципи правового забезпечення життєдіяльності людини в такому суспільстві, що створить умови для збереження цілісності людини та її здатності до розвитку. Дослідженню особливостей статусу людини в інформаційному суспільстві присвячено перший розділ монографії. При цьому, інформаційну безпеку людини неможливо розглядати відірвано від її прав та свобод у інформаційній сфері, що визначають її правовий статус у суспільстві та державі, а також правових можливостей охорони і захисту цих прав. Другий розділ монографії присвячено теоретико-методологічним та законодавчим засади інформаційної безпеки. А третій та четвертий розділ розкривають проблеми захисту безпеки людини в інформаційній сфері, а також вітчизняний та заубіжний досвід правового забезпечення інформаційної безпеки людини.

З метою дослідження існуючих підходів до розуміння інформаційної безпеки людини та її правового забезпечення у монографії було проаналізовано праці з різних сфер наукового знання – різних галузей правової науки, соціології, політології, науки про безпеку (безпекознавства) тощо. Серед вітчизняних правників, науковий доробок яких опрацьовано при підготовці цієї монографії, є: І.В. Арістова, О.А. Баранов, К.І. Беляков, В.В. Белєвцева, В.М. Брижко, О.Д. Довгань, В.М. Гарашук, В.І. Гурковський, Р.А. Калюжний, Б.А. Кормич, І.Ф. Корж, О.В. Кохановська, Т.А. Костецька, Г.М. Красноступ, О.В. Логінов, В.А. Ліпкан, Ю.Є. Максименко, А.І. Марущак, І.В. Мукомела, В.Я. Настюк, Н.Р. Нижник, Н.Б. Новицька, А.М. Новицький, О.В. Олійник, А.В. Пазюк, В.С. Політанський, В.Г. Пилипчук, Н.А. Савінова, А.О. Селіванов, П.М. Сухорольський, М.П. Стрельбицький, Є.Д. Скулиш, В.Я. Тацій, В.П. Тихий, О.О. Тихомиров, В.М. Фурашев, В.С. Цимбалюк та інші. Безперечно, наукову основу дослідження становлять напрацювання з інформаційного права. На думку автора, саме в межах інформаційного права як комплексної галузі права, мають досліджуватись питання правового забезпечення інформаційної безпеки. Проте, для глибшого зрозуміння соціальної природи людини, а також аналізу наукових підходів до інформаційної безпеки та її забезпечення в різних галузях науки, 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., Татенка В.О., Шлімакової І.І. та інших.

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

На хід дослідження значний вплив мав особистий і професійний досвід авторки. Мовні конструкції цікавили не стільки з позицій розумування,

а задля формування теоретичної основи і відповідного понятійного апарату для правового забезпечення. В той же час дослідження реалій суспільства, що прямує до інформаційного, і умов безпечного існування людини в ньому, мало на меті 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, значну роль щодо забезпечення власної інформаційної безпеки автор відводить безпосередньо людині, за умови розбудови демократичної правової держави та розвинутого громадянського суспільства. Тому інформаційна безпека людини не може досліджуватись відірвано від системи інформаційної безпеки суспільства, держави і глобальної інформаційної безпеки людства.

Автор свідомо у вступі не акцентує увагу на інформаційну складову гібридної війни, що є актуальною українською дійсністю. Адже, на нашу думку, незалежно в якій фазі знаходиться війна між державами, війна за людський розум і волю вдеться постійно – на комерційному, психологічному, ідеологічному і інших фронтах.

Тому, на нашу думку, формування науково обґрунтованих, системних і орієнтованих на людину (як основну цінність суспільства і держави) теоретико методологічних і правових засад інформаційної безпеки дозволить не лише вдосконалити підходи до законотворчої діяльності у сфері інформаційного права та формування інституційної структури спрямованої на гарантування інформаційної безпеки людини, а й переосмислити роль людини і громадянина у суспільстві та державі. Адже усвідомлена і відповідальна громадянська позиція є можливою лише за умови реалізованого основоположного принципу інформаційної безпеки – свободи інформації.

Висловлюю щирю подяку шановним вчителям, колегам, рідним та друзям, які підтримують науковий пошук і надихають на нові звернення.

В пам'ять про тата, Золотар Олексія Олексійовича

РОЗДІЛ І. ЛЮДИНА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

1.1. Людина як суб'єкт суспільства і об'єкт суспільних відносин

Сучасний людиноцентристський 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 [123, ст.1].

На офіційній сторінці Ради Європи як основні названі 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» [461]. 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 [234].

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» [238].

Якщо у 20-му столітті питання створення штучного інтелекту і похідні від того супільнозначимі 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 [568].

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 року Blue Brain Project – проекту з комп'ютерного моделювання неокортексу людини. Над проектом спільно працюють компанія IBM і Швейцарський Федеральний Технічний Інститут Лозанни. Наприкінці 2015 року розробниками було заявлено про створення першого штучного мозку з 31 тис. нейронів [570].

Майже завжди, коли йдеться про штучний інтелект, одразу згадують про нанотехнології. Нік 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 зворотньому напрямку процеси старіння людського організму. Наскільки етичним може бути варіант створення цифрової копію людської свідомості? [50, с. 496].

В середині липня 2017 року виникла суперечка між двома відомими представниками Силіконової Долини, після того як Ілон Маск назвав штучний інтелект (artificial intelligence, AI) найбільшим ризиком і загрозою для людської цивілізації. У свою чергу, Марк Цукерберг прокоментував слова Маска під час трансляції в Facebook і 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 року керівництво соціальної мережі Facebook прийняло рішення відключити систему штучного інтелекту після того, як чат-боти почали спілкуватися своєю неіснуючою раніше мовою. Експерти висловили побоювання, що коли боти почнуть активно спілкуватися власною мовою, то поступово стануть все більш самостійними і зможуть функціонувати поза контролем ІТ-фахівців. Тим більше, що навіть досвідчені інженери не можуть повністю відслідковувати хід розумового процесу спамерських пошукових роботів [492].

Другий, дескриптивний 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 [234]

Такий 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 – соціальну систему, в яку вона входить, 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:

- соціально і біологічно повноцінного;
- соціально повноцінного при біологічній неповноцінності;
- біологічно повноцінного при соціальній неповноцінності;
- соціально і біологічно неповноцінного [200, 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 [271].

Водночас, соціологічне розуміння людини дозволяє співвідносити поняття «людина – індивід – особа – особистість – індивідуальність», як якісні прояви людини.

Поняття «людина» означає вид у біологічній класифікації, розумну істоту, що має принципові відмінності від усіх інших істот.

Поняттям «індивід» позначають окремо взятого представника людського роду, якому властиві неповторні і унікальні природні і соціальні якості. Тому ми не можемо прямо і безпосередньо переносити всі характеристики роду на індивіда, як і навпаки.

Поняття «особи» характеризує певні реальні якості людського індивіда, які включають два найважливіших моменти. По-перше, особа – це суб'єкт та об'єкт соціальних стосунків, тобто той, від кого продукуються соціальні дії та до кого вони спрямовані: за цією характеристикою особа постає у певних соціальних ролях, постає представником певних соціальних прошарків. За цією характеристикою у більшості розвинених країн досить чітко визначають на юридичному рівні, кого і коли можна вважати повноцінною особою, наприклад, за ознакою повноліття, можливістю виконання всіх основних соціальних повноважень та ін.

По-друге, особа характеризується через особливий, неповторний внутрішній світ людини з її темпераментом, знаннями, переконаннями, ідеалами, ерудицією, цінностями. В даному випадку можна вести розмову про «сіреньку» особу, видатну особу, непересічну особу, моральну, принципову особу, особу інтелектуально заглиблену, примітивну та ін.

Коли людина характеризується як особистість до характеристик особи додається «самість» – вісь, центр, зосередження усіх дійових, психічних та інтелектуальних якостей: наявність у особи такої «самості» (дечого такого, що робить особу самою собою) дозволяє характеризувати її як сформовану, або розвинену, або досконалу, або духовну особистість.

Як особистість людина усвідомлює свої якості, свою унікальність, свої вади та переваги і постає самодіяльною соціальною та інтелектуальною одиницею. Коли ж це усвідомлення сягає розуміння того, що внаслідок унікальності та неповторності особистості існує дещо таке, що може

виконати лише вона (бо більше такої особистості немає, не було й не буде) і прагне це виконати будь-що, людська особистість набуває рис індивідуальності.

Поняття індивідуальності може викликати (і викликає) асоціації з індивідуалізмом, і для таких асоціацій є певні підстави. Справді, індивідуальність не може сформуватися без самоусвідомлення, без виділення себе з-поміж інших людей, без певної внутрішньої зосередженості. Але це не означає і не передбачає людської самоізоляції. Навпаки, усвідомлюючи свою незамінність, індивідуальність, усвідомлює і свою повну ідентичність з іншими людьми: адже зрозуміти свою унікальність можна лише у порівнянні із іншими людьми та лише за умови переконаності у тому, що всі інші люди є люди, але в чомусь – не такі. Мірою відповідальності людської індивідуальності стає вселюдськість, усвідомлення своїх життєвих здійснень як загальнолюдських або як здійснень, які щось змінюють у стані людства в певному змістовому значенні: коли чогось досягає якась окрема індивідуальність, то це демонструє можливості людства або людини, як родової істоти.

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 (*E. Cassirer*) [454]. 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 шаблях розвитку не відокремлювала себе від решти природи, відчуваючи свій нерозривний зв'язок з усім органічним світом, що знайшло ввідбраження

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 чужою 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, тому по суті філософія Сократа – етичний антропологізм, в якому 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. Не теоретизування про душу і світ, а пошук шляху звільнення людини від страждань є справжнім призначенням людини. 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 виголосив: «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].

Не можливо обійти стороною 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 [384]. 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 оспорюється, 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 [337, 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 Священному 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 пуг. Гуманісти Відродження вважали, що можливості людського пізнання безмежні, бо розум людини подібний божественного розуму, а сама людина є як би смертним богом, і врешті-решт люди вступають на територію небесних світил і там облаштовуються і стануть як боги. Насолода земним буттям – це неодмінна частина культури Відродження. 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 [137, 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'язує розуміння сутності людини з суспільно-історичними умовами його функціонування і розвитку, з його свідомою діяльністю, в ході якої людина опиняється і передумовою, і продуктом історії. Беручи до уваги тип виробничих відносин, Маркс окреслює певний ступінь історичного розвитку, тип суспільства в його цілісності як певної ланки історичного суспільного розвитку, застосовує поняття «суспільно-історична формація», визначальною основою якої і є базис. Всі інші суспільні інститути і способи мислення, ідеологія, уявлення – це похідні від нього і вважаються надбудовою. Із досвіду соціальної співпраці «виростає» свідомість

людини. Цим обґрунтована аксіома: «Не свідомість визначає буття, а буття визначає свідомість».

Підкреслюючи значення громадських зв'язків і характеристик людини, марксист не відкидають специфічних якостей особистості, наділеною характером, волею, здібностями і пристрастями, так само як 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. Співчуваючи – слабшаєш. Якщо не співчуває ніхто, тоді людина змушена шукати сили, щоб вибратися з отриманого стану.

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 ХХ століття, яка значною мірою відобразила перетворення суспільного життя у ХХ ст.: велика кількість соціальних потрясінь, дві світові 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” (від пізньюлат. *exsistentia* – існування) сформувався як одна з найбільш особистісно орієнтованих філософських течій, претендуючи на роль єдиної істинної “філософії людини ХХ століття” [361, 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 [361, с. 50].

Жан-Поль 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 angst (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 Альбер Камю (1913–1960) посвятив свою творчість 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. Тобто свободу людини мислитель поширює на всі модуси часу й вона набуває абсолютного характеру. Такого самого характеру набуває і міра відповідальності людини. 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” [559, с.529].

Феноменологія як особливий напрямок у філософії пов’язана з ім’ям Е. Гуссерля (1856-1938), який вважає предметом філософії царство чистих істин, апріорних змістів. Пізнання розглядається як потік свідомості, внутрішньо організований і цілісний, однак відносно незалежний від суб’єкта пізнання і його діяльності. Вихідним пунктом феноменології було вивчення позадослідних, позаісторичних структур свідомості, які забезпечували його реальне функціонування і збігались з ідеальними значеннями, вираженими у мові і психологічних переживаннях. Феномени – ідеальні сутності, зміст. Феноменологія – метод безпосереднього, інтуїтивного розгляду цих сутностей. У феноменах Гуссерль виділяє різні шари: мовні оболонки; різноманітні психічні переживання; предмет, мислимий у свідомості; смисл – інваріантну структуру і зміст мовних висловлювань. Для феноменології характерний гостра критика позитивізму, усвідомлення духовної кризи сучасності.

Персоналізм (від лат. *persona* – особистість) – теїстичний напрямок у сучасній філософії, який визнає особистість первинною творчою

реальністю і вищою духовною цінністю, а увесь світ проявом творчої активності верховної особистості – Бога¹. В основі світогляду покладено плюралізм – визнання множинності існувань, свідомостей, волі, особистостей. Особистість розглядається як основний прояв буття, у якому вольова активність, діяльність сполучається з безперервністю існування. Джерела особистості все ж коріняться в єдиному початку – 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 повинна 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.

У ХХ 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 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» [116].

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,

¹ Представники: Н. Бердяєв, Л. Шестов, Б. Боун, У. Хокінг, Е. Брайтмен, Р. Флюеллінг, П. Ландсберґ, М. Недонсель, П. Рікер, Е. Муньє, Ж. Лакруа.

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 році автор цієї дефініції, один із найбільш знаних і, очевидно, найбільш продуктивних соціологів релігії сучасності Пітер Людвіг 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 році він був вимушений публічно спростувати власний прогноз „Сучасний світ, – писав Бергер у журналі «Національний інтерес» зимою 1996 року, – за кількома винятками, є так само нестямно релігійним, яким він був завжди, причому у деяких місцях – ще більш релігійним, ніж колись” [116].

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 (від лат. scientia – знання, наука) як ідейна позиція, що представляє наукове знання найвищою культурною цінністю і основоположним чинником взаємодії людини зі світом [421], такий світогляд, позитивно оцінює соціальні наслідки НТР, передбачає головним завданням філософії – обслуговування бурхливого розвитку науки.

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 однастайними 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.

Заслуговує уваги, з огляду на предмет дослідження, проблема мови в філософії неопозитивізму. Розуміючи мову як систему знаків, яка служить засобом людського мислення і спілкування, людство в пізнанні світу і спілкуванні користується як природною мовою (мовою слів, понять, вплетених у безпосередню життєдіяльність) так і штучними формалізованими мовами (мова формул, знаків). Еволюцію неопозитивізму визначило прагнення більш глибоко вивчити суть мови. Якщо логічний позитивізм концентрував свою увагу тільки на логіку мови науки, вивчаючи інваріантний каркас штучних мов, то вже лінгвістична філософія Вітгенштейна (інша форма неопозитивізму) звертається до аналізу природної мови, більш складної і рухливої по своїй структурі. Вітгенштейн висунув і обґрунтував логіко-мовну модель відображення світу, затверджуючи, що ціла хмара філософії концентрується в краплі граматики. А постпозитивізм приходиться 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 [11, с. 148].

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

Науково-технічна революція породила не тільки суперечності, але і надії на можливості всіх складностей людського життя з допомогою тієї ж науки. Людство ніби заворожене почало споглядати науково-технічні чудеса, що були плодом розумової діяльності людей. Виникає філософський напрям, що отримав назву «сцієнтизму» (від латинського наука) та «техніцизму». Існувало кілька його течій: «кібернетична», «генетична», «комп'ютерна» і т.д. Сцієнтизм як відображення нового періоду розвитку науки і нового рівня освоєння людиною природи, при допомозі нових галузей наукового знання породив і нові соціальні теорії. Одна за одною виникали і витісняли попередню теорії індустріального, постіндустріального, інформаційного суспільства. Все це створило своєрідний культ науково-технічних знань і за своєю суттю відновляло раціоналістичне філософствування, але не в його Кантівсько-Гегелівській логічній формі, що волею чи неволею вело до ідеалізму, а в приземленій формі пристосованого до сьогоднішніх наукових відкриттів філософствуванні [84, с. 454].

У ХХ 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 ХХ 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, «обездушєння» культури [428].

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 році 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 [61].

В.І.Вернадський виділяв декілька основних передумов становлення ноосфери:

1) Людство стало єдиним цілим. Світова історія охопила як єдине ціле всю земну кулю, абсолютно покінчила з відокремленими, мало залежними один від одного культурними історичними областями минулого. Зараз «немає жодного клаптика Землі, де б людина не могла прожити, якщо б це було їй потрібно».

2) Перетворення засобів зв'язку та обміну. Ноосфера – це єдине організоване ціле, всі частини якого на самих різних рівнях гармонійно пов'язані і діють узгоджено. Необхідною умовою цього є швидкий, надійний, такий, що долає найбільші відстані, зв'язок між цими частинами, постійно йде матеріальний обмін між ними, всебічний обмін інформацією.

3) Відкриття нових джерел енергії. Створення ноосфери передбачає настільки корінне перетворення людиною навколишнього його природи, що йому ніяк не обійтися без колосальних кількостей енергії.

4) Покращення добробуту працюючих. Ноосфера створюється розумом і працею народних мас.

5) Рівність усіх людей. Охоплюючи всю планету як ціле, ноосфера за самою своєю суттю не може бути привілеєм якоїсь однієї нації або раси. Вона справа рук і розуму всіх народів без винятку.

6) Виключення війн з життя суспільства. Війна, загрожуючи самому існуванню людства, є найбільшою перешкодою на шляху до ноосфери. Звідси випливає, що без усунення цієї перешкоди досягнення ноосфери практично неможливо і, навпаки, знищення загрози війни буде означати, що людство зробило великий крок до створення ноосфери.

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... породжували болісні запитання «Чому так?» і «Що далі?». Йшлося не лише про кризу розуму – а про кризу ідеалів європейської культури. Освічена, цивілізована людина ХХ ст. виявилася не в змозі забезпечити ані собі, ані людству справедливість, щастя та мир. Постає питання, чому світ, організований на основі науки, техніки, технологій обернувся проти людини та їй загрожує? [342]

Людська історія ХХ ст. засвідчила, що науковий та технологічний розвиток безпосередньо не гарантує культурного піднесення та виваженості. Навпаки, бурхливий розвиток науки, техніки та технологій породив у людини ілюзію, що вона всемогутня та може творити світ на власний розсуд.

Дослідивши праці фахівців різних галузей науки, що вивчали концептуальні питання становлення інформаційного суспільства, зокрема Ю. Хаяші, Д. Белла, Д. Лайона, М. Маклюена, 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 і 60-ми рр. ХХ 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.), «Конттури політики сприяння інформатизації японського суспільства» (1969 р.), «План інформаційного суспільства» (1971 р.), «План створення інформаційного суспільства – національна мета до 2000 року» (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 [540], 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” [540], 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» [540].

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» [540]. 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 приходиться до висновку про трансформацію сутності особистості і появу нового типу людей: на зміну «Homo sapiens» приходять «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 сформуєть поліцентроване, комбіноване суспільство, схоже на живий організм, з розгалуженою мережею безпосереднього зв'язку, спроможного швидко і динамічно реагувати на зміну зовнішнього середовища [539].

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 [538].

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 [577]. 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 зароджується в наших

життях, і ті, хто не здатний побачити її, намагаються подавити її. Ця 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. Частина нової цивілізації існують вже зараз. Мільйони людей вже налагоджують своє життя відповідно до ритмів завтрашнього дня. Інші люди, що бояться майбутнього, біжать в безнадійне, даремне минуле; вони намагаються відновити вмираючий світ, у якому вони з'явилися. Початок цієї нової цивілізації – єдиний і такий, що володіє найбільшою вибуховою силою, факт часу, в якому ми живемо. Це – центральна подія, ключ до розуміння часу, що слідує за сьогоднішнім. Це – явище таке ж глибоке, як і Перша хвиля змін, викликана 10 тисяч років назад впровадженням сільського господарства, або як Друга хвиля змін, пов'язана з промисловою революцією. Ми – діти подальшої трансформації – Третьої хвилі» [578].

В 70-ті роки відбувається конвергенція двох майже одночасно створених концепцій: інформаційного суспільства і постіндустріалізму. Концепція професора соціології Гарвардського університету Данієля Белла була сформульована у його роботі «Прихід постіндустріального суспільства»(1967), де він виокремлює низку аспектів постіндустріального суспільства: перехід від індустріального суспільства до сервісного (обслуговуючого) суспільства; вирішальне значення кодифікованого теоретичного знання для здійснення технологічних інновацій; – перетворення нової «інтелектуальної технології» у ключовий інструмент системного аналізу і теорії прийняття 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 – дороги, канали, залізничні та повітряні магістралі; все це дозволяло пов'язувати воедино різні локалітети суспільства і здійснювати переміщення товарів і людей. Другою інфраструктурою були засоби передачі енергії – водяне колесо, парові машини, газ, електрика, нафтопроводи. Третьою інфраструктурою були комунікації – спочатку пошта і газети, потім

телеграф і телефон, зараз радіо і телебачення; все це зіграло роль каналів колосального інформаційного вибуху, свого роду бомбардування сенсорного апарату людини, розширення соціальної та психологічної взаємодії людей, яка зараз зростає експоненціально. У наступні два десятиріччя будь-які зміни в першій інфраструктурі – на транспорті – малоймовірні. ...У другій інфраструктурі – енергетичній – є деякі нові тенденції... По-справжньому важливі соціальні зміни в майбутні два десятиріччя відбудуться в третій інфраструктурі в міру того, як злиття воедино технологій телефону, комп'ютера, факсиміле, кабельного телебачення і відеодисків буде вести до все більш глибокої реорганізації способів комунікації між людьми, до скорочення, якщо не до повної ліквідації паперу як матеріального носія інформації, до нових способів проведення дозвілля, до реорганізації освіти на основі комп'ютерного навчання і широкого розповсюдження відеодисків. Можна скептично ставитися до екстравагантних заяв про прийдешню революцію в освіті під впливом комп'ютерів, відеомагнітофонів, але як би там не було, у сфері передачі даних (особливо економічної інформації у сфері бізнесу) і розвитку мереж даних комп'ютеризація викличе небачені соціальні зміни» [32, с. 335].

В суспільстві він прогнозує поділ населення за родом занять і надання перевага професійно-технічного класу. Таке суспільство організується навколо знання з метою суспільного контролю й спрямування нововведень і змін; а це, у свою чергу, започатковує нові суспільні відносини і нові структури, які повинні скеровувати політичне життя. Вирішальними у організації рішень і спрямуванні змін, тобто основою теоретичного знання, є першість теорії над емпірією і кодифікація знання в абстрактну систему символів, які, як і в будь-якій аксіоматичній системі, можуть використовуватися для висвітлення багатьох відмінних одна від одної й різноманітних ділянок досвіду. У постіндустріальному суспільстві, на думку Бела, еліта – це еліта знаючих людей. «Така еліта має владу в межах інститутів, пов'язаних з інтелектуальною діяльністю – дослідних організацій, університетів тощо, – але у світі великої політики вона володіє простим впливом, не більше. Остільки, оскільки політичні питання все

тісніше переплітаються з технічними проблемами (у широких межах – від військової технології до економічної політики), «еліта знання» може ставити проблеми, ініціювати нові питання і пропонувати технічні рішення для можливих відповідей, але вона не має влади сказати «так» чи «ні». Останнє є прерогативою політиків, але не науковців чи економістів. У зв'язку з цим вкрай перебільшеною є ідея про те, що «еліта знання» може стати новою елітою влади. Що, однак, вірно, так це те, що в сучасному суспільстві зростає егалітаризм, чому великою мірою сприяють різні групи «еліти знання», особливо молодіжного. У цілому сучасне суспільство складається з безлічі утворень, внаслідок цього з'являється і безліч еліт, так що їх координація стає все більш складною проблемою.» [32, с.340].

Таким чином, Бел вже тоді передбачив, що на новому етапі розвитку суспільства ускладниться соціальна структура. Проте, більше про цю рису нового типу суспільства пише Мануель 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. Термін «Інформаційна епоха», на його думку, має велику аналітичну цінність, оскільки дозволяє описати якийсь період змін, які поступово наростали, починаючи з 70-х років минулого століття.

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, пише М. Кастельс, 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» [456, 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 дезинтеграції.

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 Алена Турена, вводить поняття «Ідентичність опору» і «ідентичність, спрямована в майбутнє» [455, с.16]. Цей опір спрямований проти основної тенденції розвитку сучасного суспільства – глобалізації.

М. Кастельс наводить основні групи співтовариств, які, на його думку, можуть через ідентичність опору перейти до ідентичності, спрямованої в майбутнє і тим самим сприяти перетворенню суспільства загалом із одночасним збереженням цінностей опору інтересам глобальних потоків капіталу й інформації. Поширення логіки мережевих товариств 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 мережа 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 Інтернет. 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 група працівників експертної інформаційної праці. В той же час, робочий клас «вимивається» і з'являється маса «працівників загального типу». З'являється небезпека сусідства декласованих елементів з новою культурою інформаційних працівників. Інформаційний працівник стає головним джерелом багатства і не прив'язаний до конкретного робочого місця. Також традиційна форма роботи (повний робочий день, чітко визначені посадові обов'язки) повільно, але розмиваються. Таким чином відбувається індивідуалізація праці у трудовому процесі. Кастельс стверджує, що ядро трансформацій, які переживає сучасний світ, пов'язане з технологіями обробки інформації і комунікацією.

Процеси перетворень істотно міняють і політичні процеси. Лідерство стає все більш персоніфікованим, а шлях до влади лежить через створення іміджу – політичні діячі виявляються залученими в гру, що ведеться через засоби масової інформації і самими засобами масової інформації. «Залежність від мови засобів масової інформації, що мають під собою електронну основу, підкреслює М. Кастельс, приводить до наслідків, що далеко йдуть, 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» [150, с.27]

При цьому, легко застосовувати акценти, встановлені Кастельсом, та його розуміння явищ з економічної площини в соціальну. На прикладі, брендінгу можна звернути увагу, що для одержання інвестицій потрібний символ загально визнаної здатності додавати товарам і послугам ціннісні якості. В світі складних мереж виробництва і дистрибуції брендінг може здійснюватися головним чином на основі управління процесом впровадження інновацій і суворого контролю кінцевих результатів. Ефективне використання інтернет-технологій дозволяє забезпечити зворотний зв'язок між всіма компонентами мережі та процесами виробництва/реалізації, а також виявлення і виправлення помилок. Таким самим чином зараз працює соціальний, в т.ч. політичний брендінг. 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 он-лайн. Цей підхід Кастельса органічно екстраполюється на політико-правову сферу. Нормотворчість та правозастосування вимагає не лише публічних обговорень на етапі підготовки проєктів 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» [149]:

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 галузях генної інженерії, нанотехнологій і мікроелектроніки, конвергенція яких може привести до несподіваних відкриттів, використання яких пов'язане з високою соціальною і етичною відповідальністю.

Ці проблеми ставлять велику кількість запитань, 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? [149].

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» Петер Друкер (Peter Ferdinand Drucker) 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 [451]. Хоча Друкер говорив в основному, про економічний вимір – компанії найкраще працюють, коли вони децентралізовані – проте сьогодні свідчить, що децентралізація є необхідною умовою існування демократичного суспільства.

2) У книзі 1959 року «Орієнтири майбутнього» [477] 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 [479], 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 [480, 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 [552, 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» [476, 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 [478, 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 [134, 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» [40, 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 [13, 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*». Це жива істота, яка володіє мовою і свідомістю, здатна створювати знаряддя праці і користуватися ними.

«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 [359].

«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 і «створюють» 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 [359].

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. Ананьєв зазначав, що людиною народжуються,

особистістю – стають, а індивідуальність завойовують [10, 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, особливості 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 спільності, в якій вона існує; 4) поведінка особистості залежить від її неповторних особистісних характеристик, через які заломлюється громадський і особистий життєвий досвід [88, 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 [ibid., 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, з одного боку, індивідуально виражає значимі риси певного суспільства, інтегрує соціальні відносини зовнішнього середовища і виробляє своє, особливе ставлення до зовнішнього світу. З іншого боку, економічні, політичні та соціальні відносини переломлюються через внутрішній світ особистості, виявляються в її діяльності як особисте ставлення до об'єктивної дійсності. В цьому випадку особистість виступає як суб'єкт соціальних відносин, який керується в поведінці своїми потребами, інтересами, соціальними установками, ціннісними орієнтаціями. Соціальні відносини, інтегровані особистістю як певна система зв'язків індивідів, які склалися в процесі їхньої взаємодії в умовах певного соціального середовища та які виявляються в діяльності і поведінці, як і її соціальні якості, є предметом соціології особистості. Основні складові

структури особистості, які впливають на її поведінку в суспільстві, і визначають її як суб'єкта соціальних відносин.

Як об'єкт соціальних відносин особистість характеризується соціологічною теорією за допомогою таких понять як соціалізація, тобто процес виникнення особистості, перетворення біологічно заданого матеріалу силами соціальної дійсності; соціальна ідентифікація – усвідомлення особистістю своєї належності до певної спільноти; рольова ідентифікація – сприйняття суспільно заданих функцій і групових вимог як таких, що відповідають інтересам і потребам суб'єкта.

Як суб'єкт соціальних відносин особистість розглядається соціологічною теорією через систему таких понять: самоусвідомлення особистості, тобто усвідомлення власної самобутності в межах соціуму; нормативна свідомість і система ціннісних орієнтацій (сприйняття і оцінка соціальної діяльності, поведінка за конкретних умов); потреби, мотивації, соціальні установки, соціальна поведінка, тобто поняття, які широко використовуються в психології.

Поняття «соціалізація», як уже згадувалося, виникло в західній соціології наприкінці XIX ст. з метою позначення основного механізму взаємодії однієї людини з іншою, із суспільством загалом. Таким механізмом вважалося соціальне наслідування, що регулювалося суспільством через систему освіти і виховання, сім'ю та громадську думку.

У процесі розвитку наук про людину сформувалася сукупність поглядів на соціалізацію, що об'єднує такі ідеї: про нерозривний зв'язок з освітою та вихованням; про зв'язок соціалізації з адаптивними процесами; про соціальні контакти як один із змістовних аспектів соціалізації; про значення самосвідомості, соціальної орієнтації та розвитку мови для ефективної соціалізації. У контексті цих ідей соціалізація розглядається як набуття людьми соціального досвіду та ціннісних орієнтацій, потрібних для виконання соціальних ролей.

До сучасних моделей соціалізації належать психоаналітична, або «особистішого контролю» (З. Фрейд); «рольового тренінгу» (Т. Парсонс); «соціального навчання» (Г. Долат, Б. Скіннер та ін.); «міжособистісного

спілкування» (Ч. Кулі, Дж. Мід та ін.); «когнітивна» (Ж. Піаже, А. Маслоу та ін.); «еволюційна» (Е. Еріксон). Усі вони розглядають соціалізацію як процес взаємодії людини з навколишнім світом, хоча деякі з них обмежують терміни перебігу соціалізації віковими рамками – дитинство, юність, зрілість. Проте за різних умов змін у навколишньому середовищі соціалізації зазнає значна частина населення [200, с.89].

Одне із загально визначень визначень таке: «соціалізація (від лат. *socialis* – суспільний) – процес засвоєння індивідом знань, досвіду, норм і цінностей, включених до системи соціальних зв'язків і відносин, необхідних для його становлення і життєдіяльності в даному суспільстві» [357, с. 479]

При цьому деякі автори розглядають соціалізацію як залучення індивіда в соціальне середовище під впливом дії на особистість різних сторін суспільного життя, соціальних інститутів; при такому підході особистості відводиться пасивна роль. Деякі вважають, що соціалізація – процес саморозвитку особистості, формування активної життєвої позиції. На думку інших науковців, соціалізація – не що інше як просте пристосування до умов життя. Virізніють: професійну соціалізацію – як формування компетентного спеціаліста, а також політичну соціалізацію – як формування політичного діяча тощо.

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 [431, 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» [76, 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 [156].

Вплив інформатизації 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 [132, 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. Особливої уваги заслуговує «забруднення» інформаційного середовища і проблема «інформаційного шуму». Це питання досліджувалось нами раніше [136], 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 переважання 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 чужорідної інформації. Небезпеки виникають насамперед тоді, коли людина не має надійного «інформаційного щита».

Особливої уваги з цього приводу заслуговує питання правового виховання і правової освіти. Правова освіта в цивілізованих суспільствах є невід'ємною складовою всіх щаблів загальної системи освіти, починаючи з дошкільних закладів, продовжуючи у середній і вищій школах. В Україні правова освіта є «прерогативою» юристів. Для пересічних громадян – в шкільних і вузівських навчальних планах в кращому випадку присутня дисципліна «Правознавство» з однією годиною на тиждень. В переліку предметів, з яких проводиться зовнішнє незалежне оцінювання «Правознавство» «з'являлось» лише один раз – в 2008 році. З переліку обов'язкових дисциплін для викладання у вищій школі «Правознавство» було вилучено в 2010 році.

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 “покрашена”, не обов’язково має правильне усвідомлення.» [13, 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, оточуючий нас предметний світ складаються з зусиль конкретних індивідів, є результатом їх, діяльності, продуктом конкретно-історичної форми відношення людей до природи. Проте саме цей результат стає об’єктивною умовою людського існування. Незважаючи на те, що люди самі творять свою історію і суспільне життя, форма «включення» їх в суспільно-історичний процес обумовлена не тільки ступенем освоєння ними культурної спадщини, не тільки їх, суб’єктивними прагненнями, свободою вибору, але й об’єктивними умовами матеріального виробництва, досягнутим рівнем суспільного розвитку, в тому числі – рівнем суспільної свідомості.

Отже, те, що має назву «соціальної детермінації», є фактором залежності людей від продуктів та результатів їх, власної діяльності [370, 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.

Суспільне життя відбувається в трьох основних сферах, або реальних процесах життєдіяльності, – в матеріально-економічній, соціально-політичній і духовно-культурній. Потрібно підкреслити, що визначення трьох основних сфер суспільного життя має певною мірою відносний, умовний характер, тому що реальна людська життєдіяльність – це тісний взаємозв'язок і взаємовплив цих сфер.

Соціальні відносини охоплюють всі сфери суспільного життя та діяльності. Матеріально-економічні відносини включають у себе виробничі відносини, технологічні, відносини розподілу, обміну; соціально-політичні – політичні, правові, моральні, класові, національні, соціально-групові; духовно-культурні – моральні, релігійні, художньо-естетичні, наукові відносини. Суб'єктами суспільних відносин є індивіди та соціальні спільноти, саме їх, інтереси та потреби лежать в основі суспільних відносин.

Звернемо увагу на окремі аспекти змін в соціальному бутті людини у зв'язку зі становленням інформаційного суспільства.

Географічний аспект. В інформаційному суспільстві геопростір не зникає, однак суттєво змінюється суспільно-географічне бачення людини. В інформаційному суспільстві, за рахунок розвинутих транспортних та інформаційних комунікацій, людина перетворюється з точково-локалізованого об'єкта в геопросторово-поширений об'єкт, який не має чіткої точкової просторової локалізації. 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. Стає дуже проблематично визначити соціальні статуси конкретних учасників даних спільнот, оскільки система позначення стає цілком умовною

Психологічний аспект. «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». [33, с.409]. Виникає так звана ситуація плюралізму життєвих стилів у межах подолання суперечностей між збереженням цілісності та різноманітністю. Іншими словами, ідентичність проявляється як необхідність впорядковувати різноманітність. Специфіка такого вибору полягає у тому, що традиційні метенаративні ціннісні системи, через які обґрунтовується моральна поведінка, застосовуються, враховуючи конкретну ситуацію. Таким чином постає проблема якісної характеристики тих альтернатив, які пропонуються людині для вибору. Загалом часто така «свобода вибору» скеровує нас до зайвих, непотрібних, навіть шкідливих речей, тоді як насправді кардинально сутнісні моменти не те що не вибираються, але й не усвідомлюються. А 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). Саме

міщанський етос став безпосереднім чинником формування сучасної масової людини і культури без усталених мотивованих ідеалів, моральних принципів та соціальної відповідальності. Найголовніші ознаки філістерської 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 – є водночас ознаками духовної кризи сьогодення. Людина на цьому рівні є результатом гри анонімних сил, за яку вибирає світ. Їй потрібно тільки насолоджуватись життям, а не відволікатися на думки про оточуючих. Цей стан ще можна дефініювати як еру індивідуалізму з втратою індивідуальності, унікальності та епоху нарцисизму. «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» [328, с.125].

3. 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» [24, 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)). Наприклад, доволі показовими є дослідження у цій сфері Є. Сапожнікова, який аргументовано виводить розлади психіки (найперше, депресію) зі споживацьких пріоритетів суспільства [333, 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» [333, 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 неупорядковані зміни» [150, 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.

Культурний аспект. І. Герасимова, 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.

Надмірна індивідуалізація. Людина апіорі є індивідуальною, але зловживання цим принципом, що багато в чому характерне для сучасного людства призводить до зневіри в колективних цінностях, меркантилізму та орієнтації на споживацький спосіб життя. Людина має повернути собі колективне відчуття існування, паралельно розвиваючи індивідуалізм, бо в протилежному випадку, людина ризикує потонути в власному егоцентризмі, криза у когнітивній сфері виражається у забутті духовних основ творчості та слабкій реалізації морального-духовного аспекту творчості [70, с.224].

У сучасному світі на людину найбільше впливають ЗМІ, які нав'язують стереотипність мисленнєвих актів, програмування рішень. Матеріальний світ опиняється під впливом новітніх технологій, соціальний – під впливом медіатизації та віртуалізації, внутрішньо-суб'єктивний – під владою афектів внаслідок нівеляції й розпаду етичних норм.

Техногенна, інформаційна епоха, в котру живе сучасна людина, розкриває принципово нові сторони та моменти людської сутності, котрі акцентують увагу на таких моментах як: людина – комунікатор, людина – винахідник, людина – інформаційна істота, яка живе за принципово новими моделями взаємодії. Ці сторони людини найбільш повно розкриваються в сучасній епосі, можемо побачити трансформацію людської свідомості, культури, моралі, що свідчить про появу нового типу людини, яка суттєво відрізняється від своїх попередників [393].

Стрімко змінюється ситуація в сучасному суспільстві, що ставить перед людиною завдання, до вирішення яких її не готували ані система виховання, ані весь попередній досвід людства. Людина може успішно

функціонувати в соціальній системі, володіючи певними особистісними рисами і поведінковими навичками. Зміна типу соціалізації обумовила виникнення нового соціального типу особистості – особистості суперечливої, перехідної, що сполучає в собі ціннісні орієнтації й норми індустріальної і інформаційної епох.

Економічний аспект. Перехід від прискореного технологічного розвитку до передових технологій у світовій економіці вимагає нової якості трудових ресурсів і їхньої здатності до інновацій. «Інформаційна економіка» кінця ХХ ст. створює високооплачувані робочі місця, що вимагають від працівника іншого рівня і якості його кваліфікації. Так, наприклад, перехід від ієрархічних структур до мережевих дозволяє формувати новий тип виробництва. Крім індустріальних гігантів у конкурентній боротьбі на світових і національних ринках діють малі й середні фірми. На ринку найбільше цінується нове. Тому великі корпорації створюють гнучкі децентралізовані організаційні структури, змінюють ієрархічні системи управління мережевими, намагаються привчити працівників відповідати цілям фірми. Кадрова політика базується на принципі : «Високим технологіям – висока техніка контактів з людьми». 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.

Екологічний аспект. Людина може і повинна жити в гармонії з природою, про свідчить наша історія, котра говорить про те, що діяльність людини може реалізовуватись в унісон з природою, і людське щастя багато в чому визначається саме цим критерієм. В той самий час, бурхливий розвиток цивілізаційної діяльності призвів до експлуатації природи людиною і сьогодні ця проблема стає однією з найфундаментальніших.

Політичний аспект. 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. ІКТ можуть використовуватися в різних формах, а не тільки для голосування. В рамках підходів за принципом «знизу- вгору» громадяни і організації можуть використовувати їх як засоби для того, щоб їх голоси були почуті, партії – для проведення кампаній, а уряди і адміністративні органи – для вдосконалення тих послуг, які вони надають громадянам, шляхом впровадження електронних методів подачі звернень чи проведення консультацій [110].

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.

Правовий аспект. 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. Про це ширше в наступних підрозділах.

1.2. Генеза прав і свобод людини: від античності до інформаційного суспільства

Інтенсивний розвиток і вплив інформаційних технологій у всіх сферах суспільного життя доправили до становлення нового статусу людини – суб'єкта відносин, які вимагають наділення його відповідними правами та обов'язками. Глобальний інформаційний простір ігнорує кордони, змінює спосіб сприйняття дійсності і чинить визначальний вплив на формування людської особистості, як це було досліджено в попередньому розділі.

Ці нові реалії інформатизації і глобалізації, стрімкі соціальні зміни об'єктивно вимушують державу, суспільство і кожну людину переосмислити концептуальні підходи до прав і свобод людини і громадянина.

Питанням прав і свобод людини присвячено величезну кількість праць різними мовами. Для цілей цього долідження використано англо-, польсько-, російсько-, українськомовну наукову літературу, статистичні дані та результати інших соціологічних досліджень, законодавство і судову практику, в т.ч. міжнародну, публіцистику та контент нових медіа.

Проте перш ніж звернутись до визначення особливостей прав і свобод людини як складової інформаційної безпеки, вважаємо за потрібне звернути увагу на становлення теорії прав людини.

Людина посідає центральне місце в соціальних науках. В філософії, соціології, психології чи праві вибір відповідно концепції визначає предмет і метод, а отже – і обумовлює результати досліджень. Як вже було вище згадано для означення людини різні науки використовують різні поняття – людина, індивід особа, особистість, індивідуальність. В праві отримуємо ще кілька категорій, пов'язаних з участю людини у суспільних відносинах, виконуваними функціями та соціальними ролями – громадянин, особа без громадянства, іноземець, фізична особа, публічна особа, дитина, особа з особливими потребами (інвалідністю)², державний службовець та інші. В правовій доктрині від використаної категорії буде залежати

² Наявність особливих потреб не завжди передбачає інвалідність, особливо в умовах корумпованої медицини, недосконалого правового регулювання надання статусу і соціального захисту осіб з інвалідністю.

зміст суб'єктивних прав та свобод, а також їх правове забезпечення. Для прикладу, в радянській та пострадянській правовій літературі в основному використовувались дефініції – людина, особа, громадянин. При цьому коли йшлося про «людину», мала на увазі, насамперед, біологічна істота, «особа» визначала соціальний характер людини, що мала історично обумовлений ступінь розвитку, користалася правами, які передбачило суспільство і виконувала обов'язки, ним же покладені. І з появою держави і політичної влади, соціальна категорія «особи» набуває політичного змісту і змінюється на категорію «громадянин», яка відображає відносини між людиною і державою. В трьох згаданих категоріях можна простежити домінуючу концепцію політичної і правової доктрин в пострадянському просторі, рудиментом якого є ідея «людина для держави», а не «держави для людини».

В публічному праві, особливо міжнародному, маємо ще одну категорію, яка українською перекладається зазвичай як «кожен», англійською «everyone», як людина, що є частиною суспільства. Такий підхід є властивий лібералізму, як суспільно-політичної доктрини що визначає свободу як підставу людської природи і найвище вартість, що базується на індивідуалістичному баченні людини і суспільства. Для прихильників лібералізму найвищою цінністю є людина і її воля.

В правовій мові категорія «фізична особа» вживається задля визначення людини в цивільних правовідносинах, в період від народження до смерті, на відміну від юридичних осіб.

Особа як категорія привертає увагу до персоналістичної концепції (від лат. *Persona*, тобто особа) і виняткового морального статусу людини, який є головним в християнському і нехристиянському персоналізмі. [398, с. 42]

Кріль 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 [590, 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 усєї спільноти (людства).

Зовсім протилежну думку висловлює Петер Зінгер (Peter Singer), сучасний філософ, визнаючи особою тільки істоти із самосвідомістю [526]. Згідно його праць, приналежність до виду *Homo sapiens* не є визначальною і етично значимою. Зінгер вважає допустимими легалізацію абортів, добровільну і адобровільну (на відміну від недобровільної), а також зоофілію.

Чому мають значення ці всі роздуми щодо змісту категорій? Ким є людина? Від чого залежить його людськість? Якщо від здатності себе усвідомлювати (самосвідомості), то коли він її набуває і чи може втратити? Чи набуття самосвідомості штучним інтелектом чинить його людиною? Від відповідей на ці питання залежить визнання (або не) прав і свобод людини.

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 [549]. Гідність людини є нерозивно пов'язана з фактом буття людиною. На буття людиною не маю 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. [462, с. 43] Гідність людини не може залежати також від громадянства як правового зв'язку з державою [ibid., с. 42].

Зараз визнається, що гідність людини властива їй від природи, а не з будь-якого рішення влади, є основою прав людини, прав громадянина. [519, с.28].

Зараз це здається очевидним, однак в історії було по-різному. Розмірковуючи про історичне становлення прав людини, слід мати на увазі, що не йдеться про виникнення чи еволюцію прав людини як таких. Згідно теорії прав людини вважається, що вони закорінені в людській природі, яка в своїй основній онтологічній суті є незмінною і залишається

тією ж як в епоху стоїків і Цицерона, так і сьогодні. Тільки формулювання прав людини і їх обсяг, їх закріплення в праві (зокрема, міжнародному), є змінними і залежать від культурного розвитку людства і цивілізації часу. Як морально-правові дефініції вони є спадщиною багатотисячолітньої людської культури, що розвивалась в різних частинах Земної кулі [592, с.169].

Найстаршим джерелом знання про права людини і про головні засади суспільного життя вважаються релігійне передання, з яких для європейської культури найбільше значення має Декалог [537, с.142]. Зміст Декалогу має, насамперед, релігійний характер, проте через спрямованість до людської особи, відображає природу людини і умови її існування. Містить також основоположні норми суспільного життя, з яких можна вивести розуміння базових прав людини. М. Кранпец (М. Крапеч) звертає увагу, що «частина заповідей Декалогу сформульована позитивною мовою і стосується культу Бога, поваги до батьків, а друга частина – негативною мовою, тобто мовою що зобов'язує усіх і завжди» [525, с. 140]. В першій групі найважливішим є право релігійної свободи (у поєднанні з свободою вільно виражати релігійні переконання). Друга група зачіпає право на життя, сім'ю і сімейне життя, право на пізнання правди (відоме потім в епоху Ренесансу як *ius cognoscendi veritatem*), право власності. Нескладно помітити, що всі ці права сьогодні є базою правового статусу людини.

Сам Декалог, хоча і сформував свідомість народів християнської Європи (разом з євангельським законом), проте не був елементом світського законодавства (монаршого чи пізніше парламентарного). Його вплив на позитивне право є опосередкованим і більшою мірою морально-етичним [592, с. 173].

Існують суперечливі думки, що одним з найстарших кодексів світу щодо охорони прав людини є Звід законів (кодекс) Хаммурапі [531, с. 22]. Проте в ті часи не було мови ще ні про людину, ані про її права. Створений в XVIII/XVII ст. до Різдва Христового за часів царя Хаммурапі, володаря Вавилону. Його метою була уніфікація приписів звичаєвого права. Кодекс становили 282 статті, пролог і епілог, стосувались вони кримінального, цивільного і процесуального права. Кодекс Хаммурапі мав

казуїстичний характер, а система покарань опиралась на принципи таліону і на т.з. «дзеркальних покараннях» [ibid., с. 23]. Кодекс також визначав, що володарює для того, щоб гарантувати справедливість і захищати «слабких від злих вчинків сильних» [562].

На думку Е. Стилїанідиса (E. Stylianidisa), боротьба за захист прав індивіда розпочалася в античній Греції, де повсталала ідея, що проголошувала свободу природним правом громадянина [567, с.122]. В стародавніх Афінах (5 ст. до Різдва Христового) з'явилися перші закони, що забезпечували юридичну охорону основних громадянських свобод: свободи вчинку і слова у межах права, а також рівності прав громадян. Проте, у Афінійській демократії громадянські права надавалися лише вільно народженим чоловікам, проживаючим в межах міста. Цього періоду сягають також ж корені перших політичних прав. У прадавніх Афінах громадяни, за винятком жінок, дітей, приїжджих і невільників, користувалися активним і пасивним виборчим правом.

З того ми можемо зробити висновок, що якщо у філософській думці опрацьовано багато концепцій прав людини, то на рівні держави і права виступають перш за все права громадян.

Дуже рано, вже в софістів, знаходимо розмірковування над двоїстою природою права – натуральним правом і встановленим (позитивним) правом, а також щодо співвідношення цих двох джерел прав і обов'язків. Права і обов'язки людини, звичайно, знаходяться в межах обох видів прав, і, отже, справедливості (*dike*) і суспільного права (*nomos*), але по-різному. Розуміння цього співвідношення пов'язано з природою людини, яка становить основу для різних теорій природного права [592, с. 168].

Ідею природного права перейняли римські мислителі і юристи, які додали до природних законів переконання, що основним джерелом суверенітету є народ, який передає свою владу імператору [541]. Римський юрист Ульпіан (228 після Р.Х.), вводячи потрібний поділ закону (присутній вже у Цицерона) визначає закон природи, як *...quod natura omnia animalia docuit: nam ius istud non humani generis proprium, sed omnium animalium...* «Натуральне право є спільним для людей і тварин» [277, с. 56]. Юстиніан

в «Інституціях» впроваджує та визначає *ius gentium* як права, які «природній розум встановив для всіх людей» [520, с.17].

Від цих визначень можна перейти до Фоми Аквінського, який говорить, що кожен закон заснований на природному праві – оскільки він є реалізацією суспільного блага. Томістичний образ людини нерозривно пов'язаний із образом світу. Людина відчуває себе, що вона є тією, хто пізнає і відчуває. [576, с.76]. Людина в своєму внутрішньому досвіді виявляє, що діє автономно і, таким чином, через її дії виявляє себе як існуюче «Я». У контексті суспільного життя людина є метою (а не засобом) будь-яких дій, тому що вона є особою гідною, суверенною і виступає суб'єктом права [553, с.1009]. Влада не надає права, оскільки вони є невіддільними від самої природи людини, якою її обдарував Творець. Норми, створені владою, мусять відповідати природному праву, а інакше вони втрачають свою силу. Позитивне право не може бути справедливим, якщо не буде похідним від природного права. Варто нагадати, що св. Томі Аквінському приписується визначення концепції права опору, яка передбачає, що володар, який порушує встановлені Богом норми правління, втрачає помазання (*sacre*) і перетворюється в тирана, якого можна і потрібно усунути [496, с.85].

У середньовіччі виникають також перші документи, що мають правову силу, які поступово і вибірково започатковують повагу до прав людини. Ранній конституціоналізм був перш за все підтвердженням давніх привілеїв і власності, а також певним видом договору між королем і феодалами: привілеї в обмін на лояльність, лицарську службу або за гроші, як у випадку англійської *Magna Charta Libertatum* [550, с.25]. Привілеї, виданий в 1215 році, в середньовічній Англії королем Іваном Безземельним, став підставою громадянських прав і конституційних обмежень королівської влади. Визначались в т.ч. право на суд, свобода пересування, право власності. Бенефіціантом цих прав була лише частина населення т.я. магнати, феодали, міщанство і духовенство.

З часом відбулося відділення *sacrum* від *publicum*, а також відхід від цезаропапізму як наслідок розпад Західноримської імперії. Як пише Шусц

(Szuse): «Проведений на Заході розподіл світських справ від святих, сфер ідеології від політики виявився виключно плідним: без нього не було б майбутніх „свобод”, теоретичного виокремлення поняття „суспільства”, національних держав, ані реформації» [569, с.25].

Середньовічні права істотно відрізнялись від сучасної концепції прав. Хоча ідея власної ідентичності особистості і концепція індивідуалізму з'явилася вперше в середньовічному Заході, але права, як правило, стосувались не стільки окремих осіб, кільки спільнот або станів [550, с.26]. Середньовічні права та імунітети королі надавали конкретним людям або станам. Сен Амартія (Sen Amartya) звертає увагу на нерівномірний розвиток двох основних елементів сучасної концепції прав людини: свободи (толерантності) і рівності [560, с.175].

Засади рівності і свободи в новий спосіб прозвучали в школі природного (натурального) права. Її появі передувало так звана школа з Саламанкі видатних іспанських юристів (de las Casas, Francisco de Vitoria, Francisco Suárez). Школа природного права повстала на ґрунті епохи Ренесансу із властивими їй змінами у сфері економіки (народження капіталізму), техніки, суспільної думки і мистецтва, науки (у тим географічні відкриття), врешті державного ладу – в способах правління. Розвиток школи природного права припадає на XVII ст. Головні постаті цієї школи: Гуго Гроцій (Про право війни і миру, 1624), Томас Гобс (Левіафан, 1651), Джонн Локк (Два трактати про правління, 1690 р.), Самуїл фон Пуфендорф («Про право природне і право народів», 1672 р.). Головний принцип цієї теорії стверджує, що люди, які живуть в природному стані, тобто перед перетворенням своїх спільнот в суспільство, користувались безперешкодно і безумовно, правами, що пов'язані з їх людською природою: на життя, свободу, рівність і власність. Ці чотири закони згодом стануть каноном ліберальної концепції прав людини [527, с.22]. Школа природного права не опирається на релігійних передумовах, відходить від теоцентризму на користь антропоцентризму.

Доповненням школи природного права стала теорією суспільного договору (соціального контракту). Громадськість укладає договір з державою,

який передає владу, отримуючи натомість захист прав громадян на життя, свободу, власність і рівність перед законом. Укладаючи договір з державою, люди не відмовляються від своїх природних прав, навпаки – отримують формальні гарантії цих прав. Метою суспільного договору є їх посилення, тобто держава має завдання «позивітизувати» природні права (закріпити в рамках законодавства), а також забезпечення їх дотримання шляхом створення інституційних гарантій [527, с.22]. На думку Джона Локка люди передають державі всього лише обмежені прерогативи, що означає держава не може «творити» собі будь-які інші права в галузях, в яких індивідів мають свої невід’ємні права.

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. Монтеск’є сформулював принцип поділу влади на законодавчу, виконавчу і судову, і в його роботі «Про Дух законів» (1748) [218] він підкреслив взаємозалежність між свободою і верховенством закону. Жан-Жак Руссо в роботі «Суспільний договір» (1762) [331] 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. Невід’ємний суверенітет народу покликаний забезпечити захист прав особистості від зловживань влади. Ідея свободи, яка займає центральну позицію в моральній філософії Еммануїла Канта, повинна бути відображена в правовій свободі, на яку має право кожна людська істота в силу її людськості [527, 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). Далі більше. У другій половині вісімнадцятого століття дійшло до великих соціальних революцій: американської та французької, після чого були проголошені такі 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 [550, 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 Джона 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 сімнадцятому столітті в Англії, особливо в американських колоніях, які в вісімнадцятому столітті, вювали 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. Джон Локк у Другому трактаті про правління виправдовує систему рабовласництва.

У той час на континенті переважає інша концепція. Держава вважається «гарантом спільного блага і відповідальною за забезпечення

індивідуальних потреб» [555,с.11]. Як у російського письменника і публіциста Миколи Некрасова в «Забытой деревне»: «Вот придет барин – барин нас рассудит, Барин сам увидит, что плоха избушка, И велит дать лесу», – думает старушка» [230]. 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 [508, 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.

Дев'ятнадцяте століття відзначене апогеєм колоніалізму і зростанням капіталізму, з одного боку, і скасуванням смертної кари, антиімперіалізмом, робітничим рухом і початком руху за права жінок – з іншого.

В середині дев'ятнадцятого 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 більшого 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.

У 1929 році в Нью-Йорку Міжнародний інститут права прийняв Декларацію про міжнародні права людини, автором якого був російський

юрист і жертва більшовиків Андрій Мандельштам. Ця заява швидко і широко поширилася в середовищі неурядових організацій та університетів.

Необхідність міжнародних гарантій прав людини стала особливо очевидна на тлі подій в Німеччині. Починаючи з 1933 року, коли зароджується «новий німецький порядок» – аж до геноциду, вчиненого в Європі. Все це призвело до відродження ідеї прав людини в новому світлі.

Міжнародні акти – від Атлантичної хартії (1941) і Декларації Організації Об'єднаних Націй (1942 г.) до Статуту Організації Об'єднаних Націй (1945) – підтверджували важливість основних ідей прав людини. Всі ці ідеї «з західним корінням» тепер повинні були стати правами людини для всіх людей у світі. «Ця ідея була приваблива для західних інтелектуалів і неурядових організацій, але менше ентузіазму викликала у західних урядів, особливо великих держав. Всі вони були винні у вчиненні діянь, що суперечать проголошеним стандартам: Росія – великий терор і ГУЛАГ, Англія і Франція – колоніалізм, США – расизм і офіційна расова сегрегація» [550, с. 43]

Глендон пише «Проект права людини став периферійною поступкою на користь малих держав і реакцією на вимоги багатьох релігійних і гуманітарних організацій ... в квітні 1945 року, коли в Сан-Франциско на конференції ООН, було зрозуміло, що домінуючі держави не будуть підтримувати ідеї прав людини» [501, с.15].

Проте, серед офіційних представників більш ніж 50 країн з усього світу палкими прихильниками Декларації стали делегати з країн Латинської Америки, до яких згодом приєдналися представники ісламських, буддійських і деяких африканських незалежних держав. Насправді, ця коаліція з малих і бідних країн підтримувала прийняття Декларації прав людини і мала значний вплив на її форму. Ухвалення Загальної декларації прав людини 10 грудня 1948 року вважається першим значним досягненням Організації Об'єднаних Націй в області захисту прав людини. Це було зроблено без жодного голосу проти, з вісьмома такими, що утрималися. Є кілька версій, за якими Радянський Союз і країни-сателіти утрималися: чи через відсутність згадки про боротьбу проти фашизму, чи через недостатню

увагу до соціально-економічних прав, або ж тому, що Декларація заснована на принципі суверенітету держав, і тому суперечить Статуту Організації Об'єднаних Націй [523].

Саудівська Аравія утрималася, тому що протестувала проти рівності між жінками та чоловіками, а також свободи змінювати релігію, яка гарантовувалась декларацією. У Південно-Африканській Республіці в 1948 році почалося побудова системи апартеїду, що і послужило причиною утриматися при голосуванні.

Проте, підтримка країн третього світу для декларації не означала автоматичного впровадження в них прав і свобод людини. З дев'ятнадцятого століття, філософи і політики колоніальних країн розглядали свободу з точки зору нації, а не окремих осіб. Ідея індивідуальних прав і свобод, підпорядкована ідеї самовизначення і побудови сильної держави як гаранта прогресу.

Беручи до уваги аналіз історичних фактів і наукових публікацій, напрошується парадоксальний висновок – як демократичні, так і авторитарні режими виступають проти введення інструментів для забезпечення дотримання прав людини.

Цікавою деталлю є повна відсутність прав меншин в Статуті ООН і Загальній декларації прав людини. З одного боку, він передбачає, відмову від ідеї надання будь-яких колективних прав німцям після Другої світової війни. У той же час це влаштувало великі держави.

Загальна декларація прав людини стала результатом багатьох компромісів, поєднуючи різні традиції і цінності. По-перше, вона об'єднала обидві вищезгадані західні традиції розуміння прав. Основна частина декларації відповідно англо-американської традиції стосується базових прав і свобод «кожного», а також політичних і громадянських прав, але ключове поняття гідності походить з християнської думки. Ідея вільного і повного розвитку особистості запозичена з персоналістической філософії [208] Жака Марітена (Jacques Maritain).

Важливими елементами цього синтезу є поєднання свободи з економічною безпекою, і з головною метою Декларації – збереженням

миру в усьому світі. Тому, громадянські свободи і політичні права, як і права соціально-економічні та культурні розглядалися як рівно важливі. Розширено також порівняно з каталогом прав вісімнадцятого століття коло носіїв цих прав. Замість поняття «особа» вживається поняття «людина», чії права не є наслідком договору, але безпосередньо пов'язані з гідністю.

Декларувалося, що права людини є загальними. Проте, Загальна декларація прав людини (як і будь-яка інша) має місце бути в просторі і часі. Це породжує безліч питань: Якщо права існували споконвіку, вкорінені в природі людини, чому ж їх виявила тільки частина людства? Як пояснити той факт, що суспільство, яке проголосило універсальність прав, не визнає права інших спільнот на власне бачення? Концепція універсальності також є проблемою. Про яку універсальність йдеться – географічну, філософську або моральну? Раймон Паніккар (Raimundo Pániker Alemany) ставить під сумнів загальність прав: «Чи має сенс питання про виконання умов універсальності, якщо те ж питання універсальності далеко не загальна проблема?» [528, с.88].

На етапі створення другого покоління прав людини принцип універсальності застосовувався з метою усунення розбіжностей. Ален де Бенуа (Alain de Benoist), 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» [450].

Якщо ми припустимо, що ідеологія прав людини всупереч її західним коріння, 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 Макінтайр (Alasdair Chalmers MacIntyre), ставить під сумнів реальність і змістовну наповненість цих прав [450].

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), *puayata* (справедливий), *dharma* (обов'язок), китайський – *chuan* і *li* – влада і інтереси, арабська *haqq* – закон, який перш за все означає істину [ibid.].

Другим викликом стає універсальність теорії людської природи незалежно від часу і простору. Її інтерпретація призводить до потрібного протиставлення: між людиною та іншими живими істотами (людина є єдиним носієм природних прав?), між людиною і суспільством (людська особистість, по суті, індивідуалістична; соціальне середовище не визначає її характеру?), а також між людиною і Всесвітом (людська природа не пов'язана з загальним порядком речей?). Аналогічного протиставлення не зустрінеш в більшості незахідних культур. Чергову складність створює концепція індивідуалізму. У витоків європейської культури категорія «особа» (або особистість) сама по собі не існувала. Воно розглядалася як частина родини, роду або народу, складова буття Всесвіту. У холістичних культурах концепція індивідуальних прав не існує, оскільки вони заперечують сприйняття людини як самодостатнього атома, і домінують категорії двосторонніх зобов'язань.

Незважаючи на всі невідповідності, концепція двадцятого століття 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 Рене Кассін (Rene Samuel Cassin),

який виступав за культурний релятивізм в колоніальних війнах, писав: «в відсталих колоніальних суспільствах права людини можуть поставити під загрозу громадський порядок» [452, с. 962].

Під час холодної війни політики неохоче згадували про права людини. У кожній державі 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. Джон Фостер Даллес (John Foster Dulles) заявив, що США «не буде учасником жодного документа з прав людини, прийнятого Організацією Об'єднаних Націй» [515, с.59].

І тільки в 1966 році стало можливим прийняття наступних актів з прав людини – Міжнародного пакту про громадянські і політичні права та Міжнародного пакту про економічні, соціальні і культурні права.³ 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. [551]

В кінці ХХ століття в більшості конституцій світу були закріплені права людини. Віденська декларація 1993 року заявляє про заохочення і захист прав людини як питання першорядного значення для міжнародного

³ США не ратифікували останнього.

співтовариства і одночасно розширює перелік прав на такі категорії як біженці, переміщені особи, меншості, жінки і діти, інваліди тощо. У 90-ті роки міжнародне співтовариство прийняло низку конвенцій щодо захисту прав меншин – Декларація про права осіб, що належать до національних або етнічних, релігійних і мовних меншин (1992), Рамкова конвенція про захист національних меншин (1995). Права людини стали джерелом стандартів для міжнародних трибуналів, в тому числі Міжнародного кримінального суду.

По завершенню холодної війни, падіння комунізму, подолання апартеїду і поширення ідей демократизації, могло здаватися, що ідея прав людини прийнята в усьому світі. Але, як виявилось, щоб «перемігши» ідеологічні загрози в сучасному світі під загрозою опинилася сама ідея прав людини.

У матеріалах Європейської регіональної конференції, організованої Комісією Франції у справах ЮНЕСКО та Радою Європи «Етика і права людини в інформаційному суспільстві» є думка, з яким не може не погодиться автор: «У 1950 р було простіше проголошувати загальні права людини (зокрема, свободу вираження думок), ніж сьогодні, коли в своєму власному будинку і в своєму приватному житті ми стикаємося з настільки різноманітними увявленнями про світ» [483, с.18].

На рубежі XX і XXI століть інформаційна революція торкнулася всіх сфер життєдіяльності суспільства – політики, економіки, права, державного управління та міжнародних відносин, фінансів, науки, освіти, культури. Інформаційні ресурси суспільства стали визначальним фактором його розвитку і більшість країн констатували початок нової епохи – інформаційного суспільства. Вперше досить чітко увявлення про інформаційне суспільство були сформульовані в 60-х – початку 70-х років двадцятого століття. Не вдаючись в подробиці розвитку відзначимо, що протягом кількох десятиліть термін «інформаційне суспільство» перемістився зі сфери футурології в лексикон фахівців з інформаційно-комунікаційних технологій, і на початку тисячоліття – став широко вживаним політичними діячами, економістами, вченими і т.д. У 1998 році на конференції Міжнародного телекомунікаційного союзу прийнята резолюція

про проведення Всесвітнього саміту з питань інформаційного суспільства. У 2000 році на саміті країн Великої вісімки була прийнята Окінавська хартія глобального інформаційного суспільства. У 2002 році Генеральна асамблея ООН прийняла резолюцію про проведення двоетапного Всесвітнього саміту з питань інформаційного суспільства, а в 2003 і 2005 роках відбулись Женевський і Туніський етапи цього саміту. Міжнародна спільнота дійшла до єдиної думки, що права, закріплені у Загальній декларації прав людини, повинні бути реалізовані в інформаційну епоху, перебувати під захистом держави і суспільства незалежно від розвитку і впровадження нових технологічних досягнень [581].

У Окінавській хартії 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, взаємна терпимість і повага до особливостей інших людей» [242].

У той же час в інформаційному суспільстві переважає децентралізованість, 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» [216].

Джон Локк стверджував, що існують дві сили, за допомогою яких «людина захищає свої природні права ... перша – робити те, що він вважає за необхідне, щоб зберегти себе і інших на основі законів природи, друга – карати за злочини, вчинені з порушенням закону» [73, с. 215]. Право на безпечне довкілля відноситься до природних прав. Проте, під цим середовищем, в класичному розумінні, мали на увазі навколишнє середовище. Як же бути з інформаційним середовищем?

Людина пристосовується до соціального життя, сприймає соціальні ролі, приймаючи і передаючи певну інформацію. Кожен стає членом суспільства через засвоєння і дотримання (або заперечення і порушення) соціальних норм, які історично склалися в ньому. Саме тому суспільство

стає носієм однієї з найсерйозніших загроз для інформаційної безпеки людини – інформаційної дискримінації, яка проявляється не тільки в поділі людей на тих, хто має доступ до інформації і тих, хто його не мають. Пуруч з поняттям «інформаційне суспільство» в міжнародний обіг увійшло поняття «digital divide» – «цифровий розрив» або «цифрова прірва». Ця категорія поширилася в 1995 році після публікації звіту від Міністерства торгівлі США про дослідження доступу громадян до комп'ютерів та Інтернету [493], і спочатку мало на увазі поділ суспільства на підключений і не підключений до глобальної мережі Інтернет [493].

Спочатку проблема цифрового розриву було розцінена як суто американська, однак пізніше стала очевидною її глобальність. На саміті країн Великої вісімки (G8) в Окінаві і пізніше в Женеві йшлося про «мобілізацію ресурсів для поліпшення інформаційної та комунікаційної інфраструктур, оскільки вони є одним з найбільш важливих факторів, що впливають на суспільство 21 століття. Розрив між тими, хто має доступ до комп'ютерних технологій, і тими, хто позбавлений такої можливості, проявляється в самих різних сферах життя суспільства, в тому числі обмежує можливості в пошуку роботи, налагодженні соціальних зв'язків, культурному обміні і може негативно впливати на економічну ефективність, розвиток і збереження культури, рівень освіти. Умови для дотримання прав людини в інформаційному суспільстві залежать не тільки від ступеня сприяння інформаційного середовища, але також від внутрішніх характеристик самого суб'єкта (наприклад, інформаційного потенціалу, когнітивності, здатності до саморозвитку).

Згідно з концепцією інформаційного суспільства, його ознакою є можливість вільного обміну інформацією, яка сприяє подоланню бідності і нерівності. Однак є і зворотна сторона медалі, як стверджує один з основоположників концепції «мережевого суспільства» Мануель Кастельс: «Глобальний тренд полягає в тому, що інформаційна економіка підключає до своєї мережі тих, хто представляє для неї цінність (тим самим надаючи їм додаткову цінність), але відключає тих, хто не має для неї цінності (тим самим ще більше зменшуючи їх шанси набути будь-якої цінності)» [407, с.82].

Одним з основних етичних і правових принципів, який за таких умов вимагає переосмислення, є «повага гідності людини та її автономності (здатності керувати самим собою, ґрунтуючись на власних принципах), тобто здатності до особистого розвитку. Гідність, згідно з вченням Канта, означає переконання в тому, що людина є самоціллю і що вона ніколи не може бути засобом для досягнення мети, будь то економіка або безпека. Саме цей етичний принцип лежить в основі Статуту ЮНЕСКО, що і відображено в його преамбулі (досить цікаво, що з 1998 р цей же принцип проголошений однією з фундаментальних цінностей Конфедерації європейських асоціацій користувачів комп'ютерів). Чи можна говорити про гідність тепер, в епоху «Інтернету речей», де цінність людини, точніше, її статус в мережах, роботу яких він не може контролювати, виявляється зведеним до статусу оточуючих його речей, з якими він взаємодіє? Чи можна говорити про повагу особистості, коли системи функціонують в непрозорому режимі на основі баз даних або метаданих, віддалених від індивідуального «я» [483, с.11].

Людина в інформаційному суспільстві наражається на небезпеки і загрози абсолютно нового порядку і якості. Здавалося б, класичні права і свободи набувають нового розуміння. Інформаційне середовище не збігається зі звичною для суспільства часово-просторовим; норми, розроблені для регулювання відносин в [реальному] суспільстві, не завжди адаптованості для цієї часто віртуальної реальності.

Сьогодні грань між реальним світом і віртуальним дуже нечітка. «Наші телефони і фотоапарати стають очима і вухами» – говорить Тім О'Рейлі, видавець книг на комп'ютерну тематику. Глобальна мережа поступово замінює весь світ – і все тому, що все в світі відкидає так звані «інформаційні тіні» [35]. Поширення масової культури, неминуче зіткнення віртуальної реальності, в якій важко провести межу між ілюзією і реальністю, створює не тільки психологічні та культурні проблеми, але також правові. Створюючи свій образ у віртуальному просторі, людина втрачає адекватне сприйняття реального світу, в тому числі правового аспекту. Сьогодні, більш ніж у дев'яти мільйонів землян є «друге життя» в Інтернеті, переважна більшість з них – діти та молоді люди. [132, с.65]

Філіп Росдейл, засновник «Second Life», як-то сказав: «Я не створюю нову гру, а нову державу» [66]. І справді, віртуальна реальність (не важливо, чи то це віртуальні світи, то чи соціальні мережі) істотно впливає на життя людини в реальному суспільстві.

Причини цього численні, від психологічних механізмів відповідальності, впевненості в собі і самозахисту. З психологічної точки зору, Інтернет розглядається людиною як щось на кшталт натовпу. І в натовпі, наскільки відомо, зникають почуття власної ідентичності, разом з нею – почуття відповідальності. Натовп анонімний, а, отже, не несе відповідальності [529, с.54].

У натовпі значно знижується рівень інтелекту по відношенню до рівня інтелекту окремих осіб; підвищується сприйнятливість на навіювання і маніпулювання свідомістю, знижується рівень здатності мислити раціонально. «Ви можете принизити людину. Можна влаштувати скандал, до якого приєднаються всі ті, хто в цей час опинився на злощасній сторінці, і т.п.. Відчуття, що можна уникнувши відповідальності, підвищити самооцінку «за рахунок іншого», і в той же час, щоб втікти від реальності, принижуючи когось у віртуальному просторі, превалює у свідомості багатьох громадян.

Віртуальний світ можна розглядати як потенційне джерело шахрайства. У ньому заробляються гроші, але відсутні податки, є робота – немає норм, які захищають соціальні права, є крадіжки віртуальних товарів – відсутні органи переслідування [593].

Більш того, Інтернет покликаний сприяти розвитку автономності не тільки на рівні окремої людини, але і на рівні нації, а в кінцевому підсумку – людства в цілому. Те, що Інтернет дозволяє кожній спільноті висловлюватися, збагачувати і розширювати власну культуру, передбачає визнання за кожною мовою права на простір для існування, а за кожною нацією – права на володіння засобами власних форм самовираження [483, с.11].

Одним з істотних відмінностей, які перешкоджають здійсненню якісної комунікації в мережі, є мовна диспропорція. Вона заснована на домінуванні англійської мови як основної мови Інтернет, програмного забезпечення і технічної підтримки комп'ютерних систем і телекомунікацій. Розквіт англійської мови як інструменту глобалізації не тільки залишає

мало місця для інших мов в кіберпросторі, а й обмежує доступ до знань і спілкування для тих, хто має потребу в них найбільше.

Домінування англійської мови в галузі науково-технічних знань призводить до нівелювання цінності (і іноді втрати) знань, виражених в інших мовах. Критерій економічної видимості, який керує глобальним інформаційним суспільством, часто виключає «невидимі» знання⁴ [579,с.150], оскільки економіка ґрунтується, перш за все на обробці «оцифрованих» знань, перетворених на дані. Завдяки цьому цьому ще більш відчутною стає загроза прихованих форм «техно-апартеїду».

Таким чином, що в кінцевому підсумку. Діячі епохи просвітництва і їх послідовники сформуvalи або актуалізували ряд наукових теорій, які були життєво необхідні для забезпечення розвитку держави і суспільства, в т.ч. прав людини, суверенітету, поділ влади, теорія національної держави тощо. Але їх інтерпретація і життєздатність знаходиться в постійній залежності від суспільства, в якому вони мають місце бути. Інформаційне суспільство, як новий етап буття, породжує необхідність переглянути часово-просторовий підхід до класичної теорії прав людини. Змістове наповнення окремо взятих прав людини видозмінюється постійно, практично в кожному виді прав людини з'являється його «інформаційна» складова – пов'язана з доступом до інформації, захистом вразливих даних, інформаційно-психологічної безпекою т.д. Помилкою буде розглядати «інформаційне суспільство» тільки в якості лібералізації в телекомунікаціях, і розвиток галузі інформаційних технологій, не виходячи за рамки технологічної точки зору на сутність «інформаційного суспільства». Сама теорія інформаційного суспільства також зазнає значної наукової критики [522]. Але не це головне.

Людина має залишатися головною цінністю будь-якого суспільства, інформаційного у тому числі, а значить, питання як захистити її права та свободи ще більш актуалізується за наявності нових загроз не тільки для свободи розвитку особистості, але і для її фізичної і психологічної цілісності.

⁴ Невидимі знання - неоднорідна сукупність знань, майже інтуїтивного характеру, не виражені в текстовій формі і часто передаються усно з покоління в покоління, в постійній взаємодії з природою; а також – знання місцевих і корінних народів

1.3. Правовий статус людини в інформаційному суспільстві

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 Жан 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» [585, с.22].

І ось тепер маємо і категорію «цифрових прав», і кібербезпеку, і віртуальну землю у реальному володінні з усіма похідними. Проте незалежно від цього людина тяжіє до становлення як особистості і зайняти належне їй місце в суспільстві, де будуть гарантовані її права і свободи, створено можливості для їх реалізації.

Правовий статус людини залежить від сутності соціального ладу, в умовах якого він складається і функціонує [349, с. 223], тому становлення інформаційного суспільства обумовлює необхідність юридичного закріплення і державного гарантування правового статусу людини на новому якісному рівні. В інформаційних суспільних відносинах людина може брати участь і як суб'єкт (наприклад, відносини щодо доступу до інформації, право на приватність тощо), може бути їх об'єктом (відносини щодо інформаційної безпеки), а навіть – засобом (відносини щодо маніпуляції свідомістю). Поруч з інформатизацією у вищевикладеному «позитивному» розумінні відбувається відповідний негативний соціальний процес. Оскільки основною ознакою інформаційного суспільства є всепроникнення інформаційних технологій, сьогодні необхідно говорити про інформаційні загрози безпеці людини, суспільства, держави, міжнародного співтовариства, інформаційні війни, кібертероризм і «інформатизацію злочинності» та інші антисоціальні напрями застосування ІКТ [135, с. 59].

Ще у 1946 році 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»* [334, 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.

Конституції більшості демократичних (і не лише) держав визначають пріоритетність людини як основної соціальної цінності. А гарантування її прав і свобод – основне завдання. 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.

То що ж ми маємо: нове, четверте, покоління – права людини в інформаційній сфері чи новий інформаційний вимір прав і свобод людини?

Конституція України, втілюючи міжнародно-правові стандарти конституційного статусу людини, встановила, що права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави (ст. 3 Основного Закону) [171, с.115].

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 року (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 [168, с.94]. Хоча окремі науковців зазначають, що права і свободи людини в сфері інформаційних відносин можна віднести до третього покоління [419, 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 «Інтернет»), 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 [355, 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 [119].

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 [379, 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 [146; 198]

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 [211, 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. [379, 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 [27, 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 [284,с.2] включає до обсягу поняття “право на інформацію” [210, 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 [211, 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 [171, с.115].

Російські науковці відзначають існування певної правової прогалини у розумінні “права на інформацію”. У більшості випадків під цим поняттям “розуміють право на доступ до інформації, хоча... це право містить у собі низку інших аспектів. Серед них: пошук, одержання, виготовлення й поширення інформації” [9].

Зокрема, відомий російський фахівець в галузі адміністративного та інформаційного права І. Л. Бачило відзначає, що подібні права – це «основные права и свободы граждан, реализованные в информационной сфере» [25, с.220]. А Копилов В.А., в свою чергу, визначає, що «интересы

личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления: запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность» [166, с.69].

П. Сухорольський у спеціальному дослідженні підкреслює, що, наприклад, в англійських джерелах виділяються так звані цифрові права і свободи людини (digital rights and freedoms), під якими розуміють сукупність загально визнаних 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 [368, 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» [259, 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 частини 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 необгрунтовано. 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 [12, с.82]. Серед них можна виділити право на безперешкодне ознайомлення з нормативними актами. Частина 3 ст. 57 Конституції України спрямована саме на здійснення даної можливості: «Закони та інші нормативно-правові акти, що визначають права й обов'язки громадян, не доведені до відома населення в порядку, встановленому законом, є нечинними». Крім того, універсальне право громадянина на інформацію може містити в собі такі конкретні правомочності: право знати про створення і функціонування всіх конкретних 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 [12, 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 [210, 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. [211, 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 [211, 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. Зокрема, Ліпкан В. А., Максименко Ю. Є. та Желіховський В. М. відзначають наступні права стисло пов'язані з інформаційними:

1. Свобода особистого і сімейного життя (ст. 32: «...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»);

2. Таємниця листування, телефонних переговорів, телеграфної й 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»);

3. Право громадянина не зазнавати втручання в його особисте та сімейне життя, шляхом збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, знайомитися в органах державної влади, органах місцевого самоврядування, установах та організаціях із відомостями про себе (ст. 32: це відноситься до відомостей, що «не є державною або іншою захищеною законом таємницею»);

4. Право громадянина направляти індивідуальні або колективні письмові звернення або особисто звертатися в органи державної влади, органи місцевого самоврядування та до посадових і службових осіб цих органів (ст. 40);

5. Право кожного громадянина на сприятливе навколишнє середовище, достовірну інформацію про його стан (ст. 50: «...така інформація ніким не може бути засекречена»);

6. Право кожного на свободу творчості і право доступу до культурних цінностей (ст. 54: результати інтелектуальної, творчої діяльності громадянина «ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом»);

7. Право кожного громадянина на одержання кваліфікованої правової допомоги (ст. 59: «...у випадках, передбачених законом, ця допомога надається безоплатно») [141, с.112].

Науковці також відзначають, що деякі інші конституційні положення, також мають відношення до інформаційних прав і свобод. «За статтями 21, 24 усі люди є вільні і рівні у своєму праві на інформацію, яке є невідчужуваним та непорушним і не залежить від раси, кольору шкіри, релігійних та інших переконань, статі, етнічного та соціального походження тощо. Без отримання необхідної інформації, вільного її використання людина не змогла б розвивати свою особистість (ст. 23). Право на інформацію пов'язане з правом на свободу світогляду і віросповідання, яке включає свободу сповідувати будь-яку релігію або не сповідувати ніякої, безперешкодно відправляти одноособово чи колективно релігійні культури і ритуальні обряди, вести релігійну діяльність (ст. 35). Реалізація права на освіту (ст. 53) неможлива без вільного інформаційного обміну між людьми. Процес навчання означає, перш за все, пошук і отримання необхідної інформації. Ст. 34 Конституції можна також розглядати як певний розвиток і конкретизацію положення ч. 3 ст. 15, що забороняє здійснення в Україні цензури, тобто обмежувальних заходів щодо здійснення свободи слова в засобах масової інформації. Вона гарантує духовну і творчу свободу, не обмежену ніякою обов'язковою ідеологією. Положення статті гарантують доступ до засобів масової інформації політичним партіям і рухам, громадським організаціям, профспілкам, кожній окремій людині. Ніхто не може бути примушений до зміни чи висловлювання своїх поглядів і переконань.» [141, с.113].

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 [171, 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» від 28.02.1995 р., 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» від 16.09.1998 р., Розпорядження Президента «Про додаткові заходи поліпшення інформаційної діяльності» тощо. Велике значення мають Рішення Конституційного Суду України.⁵

⁵ 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.

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 України⁶.

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 [303, 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 [411, ст.302]. Іншими словами, перефразовуючи стародавній принцип, право особи на інформацію закінчується там, де починається право іншої особи [210, с.23]. В умовах становлення інформаційного суспільства невизначеність у правовій площині цієї межі прав і свобод людини *неминуче призводить до виникнення нових, притаманних такому суспільству, проблем, які вимагають наукового дослідження.*

Розробка «Декларації прав людини і правових норм в інформаційному суспільстві» [469] стала першою спробою визначення правових рамок в цій сфері. Декларація була розроблена Комітетом експертів Ради Європи з інформаційного суспільства. Основна увага на форумі було присвячено розробці норм відповідальної поведінки в інформаційному суспільстві. Експерти розглянули, яким чином різні дійові особи, включаючи уряд, приватні компанії, ЗМІ та неурядові організації можуть співпрацювати задля поваги до прав людини. 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,

⁶ Більше в 4 розділі праці.

«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» [5].

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 [469].

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 розрізнити 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)⁷ людини – право на захист персональних даних, право визначати конфіденційність інформації та розпоряджатися нею;
- 2) Право власності на інформацію.

⁷ Різниця в застосуванні категорій «особа і «особистість» в праві та інших соціальних науках розглянута в розділі I. Йдеться про соціальну природу людини, особливості її взаємодії з іншими людьми, соціальними групами та суспільством в цілому.

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 [276, с. 87]. Право на особисту свободу означає відповідну міру можливої та юридично дозволеної поведінки громадянина розпорядитися собою, своїми вчинками та часом. О.В. Кохановська доповнює цей перелік інформацією [174].

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 (ст.ст. 294-296 ЦКУ); право на таємницю особистого життя (ст. 301 ЦКУ); право на особисті папери та розпорядження ними (ст.ст. 303-305 ЦКУ); право на таємницю кореспонденції (ст. 306 ЦКУ); права особи, пов'язані з фото-,

кіно-, теле- та відеозйомкою (ст.ст. 307-308); право на свободу літературної, художньої, наукової і технічної творчості (ст. 309 ЦКУ) [379, 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 році в США професорами права Гарвардського університету Уорреном і Брейндсом [584], як наслідок активного розвитку ЗМІ і їх втручання в приватне життя.

Серед науковців немає одностайності при визначенні змісту цього права. На думку А. А. Фатянова, 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 [392, с.14].

Професор Тертишник В.М. визначає сферу приватного життя людини – як сферу існування людини (житло чи інше володіння особи, робоче місце, речі, що знаходяться при людині), обставини особистого існування людини, таємниця віросповідання, конфіденційність творчого і духовного життя, дані щодо здоров'я і фізичного розвитку людини, відомості, що містяться в документах медичних аналізів, інтимні стосунки, обставини як безпосереднього особистого спілкування з іншими людьми (розмов віч-на-віч), так і спілкування шляхом використання поштово-телеграфних, телефонних, комп'ютерних та інших технічних комунікацій, стосунки у сім'ї, спілкування та стосунки з іншими людьми, зміст приватних щоденників, листів та записок, спосіб життя та всі інші конфіденційні

обставини існування людини, які вона сама не вважає потрібним або можливим розголошувати [375, с.114]

Інакший, більш широкий підхід до визначення категорії «приватність» сформулював професор права Університету Джорджа Вашингтона Д. Дж. Солов. В своїй праці «Розуміння приватності» він називає такі її складові: 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 [563, 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 (стаття 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» [283], який набув чинності 1 січня 2014 року, 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 [160], повноваження щодо контролю за додержанням 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 року 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 року набуває чинності новий регламент Європейського союзу про захист даних (General Data Protection Regulation, далі Регламент) [497].

Він ще більше віддалить дві найбільш поширених 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 [54,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 (стаття 4 та положення Преамбули 24) – 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.

Регламент вводить категорію “контролер” и “процесор”, які беруть участь у обробці персональних даних. “Контролер” означає фізичну або юридичну особу, державний орган, установу або інший орган, який, поодиночі або спільно з іншими, визначає цілі і засоби обробки персональних даних, згідно законодавства. “Процесор” означає фізичну або юридичну особу, державний орган, установу або інший орган, який обробляє персональні дані за дорученням контролера.

Визначено 7 основних і 16 додаткових принципів. Серед основних:

1. Повідомлення – необхідно інформувати суб’єктів даних щодо 13 конкретних видів даних (наприклад, щодо типу зібраних даних, цілей обробки, можливості скаржитись в обов’язковий арбітраж і т.д.)

2. Вибір – можливість відмовитись від розкриття персональних даних та використання даних для матеріально інших цілей

3. Відповідальність за подальші Трансфери – подальші трансфери можливі тільки для обмежених і спеціально вказаних цілей і тільки на підставі договору, де отримувач даних зобов’язується надавати той самий рівень захисту як і передбачений в програмі

4. Принцип Безпеки – необхідно впровадити розумні та відповідні засоби безпеки для захисту персональної інформації від втрати, неналежного використання, неавторизованого доступу, розголошення, зміни, та знищення

5. Цілісність даних і Обмеження Цілей – необхідно обмежити збір персональних даних, що пов’язані між собою, і не обробляти їх для несумісних цілей; персональні дані повинні бути надійними для використання за призначенням, містити точну і актуальну інформацію

6. Доступ – повинні надати суб’єктам доступ до особистих даних щоб виправляти, змінювати або видаляти неточну інформацію або оброблену шляхом порушення принципів.

7. Відшкодування, Захист і Відповідальність – повинні бути впроваджені легкодоступні незалежні механізми оскарження та вирішення скарг без будь-яких витрат для фізичних осіб; необхідно періодично перевіряти, що опубліковані політики конфіденційності відповідають Політиці Приватності і Принципи фактично дотримуються. [362]

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. [564]

Окрім, того вперше нормативно закріплене так зване «право на забуття» (англ. right to be forgotten), яке ще в 2014 році 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 [488]. 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 а case-by-case assessment [488].

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 [71].

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 [173]. Якщо в першому розумінні інформація є невіддільним благом від самої особи носія, то два наступних дозволяють розглядати інформацію як товар, що може відчувуватись, хоча йому й притаманні певні особливості.

Баранов О.А., аналізуючи українське законодавство, зауважує його суперечливість щодо визначення права власності на інформацію [20]. В редакції Закону «Про інформацію» в 2011 році було скасовано категорію право власності на інформацію. Дехто з правників потрактував це в такий спосіб, що інформація не може бути об'єктом право власності [172]. 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.

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. [117,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 транспарентності⁸. 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 [542].

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 [275]. З аналізу практики Європейського суду з прав людини по застосуванню цієї норми можна зробити висновок, що право на свободу вираження поглядів включає такі складові:

⁸ Від лат. *Transpareo* – відкрите, видиме наскрізь, зрозуміле.

- свободу дотримуватися своїх поглядів;
- свободу одержувати інформацію та ідеї;
- свободу передавати інформацію та ідеї.

Щоби мати свої 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 [275].

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 Інтернет; 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 Мертсона), 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 році 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/), так і на рівні окремих держав-членів (Наприклад, Франція data.gouv.fr/fr/, Німеччина govdata.de/, Італія it.ckan.net/, Польща insigomg.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) [574].

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 [578].

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 – WhatDoTheyKnow⁹. 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.

Car Gemini 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 (обсяг і деталізація даних, оновлення даних, легкість використання даних),

⁹ <https://www.whatdotheyknow.com/>

державна політика в галузі відкритих даних (Ініціативність та підтримка уряду) і функціональні можливості централізованого порталу відкритих даних (користувацький інтерфейс, функції пошуку, участь зі сторони користувачів) [574].

В Україні історія розвитку відкритих даних розпочинається після прийняття Закону «Про доступ до публічної інформації» [287], але реально ресурси запрацювали у 2015 році, після того як був прийнятий Закон № 319 «Про внесення змін до деяких законів України щодо доступу до публічної інформації в формі відкритих даних» [282] та Постанова Кабінету Міністрів України № 835 «Про затвердження Положення про набори даних, що підлягають опублікуванню в формі відкритих даних» [297]. 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 даних¹⁰ 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 році було прийнято Закон «Про відкритість використання публічних коштів», що став правовою підставою оприлюднення інформації про використання публічних коштів функціонують на офіційному державному інформаційному порталі.

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

¹⁰ <http://www.data.gov.ua/>

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 рік до Секретаріату Уповноваженого Верховної Ради України з прав людини не надходили скарги щодо порушення розпорядниками інформації вимог оприлюднення публічної інформації у формі відкритих даних [188].

Водночас, відповідно до пункту 3 постанови Кабінету Міністрів України «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних» Державному агентству з питань електронного урядування доручено забезпечити: належне функціонування Єдиного державного веб-порталу відкритих даних; проведення із залученням інститутів громадянського суспільства та представників громадськості періодичного моніторингу стану оприлюднення та оновлення наборів даних на офіційних веб-сайтах державних органів та на Єдиному державному веб-порталі відкритих даних із наступною публікацією його результатів на Єдиному державному веб-порталі відкритих даних.

Окрім того, створено низку недержавних ресурсів відкритих даних, таких як CityScale¹¹, а також ресурсів, що полегшують роботу з відкритими даними, наприклад «Пошуково-аналітична система .007»¹².

¹¹ <http://www.cityscale.com.ua/about.htm>

¹² «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/>

Проблеми, що стали очевидними за 2 роки в правовому регулюванні відкритих даних: низький ступінь поінформованості населення про можливості використання 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 [188].

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) визначити 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 (РЄ) ще в 1979 році в рекомендації Парламентської Асамблеї РЄ (ПАРС) , 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 ПАРС 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 [74]. У Рекомендації Комітету Міністрів РЄ щодо доступу до інформації, яка була оновлена в 2002 році, наголошувалося, зокрема, на важливості в плюралістичному, демократичному суспільстві прозорості публічної адміністрації та доступності інформації з питань суспільного інтересу [74]. Зазначалося, що широкий доступ до офіційних документів: 1) дозволяє громадськості мати адекватне уявлення та сформувану 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 добросесність, 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» у редакції 1992 року. Це право закріплювалося за «громадянами України, юридичними особами і державними органами» і передбачало «можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій». Законом регулювався порядок доступу до інформації, у тому числі шляхом подання інформаційного запиту. У травні 2011 року набули чинності Закон України «Про доступ до публічної інформації» та нова редакція Закону України «Про інформацію». Закон «Про доступ до публічної інформації» визначив таке: 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 (раніше створену) інформацію, якою володіє розпорядник. Для відповіді на інформаційний запит розпорядник не повинен створювати нову інформацію (готувати аналітику, надавати роз'яснення тощо).

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» [74].

До 2015 року 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 року, 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 [74].

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:

1. оскільки він нібито не розпорядник інформації в розумінні Закону України «Про доступ до публічної інформації»;

2. якою він володіє, але з якихось причин вважає «непублічною» чи такою, що не повинна надаватись на запит;

3. через порушення вимог законодавства щодо порядку оплати фактичних витрат на копіювання і друк;

4. через вимогу вказати в запиті відомості, що не передбачені статтею 19 Закону України «Про доступ до публічної інформації»;

5. якою він не володіє, але зобов'язаний відповідно до своєї компетенції;

6. оскільки відповідає не по суті запиту;

7. з будь-яких інших підстав, що не передбачені частиною першою статті 22 Закону України «Про доступ до публічної інформації»;

8. оскільки запитувану інформацію можна отримати з офіційного веб-сайту чи інших загальнодоступних джерел; оскільки відповідає не по суті запиту;

9. з порушенням встановлених законом вимог до відмови у задоволенні запиту на інформацію [433].

Серед типових порушень права на доступ до публічної інформації в Україні найбільш поширеними є порушення процедури (недотримання строків та форми), посилання до відкритих даних чи інформації, розміщеної на сайті (коли там відсутні відповідні дані); відмова з огляду на обмеженість доступу до такої інформації (конфіденційна, службова чи таємна).

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 [65].

Належний рівень правової культури державних службовців, які беруть участь у нормотворчій діяльності, тлумачать та засосовують 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 (CEDEM) заснував і активно підтримує Мережу захисників права на доступ до інформації, метою якої є гарантування правового захисту права кожного на доступ до інформації. Починаючи з 2012 року щорічно у Києві проводяться Форуми захисників права на доступ до інформації. Також Центром 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», Свобода інформації. Навчальний посібник для державних службовців тощо.

У 2014 році 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 році 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»)¹³, 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.»;

¹³ Право посадових осіб оприлюднювати інформацію про правопорушення в установі, в якій вони працюють.

Ст. 34 Конституції України: «Здійснення цих прав 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».

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 [323]. 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» [235,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 випливає зі статті 10 Конвенції про захист прав людини й основоположних свобод та статті 34 Конституції України [75].

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 Станіслав 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 [423,с.429]»

Засоби масової інформації безпосередньо займаються збором, обробкою (використанням) та поширенням масової інформації. Можливість вільно збирати (одержувати) та поширювати (передавати) інформацію, передбачає можливість вільно діяти без втручання інших осіб, зокрема держави, і без наявності в інших осіб певного кореспондучого 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»¹⁴.

Проте захисту при реалізації цієї свободи потребують і інші суб'єкти, зокрема, ті, які розкривають інформацію про зловживання. Набув значного розголосу приклад Кетрін Ган (Katherine Gun), яка працювала на посаді аналітика Головної комунікаційної штаб-квартири електронної організації прослуховування британського уряду . На початку 2003 року 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,

¹⁴ Зі справами ЄСПЛ, що розглянуті в роботі, можна ознайомитись на офіційному сайті <http://www.echr.coe.int/>

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 року обвинувачення проти неї було знято. Позиція полягала в тому, що британський 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. Кетрін Ган не була захищена за британським правом. Вона втратила свою роботу і лише уникла кримінального вироку, оскільки уряд побоювався продовжувати її судове переслідування [335]. 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 ¹⁵.

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

¹⁵ Однією з перших справ, в якій він знайшов відображення була справа «Лінгенс проти Австрії» від 08.06.1986 г.

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».

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. Розвиток міжнародного та національного законодавства, юридичної доктрини сприяє перманентному розширенню спектру прав і свобод людини та громадянина [354].

Водночас, не слід забувати що 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 [368, с.21]. Відтак доцільно говорити про інформаційні права і свободи людини та громадянина в екологічній сфері, економічній сфері, політичній сфері, управлінській сфері тощо, які корелятивно поєднані і в своїй інтегративній сукупності складають систему інформаційних прав і свобод. Адже поява інших сфер життєдіяльності суспільства не змінює сутності цього феномена. В умовах становлення інформаційного суспільства будь-які суспільні відносини знаходять свій прояв через інформацію, 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 системотворними 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 [338, 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. І то – за умови, що буде щодня освоювати по 50 сторінок [439].

У той же час сьогодні в одній тільки науковій сфері щорічно з'являється кілька мільйонів книг. І навіть якщо вивчати тільки новинки, на кожну

прочитану сторінку буде припадати 10 тисяч інших, осилити які нереально. Фахівці навіть ввели визначення «макулатурний фактор» – 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 відсотків книг [439]. Тобто мільйони сторінок, які зберігають новітні технічні знання, так і не були ніким прочитані. Мало того, що ми не встигаємо вивчити велику частину інформації, яка накопичується, вона ще й швидко застаріває і вимагає заміни. Професійні знання в середньому застарівають за 3-4 роки (потребують оновлення) [338,с.76-88]. Тобто, на момент отримання диплому про вищу освіту, 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». Під ним розумілося лавиноподібне збільшення кількості публікацій у наукових журналах, яке призвело до страшних прогнозів кінця науки як такої. Пояснювалася паніка дуже просто – жоден учений не зможе відстежувати те, що відбувається у його галузі, за таких «прискорених» умов.

У наш час термін «інформаційний вибух» прижився, і його почали розглядати під ще одним кутом – переважна більшість світових знань непотрібні для пересічної людини. Більшості за все життя можуть ніколи не знадобитися технологічні інструкції якогось підприємства або основи агрокультури.

Крім того, виникає і питання якості, адже велика частина всієї людської інформації – нескінченне дублювання одного і того ж з незначними змінами. Яскравий приклад – сучасні новини, які ЗМІ переповідають на свій лад.

Однією з причин появи нікому не потрібної інформації є зростаюча кількість безпосередніх творців контенту. Сьогодні практично будь-яка людина може опублікувати «свою» інформацію для всього світу завдяки соціальним мережам, форумам, блогам і т.д. І тут перед нами виникає питання: а яка якість цієї інформації? Адже у більшості своїй люди не публікують нічого змістовного або радикально нового. Так може, і вибуху

ніякого немає, просто засмічуємо віртуальний простір, намагаючись показати світу власне «я»?

Інформаційне перевантаження «information overload» – термін, що описує труднощі розуміння проблеми і прийняття рішень, причиною якої є надлишок інформації. Поняття згадується в книзі Бертрама Гросса «Управління організацією» [504] (1964 р.), але популяризував його Елвін Тоффлер у своєму бестселері «Шок майбутнього» [577] 1970 року. Термін і концепція передували виникнення 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 [490].

Інформаційне перевантаження має не лише психологічні, а й фінансові наслідки. За підрахунками Натана 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 [507].

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 напитись із пожежного крану – води виставить, але треба примудритись не захлинутися» [579]. Звісно, ІКТ фільтрують інформацію, проте, вони не можуть забезпечити рівня фільтрування яким володіє людський мозок.

І тут означимо питання змісту освітніх програм. На безпеці життєдіяльності чи охороні праці досі немає ні слова про культуру поведінки в умовах інформаційного перенасичення. Студенти ВНЗ розраховують норми освітлення і радіус забруднення радіацією – ніби-то вони цим користуватимуться в повсякденному житті.

Набагато важливішим 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. Заслугує на увагу думка Городенко Л. М., щодо інформаційного розриву, що виникає щодо свободи поглядів, висловлювань та вільних трактувань. 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 мережевих комунікацій сприяє поширенню будь-якої інформації, починаючи від пліток і закінчуючи засекреченими відомостями [475].

В далекому 1999 році журналістами BBC чи не вперше було вжито категорію «Cyber rights and cyber liberties», а також «digital freedom»¹⁶, коли

¹⁶ Кіберправа і кіберсвободи, цифрова свобода

йшлося про необхідність змін в правовому регулюванні відповідно до технологічного розвитку, зокрема, спів розмірного захисту даних на фізичних носіях та в електронній формі [472]. Термін «кіберправо» прижився в англійському 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 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 [475]. 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 онлайнному 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 [263]. Ця норма фактично повторює визначену 6 грудня 2012 року 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 тлумаченні 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” [416].

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. [518]»

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 році було запропоновано внести зміни до Цивільного кодексу України, які б гарантували право фізичної особи на доступ до Інтернету та встановлювали умови його обмеження [320]. 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 [536]. 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 [220].

Проте цифрові права не обмежуються правом на доступ до інтернету. Асоціацією прогресивних комунікацій¹⁷ ще у 2001 році 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 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. [162]

Конрад 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» [449].

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

¹⁷ 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/>

прав людини покликана забезпечити кожному можливість безкоштовно і необмежено користуватися цими засобами і їх потенціалом [449].

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 Ахмета 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».

Турецький регулятор заблокував доступ до усього домену Google Sites оскільки на сторінці позивача було розміщено образливі висловлювання на адресу Мустафи Кемала Ататюрка, що є порушенням турецького законодавства. ЄСПЛ визнав дії турецької влади такими, що порушують статтю 10 Конвенції (свобода вираження поглядів та свобода інформації), а також зазначив, що «обмеження доступу до інформації відповідає Європейській конвенції з прав людини лише у тому випадку, коли існує чітка правова база, що регулює підстави для блокування та гарантує можливість судового перегляду для запобігання ймовірних зловживань».

В Україні, після введення в дію Указом Президента Рішення РНБО України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» [295], було розглянуто низку справ щодо порушення цим рішенням прав і свобод людини. Зокрема, у постанові Вищого адміністративного суду України від 14 червня 2017 року по справі № 800/198/17 [267] 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 Інтернет до ресурсів певних російських сервісів.

Серед аргументів суду має місце посилання 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 журналістів¹⁸ та деяких інших досліджень обмежено доступ до мережі жителям таких країн:

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 іноформаційних 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; 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, IP, поштових 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;

¹⁸ Комітет захисту журналістів (Committee to Protect Journalists (CPJ)) - міжнародна неурядова організація зі штаб-квартирою в Нью-Йорку, що займається захистом прав журналістів.

Китай – має чи не найбільш розвинену програму по цензурі мережі у світі. Провайдери зобов'язані встановлювати фільтри, блокувати сайти, які не бажані уряду, знищувати відповідний контент і вести контроль за поштовим трафіком; заборонені нзка соцмереж;

Іран – переслідується критика уряд або релігійних діячів, блогери зобов'язані реєструватись в Міністерстві Мистецтва і Культури; блокуються сайти, де критикується режим правління; інтернет-магазини, 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 – всередині країни це просто неможливо).

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 книговидання, всі 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 відсотків інтернет-користувачів – всього 4% населення країни; монополія держави на телеком-послуги, нерозвинена

інфраструктура і політика заборони на розвиток телекомунікацій в країні призвели до неадекватно дорогих цін, окрім того мережі повністю відсутні в сільській місцевості, але саме там проживає 85% населення країни; присутня цензура і переслідування за необережні висловлювання.

Неможливо в межах однієї монографії 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.

Водночас, розглянуте дозволяє зробити деякі висновки:

Правовий статус людини залежить від сутності соціального ладу, в умовах якого він складається і функціонує, а отже становлення інформаційного суспільства обумовлює не лише виникнення нових прав (наприклад, право на доступу до інтернет), а й переосмислення змісту «класичних» прав і свобод людини (наприклад, свободи слова).

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. Цифрові права, на нашу думку, не є самостійною науковою категорією¹⁹, а становлять частину інтегральну інформаційних прав і свобод, реалізація яких пов'язана з цифровими технологіями.

Недопустимим в демократичному суспільстві, на нашу думку, є протиставлення свободи інформації (як фундаментального права людини) та інформаційної безпеки.

¹⁹ Скоріше її вживання має літературно-публіцистичний характер, хоча має місце і в окремих наукових працях.

РОЗДІЛ II. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ТА ЗАКОНОДАВЧІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Онтологічний, гносеологічний і логічний зміст інформаційної безпеки

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 – приміром, доступ до Інтернету понад 60% жителів Землі.

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 невпинно зростає.

Переважна 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.

Враховуючи, що інформаційне протиборство вважається природнім станом в умовах конкуренції сучасного глобалізованого світу, питанням забезпечення інформаційної та кібернетичної безпеки приділяється особлива увага в контексті збереження балансу інтересів на рівнях особи, суспільства, держави та міжнародного правопорядку [214].

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.

Так, зокрема: психологи розкривають її як відчуття, сприйняття і переживання необхідності у захисті життєво важливих потреб і інтересів людини; юристи (правники) – як систему встановлених законом правових гарантій захищеності особи і суспільства, забезпечення їх нормальної життєдіяльності, прав і свобод; філософи – як стан, тенденції розвитку і умови життєдіяльності соціуму та його структур, за яких забезпечується збереження їх якісної визначеності та оптимальне співвідношення свободи і необхідності; політологи – як властивість (якість) системи і результат діяльності ряду систем і органів держави, а також сам процес діяльності, спрямованої на досягнення поставлених завдань щодо забезпечення захищеності особи, суспільства, держави [365].

Інформаційна безпека повинна розглядатися з урахуванням трансдисциплінарної стратегії досліджень Іммануїла Валлерстейна, американського соціолога та історика, задля виявлення подібності та зв'язків між явищами, а не створення бар'єрів щодо предмету дослідження [583]. 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 [583]. Очевидною є доцільність використання трансдисциплінарності, як одного з основних способів дослідження складних багатофакторних проблем

XXI століття. Про це свідчить текст «Всесвітньої Декларації про Вищу освіту для XXI століття: підходи і практичні заходи» [509]. Стаття 5 і стаття 6, Декларації, містять рекомендації – заохочувати до трансдисциплінарності програм навчального процесу і вчити майбутніх фахівців, використовувати трансдисциплінарний підхід для вирішення складних проблем природи і суспільства [509].

З метою комплексності дослідження необхідним вбачається послідовне виявлення знання, розпорошеного в різних соціальних науках. Зовсім інший підхід до інформаційної безпеки спостерігається в юридичних наук, соціології, політології, економіці. Нові реалії глобалізації і постійно зростаючі соціальні зміни об'єктивно вимагають переглянути зміст як безпеки в цілому, так і інформаційної безпеки.

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 [397]. 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 [396].

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. Він є відображенням об'єктивно існуючого відношення «людина – світ». А тому філософія, 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 [396]. 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 [436].

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 [194].

В історичному процесі складається структура предмета, тобто єдність внутрішнього змісту і зовнішніх проявів, співпадаючих і неспівпадаючих суперечливих сутностей. Сутність – сукупність глибинних зв'язків, відносин і внутрішніх законів, які визначають основні риси і тенденції розвитку системи. Сутність може вважатися пізною, коли відомі причини виникнення і джерела розвитку розглядуваного об'єкта, шляхи його формування або технічного репродукування, якщо в теорії або на практиці створена його достовірна модель. Одна й та сама сутність може мати множину різних явищ [194].

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 [396].

У загальному соціологічному плані 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 [28].

Безпека в повному розумінні є усвідомленим явищем певного суб'єкта суспільних відносин. Воно виступає і проявом активності, і відносної

самостійності суспільної свідомості у відношенні до суспільного буття. Тому уявлення, відчуття, знання, досвід про безпеку мають або виконують активну, значущу роль у суспільному житті. Виходячи з того, що безпека є усвідомлене явище, можна зробити висновок, що усвідомлення її необхідності обумовлює глибоке розуміння сутності проблем, що виникають, реальних загроз. З цього випливає й усвідомлення необхідності формування ефективної системи охорони та захисту як множини засобів, теоретичних підходів і практичних дій, що визначають максимальну життєздатність соціальної системи, з урахування всіх можливих загроз або ризиків її існування. У основі будь-якої безпеки як системи мають місце життєво важливі інтереси особи, нації, держави чи міжнародного співтовариства.

В цьому, як процесі, проявляється розуміння, сенс, 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 Кшиштоф Лідерман, польський безпекознавець, стверджує, що в той час як забезпечення стосується в більшій мірі заходів (технічних, організаційних, правових тощо), то безпека – суб'єктивного відчуття [532]. 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 Krzysztof Liedel, польський юрист, фахівець з міжнародного тероризму. На його думку, безпека і загрози є нерозривно пов'язаними явищами. Вони становлять протилежні одиниці виміру соціальних явищ [533].

Сутність іншого підходу полягає в тому, що безпека повинна мати місце завжди, якщо навіть небезпеки або загрози, як реалізації небезпеки і форм її прояву, нема. Є такий відомий вислів: прагнеш до миру – готуйся до війни.

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 неможливий 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 [453]. 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 [594, 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.

Задаючись питанням: “Що ж таке є “безпека”? Ступінь захищеності, або стан об'єктів, які захищає держава?” – Г.А. Пастернак-Таранушенко доходить висновку, що безпека – це стан об'єкта захисту, що відрізняється динамічною стабільністю та своєчасною можливістю вплинути на хід подій

з метою збереження цього об'єкта [252,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 [344, с.278-282].

Третій, логічний аспект відображення предмета філософії в теорії полягає в тому, що результати практично-діяльнісного і пізнавального відношення до дійсності, відображені в змісті філософського знання, фіксуються, знаходять свій вираз в понятійно-категоріальному апараті. У системі понять, категорій, законів знаходять своє вираження гранично загальні основи буття людини і світу, усвідомлення людиною своєї сутності і сутності світу в їхньому взаємозв'язку, свого місця у світі, цілей і сенсу життя. Тому поняття і категорії є показником ступеня усвідомлення людиною свого відношення до світу і до себе. Зміст понятійно-категоріального апарату, його структура, динаміка відбивають динаміку розвитку як самої дійсності, людини, так і їхнього взаємозв'язку [396].

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» [376]. Слово «безпека» створено з прийменника «bez» і основи іменника «река», пов'язаного з дієсловом «ректі» (українською – «пекти») [113,с.163]. Прийменник «без» має загальнослов'янський індоєвропейський характер. Його вихідне, початкове значення за одними джерелами – «поза», за іншими – «крім» [113,с.161]. Слово «пека» походить від слова «пек», яке запозичене з голландської мови («рек» – смола). У старослов'янській мові – «пкъь», «пкъль» – 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 [113,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 «провальювалися» 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 [260, с.181-182].

В староросійській мові загальнослов'янське «ректі» існувало в двох похідних формах: «пекь» (пека) – «жара, спека», і «печа» – турбота, опіка (рос. попечение) [17]. 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 [17].

Тому так важливим, на нашу думку, є інтегрований підхід до вивчення феномену інформаційної безпеки, що ґрунтується на суспільно-історичній і соціально-діяльній сутності людини, в діалектичній єдності людини і світу. Внаслідок практичної зумовленості пізнавального ставлення людини до світу теоретичне відображення дійсності у свідомості наповнюється 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 [396].

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 [28].

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 природніх процесів, поширенням наково-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 [28]. У розуміння ідеального входить поняття безпечного, що визначає їх взаємодоповнюваність у системі соціальних відносин [3].

Спробуємо проаналізувати принаймні окремі з них.

Згідно енциклопедичному визначенню під категорією «інформаційна безпека» слід розуміти:

- 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 [175,с.744].

Російська вчена, фахівець з інформаційного права Бачило І.Л. акцентує увагу на багатоплановості поняття «інформаційна безпека». Вона 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 [27, 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 [374,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 [409]. В дослідженнях науковців досі можна зустріти подібне безпідставне ототожнення. Редакція наукового журналу «Безпека інформації», який було засновано у 1995 році, визначила основною метою журналу висвітлення результатів наукових досліджень та поширення інформації з усіх аспектів інформаційної безпеки. [31]

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 [68,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 [400,с.113-119]. При визначенні поняття інформаційна безпека він дотримується однієї з поширених в науковому світі позицій, яка розглядає стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через: негативний інформаційний вплив за допомогою, в першу чергу, несанкціонованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невчасної, невірогідної та упередженої інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням [399, с.59-66].

Близькою за змістом видається позиція Дзюбаня 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 [96.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 [21, 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 [98].

Богуш В. визначає, що інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [46].

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” [395].

Подібною є позиція Гаєвського В.К., Авраменко В.А., які визначають інформаційну безпеку також як стан захищеності життєво важливих інтересів особи, суспільства та держави, що виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації, тоді як Додонов О.Г. визначає інформаційну безпеку як стан захищеності інформаційного простору, що забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави [194].

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 [128, 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, 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. У цьому плані безпека усвідомлюється як основа цілепокладання політики, а забезпечення безпеки – як діяльність з досягнення безпечного стану суспільства або соціальної групи. Цієї ж думки дотримується Ліпкан В.А. [194].

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 [[79, 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 [435, 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 [86].

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 [189,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:

1. Зони інформаційної безпеки перебувають на перехресті функції національної безпеки та інформаційної функції держави.

2. Питання інформаційної безпеки держави носить екстериторіальний характер.

3. Суспільні відносини, що входять до сфери інформаційної безпеки, є неоднорідними і різноплановими.

4. Компетенція держави у сфері інформаційної безпеки обумовлюється конкуренцією між інформаційними правами особи та функціями держави і її органів по регулюванню інформаційних процесів.

5. У демократичному суспільстві державне регулювання інформаційної сфери можливе лише шляхом встановлення правових норм.

6. Політика інформаційної безпеки носить багатовекторний характер, її головними складовими (векторами) є:

- регулювання інформаційних відносин з метою забезпечення національної безпеки, територіальної цілісності та громадського порядку, підтримання законності;
- регулювання інформаційних відносин з метою забезпечення прав і свобод громадян, здоров'я та моральності;
- регулювання інформаційних відносин у сфері комерційної інформації [167, 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 [232].

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» [256].

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 [197, с.155].

Тихомиров О.О., опираючись детально розроблений в теорії держави і права діяльнісний підхід вважає за доцільне виокремити ті 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 (процедуру) здійснення діяльності або її окремих фрагментів – діянь [378].

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» [390,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 [224].

Під час розробки проекту Закону України “Про засади інформаційної безпеки України” співробітниками Інституту Пилипчиком В.Г., Коржом І.Ф., Савіною Н.А., Стельбицьким М.П та Фурашевим В.М. 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 [294].

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.

Визначеність логічного змісту інформаційної безпеки залежить від розвитку наукового пізнання, а також від розбудови механізму державного управління. В наступному підрозділі монографії простежимо становлення нормативного визначення інформаційної безпеки в законодавстві України.

2.2. Інформаційна безпека 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» [184].

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. В пошуках нових шляхів до розв'язання наукових проблем зародилися передвісники системного підходу, основною змістовною складовою якого є система. Ще антична філософія висунула онтологічне тлумачення системи як упорядкованості та цілісності буття. Як систему в той час сприймали загальну організованість Всесвіту, розглядаючи її 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 [371, с.130-139].

Г. Гегель розглядав предмети як органічну 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 воедино 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» [387].

У німецькій класичній філософії, в якій розроблялися принципи системної природи знання, В. Садовський звертає увагу на праці І. Канта (наукове знання як система, в якій ціле панує над частинами), Ф. Шеллінга й Г. Гегеля (системність пізнання – найважливіша вимога діалектичного мислення) [371, с.130-139].

З сучасних позицій зрозуміло, що це поняття є способом кінцевого подання нескінченно складного об'єкта, і в цьому полягає його гносеологічна сутність.

У ХХ столітті поява загальної теорії систем Л. Берталанфі знову повернула онтологічне розуміння системи, але в іншому логікометодологічному аспекті. Почалося обговорення різноманіття властивостей «органічних цілих». Об'єкт знову розглядається як складний з безліччю властивостей, якостей та їхній взаємозв'язків. В кінці ХІХ – на початку ХХ ст. принцип цілісності став дуже популярним у наукових дослідженнях. Цей період позначився відмовою від таких світоглядних позицій, як елементаризм (який стверджував, що складні явища можна зрозуміти тільки через їхні елементарні складові) та механіцизм (що зводив складні закономірності розвитку до найпростіших законів механіки).

У соціології, як зазначає Н. Черниш, в основі однієї з перших цілісних концепцій соціальної системи (В. Парето) – механістичне розуміння суспільства, яке складається із сукупності соціальних атомів-людей, подібно до природної системи, яка збудована з атомів і молекул. За визначенням В. Парето, суспільство – це система, яка перебуває у стані рівноваги, але рівноваги відносної, оскільки вона постійно порушується і відновлюється. Всі частини соціальної системи тісно взаємопов'язані й механічно впливають одна на одну.

На зміну елементаризму та механіцизму прийшов органіцизм – методологічний принцип, відповідно до якого соціальні явища розглядалися 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. Це динамічне утворення, яке перебуває у постійному розвитку, як будь-який живий організм. На відміну від механістичних уявлень про суспільство, органіцизм звертає увагу передовсім на динамічні процеси всередині соціальних систем. Однак механічне перенесення біологічних закономірностей на суспільство виявилось неспроможним забезпечити наукове розуміння його законів.

Важливою подією у розвитку системних уявлень вважається публікація у 1948 році книги Н. Вінера «Кібернетика». На думку Дж. 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. О. Горбань, В. Бахрушин вважають, що з кібернетикою пов'язані такі досягнення, як «типологізація моделей систем, виявлення особливої ролі зворотних зв'язків у системах, формулювання й застосування принципу оптимальності в управлінні ними та їх синтезі, усвідомлення інформації як загальної властивості систем і розробка методів її кількісного опису, розвиток методології математичного моделювання й математичного експерименту за допомогою ЕОМ» [77, с.9]. На відміну від Л. Берталанфі, який особливу увагу приділяв вивченню обміну системи із зовнішнім середовищем речовиною, енергією та інформацією, вінеровський підхід передбачає вивчення зворотних зв'язків усередині системи, а функціонування системи розглядається як відгук на зовнішній вплив.

Зазнавши тривалу історичну еволюцію, поняття «система» з середини ХХ ст. стає одним з ключових філософсько-методологічних і спеціально-наукових понять. Як форма подання предмета наукового пізнання система є фундаментальною й універсальною категорією. Наявність великої кількості тлумачень підтверджує справедливність висловлювання В.Н. Садовського про

те, що поняття «загальна теорія систем» не має чітко визначеного розуміння, і мова йде не про єдину концепцію, а про «новий напрям дослідницької діяльності, про вироблення нової системи принципів наукового мислення, про формування нового підходу до об'єктів дослідження».

В словниках та енциклопедіях можна зустріти такі визначення цього поняття:

«план, порядок розташування частин цілого, визначене улаштування, хід чого-небудь у послідовному, доладному порядку» [381];

«сукупності об'єктів, підпорядкованих чітко або за якимось особливим порядком, як правило, логічним або науковим; єдине ціле об'єктів, пов'язаних якимось спільним законом, принципом, або метою; постійне об'єднання принципів або елементів, які становлять єдине ціле» [586];

«сукупність чогось, упорядкована як ціле; план або схема, яка складається з багатьох частин, об'єднаних таким чином, щоб створити ланцюг взаємозалежностей; постійне об'єднання принципів або елементів, які становлять єдине ціле» [586];

«будова, структура, що становить єдність закономірно розташованих і функціонуючих частин [417];

«щось ціле, що являє собою єдність частин, які закономірно розташовані і знаходяться у взаємному зв'язку» [382];

«1) постійно взаємодіючі або взаємозалежні елементи групи, які формують єдине ціле; 2) організаційно впорядкована сукупність доктрин, ідей чи поглядів, які зазвичай обґрунтовують механізм функціонування системного цілого» [543];

«щось, складене з багатьох взаємозалежних або пов'язаних між собою частин» [543];

«безліч елементів, що знаходяться у відносинах і зв'язках один з одним, яка утворює певну цілісність, єдність» [50];

«...3) сукупність яких-небудь елементів, одиниць, частин, об'єднаних за спільною ознакою, призначенням; ... 5) будова, структура, що становить єдність закономірно розташованих та функціонуючих частин» [60];

«внутрішньовпорядкована структура елементів, яка становить цілісність» [391];

«сукупність елементів, що знаходяться у відносинах і зв'язках один з одним і яка утворює певну цілісність, єдність» [234];

«категорію, що позначає об'єкт, організований як цілісність, де енергія зв'язків між елементами системи перевищує енергію їхніх зв'язків з елементами інших систем і задає онтологічне ядро системного підходу» (стаття А. Бабайцева) [234];

«...Сукупність або група елементів або частин (наприклад, організм або машина), організована з певною метою і у відношенні до зовнішнього навколишнього середовища. Такі системи можуть бути природними або штучними і включають соціальні системи. Отже, суспільство або соціальна організація в цьому значенні є системою» [352].

Аналіз вищенаведених 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» [371].

У науковій літературі зустрічається більш 40 різних визначень поняття «система». Усі вони в залежності від підходу можуть бути поділені на три групи. Перша група визначає систему через поняття системного підходу – «елементи», «відносини», «зв'язки», «ціле», «цілісність». У другій групі системи розглядаються з позиції теорії регулювання через поняття «вхід», «вихід», «переробка інформації», «закон поведінки», «керування». У третій групі система визначається як деякий клас математичних моделей [157].

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 можуть бути: 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 [59].

У загальнодоступній вільній багатомовній онлайн-енциклопедії Вікіпедія властивості систем класифіковані в 4 групи наступним чином: пов'язані з цілями та функціями – ефект синергії, ієрархічність, емерджентність, мультиплікативність, цілеспрямованість, альтернативність шляхів функціонування та розвитку, робастність; пов'язані зі структурою – цілісність, не адитивність, структурність, ієрархічність; пов'язані з ресурсами та особливостями взаємодії із середовищем – комунікативність, взаємодія і взаємозалежність системи і зовнішнього середовища, адаптивність, надійність, інтерактивність; інші – інтегративність, еквіфінальність, спадковість, розвиток, самоорганізація. [343].

Слід також пам'ятати, що безпечний розвиток будь-якого суспільства, держави, людини прямо пов'язаний з їхньою інформаційною безпекою, оскільки інформаційне середовище є системотворчим фактором цього розвитку [93].

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, як було визначено в Доктрині інформаційної безпеки, яка втратила чинність в 2014 році, і багаторазово стверджувалось фахівцями-безпекознавцями інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки [100,256]. Відсутність системи забезпечення інформаційної безпеки унеможливорює надійне забезпечення не лише інформаційної, а й національної безпеки» [141].

Таким чином, обгрунтованим 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 так чи інакше віддзеркалює її сутнісний чи функціональний аспекти і відрізняється одне від одного набором певних характеристик і компонентів. В сучасних умовах Україна ще має чітко визначити та відстояти своє справжнє місце в системі континентальної і глобальної безпеки. Зазначене також стосується інформаційної складової у забезпеченні національної безпеки.

По-перше, інформаційний простір України трансформується в систему нового міжнародного інформаційного порядку. Він стає більш відкритим, а за низького рівня інформатизації і слабого інформаційного захисту – більш доступним.

По-друге, система національної безпеки України протягом останніх років піддається величезним випробуванням національного, регіонального та глобального рівнів в умовах гібридної війни, однією з ключових складових якої є саме інформаційна сфера.

По-третє, становлення системи національної безпеки України відбувається в умовах утвердження української державності й нових суспільних відносин. Внутрішнє життя України нині характеризується болісною соціальною модернізацією, політичною невпорядкованістю, політичним і соціальним розшаруванням, яке доходить до рівня протистояння, перманентною фінансовою та економічною кризою. У цих екстремальних умовах, хоча й повільно, але йде процес становлення та інформатизації інститутів громадянського суспільства як одного з найважливіших елементів системи національної безпеки. На глобальному рівні саме сучасні кризові явища здебільшого й детермінують стан інформаційної безпеки перехідних країн, у тому числі й України [93].

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 [219].

Водночас, інформаційна безпека являє собою складну, динамічну, цілісну соціальну систему, компонентами якої є підсистеми безпеки особистості, держави і суспільства. Саме взаємозалежна, системна інформаційна єдність останніх складає якісну визначеність, покликану здійснити захист життєво важливих інтересів людини, суспільства і держави, забезпечити їх конкурентноздатний, прогресивний 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 : доктрина і правова основа, якими визначаються основні завдання і принципи діяльності щодо захисту безпеки; інституціональний механізм, тобто сукупність міжнародних і національних державних і громадських органів, які у своїй діяльності вирішують певні завдання щодо підтримання стану безпеки різних рівнів; методологічна база, тобто способи, засоби і ресурси, що використовуються для реалізації конкретних завдань у межах політики безпеки [168, с.119].

Іноземний досвід свідчить, що такі системи мають ряд загальних ключових ознак: ієрархічність побудови системи; наявність керівного, а не дорадчого органу системи; чітка організація взаємодії між усіма елементами системи; активне залучення до реалізації інформаційної політики не тільки національних, а й іноземних ЗМІ. Загальне керівництво системою здійснюється, як правило, головою виконавчої влади через відповідний робочий орган, який розробляє державну інформаційну політику і координує діяльність її складових елементів, якими є підсистеми інформаційної безпеки профільних державних структур. Найбільш розвинуті системи інформаційної безпеки функціонують у США Великій Британії, Ізраїлі, ФРН, Російській Федерації, Китаї, тобто у тих країнах, які постійно знаходяться під потужним зовнішнім інформаційним впливом, а тому вимушені створювати національні

системи інформаційного захисту [184].

Використовуючи методологію системного дослідження, розроблену У. Баклі, К. Бейлі, Н. Луманом та ін., якщо взяти до уваги думку Н. Лумана, котрий розуміє суспільство як всеосяжну соціальну систему, що включає всі інші соціетальні системи, то як одну із соціетальних систем можна розглядати й систему забезпечення інформаційної безпеки, дослідники НДІ інформатики і права називають основними структурними елементами системи інформаційної безпеки особу, суспільство і державу, їх життєво важливі інтереси, загрози в інформаційній сфері [448].

При цьому, 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.

Погоджуючись в методологічній частині з колегами, 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 забезпечення;
- 3) політика інформаційної безпеки;
- 4) засоби і способи забезпечення інформаційної безпеки.

При цьому, метою реалізації інформаційної безпеки вбачається побудова системи забезпечення інформаційної безпеки конкретного об'єкта.

Звернемося до окремих складових запропонованого підходу. Аналізу першого елемента було присвячено увагу в попередніх розділах.

Ст. 3 Закону України «Про основи національної безпеки України» [311] визначає, що об'єктами забезпечення національної безпеки є:

людина і громадянин – їхні конституційні права і свободи (виділено

нами – авт.);

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 [309].

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 [377].

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 свідчить про плюралізм підходів до суб'єктного складу системи забезпечення інформаційної безпеки [170].

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) [183,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 – ті, що наділені державно-владними повноваженнями, і ті, що ними не наділені, хоча в окремих випадках можуть мати певний обсяг делегованих державно-владних повноважень. Тобто формально виділяються дві складові забезпечення національної безпеки: державне забезпечення і недержавне забезпечення [378,с.109].

Тихомиров О.О. пропонує серед суб'єктів забезпечення інформаційної безпеки узагальнено виділити три групи: міжнародні організації; держава в особі державних організацій; недержавні організації, громадяни та їх об'єднання [378,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 [100]. Окрім того, заходи щодо забезпечення інформаційної безпеки України фактично відображали міжнародний, державний і недержавний рівні забезпечення інформаційної безпеки.

В.І. Гурковський до системи органів (суб'єктів) щодо підтримання

інформаційної безпеки відносить: 1) органи законодавчої влади і державного управління загальної компетенції – Верховна Рада України, Кабінет Міністрів України; 2) Конституційний суд, суди загальної юрисдикції; 3) органи виконавчої влади: а) правоохоронні органи – Прокуратура України, Міністерство внутрішніх справ України, Служба безпеки України; б) галузеві органи державного управління, що регулюють інформаційні відносини в певних галузях – Державний комітет зв'язку та інформатизації України, Державний комітет телебачення і радіомовлення України, Державний департамент інтелектуальної власності, Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України; 4) громадські структури – підприємства, установи, організації різних форм власності, діяльність яких пов'язана з наданням послуг зв'язку, із захистом інформації, інформаційні агентства, суб'єкти видавничої справи [85,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 [244,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, за О.В. Олійником, організаційно-виконавчий, відомчотериторіальний, 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 [244,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 [244,с.220].

Хотілося б звернути увагу на розуміння важливості правового закріплення критична інфраструктури держави в цілому, та її інформаційної складової зокрема. 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 року Європейська комісія вдалась до розробки 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 [502].

Європейська Рада в червні 2004 року доручила Європейській комісії підготувати спільну стратегію для захисту критично важливих об'єктів інфраструктури. Ця стратегія була завершена Європейською комісією в грудні 2006 року, і вона називається Європейська програма по захисту критичної інфраструктури (ЄПЗКІ) – The European Programme for Critical Infrastructure Protection [489]. З огляду на цю програму почато розробку Європейської інформаційної мережі попередження загроз критичній інфраструктурі – Critical Infrastructure Warning Information Network (CIWIN). Її було офіційно затверджено рішенням Ради [489]2008/0200, а у квітні 2009 року Європейський парламент прийняв відповідне законодавче рішення про CIWIN.

Європейська комісія рекомендувала всім країнам ЄС вжити заходів, сформульованих в ЄПЗКІ: 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 [458].

У відповідь на це повідомлення низкою держав ЄС були прийняті відповідні акти і вжиті заходи. Уряд Словаччини у 2007 році ухвалив «Концепцію критичної інфраструктури Словацької Республіки, її захисту та оборони», де визначено загальну стратегію захисту життєво важливих об'єктів, але немає детального плану дій у кризових ситуаціях, а у 2011 року було прийнято закон про критичну інфраструктуру Словацької Республіки, котрий чітко визначає об'єкти критичної інфраструктури, державні органи, що відповідають за захист останніх, а також детальний план заходів у разі виникнення надзвичайної ситуації. У 2007 року польський уряд ухвалив Закон про управління кризовими ситуаціями, в рамках якого подано чітке розуміння параметрів критичної інфраструктури та її захисту. Угорщина у 2012 року прийняла Закон про захист критичної інфраструктури, котрий можна назвати одним із найбільш комплексних документів у цій царині. Власне, закон чітко визначив порядок і принципи зарахування об'єктів до категорії критичної інфраструктури, умови забезпечення їхньої безпеки, проведення інспекцій, а також механізм взаємодії між державними інституціями у критичних ситуаціях, створення резервних ресурсних фондів тощо [350].

Четвертий рівень – рівень суб'єктів невідного характеру, до яких О.В. Олійник відніс громадян України та їх об'єднання, державні і приватні засоби масової інформації.

Державна інформаційна політика повинна відбивати нагальні питання,

що склалися у міжнародній сфері та сфері інформаційної безпеки тощо. Необхідним є забезпечення законодавчого захисту прав та інтересів всіх суб'єктів інформаційних відносин. Найскладнішими тут є такі завдання, що передбачають гармонійне забезпечення інформаційної безпеки держави, особи і суспільства з одночасним виокремленням нагальних пріоритетів, до яких слід віднести створення/відновлення основних точок захисту системи національної безпеки в інформаційній сфері, практичну реалізацію наведеної вище схеми створення ефективної системи інформаційної безпеки держави, перегляд списку нових інформаційних загроз, усунення наявних із визначенням ступеня можливих наслідків та рівнів їх інтенсивності. Основні акценти державної інформаційної політики повинні базуватись на забезпеченні права на достовірну, повну та своєчасну інформацію, свободи слова та інформаційної діяльності в національному інформаційному просторі, недопущення втручання в зміст та внутрішню організацію інформаційних процесів, крім випадків, визначених законодавством відповідно до Конституції України; збереженні та вдосконаленні вітчизняного національного інформаційного продукту та технологій, національно-духовних та культурних цінностей України; забезпеченні інформаційної та національно-культурної ідентифікації України у світовому інформаційному просторі; гарантування державної підтримки та розвитку ресурсів науково-технічної продукції та інформаційних технологій [48].

Вибір політики національної безпеки обумовлюють чинники сили чи слабкості держави, до яких, на думку Фредеріка Х. Гартмана, слід відносити:

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

суспільство до влади, ефективність діяльності влади;

військовий чинник – спосіб організації і стан ефективності збройних сил, їх розмір у співвідношенні до населення призовного віку [506].

І.Р. Боднар пропонує національну безпеку України в інформаційній сфері розглядати як інтегральну цілісність чотирьох складових – персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки [48]. 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 [92].

Забезпечення інформаційної безпеки можна визначити як комплекс адміністративних заходів необхідний для досягнення такого стану інформаційного розвитку (духовного, соціально-політичного, технічного) та захищеності особи, суспільства, держави, за якого сторонні інформаційні впливи не завдають суттєвої шкоди національним інтересам [256].

Діяльність із забезпечення інформаційної безпеки має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства та людини за трьома головними напрямками:

- інформаційно-психологічному, зокрема щодо забезпечення конституційних прав і свобод людини й громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі для утвердження загальнолюдських та національних моральних цінностей;

- технологічного розвитку, зокрема стосовно розбудови та

інноваційного оновлення національних інформаційних ресурсів, упровадження новітніх технологій створення, оброблення та поширення інформації;

– захисту інформації, зокрема щодо забезпечення її конфіденційності, цілісності й доступності, в тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак [256].

2.3. Місце та роль інформаційної безпеки в інформаційно-правових дослідженнях

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, 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 невідомої 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 загально визначених норм справедливості – сягає до часів античності, а наукове обґрунтування проблем національної безпеки взагалі й інформаційних її аспектів зокрема, вбачають у творах Томаса Гоббса та Іммануїла Канта [96, с. 140]. Ці філософи прийшли до розуміння необхідності встановлення громадянського устрою, який би забезпечував безпеку індивіда.

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 Анрі 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» [34].

Концептуально погоджуємось з позицією Пилипчука і Дзьобаня, що «подальші адекватні реальній соціальній дійсності наукові розвідки в царині інформаційної безпеки без опори на класичну спадщину уявляються досить сумнівними» [96,с.146].

При цьому, ці автори окреслюють чотири аспекти, на які звертали увагу класики в своїх працях:

Інформаційно-етичний – Августин Блажений, І. Кант, Р. Оуен, А.Бергсон, А.Швайцер);

Зв'язок досягнення безпечного стану і господарської та економічної структури, а також колізії природного й громадянського станів особистості – Цицерон, Гоббс, Локк;

Договірні відносини між державами задля формування відповідних організаційно-правових передумов і утворення об'єднань держави – Гроцій, Сен-Сімон, Ясперс, Тойнбі;

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. Оскільки інформації у всіх концепціях згаданих дослідників (незалежно від назви) надається телеологічний статус, це обумовлює онтологічний виміру інформаційної безпеки будь-якої соціальної системи сучасності, осьювою детермінантою якої є зростання впливу розвитку інформаційно-комунікативних технологій.

Оскільки небезпека, що породжується процесом інформатизації, зумовлена розвитком цього процесу в моделі нестійкого розвитку суспільства, то інформаційна безпека повною мірою може бути забезпечена лише при переході до стійкого розвитку суспільства. Необхідною умовою

забезпечення інформаційної безпеки і національної безпеки в цілому є перехід до стійкого розвитку суспільства ноосферної орієнтації [95].

Російські теоретики інформаційної безпеки (Артамонова Я.С. [14], Петров С.В., Петров В.П. [258] враховуючи вплив на трансформацію ідей інформаційної безпеки, розвитку інформаційних комунікацій виділяють сім етапів:

I етап (до 1816 року) – використання природніх інформаційно-комунікаційних засобів. На цьому етапі основним завдання інформаційної безпеки є захист відомостей про події, факти, майно, місцезнаходження і інші дані, що є життєво значимими для людини особисто або спільноти, до якої вона належить.

II етап (починаючи з 1816 року) – пов'язаний з початком використання технічних засобів електро- і радіозв'язку. Для забезпечення конфіденційності і перешкодостійкості радіозв'язку необхідно було використовувати досвід першого етапу інформаційної безпеки на вищому технологічному рівні, а саме кодування повідомлення (сигналу) з подальшим декодуванням прийнятого повідомлення (сигналу).

III етап (починаючи з 1935 року) – 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 впливів на їх приймальні пристрої активними маскуючими і пасивними імітуючими радіоелектронними перешкодами.

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

V етап (починаючи з 1965 року) – обумовлений створенням і розвитком локальних інформаційно-комунікаційних мереж. Завдання інформаційної безпеки також вирішувалися, в основному, методами і способами фізичного захисту засобів добування, переробки і передачі інформації, об'єднаних

в локальну мережу шляхом адміністрування і управління доступом до мережевих ресурсів.

VI етап (починаючи з 1973 року) – пов’язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань. Для забезпечення інформаційної безпеки в комп’ютерних системах з безпроводними мережами передачі даних необхідною умовою є розробка нових критеріїв безпеки. Інформаційний ресурс став найважливішим ресурсом держави, а забезпечення його безпеки – найважливішою і обов’язковою складовою національної безпеки. На цьому етапі формується інформаційне право як нова галузь міжнародної правової системи.

VII етап – починаючи з 1985 року – пов’язаний із створенням і розвитком глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення. Для вирішення завдань інформаційної безпеки на цьому етапі необхідним є створення макросистеми інформаційної безпеки людства під егідою провідних міжнародних організацій [14, 259].

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, чий дослідження інформаційної сфери розпочинались в межах адміністративного права, а згодом значної уваги в їх працях набули питання інформаційного права – зокрема, Арістова І.В., Бачило І.Л., Брижко В.М., Белєвцева 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., Тихоміров Ю.А., Цимбалюк В.С. та інші [412, 413, 414].

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. Жиляєв,

Д.В. Ланде, В.А. Ліпкан, А.І. Марушак, 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, що включає інституціональні форми, організаційні методи, правові норми та принципи регулювання правовідносин щодо захисту інформаційної безпеки держави, суспільства, людини, стала захищена у 2014 році Кормичем Б.А. докторська дисертація «Організаційно-правові основи політики інформаційної безпеки України» [169]. 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.

Зокрема, з огляду на особливості природи правових норм, якими визначається правовий статус різних об'єктів інформаційної безпеки, автор виокремлював два комплекси питань. По-перше, це інформаційна безпека людини і суспільства, яка базується на нормах природного права і вимірюється ступенем свободи від втручання держави та інших осіб, можливостями самореалізації та самовизначення. По-друге, це інформаційна безпека держави, яка побудована на позитивному праві і пов'язана із застосуванням обмежень, заборон, жорсткою регламентацією, невід'ємним елементом яких є сила державного примусу.

Також заслуговує на увагу позиція Кормича Б.А. щодо правової бази інформаційної безпеки, яка на його думку, поєднує в собі норми декількох галузей права, насамперед: конституційного, адміністративного, інформаційного, але її головним системоутворюючим чинником виступають єдині концептуальні засади державної політики інформаційної безпеки [169].

Окрім того, Кормич Б.А. визначав правовий статус людини як об'єкта інформаційної безпеки, що визначається її правами в галузі інформації. По-перше, це комплекс прав людини вільно, безперешкодно, на власний розсуд

бути суб'єктом інформаційних процесів: шукати, одержувати і поширювати інформацію, при чому це право не пов'язано з територіальною юрисдикцією держави і не обмежується територіально державними кордонами. І по-друге, це комплекс прав людини на захист від неправомірного інформаційного втручання, яке охоплюється англійським терміном *privacy*, тобто правом на конфіденційність інформації щодо особистого життя та правом на захист від розповсюдження вигаданої та перекрученої інформації, що завдає шкоди її честі і репутації [169,с.36].

Хоча в тогочасних працях автора не присвячено значної уваги таким об'єктам інформаційної безпеки як суспільство і міжнародне співтовариство, проте важливим було розуміння, що ефективність правового регулювання в сфері інформаційної безпеки залежить від дотримання низки основних принципів, до яких він відносив: комплексний підхід до правового будівництва в галузі інформаційної безпеки; забезпечення примату гарантованих Конституцією прав і свобод людини і громадянина; розуміння та слідування в процесі правотворчості загальновизнаним міжнародно-правовим нормам і стандартам та задекларованим конституційним засадам державної політики України; чітке визначення та максимальне звуження кола питань і відповідно оптимізація кількості правового матеріалу, який включається до сфери інформаційної безпеки» [167,с.128]

В 2004 році було видано перший український навчальний посібник з інформаційного права «Основи інформаційного права», до складу авторського колективу якого входили В.С. Цимбалюк, В.Д.Гавловський та інші. У ньому питанням інформаційної безпеки було присвячено окремий розділ– «Інформаційна безпека як об'єкт інформаційного права» [247]. Зокрема, автори відзначали необхідність «формування правил поведінки, відносин у так званому віртуальному або кібер-просторі» [247]. Когнітивно-юридичний аналіз нормативно-правових актів у сфері суспільних інформаційних відносин, з позицій накопичених на той час наукових знань, свідчив про те, що вже на початку 2000-х років в суспільстві сформувалося усвідомлення необхідності правового регулювання одного з інститутів інформаційної безпеки: захисту інформації. Водночас, 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 [247].

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. Беляков К.І. в монографії «Інформація в праві: теорія і практика» відзначає, що розробка кодекса дозволила б також вирішити термінологічні проблеми в сфері інформаційного законодавства, які пов'язані з неузгодженістю дефініцій, що вживаються [41,с.87-89].

Слід звернути увагу, що в згадуваній праці відокремлювались категорії «інформаційна безпека» і «безпека в інформаційному суспільстві», в останньому розділі увагу, зокрема, було присвячено безпеці в інформаційному суспільстві через нові парадигми науки кримінального права [247]. Хоча зміст їх не був конкретизований, ба – навіть помилково ототожнювався з «захистом інформації».

На цьому етапі становлення наукової та правової категорії «інформаційна безпека» подібне ототожнення її із захистом інформації було досить поширеним явищем, а подекуди має місце і досі здебільшого в зарубіжній науковій літературі [102,532,533]. Безперечно, правове регулювання захисту інформації є складовою інформаційної безпеки, проте не є їй тотожним.

Зокрема, адміністративно-правовому захисту інформаційної сфери було присвячено монографію Настюка В.Я. та Белецева 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» [225].

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» [244]. Автор відзначає, що «важливою проблемою для сучасної України є необхідність подолання як в теорії, так і на практиці абстрактного, відірваного від реальної життєдіяльності вузького розуміння забезпечення інформаційної безпеки лише у сфері обігу інформації, її виготовлення, поширення, використання, захисту та діяльності ЗМІ. Водночас, пропонує широке розуміння забезпечення інформаційної безпеки як здійснення комплексу системних превентивних заходів з надання гарантій захиту 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» [244,с.368-369]. Таким чином, інформаційна безпека визначається як складне соціальне і політико-правове явище, що вимагає комплексного і системного підходу, як, зрештою, і її правове забезпеченням. В цьому аспекті одним із важливих здань, 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» [22,с.119], зауважимо, що інформаційні правовідносини щодо інформаційної безпеки людини регулюються також іншими нормами

права, а отже 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 [47,с.34-38, 127,с.36-45].

Важливо, що повстає нова плеяда науковців, чие коло наукових інтересів зосереджене на інформаційно-правових дослідженнях, зокрема, Баскаков В. Ю., М. І. Дімчогло, В. А. Залізняк, Г.М. Красноступ, Т.М. Кронівець, Г.М. Линник, К.С. Мельник, Ю.Є. Максименко, А.Ю. Нашинець-Наумова, Л.І. Руднік, І.М. Сопілко, О. В. Стоєцький, Д.В. Сулацький, К.Г. Татарнікова, В.С. Шапіро, І.О. Трубін, Р.В. Радейко, В.С. Політанський, О. В. Шепета та інші [126,с.6-48,186, 206,418].

Значна, частина з перерахованих 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 [206,с.17-18]. Як можемо бачити, значна кількість означених у 2007 році проблем й досі залишається не вирішеною.

В 2011 році Линником Г.М. було здійснено дослідження на тему «Адміністративно-правове регулювання інформаційної безпеки України» в якому обгрунтовано 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 та отримання правової допомоги в роз'ясненні змісту конкретних норм права; проводити безкоштовні курси громадянам щодо оволодіння навичками користування інформаційними технологіями; створити спеціалізовані служби, основним завданням якої було б координація дій державних та недержавних інституцій у сфері забезпечення інформаційної безпеки України, а також чітке визначення їх завдань, функцій, повноважень в цій сфері [186,с.18].

Зокрема, 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 [262,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; (є) врегулювання вільного доступу до інформації; (ж) надання недостовірної чи неповної інформації тощо [262,с.17].

Основними осередками правових досліджень в галузі інформаційної безпеки 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 Київському національному університеті імені Тараса Шевченка, Національному юридичному університеті імені Ярослава Мудрого, 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 року – 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 року 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 року 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 державі”; “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” [364].

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 зачасту 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 [134].

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 [187,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, зареєстрованого в Міністерстві юстиції України 30.09.11 р. за № 1133/19871, щодо включення спеціальності 12.00.13 “Інформаційне право; право інтелектуальної власності (юридичні науки)”, проте його положення досі залишаються нереалізованими [296,с.3].

Слід зауважити, що інформаційна безпека як галузь наукових досліджень залишаються комплексною сферою, на межі соціальних і технічних наук, а отже, цінним вбачається використання трансдисциплінарної стратегії досліджень Іммануїла Валлерстейна, американського соціолога та історика, задля виявлення подібності та зв'язків між явищами, а не створення бар'єрів щодо предмету дослідження [583,с.13-40].

2.4. Правове забезпечення інформаційної безпеки в законодавстві України

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 протидії загрозам цих інтересів та впорядкування відповідного правотворчого процесу [243,с.132-137].

В дослідженні Ю.Є. Максименко під нормативно-правовим регулюванням інформаційної безпеки України пропонується розуміти форму владного правового впливу на суспільні інформаційні відносини, що здійснюється державою з метою їх упорядкування, закріплення і забезпечення [206,с.118].

О. В. Олійник, у свою чергу, 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 [143,с.132-137].

Дозволимо собі не погодитись з доцільності використання категорії «правове регулювання інформаційної безпеки». Правове регулювання – це упорядкування суспільних відносин, яке здійснюється державою за допомогою права і сукупності правових засобів. Оскільки інформаційна безпека є невід’ємною властивістю її об’єктів, то говорити про регулювання

інформаційної безпеки немає підстав. Правове регулювання може розглядатись лише як складова забезпечення інформаційної безпеки.

Цимбалюк В.В. стверджує, що «забезпечення безпеки» – це тавтологічний вираз, непридатний для наукового вжитку. Водночас, звернемо увагу на значення цих слів і явище, що ними описується.

На думку ж 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 [214].

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) [69].

Українські мовники схиляють до позиції, що «безпеку» слід «гарантувати», а не «забезпечувати» [353]. 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, посилюється 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» [481]. 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 парафоровані 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 [207,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 не існує, незважаючи на об’єктивну потребу такого акту 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.

Інформаційна безпека не є винаходом останніх десятиліть. Усвідомлення її значимості в історії людства змінювалось з усвідомленням суспільної цінності інформації, проникненням інформаційної діяльності в усі сфери життєдіяльності суспільства і узалежнення життя людини, існування держави від інформаційних процесів [133,135].

Не слід також ототожнювати правове забезпечення з нормативним, а тим паче з законодавчим. Погоджуємось з професором Ліпканом у твердженні, що «право не зводиться до норм» [194].

На думку Остроухова В.В. 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 [140].

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. Баранову належить вислів, що відображає початки створення нормативно-правового забезпечення становлення інформаційної сфери в Україні: «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» [19,с.62]. За кілька тижнів після референдуму 1 грудня 1991 року, 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» (від 13 грудня 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.

Але власне 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. Цим зумовлена необхідність пріоритетної державної підтримки розвитку науки як джерела економічного зростання і невід'ємної складової національної культури та освіти, створення умов для реалізації інтелектуального потенціалу громадян у сфері наукової і науково-технічної діяльності, цілеспрямованої політики у забезпеченні використання досягнень вітчизняної та світової науки і техніки для задоволення соціальних, економічних, культурних та інших потреб. З перспективи часу,

цей Закон виглядає як передвісник становлення і розбудови інформаційного суспільства і суспільства знань, як його наступного етапу.

В українському національному праві системоутворюючим фактором і поштовхом до виникнення і формування інформаційного права як інституції публічного (державного) права можна вважати прийнятий 2 жовтня 1992 р. Закон України «Про інформацію», який був прийнятий на підставі Декларації про державний суверенітет України та Акта проголошення незалежності України [247]. В першій редакції закону визначались Мета і завдання – «Закон встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації». А також визначалась категорія «законодавство України про інформацію», до якого віднесено: Конституція України; Закон України «Про інформацію»; законодавчі акти про окремі галузі, види, форми і засоби інформації; міжнародні договори та угоди, ратифіковані Україною; принципи і норми міжнародного права.

Вперше на законодавчому рівні принципи інформаційних відносин та напрями державної інформаційної політики знайшли закріплення в Законі України «Про інформацію». Так, Основними принципами інформаційних відносин визнано:

- 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.

А основними напрямками державної інформаційної політики визначались:

- забезпечення доступу кожного до інформації;
- забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;
- 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;
- постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;
- забезпечення інформаційної безпеки України;
- сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

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 (конкретизовані): 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 праводносин, 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 [257,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 (пресу) в Україні» (від 16 листопада 1992 р.) [294], Закон України «Про науково-технічну інформацію» (від 25 червня 1993 р.) [311], «Про охорону прав на винаходи і корисні моделі» (від 15 грудня 1993 р.) [320], «Про телебачення і радіомовлення» (від 21 грудня 1993 р.) [324], «Про авторське право і суміжні права» (від 23 грудня 1993 р.) [285], Про державну таємницю» (від 21 січня 1994 р.) [292], «Про національний архівний фонд і архівні установи» (від 24 грудня 1993 р.) [312], «Про захист інформації в автоматизованих системах» (від 5 липня 1994 р.) [306], «Про зв'язок» (від 16 травня 1995 р.) [308], Закон України «Про бібліотеки і бібліотечну справу» (від 27 січня 1995 р.) [286], «Про рекламу» (від 3 липня 1996 р.) [322], «Про систему Суспільного телебачення і радіомовлення України» (18 липня 1997 року) [323], «Про Національну раду України з питань телебачення і радіомовлення» (від 23 вересня 1997 року) [314], «Про державну підтримку засобів масової інформації та соціальний захист журналістів» (від 23 вересня 1997) [285] та інші.

В тому ж таки 1992 році у національному нормативно-правовому просторі вперше вжито категорію “інформаційна безпека”. Розпорядження Президента України “Про затвердження складу Консультативно-експертної групи по підготовці концепції національної безпеки України” [64], 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 [595, 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 майже 20 років після прийняття Конституції, все ще не прийнято закону, який би визначав концепцію державної інформаційної політики України. Відповідно, на законодавчому рівні неврегульованим залишається і забезпечення інформаційної безпеки. 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 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 році було прийнято два закони, що стосувались інформатизації – Закон України «Про Національну програму інформатизації» [307] (від 4 лютого 1998 р.) та Закон України «Про Концепцію Національної

програми інформатизації» (від 4 лютого 1998 р.) [304], 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.

Бачило І.Л. вважала, що завдання регулювання телекомунікаційних відносин не вирішується в рамках традиційних галузей законодавства [26].

Таким чином, Закон України «Про радіочастотний ресурс України» [315] 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 [315].

В 2002 році законодавчого закріплення набуло правове забезпечення функціонування загальнонаціональної спеціальної інформаційно-телекомунікаційної системи, яка дістала назву Національна система конфіденційного зв'язку. Згідно з нормами ст. 1 Закону України «Про Національну систему конфіденційного зв'язку», Національна система конфіденційного зв'язку – сукупність спеціальних телекомунікаційних систем (мереж) подвійного призначення, які за допомогою криптографічних та/ або технічних засобів забезпечують обмін конфіденційною інформацією в інтересах органів державної влади та органів місцевого самоврядування, створюють належні умови для їх взаємодії в мирний час та у разі введення надзвичайного і воєнного стану. Однією з особливостей даної системи є те, що вона функціонує як система подвійного призначення, тобто у мирний час мережі даної системи можуть використовуватися організаціями для передачі сучасними видами зв'язку конфіденційної інформації в інтересах як органів державної влади, так і інших юридичних осіб, у тому числі суб'єктів фінансово-економічної сфери. Тоді як у разі виникнення надзвичайних

ситуації ресурс даної системи задіяний для передачі конфіденційної інформації в інтересах національної безпеки та оборони держави.

В 2003 році було врегульовано на законодавчому рівні питання електронного документообігу. Це питання вже довгий час потребувало правового регулювання і прийняття законів «Про електронний цифровий підпис» та «Про електронні документи та електронний документообіг» стало відповіддю на нагальну потребу створення і розвитку інфраструктури електронного документообігу [289,291]. Цими законами було встановлено основні організаційно-правові засади електронного документообігу та використання електронних документів. Згадані закони регулюють правові відносини щодо електронного підпису; електронного цифрового підпису; оригіналу електронного документа; правового статусу електронного документа та його копії; відправлення та передавання електронних документів; держання електронних документів; перевірки цілісності електронного документа; зберігання електронних документів та про архіви електронних документів; організації електронного документообігу; обігу електронних документів, що містять інформацію з обмеженим доступом; права та обов'язки суб'єктів електронного документообігу; вирішення спорів між суб'єктами електронного документообігу; відповідальності за порушення законодавства про електронні документи та електронний документообіг.

На реалізацію положень цих законів було прийнято низку підзаконних актів, зокрема Постанова Кабінету Міністрів України «Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу» (26.05.2004), Постанова Кабінету Міністрів України «Про затвердження Порядку акредитації центру сертифікації ключів» (13.07.2004), Постанова Кабінету Міністрів України «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності» (28.10.2004), Розпорядження Президента «Про приєднання до Угоди про створення Міжнародної системи документального шифрованого зв'язку Співдружності Незалежних

Держав» (06.12.2005), Постанова Кабінету Міністрів України «Про затвердження Порядку обов'язкової передачі документованої інформації» (28.10.2004), Постанова Кабінету Міністрів України «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади» (28.10.2004), Постанова Кабінету Міністрів України «Про затвердження Положення про центральний засвідчувальний орган» (28.10.2004), Постанова Кабінету Міністрів «Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу» (26.05.2004), Постанова Кабінету Міністрів «Про затвердження Порядку акредитації ЦСК» (13.07.2004), Постанова Кабінету Міністрів «Про затвердження Положення про ЦЗО» (28.10.2004), Постанова Кабінету Міністрів «Про затвердження Порядку застосування ЕЦП» (28.10.2004), Постанова Кабінету Міністрів «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади» (28.10.2004), Постанова Кабінету Міністрів «Про затвердження Порядку обов'язкової передачі документованої інформації» (28.10.2004) та інші. Слід зауважити, що законодавчо не було врегульовано питання щодо застосування мов у документообігу.

В 2004 році було прийнято Закон України «Про телекомунікації» [319], 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 [319]. 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 [118].

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 році нового Кримінального кодексу України [177] 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.

В Законі України «Про основи національної безпеки України» (2003р.) [311] вперше офіційно визначено інформаційну безпеку як невід'ємну складову національної безпеки України. Зокрема, серед об'єктів національної безпеки названо інформаційне середовище (ст. 3)²⁰. 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

²⁰ На жаль, ані цей закон, як і жоден інший не визначає що таке інформаційне середовище.

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; життя 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 року 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 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 року 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.

Пріоритетами забезпечення інформаційної безпеки визначено: 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; розробка і реалізація скоординованої інформаційної політики органів державної влади; виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією 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, упровадження загальнонаціональних освітніх програм з медіакультури із залученням громадянського суспільства та бізнесу.

А пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів – розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації;

розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав – членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

Як вже згадувалось вище, в 2005 році Україна ратифікувала Конвенцію про кіберзлочинність [161]. Її проект був розроблений у червні 2001 р. Європейським комітетом з проблем злочинності. У листопаді того самого року 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 [161].

В цій конвенції вперше на міжнародному рівні була запропонована класифікація кіберзлочинів. У першу групу виділено злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему. У другу групу – злочини, пов'язані з використанням комп'ютера, як засобу скоєння злочинів – а саме, як засіб маніпуляцій з інформацією. У цю групу входять комп'ютерне шахрайство та комп'ютерне підроблення. Третю групу складають злочини, пов'язані з контентом (змістом даних). Найпоширеніший і караних практично у всіх державах вигляд цих кіберзлочинів – злочини, пов'язані з дитячою порнографією. У четверту групу увійшли злочини, пов'язані з порушенням авторського права

і суміжних прав, при цьому встановлення таких правопорушень віднесено документом до компетенції національних законодавств держав. П'ята група злочинів з'явилась пізніше, після прийняття окремого протоколу – це акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж.

В 2008 р. Віктор Ющенко своїм Указом ввів в дію рішення РНБО «Про невідкладні заходи щодо забезпечення інформаційної безпеки України» [309]. 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, враховано понад 200 конкретних пропозицій, у тому числі від представників громадських організацій, експертного середовища [100].

Основною метою реалізації положень Доктрини інформаційної безпеки України визначалось створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету. Доктрина передбачала три основні напрями забезпечення національного інформаційного суверенітету: законодавче визначення стратегічних шляхів розвитку та захисту національних ринків інформаційних та телекомунікаційних

послуг на основі єдиної державної політики; формування норм, засад і меж діяльності зарубіжних та міжнародних суб'єктів в національному інформаційному просторі; визначення та захист національних інтересів в світовому інформаційному просторі та міжнародних інформаційних відносинах. В інформаційній сфері відокремлювались життєво важливі інтереси особи, суспільства й держави. Окрім того було закріплено основні засади інформаційної безпеки України, реальні та потенційні загрози інформаційній безпеці України та напрями державної політики у сфері інформаційної безпеки України.

Доктрина втратила чинність відповідно до Рішення РНБО України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [301], 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 рік було розроблено і введено в дію Указом Президента України лише Стратегія кібернетичної безпеки України [363], інші ж акти проходять річні 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. Створення такого центру, на нашу думку, є обгрунтованим, оскільки повноваженнями щодо забезпечення інформаційної безпеки наділена значна кількість державних органів та установ, серед яких –

Національна рада України з питань телебачення і радіомовлення, Держкомтелерадіо України, Служба безпеки України, Держспецзв'язку України, Служба зовнішньої розвідки України, Міністерство оборони України, МВС України, Міністерство закордонних справ України, Міністерство культури України, Міністерство юстиції України та інші, що призводило до дублювання функцій і браку координованості діяльності.

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 сфері 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 [355].

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». Представники правозахисних організацій та медіа відразу зреагували на ці положення з деяким побоюваннями утисків свободи слова [99].

Складно на даний момент оцінити ймовірний 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.

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». 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», яким ще в січні 2007 року 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 [313].

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 визначалось, що вирішення проблеми інформаційної безпеки має здійснюватися шляхом: створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів; підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань; вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері; розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Очікувалось, що впровадження Основних засад розвитку інформаційного суспільства в Україні на 2007-2015 роки дасть можливість забезпечити позитивні зміни в життєдіяльності суспільства і людини, а саме: збільшити рівень захисту прав і свобод людини та її добробуту, активізувати участь громадян в управлінні державою, сприяти розвитку демократії; підвищити конкурентоспроможність України, ефективність державного управління, продуктивність праці у всіх сферах економіки, рівень інформаційної безпеки людини, суспільства, держави, ступінь розвитку інформаційно-телекомунікаційної інфраструктури, зокрема українського сегменту Інтернету; забезпечити перехід економіки до моделі науково-технічного та інноваційного розвитку, збільшити частку наукоємної продукції, сприяти якості та доступності послуг освіти, науки, культури, охорони здоров'я за рахунок впровадження ІКТ; розширити можливості людини отримувати доступ до національних та світових інформаційних електронних ресурсів; створити нові робочі місця, поліпшити умови роботи і життя людини; поглибити запровадження нормативно-правових засад інформаційного суспільства.

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 року, щорічно видається Всесвітнім економічним форумом (World Economic Forum), Україна в 2015 році 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 році (62 місце). Після цього упродовж двох наступних років було втрачено 28 пунктів, внаслідок чого у 2011 році 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 року є, передусім, відставання за складовими, що характеризують політичне і регуляторне середовище – 122 позиція та низький рівень використання ІКТ урядом – 124 позиція [72].

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 проти Російської Федерації.

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 [151]. О. Г. Марценюк виокремлює наступні:

1. Відсутність легальної, чіткої, ієрархічної єдності законів, що призводить до суперечливого тлумачення та застосування норм права на практиці.

2. Різні закони та підзаконні акти, що регулюють суспільні відносини, об'єктом яких є інформація, приймалися в різні часи і, особливо, без узгодження понятійного апарату. Такі нормативні акти не мають чітко визначеного змісту, недостатньо коректні. Термінологічні розбіжності, різне тлумачення однакових за назвою та формою визначень призводить до варіантного розуміння та застосування норм на практиці. Найбільш важливі терміни, які передбачають тільки одне визначення, мають різні визначення в різних нормативних актах. До них відносяться «таємна інформація», «таємниця», «документ», «документована інформація», «майно», «власність», «володіння», «інтелектуальна власність», «автоматизована система», «суб'єкт суспільних відносин», «учасники суспільних відносин», «система інформаційних відносин» та деякі інші.

3. Значна кількість законів та підзаконних нормативних актів в сфері інформаційних відносин ускладнює їх пошук, аналіз та узгодження для практичного застосування.

4. Має місце розбіжність відносно розуміння структури та складу системи законодавства в сфері інформаційних відносин та підходів до їх формування. В окремих законах до системи законодавства залучаються норми, що встановлені в підзаконних актах. В практиці правозастосування це призводить до колізії норм, ігнорування норм закону на користь норм підзаконного акту.

5. Нові правові акти в сфері суспільних інформаційних відносин часто неузгоджені концептуально з раніше прийнятими, що призводить до правового хаосу [212,с.38].

Заслугує на увагу позиція В. А. Ліпкана, який зауважив, що «...в інформаційному законодавстві відсутній чітко сформульований склад багатьох правопорушень, а також не виділено ознаки, за якими ті чи інші інформаційні правопорушення мають бути згруповані до однієї глави. Більше того у даному контексті ми хотіли б звернути увагу на ту обставину, що нині через кваліть із розвитком методологічних засад інформаційного права, відбувається штучне гальмування розвитку інформаційно-правової науки. Зокрема відсутні напрацювання щодо таких актуальних питань як: інформаційні конфлікти, інформаційно-правовий компроміс, інформаційно-правова відповідальність, інформаційна деліктологія, інформаційна функція держави тощо. Зокрема, теоретичний вакуум щодо концептуального оформлення інформаційно-правової відповідальності унеможливорює розроблення інформаційної деліктології, які разом складають могутній пласт майбутнього Кодексу України про інформацію. За таких умов, коли відповідальність за вчинення інформаційних правопорушень передбачена нормами різних кодексів утворюються штучні колізії, а в цілому нівелюється принцип невідворотності покарання. Так само невирішеними лишаються процедурні питання процесуального порядку притягнення до інформаційно-правової відповідальності» [147,с.5-11].

Кількість Законів в інформаційній сфері нажалі не переростає в якість. Красноступ Г.М. зауважила «...нам 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» [176,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 правове забезпечення формується безсистемно і непослідовно, а отже не здатне 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 [147, с.5-11].

Значущими вбачаються висновки, що пропонує Максименко Ю.Є. задля удосконалення українського інформаційного законодавства шляхом його кодифікації. Зокрема, вона стверджує, що на правовому рівні інформаційна безпека має розглядатися в трьох аспектах – як інформаційно-психологічна безпека, інформаційна безпека у сфері прав та свобод, інформаційно-технічна безпека. При цьому, на її думку нормативно-правове регулювання інформаційно-психологічної безпеки та інформаційної безпеки у сфері прав та свобод де-юре відповідає міжнародним і європейським стандартам у цій сфері, причому здійснюється на рівні законів України, в той час як інформаційно-технічна безпека урегульована переважно підзаконними нормативно-правовими актами і потребує узгодження з європейськими стандартами [206].

До недоліків чинного законодавства з інформаційної безпеки Максименко Ю.Є. відносить розпорошення норм у численних нормативно-правових актах різної юридичної сили; неузгодженість нормативно-правових актів як між собою, так і з чинною Конституцією; декларативність значного масиву норм без визначення шляхів їх реалізації, внаслідок чого спостерігається низький рівень реалізації норм права, що регулюють суспільні відносини у сфері забезпечення

інформаційної безпеки; а також наявність численних бланкетних чи відсильних норм права, багатьох абстрактних, суб'єктивних понять, що потребують офіційного тлумачення або чіткого визначення, а також відсутність закріплення фундаментальних, базових дефініцій (наприклад, інформаційної безпеки) [206].

Нагальною потребою вбачаємо необхідність розробки і прийняття базового для правового забезпечення 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 [56, 198, 400].

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» [557] від корпорації «ПЕНД» на замовлення сухопутних військ (армії) ЗС США (звіт 2013 року, код звіту по проекту – RAND10473) 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.

Олійник О.В. вважає, що вимоги інформаційної безпеки повинні органічно включатися у всі рівні законодавства, в тому числі і в конституційне законодавство, основні загальні закони, закони щодо організації державної системи управління, спеціальні закони, відомчі правові акти тощо [243,с.137]. При цьому він наводить як приклад структуру правових актів, орієнтованих на забезпечення інформаційної безпеки держави, яка запропонована російським безпекознавцем Ярочкиним В.І. [434, с.36-37].

Перший блок – конституційне законодавство. Норми, що стосуються питань інформатизації, інформаційної безпеки тощо, входять у нього як складові елементи.

Другий блок – загальні закони, кодекси (про власність, про надра, про землю, про права громадян, про громадянство, про податки, про антимонопольну діяльність тощо), які включають норми з питань інформаційної безпеки.

Третій блок – закони про організацію управління, що стосуються окремих структур господарства, економіки, системи державних органів та визначаючих їх статус. Вони включають окремі норми по забезпеченню інформаційної безпеки. Поряд із загальними питаннями інформаційного забезпечення та інформаційної безпеки конкретного органу ці норми повинні встановлювати його обов'язки по формуванню, актуалізації інформаційної безпеки, що представляє загальнодержавний інтерес.

Четвертий блок – спеціальні закони, які регламентують конкретні сфери відносин, галузі господарства, процеси. До них входить і Закон України «Про інформацію» та інші. Саме склад і зміст цього блоку законів і створює спеціальне законодавство як основу правового забезпечення інформаційної безпеки.

П'ятий блок – підзаконні нормативні акти із забезпечення інформаційної безпеки.

Шостий блок – законодавство України, що містить норми про відповідальність за правопорушення у сфері інформаційної безпеки.

Очевидно, що така структура має за основу законодавство іншої країни і, ймовірно, потребує врахування реалій українського законодавства і правової системи. Тим не менш, обґрунтованою вбачається позиція Олійника В.Д., щодо включення положень щодо інформаційної безпеки на всіх рівнях законодавства.

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.

РОЗДІЛ III. СУЧАСНИЙ СТАН ЗАХИЩЕНОСТІ ЛЮДИНИ ВІД ІНФОРМАЦІЙНИХ ЗАГРОЗ В УКРАЇНІ

3.1. Реальні і потенційні виклики та загрози інформаційній безпеці людини

Інформаційна безпека зараз безперечно є популярною темою, яку експлуатують ЗМІ, політики, навіть бізнес. Щоб не повертатись до теоретичних розмірковувань (див. розділ II), 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 людині здатності вільно і безперешкодно реалізовувати права та свободи в інформаційній сфері, зокрема право на інформацію – вільно збирати, зберігати, використовувати і поширювати інформацію [164,с.141].

Його ще називають технічним аспектом [165,с.130-131]. Технічний аспект інформаційної безпеки полягає у здатності і вмінні людини передбачати та попереджувати загрози інформації, яка циркулює в технічних системах, і загрози самим системам. Другий підхід наголошує на захищеності психіки та свідомості людини від небезпечних інформаційних впливів; маніпулювання, дезінформування, образ, спонукування до самогубства тощо [140]. Його також називають гуманітарним.

Неможливо також відкинути динамічної ознаки інформаційної безпеки. Вона водночас є процесом, який є невід'ємною частиною життя суспільства і держави, в якому здійснюються конкретні інформаційні впливи. Ця обставина передбачає наявність зв'язків між суб'єктами і об'єктами такої безпеки, їх інтереси, тенденції і закономірності розвитку, тобто визначає зміст інформаційної безпеки людини як системного явища. Саме комплексність поняття інформаційна безпека є однією з її базових ознак. Класик інформаційного права Бачило І.Л. говорить про комплексне завдання інформаційної безпеки, яке полягає в створенні балансу між потребою в інформації багатьох суб'єктів та необхідністю розумно використовувати

наявні інформаційні ресурси під девізом “не нашкодъ”. Такий девіз допомагає розкрити зміст “захищеності” – що або кого, від чого, в ім’я чого або кого, і нарешті, яким чином [27,с.253]. Основна частина розробок в галузі інформаційної безпеки донедавна здійснювалась виключно в інтересах держави. Її історичне коріння сягає 4 тисячоліття до н.е., саме так історики датують першу згадку про засоби шифрування [269,с.30]. Але 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 [167,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 [49,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 [311].

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, військовій сфері, внутрішньополітичній сфері, економічній сфері, соціальній та гуманітарній сферах, науково-технологічній сфері, в екологічній сфері. [100]

Нова редакція 2017 року 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, невідповідність стратегічного нарративу, недостатній рівень медіа-культури суспільства; поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [101].

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 [313,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;
- несанкційованим 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 [129].

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

Постанова Кабінету Міністрів України „Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” містить п. 16 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, який визначає, що для забезпечення захисту інформації в системі створюється комплексна система захисту інформації, яка призначається для захисту інформації від:

- витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші

канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

- несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;

- спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування [298].

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 [130].

Так, пункт 5 „Загроза для інформації” містить наступні визначення:

5.1. Витік інформації – неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання.

5.2 Порушення цілісності інформації – спотворення інформації, її руйнування або знищення.

5.3 Блокування інформації – унеможливлення санкціонованого доступу до інформації.

Класифікація загроз відповідно має наступний вигляд: загрози витоку інформації; загрози порушення цілісності інформації; загрози блокування інформації. Загальний критерій не визначено.

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 [138]. До 2016 року 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 однакості 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 ендегенні; 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 [194].

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 [141].

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 [196].

В свою чергу С. Гуцу [87] та О. Литвиненко [190], 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 формує 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) [114].

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.

Наприклад, М. Макарова виділяє такі ймовірні загрози в мережі:

- дані навмисно перехоплюються, читаються або змінюються;
- користувачі ідентифікують себе неправильно (з шахрайською метою);
- користувач отримує несанкціонований доступ з однієї мережі до іншої [204].

У цьому ж контексті більш ширшу класифікацію пропонує А. Погребняк. Який відмічає, що 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 [261,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; е) фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому; ж) перехоплення та ознайомлення з інформацією, яка передана по каналах зв'язку [261,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 розрізнити ознаки об'єкта класифікації [138].

Перш ніж досліджувати загрози інформаційній безпеці людини, як сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам людини, звернемо увагу на те, що саме визнано на нормативному рівні як життєво важливі інтереси людини. 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». Хто ця особа, за якими чинниками має визначатись? Про це згадувалось в попередньому розділі.

Водночас, слід звернути увагу, 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 [100].

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. Хто саме визначав досі що є негативним інформаційно-психологічним впливом? Єдина відповідь, що спадає на думку – Національна експертна комісія України з питань захисту суспільної моралі, яка в різних статусах існувала 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.

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 [366].

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" [49]. 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 [60].

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 [152,с.16.]

Г. Ситником пропонується класифікація видів небезпек, що розкриває взаємозв'язок між цими поняттями. Г. Ситник 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) [345,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 [394,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” [155,с.4-5].

В. О. Татенко прийшов до висновку, що: «...у широкому розумінні вплив – це будь-які рухи, дії чи прояви бездіяльності одних сутнісних субстанцій, що викликають зміни в інших сутнісних субстанціях або ж само зміни» [372].

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 [426]. 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» [367]. 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. Такий вплив становить загрозу безпеці інформаційно-технічної інфраструктури та фізичному стану 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 [36, 367].

Одна з найбільш розроблених класифікацій видів психологічного впливу в спілкуванні запропонована О. В. Сидоренко, що виділяє наступне: 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 іншої 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 [341, с.123-142].

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 конкретні поведінкові

акти (дії) “тут і тепер” 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, самоставлення, системи цінностей, із чим має справу практика виховання і психотерапії, а також про ідейну індоктринацію (“промивання свідомості”) [142,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, появи одних та зникненні інших почуттів, у зміні загального емоційно-психологічного фону людського буття, появи 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 реципієнта (зміна пульсу, тиску, частоти дихання, гормонального складу крові, кольору шкіри тощо).

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 [142,с.47].

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 відстрочений 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 самостійно, відокремлено від об'єкта відображення, стає вмістом пам'яті, тобто самостійно бере участь в психічних процесах, трансформується в уявлення, знання, вміння, навички [201].

Кожна людина, вступаючи в суспільні відносини, одержуючи і передаючи певну інформацію, вливається 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 року 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 року [242, с.51-56].

Як відомо, головною метою ООН, сформульованою в Декларації Тисячоліття, є зменшення бідності на планеті. ООН висунула завдання до

2015 року скоротити вдвічі частку людей, чий дохід у день є меншим за один долар США (сьогодні частка таких жителів планети становить 22 %). 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 найбільочіших проявів цих базових нерівностей. Без подолання інформаційної нерівності неможливий ні процес глобалізації, ні ефективний розвиток інформаційного суспільства, ні запровадження електронних урядів [347,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 [45]. Це не означає, що не потрібно впроваджувати електронну демократію, а свідчить про необхідність гарантування рівних можливостей доступу до інформаційних технологій.



Динамика проникновения Интернета: ежегодное измерение

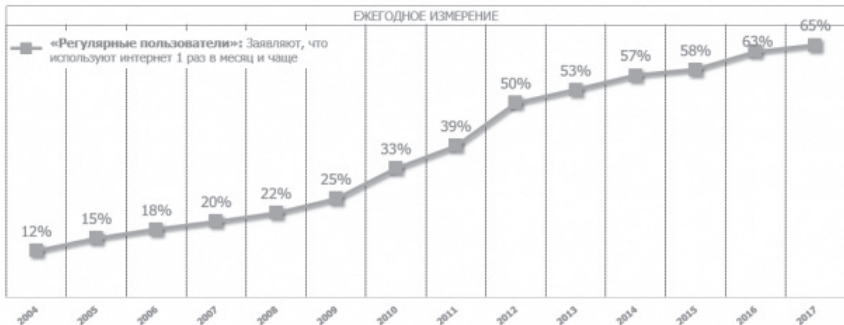


Рис. Динаміка проникнення Інтернету: щорічний вимір (за даними дослідження здійсненого Factum Group Ukraine на замовлення Інтернет Асоціації України)²¹

²¹ <http://watcher.com.ua/wp-content/uploads/pryknennya-internet.png?eac506>

Міжнародне співтовариство вже з 2000 року 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” [242, 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 [579].

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 [591], причому лівова частка з них – це мешканці великих міст. Згідно з даними Інтернет Асоціація України (опубліковано на їхньому офіційному сайті у квітні 2017 року), які представляють результати опитування, проведеного протягом лютого 2017 року, на початку року 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 [45].

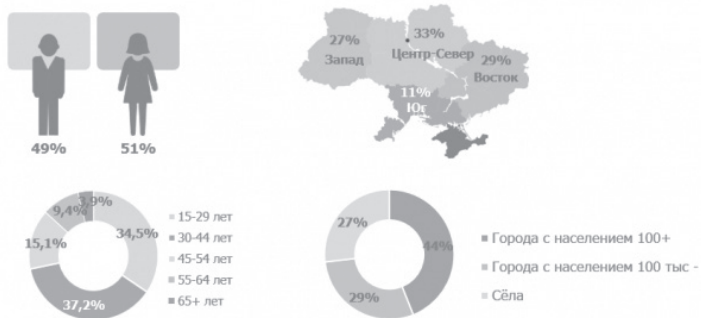


Рис. Гендерний, віковий і географічний чинники користування інтернетом в Україні станом на 2017 рік (за даними дослідження здійсненого Factum Group Ukraine на замовлення Інтернет Асоціації України)²²

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” [205]. 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

²² <http://watcher.com.ua/wp-content/uploads/prynyknennya-internet.png?eac506>

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 (hatespeech) 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 [440].

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 «Дискримінаатор року»²³.

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 [441].

Для прикладу, німецький парламент нещодавно обговорював закон проти ненависті та цькування в соцмережах. Цей закон було подано на розгляд міністром юстиції Німеччини, який ось уже два роки намагається якимось чином дати відповіді на ці питання. 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

²³ Щорічна антипремія «Дискримінаатор року» вручається у трьох номінаціях: «Дискримінація «у законі», «Реально Г (ганебний вчинок)» та «Язык 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.

порушення одразу, пропонується сім днів на ухвалення відповідного рішення. Якщо ж адміністрація «Фейсбуку» чи інших соцмереж цього не зробить – пропонуються штрафи [340]. Особливого значення набуває питання мови ворожнечі в умовах інформаційної війни.

Існує водночасі критика концепції узаконення відповідальності за мову ненависті. Мова ненависті як категорія є щільно 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 [442].

Прихильники цієї концепції, вважають «Hate speech» універсальним ярликом, за допомогою якого можна затаврувати думки, що суперечать догмам лібералізму. Руйнівне значення концепції “мови ненависті” не можна зводити виключно до того, що ця концепція має на меті заборонити називати речі своїми іменами. Засудження “мови ненависті” має сугестивну дію. Воно покликане паралізувати нашу здатність до адекватного етичного мислення.

Ірина Виртосу, головна редакторка сайту Центру інформації про права людини, журналістка, координаторка Журналістської мережі з прав людини, 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». А потім – безвідповідальність і дуже серйозні наслідки. 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...» [440].

Запровадження «гендерної рівності» в Україні в багатьох колах небезпідставно сприймається як накидання нової ідеології і культурного перепрограмування. Система освіти – це тільки одна частина цієї загальної атаки. Друга частина цього агресивного плану – дерегуляція сексуальних норм людства. Так, наприклад, гомосексуальні відносини ще донедавна були заборонені на законодавчому рівні у більшості країн. Причиною такої заборони було те, що суспільство вважало такі відносини поганими та недопустимими і тому не дозволяло їх. А всього 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 маргіальною опозицією, сьогодні є головною політичною силою на глобальному рівні [181].

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 Ніккі Катсурас [495], дівчини, що в 2006 році загинула у автокатастрофі у штаті Каліфорнія, США. Її тіло було жакхливим чином скалічене. В інтересах слідства поліція зробила декілька фотографій місця аварії. Декілька співробітників вирішили налякати своїх друзів на Хелуоін 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 Catsouras не мала ніяких підстав для позову. Справа була передана до вищої інстанції, і розгляд запланований у Верховному Суді в березні 2012 року. Проте, відповідач (СНР) погодилися виплатити родині Ніколь «Ніккі» Catsouras \$ 2375000 на етапі досудового врегулювання.

Родина Catsouras найняли Reputation Defender, щоб видалити фотографії, але вони продовжували поширюватися. За оцінками Reputation Defender, вони переконали сайти, щоб видалити 2500 з фотографій, але визнає, що видалення їх з Інтернету абсолютно неможливе. Адвокат і блогер Тед Франк писав, що хоча засоби масової інформації з розумінням

відноситься до важкого становища батьків, але так званий «ефект Стрейзанд»²⁴ призвів до неконтрольованого поширення фотографій».

Величезним питанням є так званий етикет смерті в онлайн-світі. Крім 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 році мережа магазинів роздрібної торгівлі Target мала прецедент з використанням великих даних в маркетингових цілях [513]. Одного дня в офіс компанії увірвався розлючений чоловік. Він 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?

За таких умов, значна увага має приділятися інформаційним впливам, що становлять загрозу морально-психічному здоров'ю дітей та підлітків. На території СНД, за даними деяких провайдерів, еротика і порнографія складає не менше третини всього ринку мобільних зображень. Еротика користується великою популярністю у всіх сферах індустрії розваг, в т.ч. в Інтернеті і в мобільному контенті. Найбільш популярними залишаються WAP-сайти порнографічного змісту. Аналітики відзначають, що типовим споживачем мобільного 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

²⁴ 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.

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 [132,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. За статистикою, 10-14 % підлітків в Україні страждають від комп'ютерної залежності або ігроманії [66].

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” [106].

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. В наш час дитина майже з народження потрапляє до інформаційного середовища, сформованого таким чином, щоб навчити її не мислити, а навпаки, позбавити задатків цього процесу, замінивши його на перегляд телевізора, грою у різноманітні ігри, що лише “забруднює” її свідомість, не залишаючи місця для важливих знань. Провідні світові компанії більшу частину реклами спрямовують саме на дітей. На дитячий мозок легше всього

впливати, бо він розвивається стрімкими темпами і відкритий для нових знань. Як свідчить опитування, проведене в 2003 році компанією “КОМКОН-медіа”, саме малюки складають більше половини (52,4 %) глядацької аудиторії, на яку так розраховують рекламодавці. Причому, що старшою стає дитина, то менше вона дивиться рекламу. Згідно з отриманими даними, якщо в 9-річному віці телеролик до кінця додивляється 44,8 % дітей, то до 19 років – тільки 15,9 %. Також встановлено, що діти до 12 років бачать в середньому до 25 000 телереклам в рік [322]. Реклама створює фоні життя людини. Не звертати уваги на рекламу здатна доросла мисляча людина. Коли мозок свідомо опрацьовує інформацію, він може, зробивши висновки, відкинути зайве. Коли інформація сприймається підсвідомістю, вони не обробляється, а відкладається у мозку в тому вигляді, в якому була отримана. Підсвідомість не аналізує дані, але в певних ситуаціях скеровує нашу поведінку відповідно до тої інформації, яка в ній зберігається. Тобто, для успіху реклами вона й повинна сприйматися так би мовити “на фоні” життя.

Але й без реклами інформаційний простір забруднений шкідливою для психіки інформацією. Фільми й передачі, на яких дитина зростає, також формують її подальшу поведінку. Транслявання по телебаченню сцен насильства викликає невелике, але статистично значуще збільшення агресивності глядачів. Це спричиняє 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 [351]. Образи насильства, жорстокості, ненависті пронизують всю масову, орієнтовану на молодь культуру.

З усього вищенаведеного можна побачити невтішну тенденцію того, що інформаційне середовище особистості цілеспрямовано забруднюється, щоб ця особистість не бачила інших способів поведінки й розвитку, крім тих, що їй пропонуються. Подібний процес починається з самого народження дитини, викорінюючи в ній навіть її природні здібності та схильності, замінюючи їх шаблоном поведінки, направленої лише на споживання товару, який їй пропонується. Процес комп’ютеризації шкіл, що відбувається сьогодні, безперечно, прогресивне явище. Але захоплення

оснащенням шкіл комп'ютерами, без відповідної методичної підтримки, без перепідготовки учителів-предметників – математиків, географів, хіміків, літераторів, без інтеграції комп'ютерних технологій у живу тканину діалогу з учнем зведе нанівець велику ідею. Викладання всіх шкільних дисциплін має базуватися на максимальному використанні технологій мультимедіа й Інтернету. За цієї умови якість засвоєння знань, рівень індивідуалізації навчання зростає багаторазово.

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 сама 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, знаково-символьна архітектура буття сучасної людини (жителя мегаполісу, в першу чергу) неминуче призводить до “дубляжу” або, навпаки, розрізненості відомостей; перенасичення каналів сприйняття диктує нездатність 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 року склала 63,5 %, але й ці цифри дозволяють зробити висновок про розмір загрози [358].

Дане 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 місяця для роздумів про життя. Як зазначає Томас Еріксен, “найнеобхідніше вміння в інформаційному суспільстві полягає в захисті себе від 99,99 % пропонованої інформації, якої людина не хоче” [112,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 як таке – збільшення навантаження на хребет – часто 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 [401,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 року 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 року на конференції Supernova 2005 співробітниця Microsoft Research Лінда Стоун зазначила, що в 1997 році народилося поняття “перманентна часткова увага”. Під цим мається на увазі режим існування, в якому людина зникає ні на чому довго не зосереджується, 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. Наш канал уваги розширився до крайніх меж...”. 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 [565].

Першим в світі центром підтримки інтернет-залежних став центр, створений найвідомішим і авторитетним дослідником в даній області –

Кімберлі Янг, професором психології Пітсбурзького університету (Бретфорд), автором перекладеної на багато мов книги – «Спіймани в Мережу». Створений нею в 1995 році 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 (он-лайн), азартні ігри онлайн, покупки тощо.

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.

В розвинених країнах інтрнет-залежність намагаються лікувати. Для прикладу, в США більшість філій «Товариства Анонімних Алкоголіків» відкрили групи підтримки інтернет-залежних, причому існують групи для родичів, які бажають повернути члена сім'ї в нормальне життя. Розроблено програму 12 кроків, суть якої полягає в наповненні реального життя новим змістом паралельно зі зменшенням часу, проведеного в Мережі. Ознакою одужання вважається, коли людина повністю контролює час, проведений в Мережі.

Також з 2009 року існує програма Restart, де за 45 днів і близько 15 тисяч доларів вас за допомогою занять в команді, походів в гори, роботи з психологом і відпочинком на природі вилікують від звички строчити в твіттер і фотографувати їжу для інстаграма.

У 2008 році уряд Китаю першим в світі вирішив підійти до цієї проблеми серйозно і проголосив інтернет-залежність загрозою здоров'ю населення номер один і назвали «Третьою опіумної війною». 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 ввійти до мережі, розумове або фізичне виснаження, дратівливість, порушень сну або концентрації уваги.

В Китаї 350 мільйонів геймерів, це більше, ніж населення США. Серед них чимало людей, які страждають залежністю від комп'ютерних ігор. За останні десятиріччя відкрилося величезна кількість реабілітаційних центрів, більшість з яких очолюють військові у відставці. Центри, як правило, не державні, представляють собою синтез армії, в'язниці

і психлікарні з армійської дисципліною, дідівщиною з боку лікарів, гратами на вікнах, примусовим прийомом антидепресантів, заборонаю на листи родичам і іншими радощами мимовільною життя.

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 Жаня, 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. За оцінками Китайського інформаційного центру мережі інтернет, в 2007 році налічувалося 210 мільйонів китайських користувачів світової мережі, приблизно половину цього числа складають люди у віці від 18 до 30 років [139].

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 (відповідність кодів повідомлень паттернам сприйняття, наявність або відсутність дефіциту часу і перевантаження оперативної пам'яті людини, організація інформаційних потоків відповідно до алгоритмів діяльності і т. д.);

3) наявність в інформаційних потоках специфічних елементів, цілеспрямовано змінюють психофізіологічних 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 фізіологічні носії (світлові, звукові, електромагнітні впливи) [63].

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 [109].

Таким чином, не можна залишити поза увагою ще одну загрозу – низький рівень інформаційної і правової культури, який породжує еkleктизм як панівну ознаку інформаційної “культури мас”. В найширшому значенні еkleктизм 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” [13,с.3-13].

Загрози інформаційній безпеці нерозривно пов’язані зі станом нормативно-правового регулювання інформаційних суспільних відносин. 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» [292]. 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 заборонаю об’єднувати інформацію з різних реєстрів без згоди особи» [360]. Окрім того, Закон не розрізняє загальні і вразливі дані.

Критиці з боку правозахисників Закон піддавався і після прийняття [115]. За 4-річну історію функціонування цього закону (на момент проведення дослідження) в його зміст вносились зміни і доповнення понад 15 разів. 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 звузити кількість документів реєстру власне до ідентифікаційних документів. [360]

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 поводяться 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 [55].

Величезну загрозу для безпеки фізичних осіб може бути створено у звязку з внесенням змін до законодавства щодо трансплантації органів та інших анатомічних матеріалів людини. В законопроекті 2386а-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.

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 [180].

Для зловмисників «золотою жилою» щодо персональних даних є різноманітні квести («Перевір своє знання географії», «Який у тебе словниковий запас», «Визнач свій психотип» тощо) і конкурси («Як ти будеш виглядати через 50 років», «На якого звіра ти подібний», «Яка машина тобі личить» тощо). Для користування подібними ресурсами людина «логіниться»²⁵ за допомогою власного аккаунта в соцмережі і надає

²⁵ 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 комп'ютерною системою та визначення його прав доступу до ресурсів мережі. Логін має бути унікальним в межах даної системи. (за даними Вікіпедії)

зголи 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.

Facebook, яка дозволяє користувачам оцінювати інформацію на сайті в режимі онлайн. Німецькі правозахисники у галузі захисту приватності інформації вимагали видалити цю кнопку. Вони заявили, що використання кнопки «Like» суперечить німецькому та європейському законодавству, оскільки як наслідок 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 [233].

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 [321]. Поліція англійського графства Лестершир в 2014 також вперше в Британії стала використовувати систему NeoFace, яка дозволила порівнювати особу підозрюваного з наявною у поліції картотекою в 92 тисячі осіб [329]. 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, Йоганнес Каспар зазначає: «Збирання даних – це також засіб соціальної дискримінації. Це у багатьох випадках може призводити до значних зловживань цим інструментарієм» [329]. 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 використана злочинцями. Так, за інформацією А. Аквісті, спеціаліста з інформаційних технологій, зловмисники, використовуючи цю функцію, зможуть досить швидко з'ясувати п'ять цифр полісу соціального страхування – одного з основних документів США [192].

З 2015 року з'явилась інформація про те, що Фейсбук почав збирати інформацію про всіх тих, хто будь-яким чином скористався зі служби Facebook, навіть якщо вони не знали про це. Це означає, що навіть якщо людина не має облікового запису, і читає блог, де ви можете коментувати записи через Facebook, Blogger або «лайкаєте» щось з допомогою вбудованих ресурсів – дані будуть йти до американського магната [491]. 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. Простіше кажучи, шляхом збору даних портали здатні допомогти правоохоронним органам отримати доступ до осіб або доказів.

Володіючи метаданими користувачів та мільйонів інших людей, які можуть бути об'єднані і проаналізовані за допомогою технологій Big Data, Фейсбук має 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), і так далі.

Кібер-буллінг (cyber-bullying), віртуальний терор, (від англійського слова bull – бик) із спорідненими значеннями: агресивно нападати, роз'ятрувати, 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 [153].

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 Робін Ковальські, С'юзан Лімбер і Патріція Агатстон виокремлюють такі основні типи поведінки властиві для кібербуллінгу [524]:

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 (holylwar – 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 [524].

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 [223].

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

Хоча основною категорією ризику кібербулінгу є підлітки і молодь, проте трапляються і подібні випадки серед дорослих. Так, 31-річну жительку Сочі 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 вирішив покінчити життя самогубством. Свої наміри він виконав в березні 2010-го: молодий чоловік був знайдений повішеним [248].

Кібермобінг, на думку деяких дослідників, має «ширшу аудиторію» як серед жертв, так і серед переслідувачів. Хоча його види, які виділила Nancy E. Willard у праці «Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress» є майже повністю подібні [589]:

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 (селебріти), де знаменитістю вважається людина, що часто згадується в медіа і викликає громадської 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» потрапити на око;

5) Електронне хуліганство, коли правопорушник і жертва, як правило, є членами однієї і тієї ж групи, як онлайн і в реальному житті [554].

Варто нагадати справу Меган Майєр [582]. У 2006 році 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 втрих з 13-річною Сарою і зі своєю молодією підпорядкованою 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.

Судова епопея 49-річної американської продавчині Лорі Дрю, яка на смерть зацькувала однокласницю дочки за допомогою соціальної мережі MySpace, завершилась передбачувано. Присяжні, під впливом природних людських почуттів, визнали її винною за трьома пунктами пред'явленого їй звинувачення. А федеральний суддя Джордж Ву, який головував на процесі,

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. Широкій публіці, волю якої в даному випадку виконували і обвинувачі, і присяжні, такий результат здався справедливим. 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) [467]. 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, пропорційно поширенню інформаційних технологій на все нові сфери 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-го серпня 2017 року 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 [588].

«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 Алессандро 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. Мікročіп, 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 [8].

Ще одним суперчливим 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, ресторанный 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 (PopUp-вікна) на сайтах, прямо або побічно пов'язаних з юридичною практикою, і у вигляді спеціальних сервісів або розділів сервісів (наприклад, юрист-бот в сервісі Telegram). І те й інше є реалізацією однієї програми. 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 [52].

Боти постійно вдосконалюються. В 2015 році 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 році вчені з Массачусетського технологічного інституту розробили алгоритм для аналізу твітів, який може визначати сарказм і емоційний підтекст [445]. 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. Конрад Лоренц писав, що «Є вагомими підстави вважати внутрішньовидову агресію найбільш серйозною небезпекою, яка загрожує людству в сучасних умовах культурноісторичного і технічного розвитку. [199]»

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.

3.2. Особливості правового забезпечення прав і безпеки окремих категорій осіб у інформаційній сфері

Підсумовуючи попередні підрозділи, вважаємо, що 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 («Посібник з прав людини для Інтернет-користувачів») 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 [325].

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 АТО – військовослужбовці, які беруть чи брали участь в АТО, їх сім'ї, а також сім'ї загиблих, населення окупованих територій, «сірої» зони, внутрішньо переміщені особи тощо;

6) український народ – не лише як населення країни, що проживає на її території, але скоріш як громадяни України, що творять єдину соціально-історичну спільність та/або ідентифікують себе такими у процесі здійснення своїх прав і обов'язків.

Цей перелік не є вичерпним, його метою є окреслення межі предмету дослідження цієї частини монографії.

Діти, підлітки і молодь. За даними досліджень 2011 року в США близько 80% дітей у віці до 5 років користувались інтернетом щотижня, більшість дітей проводило принаймні три години на день, дивлячись телевизор, 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 [566].

Використання домашнього інтернету зростає з віком. Кожен з трьох дітей віком від трьох до п'яти років використовує Інтернет вдома, у порівнянні з 54 відсотками шести-одинадцятирічних та 72 відсотків з 12 до 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 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 кібербулінг²⁶, 69% підлітків регулярно отримуючи повідомлення від незнайомих людей не повідомляють про це батькам чи опікунам [505].

Відповідні актуальні статистичні дані щодо України виявилось знайти досить складно. Всеукраїнське соціологічне дослідження, проведене Інститутом соціології НАН України в 2009 році, 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 [29].

Комітет ООН з прав дитини у 2011 році 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 році провів онлайн-опитування щодо досвіду молоді, пов'язаного з мовою ворожнечі в Інтернеті. За його результатами 69% не знають, де можна отримати допомогу жертві мови ворожнечі онлайн, 78% респондентів не отримували освіти щодо безпечної поведінки в Інтернеті [221].

²⁶ Умисні образи, погрози, дифамації і повідомлення іншим даних, що компрометують за допомогою сучасних засобів комунікації, як правило, протягом тривалого періоду часу.

За даними міжнародної асоціації «ІННОРЕ», 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 році 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) [516].

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). Нещодавнє всесвітнє опитування показує, що діти вважають його правом людини, необхідністю [512]. Для прикладу, 15 річний хлопчин з Сербії коментує це наступним чином: «Ми виростили з Інтернетом. Я маю на увазі, що Інтернет завжди був частиною нашого життя. У дорослих якось так: «Вау! Винайшли інтернет!», хоча це абсолютно нормально для нас.»

Вже згаданий Посібник з прав людини для Інтернет-користувачів містить підрозділ, адресований дітям і молоді. В ньому, зокрема, передбачено, що з урахуванням віку діти та молодь мають право на особливий захист і консультування при користуванні Інтернетом. «Це означає, що: 1. ви маєте право на вільне вираження своїх поглядів та участь у житті суспільства, на те, щоб бути почутими та вносити свій вклад у вирішення питань, які торкаються ваших інтересів. Вашим поглядам повинна приділятися належна увага з урахуванням вашого віку, ступеня зрілості та без дискримінації; 2. ви можете очікувати на отримання інформації мовою, що відповідає вашому віку, а також на навчання безпечному користуванню Інтернетом, в тому числі щодо захисту вашого приватного життя, з боку ваших вчителів, вихователів, батьків чи опікунів; 3. ви повинні знати, що контент, який ви створюєте в Інтернеті, або контент про вас, що створюється іншими Інтернет-користувачами, може ставати доступним у будь-якому куточку світу і завдавати шкоду вашій гідності, безпеці, приватному життю або іншим чином шкодити вам та вашим правам у цей час або на наступних

етапах вашого життя. На ваш запит такий контент повинен бути вилучений або видалений протягом розумно короткого періоду часу; 4. ви можете 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 вашого віку та обставин, а також вам повинні надати поради та підтримку з належною повагою до вашої конфіденційності та анонімності; 5. вам повинен надаватися спеціальний захист від втручання у ваше фізичне, психічне та моральне благополуччя, зокрема, захист від сексуальної експлуатації та насильства в Інтернеті та від інших форм кіберзлочинності. Крім того, ви маєте право на освіту, яке покликане захистити вас від подібних загроз. [325]»

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, 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 офлайн. Права дитини, викладені в Конвенції ООН прав дитини, дослідниця застосовує до онлайн середовища.

Серед загроз з якими дитина зіткнулась при використанні комунікаційних технологій можна виокремити такі:

технологічні: загроза як для дітей, так і для доослих 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 [191],

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 (кібурбулінг, 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 медіа²⁷, 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 [62, с.69].

²⁷ Інтерактивні електронні засоби масової комунікації, засновані, переважно, на технологіях Web 2.0.

Дослідження свідчать, що з точки зору батьків, ті фактори, які ускладнюють державне регулювання нового медіа-оточення, тягнуть за собою аналогічні складності і для батьків [535]. 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.

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» [30].

Існує думка, що 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)-державна» [415]. 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: Лист МОН України № 1/9–768 від 06.11.09 «Про захист дітей та молоді від негативних інформаційних впливів», Лист МОН України № 1/9-916. від 28.12.09 «Про проведення дня безпечного Інтернету», Лист МОН України № 1/9-815. від 11.11.10 «Про проведення конкурсу «Онляндія в моїй школі» свідчить про їх популярський 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: розпізнання елементів Інтернет-культури; активна участь у мережних соціальних спільнотах; ініціативність в розвитку мережних соціальних спільнот, створених для спільних дій [185].

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.

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 відсотків 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 [120,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 ейблізм²⁸[534], 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, аутистичну гомогенність [499]²⁹.

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 обмежень, проте якщо їх більш ніж один, наприклад близнюки, яким по одному році, 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» [499].

²⁸ 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.

²⁹ Ефект аутистичної 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.

У 1999 році Консорціум Всесвітньої павутини (англ. World Wide Web Consortium, W3C), 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 році вийшла його друга версія рекомендацій WCAG 2.0. У жовтні 2012 року WCAG 2.0 була прийнята Міжнародною організацією стандартизації як Міжнародним стандартом ISO, ISO / IEC 40500: 2012. [561]

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 [106].

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 року. 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 [105].

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.³⁰

³⁰ Більше в розділі «Міжнародний досвід правового регулювання відносин у сфері інформаційної безпеки людини»

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 свою 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, адже судам доводиться шукати його між конституційними гарантіями свободи вираження та приватними інтересами осіб. Суд при вирішенні питання стосовно конфлікту цих двох прав зазвичай обмежується аргументацією тієї чи іншої статті, аналізуючи певні випадки відповідно до статті 10 і з посиланням на частину 2 статті 10 з обґрунтуванням «захисту репутації або прав інших осіб» [457].

Нагнічук О. І. на підставі аналізу практики Європейському Суді з прав людини³¹ формулює такі 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.

³¹ 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 Italentti 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.

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, якщо мова йде про публічну особу, не є сферою приватного життя особи [222].

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 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 органах 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» «1. Охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантуються Конституцією та законами України. 2. Зняття інформації з телекомунікаційних мереж заборонене, крім випадків, передбачених законом» [319,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). Фактично, це означає, що оператори зв'язку зобов'язані за свій кошт закуповувати обладнання для підключення спецслужб до лінії зв'язку.

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 [178].

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.

Проте на сьогодні 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. Очевидно, що журналісти не мають права як читати, так і поширювати таку інформацію, оскільки 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, політологам, а також просто знайомим чи близьким публічної особи) [265].

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 [90].

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. Закон визначає, що членом сім'ї суб'єкта декларування є дружина або чоловік, навіть за умови їхнього фактичного окремого проживання [293]. Членом сім'ї також є будь-яка інша особа, якщо одночасно наявні такі три ознаки: спільне проживання з декларантом, ведення спільного господарства, а також взаємні права та обов'язки, які мають характер сімейних. Це визначення виключає, наприклад, спільну оренду нерухомості за відсутності сімейних відносин. Членом сім'ї може бути як родич декларанта – наприклад, дитина чи батьки – так і співмешканець.

Закон дозволяє членам сім'ї відмовляти в наданні інформації. Адже подання декларації – це обов'язок декларанта, і лише він несе відповідальність за неподання даних чи подання недостовірних даних.

Суб'єкт декларування може знати про наявність певного об'єкта декларування, наприклад, нерухомості у члена сім'ї, але не знати деталей і запитати про них у члена сім'ї. Останній може відмовитися надавати таку інформацію.

Тоді декларант повинен зазначити в декларації всю відому йому інформацію про такий об'єкт, а щодо решти зробити помітку «Член сім'ї відмовився надати інформацію».

При цьому якщо декларант знав ці дані, але не зазначив в декларації, і це буде встановлено, то можливе притягнення декларанта до відповідальності за подання завідомо недостовірних відомостей.

Слід також пам'ятати, що за законом, якщо хоча б одне поле в декларації позначено як «член сім'ї відмовився надавати інформацію», така декларація повинна пройти повну перевірку, під час якої НАЗК³² перевірить усі дані – як про суб'єкта декларування, так і про члена сім'ї.

³² Національне агентство з питань запобігання корупції - центральний орган виконавчої влади зі спеціальним статусом, який забезпечує формування та реалізує державну антикорупційну політику

Водночас, самі декларанти висловлювали побоювання, що «відкрите електронне декларування майна чиновників «дає пряму наводку для злочинців» та є питанням безпеки сотень тисяч людей» [438], а також що воно стало «інструментом тиску на суддів для того, аби схилити їх до прийняття тих чи інших рішень» [91].

Ще одна загроза що пов'язана з функціонуванням численних електронних реєстрів. Ганна 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. Ось і результат, коли біля під'їздів та навіть 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 у 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 Інтернет 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 Інтернет 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 [274].

Така суворя 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 [273]. 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. Сьогодні будь-яка особа може створити ФБ-акаунт під вигаданим ім'ям. Це може прослідковуватися й у разі реєстрації фейкового

профілю із застосуванням іменні реального адвоката чи адвокатської спільноти. У результаті – утрата довіри до правдивості акаунта в онлайн-комунікаціях, а як наслідок – пониження статусу не лише окремого адвоката, але й адвокатури загалом [273].

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 Інтернет є допустимими, проте суддя може розміщувати, коментувати лише ту інформацію, використання якої не завдає шкоди авторитету судді та судової влади” [158].

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.

Прийнято кодекс етичної поведінки держслужбовця було 11 лютого 2016 року. Серед іншого, документ 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» [348].

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 [348].

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.

Будь-який журналіст в Україні на сьогодні не захищений, він не може сказати гарантовано, що його права не будуть порушені при звичайному виконанні професійних обов'язків. «Тема номер один для журналістської спільноти – фізична безпека журналістів», – відзначає С. Томіленко, голова Національної спілки журналістів [373]. В той же час журналіст чи особа,

що здійснює медійну діяльність³³, 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 трьох категорій, вважаємо необхідним зупинитись на соціокультурних особливостях комунікативного процесу. У статті «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» [339,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.

³³ 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.

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 [246].

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» [268, с.229]. Переконання в тім, що люди бачать світ по-різному – крізь призму своєї рідної мови – лежить в основі теорії «лінгвістичної відносності» Е. Сепіра і Б. Ворфа³⁴. 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 [339].

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 [246].

Система національно-психологічних особливостей індивіда базується на кількох сферах: мотиваційній (своєрідність мотивів, спонукальних сил діяльності представників тієї чи іншої національної спільноти); інтелектуально-пізнавальній (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) [246].

³⁴ 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.

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 власне 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 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 [332].

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. [246].

Не менш важливою є духовна сфера суспільства, складовими якої є не лише релігійність, а, насамперед, суспільна свідомість, громадська думка і соціально-психологічний клімат (у тому числі системи освіти і виховання, системи масової інформації, що впливають на соціальну поведінку та організацію життєдіяльності людей).

Яким чином ці 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.

Більш детально особливості інформаційних загроз, виникнення яких пов'язано з проведенням антитерористичної операції, а так насправді – гібридної війни, розглянуті наступному розділі.

3.3. Проблеми забезпечення інформаційної безпеки людини в умовах гібридної війни проти України

До 2014 року категорія «гібридна війна» була мало зноюю в українському медіа середовищі, серед політиків і пересічних громадян. Поодинокі науковці, що займались вивченням політичних наук та стратегічних комунікацій, та ще військові, розуміли, що мається на увазі під цим терміном. Більш поширеними були категорії «інформаційна війна», «Інформаційне протиборство», «інформаційна зброя», хоча й вони використовувались часто з дещо футуристичним і публіцистичним забарвленням. Протягом останніх років ситуація докорінно змінилась. І від розуміння сутності і небезпек стану гібридної війни, в якій опинилась не лише окупована частина України, а вся держава, значною мірою залежить державна політика гарантування безпеки людини, її прав та свобод в кожній сфері, в т.ч. інформаційній.

Однозначного визначення гібридної війни не існує. Так, у західній науковій думці орієнтовно вже з середини 2000-х років 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 [80].

В 2010 році, 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» [514].

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 елітою “країни-жертви” 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 [403].

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 [202].

На думку Ф.Хофмана, гібридна війна включає такі сфери:

- географічну – визначення контролю над частиною чи навіть цілою територією країни суперника за допомогою інформаційних і розвідувальних систем, захоплення та підтримка сепаратистських, залучення супротивника у військові та політичні конфлікти;

- економічну – нав'язування кредитів на не вигідних для держави умовах, введення різноманітних економічних санкцій, залучення до членства в малоефективних міжнародних економічних організаціях;
- ідеологічну – використання завідомо неправдивої інформації, спотворення інформації, підміни понять, внесення ментальних вірусів і міфологем у свідомість населення супротивника;
- інформаційну – організація атак на інформаційно-телекомунікаційні системи, внесення шкідливого програмного забезпечення різного роду в обчислювальні і телекомунікаційні системи та бази даних ворога [511].

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 [270].

Требін М.П. відзначає, що гібридна війна, «по-перше, поєднує конвенційні і неконвенційні бойові дії та відповідних учасників цієї війни (поряд зі збройними силами дійовими учасниками стають терористи, найманці, партизани, ополченці, бандформування, спецпідрозділи інших держав тощо); по-друге, початок «гібридної» війни пов'язаний з використанням неконвенційних методів ведення бойових дій незаконними збройними формуваннями; по-третє, протягом усієї «гібридної» війни дуже важливе значення надається боротьбі за розум і душі людей, тобто інформаційній боротьбі, де основними дійовими суб'єктами виступають також не військові, а цивільні: ЗМІ, телебачення, Інтернет, інші засоби масової комунікації» [386].

Таким чином, 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, найточніше 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 [80].

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 задовгодо 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, протиставлення 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 [80].

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. Різноманітні реальні й удавані «хактивісти», «кіберпартизани», «кіберополчення», а також спеціальні підрозділи різних безпекових відомств для ведення протистоянь у кіберпросторі – всі вони стають важливим елементом кібератак, а також ведення спеціальних психологічних операцій у соціальних мережах та в мережі Інтернет загалом.

За даними аналітиків на 2014 рік 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; засоби генерування акустичних і електромагнітних полів тощо [383,с.23-28].

На думку психологів, негативні інформаційно-психологічні впливиможуть призвести до таких негативних взаємозалежних змін:

1) зміни психіки, психічного здоров'я людини. У зв'язку зі складністю визначення меж норми й патології ці зміни важче простежити. Показниками таких змін може бути втрата адекватності щодо відображення світу у свідомості й індивідуальному ставленні до світу, інформації. На деградацію особистості вказує спрощення відображення форм дійсності, огрубіння реакцій та перехід від вищих потреб (у самоактуалізації, соціальному визнанні) до нижчих (фізіологічних, побутових).

2) 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 [195,с.104].

Враховуючи, що Російська Федерація як наступник «спадщини» школи безпеки СРСР, володіє значним досвідом використання науково розроблених і перевічених на практиці традиційних і нових методів впливу, то весь цей арсенал комплексно використовується в інформаційній війні проти України.

Серед таких різні автори називають:

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; засоби генерування акустичних і електромагнітних полів та ін. [7],с.77-86];

пропаганда, напівправа, фейк або симулякр [254,с.30-37];

дезінформування та маніпулювання; пропаганда; диверсифікація громадської думки; психологічний та психотропний тиск; поширення чуток [78,с.136-141];

ЗМІ; спеціальні засоби інформаційно-пропагандистської спрямованості; глобальні комп'ютерні мережі; програмні засоби швидкого поширення в мережах інформаційних і пропагандистських матеріалів; засоби та технології нелегальної модифікації інформаційного середовища, на основі чого опісля приймаються рішення особою; засоби створення віртуальної реальності; чутки, міфи, легенди; засоби підпорогового семантичного впливу; засоби генерування акустичних та електромагнітних полів [255];

поступове зниження міжнародного іміджу України з метою послаблення її геополітичного значення; відповідне дозування та спотворення інформації з метою дестабілізації ситуації в державі та впровадження власної політики «керованого хаосу»; формування стереотипу меншовартості та вторинності українців, а також відповідне руйнування почуття нації та народу; домінування російської мови, культури та традицій для утвердження самоідентифікації при одночасному витісненні української мови та культури [422];

формування іміджу РФ як могутньої держави, що обстоює принципи демократії та свободи, захищає своїх громадян та етнічних росіян; підрив морального здоров'я українців; формування уявлення про начебто широку підтримку жителями сходу України дій з боку РФ; деморалізування особового складу силових відомств України, зокрема Збройних сил і Національної гвардії; дезінформування власного населення та світового простору щодо перебігу подій, а також причин конфлікту; спростування інформації щодо присутності російських військових на території України; зомбування власного населення кремлівськими вигадками про американських військових, які ведуть бойові дії на сході України; підтримка проросійських громадян України [[182,с.124-133].

Таким чином, можемо помітити певне змішування категорій – форм, засобів, способів, а в деяких випадках – цілей інформаційно-психологічного впливу.

Науковці виокремлюють вербальний та невербальний механізми інформаційного впливу [15]. Так, в основі вербального лежать закономірності усвідомленого сприйняття змісту інформації. Він відбиває

загальні закономірності інформаційних процесів у соціальному середовищі. Спочатку у людини формуються певний спосіб мислення, світогляд, система цінностей та інтересів, тоді відбувається процес їхнього збагачення та розвиток у якийсь конкретний бік, у результаті утворюється певний морально-семантичний фільтр, і нарешті, після отримання уже нової інформації відбувається аналіз та абсорбація із допомогою вищезгаданого фільтру, і в результаті цього процесу формуються нові вчинки, поведінка індивіда відповідно до певної ситуації. Самі орієнтації та усталеність фільтру впливають на той чи інший кінцевий результат. Якісні та змістовні характеристики такого фільтру залежать від ідеологічної пропаганди, релігії, філософських учень, національно-етнічних показників, системи освіти, історичних факторів, а також засобів масової інформації [83]. Стійкий «фільтр», інформаційно-психологічна позиція, здатність до прийняття адекватного рішення особистістю, конкретні ситуація, час, обставини та типова поведінка людини, якість інформування, що залежить від своєчасності, повноти, всебічності та достовірності, є провідними факторами адекватної поведінки індивіда. Однак, слід зазначити, що існує ряд чинників власне вербального інформаційно-психологічного впливу, які можуть кардинально видозмінювати сформований у людини механізм прийняття адекватного рішення, а відтак поведінки з метою управління прийняттям рішень на користь зміни поведінки адресантом, корисної для адресата такого інформаційного управління. До них належить продумана цілеспрямована правдоподібна дезінформація, навмисно спотворена інформація, вибірково неповна інформація. Так, людина навіть за наявності стійкого та міцного фільтру може приймати рішення, отже і діяти відповідно до адекватного змісту інформації, при цьому її поведінка буде неадекватною реальній ситуації [406,с.184-191].

Експерти вважають, що інформаційний вплив з метою підготовки плацдарму для гібридної війни розпочався щонайменше «в 2004 році, 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 [182, с.124-133].

Пропаганда набувала різних форм в залежності від етапу інформаційної кампанії та цільової аудиторії, на яку була скерована. Прикладів є безліч.

Ще задовго до 2014 року на російському телебаченні, яке транслювалось також і на всій території України масово з'являлись передачі з «суперечливими історичними» фактами – як Крим раптом став частиною УРСР, чиею 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.

Викорстовувалось також поєднання фактів, наприклад, у програмі «Сегодня» 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 року) та Каталонії (9 листопада 2014 року) [336].

І великого поширення набули симулякри³⁵ (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

³⁵ Симулякр (фр. Simulacres, від лат. Simulo, «робити вигляд, прикидатися») - «копія», яка не має оригіналу, термін який ввів в обіг постмодерніст Жорж Бата

Фредріком 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 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 живлення; 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 маніпулювання громадською свідомістю [406,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» [430].

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 насторями масово трансливалися загальнонаціональними в українському теле і райдоефірі.

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 не складно упізнати президента України, Прем'єр-міністра та Секретаря РНБО. Таке перекручування фактів, паплюження та зневага до перших осіб держави формує у дитячій свідомості викривлену картину сприйняття сьогодення, змінює їх цінності та життєві орієнтири і навряд чи зможе виховати з них гідну особистість з високим рівнем правосвідомості та громадянською позицією [58].

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-портал «Sputnik», що є інтерактивним майданчиком з можливістю підключення інтернет-радіостанції «Sputnik», а також інтернет-доступу до телеканалів RT, де мовлення здійснюється 45 мовами [330].

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») [254,с.30-37].

Поширеним явищем є приклади використання медіаресурсів, що знаходяться у приватній власності громадян РФ в цілях пропаганди. Наприклад, на початку 2016 року телеканал Life news повідомив, що ФСБ

РФ отримала інформацію про підготовку терористичних нападів з боку ІДІЛ в місцях масового скупчення людей в Києві. Більше того ФСБ встановило десять осіб потенційних терористів, дані про яких буцімто були передані до СБУ. Реакція СБУ була короткою і виваженою – суха констатація того, що не існує жодних контактів с ФСБ, а даний посил – чергова підробка. «Сенсація» навіть залишилася майже поза увагою українських ЗМІ. 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». За даними газети, Київ готується відправити військовий контингент до Сирії для підтримки Заходу в боротьбі з ІДІЛ. Плюс один із мотивів є можливість зіткнутися з російськими військами, тому що українці зараз найкращі у світі «у знанні тактики і мови росіян», – зазначали в The Independent. На відміну від попередньої новини, дана «сенсація» мала певний резонанс в Україні. МО України заперечило наведені «одкровення». Також було привернуто увагу, що The Independent належить російському олігархові Олександру Лебедєву, що має вагомі частки в таких гігантах російського бізнесу як РАО ЄЕС «Россия» і «Аерофлот» [272].

Слід звернути увагу, що ситуація щодо інформаційної безпеки прав громадян України умовно може бути класифікована на кілька категорій:

- 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 в АТО, членів їх сімей, а також мирного населення української території, де відбувається АТО;
- 3) інформаційна безпека населення України, що проживає на «мирних» територіях.

Моніторинговий Огляд підготовлений Кримською правозахисною групою на підставі матеріалу, зібраного у травні 2017 року, зазначає про порушення права на свободу зібрань, свободу слова і висловлювання думки [278]. 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 [272]. 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. Зокрема, інформаційне агентство «Крымские новости QHA» отримало відмову в реєстрації, припинило свою діяльність на території Криму і переїхало до Києва. ФСБ Росії неодноразово перевіряла кримськотатарську газету «Авдет». 1 квітня 2015 р. припинили своє мовлення телеканал АТР та інші ЗМІ однойменного медіа холдингу (телеканал Lale, радіостанції «Мейдан» і «Лідер»), які не пройшли перереєстрацію відповідно до російського законодавства через відмову в ліцензіях від Роскомнагляду. АТР розпочав свою роботу в Києві і транслює мовлення на Крим через супутник. У лютому 2016 р. канал ініціював кампанію «Врятуй АТР» щодо припинення роботи каналу вже в Україні через фінансові проблеми та відсутність належної підтримки з боку Кабінету міністрів України [389]. Постановою Кабінету Міністрів України №303 від 20 квітня 2016 р. про фінансову підтримку ТОВ «Телевізійна компанія «Атлант-СВ» (юридична особа телеканалу АТР), досягнуті домовленості про реструктуризацію боргу за супутникове мовлення та питання його погашення [125]. Реакцією на обшуки у незалежних журналістів, які почалися зранку 19 квітня 2016 р. стало відкрите звернення від представників експертного та правозахисного середовища до Президента України, ВРУ, МЗСУ, силових структур АР Крим на теренах України з вимогою озвучити офіційну позицію держави щодо кожного конкретного випадку порушення прав людини на тимчасово окупованій території АР Крим, фіксувати та розслідувати ці злочини.

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 року 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 широкій 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 [144].

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 [264].

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 [388]. 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 [144].

Стан масової свідомості в «ЛНР-ДНР», за оцінками спостерігачів, також є досить типовим для територій збройних конфліктів і визначається ними як «фрустраційний, травмований» [103]. 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 здійснюється АТО. 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) [7, 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. [7,с.77-86] Важливою складовою інформаційної безпеки цієї категорії осіб є якісне і своєчасне надання психологічної допомоги як під час перебування в АТО, так і після повернення додому. Значення має також інформаційна та правова підтримка учасників АТО 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 року, 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) [104].

При цьому, рівень довіри до ЗМІ є значно вищим. У лютому 2017 року найбільш високий рівень довіри українці відчували до такого постачальника політичної інформації, центральні ТБ канали країни (49%). Далі за рівнем довіри йдуть українські інтернет-ЗМІ – 19%, родичі і знайомі – 12%, соціальні мережі – 9%, місцеве ТБ – 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, літня частина значимо частіше довіряє

центральною ТБ каналах, 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 центральною ТБ каналам країни. А ось вітчизняним інтернет-ЗМІ міські жителі довіряють частіше, ніж жителі сіл [429].

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» [386, 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.

РОЗДІЛ IV. МІЖНАРОДНИЙ ТА ЗАРУБІЖНИЙ ДОСВІД ПРАВОВОГО РЕГУЛЮВАННЯ ВІДНОСИН У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ

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 міжнародної 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.

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» [107, 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 [107,с.12].

І. Г. Ханін вважає, що глобалізація підходів до досягнення і підтримки інформаційної безпеки зумовлена декількома причинами [404]. 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 інформаційно-комунікаційних технологій (далі – ІКТ), пов'язаних як з процесами природнього і антропогенного характеру, так і діяльністю людини;

4) неефективності традиційних стратегій (таких, як заходи, що аналогічно застосовуються в процесі контролю за озброєнням або їх стримування);

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 [121].

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 [217]. 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 [217].

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 геостационарній 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 [89]. 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 найбільш кваліфікованих 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 відносини 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 НМІП 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 НМІП 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 НМІП 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 НМІП 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 [89].

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 актів³⁶.

Необхідною умовою становлення глобального інформаційного суспільства є розвиток глобальної інформаційної інфраструктури (ГІІ, Global information infrastructure, GIІ). В середині 90-х років 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 (ГІІС) – 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.

ГІК відзначають також, що інформаційна революція відбувається хаотично і суперечливо. Тому ГІК зобов'язується забезпечити унікальну,

³⁶ Зокрема, в Україні було прийнято Закон «Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015», що залишається чинним досі.

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 застосунків або 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 [573].

Водночас, розбудова інфраструктури не є самоціллю, а лише засобом. Під побудовою інформаційного суспільства в Декларації принципів вбачалась орієнтоване на інтереси людей, 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. [89]»

Таким чином, підтверджувалась особлива значимість у сучасному суспільстві інформаційних прав людини, які визнані на міжнародно-правовому рівні у Міжнародній хартії прав людини ³⁷.

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).

³⁷ 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).

Норми цієї Конвенції були покладені в основу Модельного закону СНД «Про захист дітей від інформації, що завдає шкоду їх здоров'ю та розвитку» [299], який встановлює правові та організаційні основи державної політики і міжнародного співробітництва держав-учасниць СНД у сфері забезпечення інформаційної безпеки дітей.

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 екстерні 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 Бройля, підсилювальних і альтернативних способів спілкування й усіх інших доступних способів, методів і форматів спілкування за вибором інвалідів;

в) активне спонукання приватних підприємств, що надають послуги широкій публіці, зокрема через Інтернет, до надання інформації та послуг у доступних і придатних для інвалідів форматах;

г) 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 (СЄС) та Європейським судом першої інстанції (ЕСПІ).

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»³⁸. В подальшому, у своїх рішеннях ЄСПЛ зазначив, що громадськість має право отримувати інформацію та ідеї, що становлять суспільний інтерес³⁹.

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»⁴⁰.

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*⁴¹. 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*⁴² 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

³⁸ Справа *Sunday Times v. United Kingdom*, 26 квітня 1979 року, § 66.

³⁹ *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

⁴⁰ Рішення ЄСПЛ у справі *Leander v. Sweden*, 26 березня 1987 року, §74-75.

⁴¹ 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.

⁴² Рішення ЄСПЛ у справі *Guerra and others v. Italy*, 19 лютого 1998 року, §52-54 та Окрема думка судді Ямбрека, що збігається з рішенням.

міста. Всупереч позиції Європейської комісії, яка до 1998 року 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 Петер 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.

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 році, ЄСПЛ розглянув справу *Sdružení Jihočeské Matky v. Czech Republic*⁴³, 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,

⁴³ Рішення ЄСПЛ у справі *Sdružení Jihočeské Matky v. Czech Republic*, 10 липня 2006 року, §1.1.

яку оспорує заявник. За цих умов Суд визнає, що відхилення зазначеного запиту становило втручання у право заявника отримувати інформацію». Хоча, рішення містило і таке твердження: «Суд також приходиться до висновку, 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, і тому цей випадок повинен розглядатися на предмет дотримання вимог статті 10 Конвенції.

Професор Гентського університету Дірк Воорхооф та викладач Амстердамського університету Вутер Хінс, аналізуючи цю справу, дійшли висновку, 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. [510,с.124-125]

І найбільш фундаментальним рішенням ЄСПЛ щодо розширення розуміння статті 10 винесено було у справі *Társaság a Szabadságjogokért v. Hungary*⁴⁴. Угорська громадська організація «Угорське об'єднання громадських свобод» звернулася до Конституційного Суду Угорщини з проханням надати їй скаргу, що знаходилася на розгляді Суду. Цю

⁴⁴ Рішення ЄСПЛ у справі *Társaság a Szabadságjogokért v. Hungary*, 14 липня 2009 року; §26-39.

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. Натомість органи влади перешкодили йому це зробити. Європейський суд зауважив, що «монополія Конституційного Суду на інформацію таким чином виступає однією з форм цензури».

ЄСПЛ погодився із тим, що втручання органів влади ґрунтувалося на законних підставах і мало легітимну мету – захист прав особи (зокрема, на приватність). Однак таке втручання, на думку Європейського суду, не було необхідним у демократичному суспільстві.

Суд навів свої традиційні твердження про те, що 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. Однак до цих тез ЄСПЛ додав: «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 «вартового пса» суспільства через «цензуру інформаційної монополії», а не просто 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.

Аргумент про захист приватності ЄСПЛ спростував, адже скарга народного депутата стосувалася питань суспільного життя. Якщо ж у запитаній скарзі і містилися якісь особисті відомості про її автора, то їх можна було вилучити із документа. Суд також додав, що «для свободи вираження поглядів у політичній сфері було б фатальним, якби публічні особи могли цензурувати пресу і громадські дискусії заради захисту своїх особистих прав, стверджуючи, що їх думки із суспільних питань стосуються їх особистостей і становлять приватну інформацію, що не може бути поширена без їх згоди».

Таким чином, Європейський суд одноголосно прийняв рішення про те, що у цій справі держава Угорщина вчинила порушення статті 10 Конвенції.

Принципи, вироблені Європейським судом у цій справі, лягли в основу наступних рішень – *Kenedi v. Hungary*⁴⁵, 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*⁴⁶. Вчений Крістофер 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 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.

⁴⁵ Рішення ЄСПЛ у справі *Kenedi v. Hungary*, 26 серпня 2009 року; §40-45.

⁴⁶ Рішення Великої палати ЄСПЛ у справі *Gillberg v. Sweden*, 3 квітня 2012 року; §82-97

Крістофер 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 році 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 статтею 10... отримувати інформацію шляхом доступу до запитаних публічних документів»⁴⁷.

Таким чином, відбулася зміна в розумінні позиції Європейського суду, що повинно визначати також і підходи у національних судових установах. 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 [424].

Окрім того, рішення ЄСПЛ на користь заявника, не тільки зобов'язує державу виплатити заявникові справедливую компенсацію, а також спонукає розвиток національного законодавства в напрямку зближення до міжнародних стандартів, визначаючи обов'язок держави усунути ті недоліки національного законодавства, які спричинили таке порушення.

⁴⁷ 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.

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 [404].

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 МСЄ та ін. [420]

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 [111].

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 [122, 67, с.42-44, 425, с.76-81, 179].

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 (постматеріальні цінності), 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 спиратись 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 [346,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, концепції ведення мережевих 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» [369].

Тим не менш, і за відсутності єдності, що пошуки прийняттого 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» № 53/70 від 04.12.1998 р., № 54/49 від 01.12.1999 р., № 55/28 від 20.11.2000 р., № 56/19 від 29.11.2001 р., № 57/53 від 22.11.2002 р., № 58/32 від 08.12.2003 р., № 59/61 від 03.12.2004 р., № 60/45 від 08.12.2005 р., № 61/54 від 06.12.2006 р., № 62/17 від 05.12.2007 р., № 63/37 від 02.12.2008 р., № 64/25 від 02.12.2009 р., № 65/41 від 08.12.2010 р., № 66/24 від 13.12.2011 р., № 67/27 від 03.12.2012 р.), (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.) [121].

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 (наприкладі, ЄС);
- 5) інститути, що створюються військово-політичними організаціями (наприкладі НАТО);
- 6) національні доктрини, концепції та стратегії [404].

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; Information Systems Audit and Control Association; Internet Security Alliance; Information System Audit and Control Association. [121]

Після Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства і Повноважній конференції МСЕ 2006 року 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 [580].

Термін кібермир використовувався і раніше, але без однозначного підходу до його розуміння. Зокрема, у 2007 році 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 [575].

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, (б) створює перешкоди прав на свободу думки,

совісті і віросповідання, (с) 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» [402].

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 посуті була вичнена Генеральною Асамблеєю ООН в «Декларації і Програма дій по культурі миру» від жовтня 1999 року містить каталог складових і передумов миру, а також окреслює шляхи досягнення і підтримки його за допомогою культури миру [444]. 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:

1. Кожна держава має взяти на себе зобов'язання надати своєму народові доступ до засобів зв'язку.

2. Кожна держава візьме на себе зобов'язання захищати своїх людей в кіберпросторі.

3. Кожна держава візьме на себе зобов'язання не приховувати терористів / злочинців на своїх територіях.

4. Кожна держава повинна взяти на себе зобов'язання не застосовувати першою кібератаки до інших країн.

5. 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, затвержені ООН, що стосуються кіберсередовища в Декларації Еріче про принципи кіберстабільності і кібермиру [482]. 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.

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 [203,с.51-62].

Проблематика міжнародної інформаційної безпеки⁴⁸ 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 році 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 використання

⁴⁸ А власне таке формулювання прийняли для себе держави учасниці ШОС

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 [159].

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»⁴⁹, демонструють внутрішню і зовнішню політику, що суперечить таким намірам.

В свою чергу, інформаційна безпека в діяльності регіональної організації АТЕС⁵⁰, 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 протсежується 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

⁴⁹ Бішкекська декларація глав держав-членів Шанхайської організації співпраці

⁵⁰ Азійсько-Тихоокеанське економічне співробітництво (англ. The Asia-Pacific Economic Cooperation, скорочено АТЕС)

сектор, необхідність співпраці на політичному рівні між всіма державами-членами АТЕС з метою вироблення комплексної стратегії протидії інформаційним загрозам і розвитку регіональної 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» [517]. 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 році про результати цього дослідження. В подальшому така група скликала 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 кберпростору 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). [404]»

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. [404,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. Правове регулювання відносин у сфері інформаційної безпеки людини в США, ЄС та країнах Східного партнерства

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 [53,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 [57]. Її історичні корені сягають початку значно глибше, ніж утворення у 1957-му році 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 році 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 році 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 з 1984 року багаторазово доповнювався і в чинній редакції як § 1030 у Титул 18 Зводу законів США установлює відповідальність за сім основних протиправних діянь, якими визнаються:

- 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;

- 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;

- 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;

- 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 року, тобто без оплати користування комп'ютерних мереж і серверів;

- умисне або необережне пошкодження захищених комп'ютерів;

- шахрайство шляхом торгівлі комп'ютерними пароллями 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;

– 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 компютерів (§ 2511 Титулу 18); за порушення конфіденційності електронної пошти шляхом незаконного доступу до збережених повідомлень, а також за створення перешкод для санкціонованого доступу до таких повідомлень (§2701 Титулу 18)

Відповідальність за інші злочини з використанням комп'ютерної інформації або складових інформаційного комп'ютерного простору передбачає § 1343 Титулу 18 Зводу законів США. Його нормами, зокрема, передбачена можливість притягнення до кримінальної відповідальності за передання повністю або частково дротовими засобами зв'язку, по радіо або телебаченню повідомлення з метою використання для подальшого вчинення шахрайства. Приписи § 1343 підлягають застосуванню у випадках, коли термінали, використовувані для ведення шахрайських дій, обмінюються інформацією за допомогою каналів електровзв'язку.

Передбачені також в федеральному законодавстві такі види правопорушень як умисне проникнення до інформаційних систем (Electronic Communications Privacy Act, 1986); навмисне отримання несанкціонованого доступу до комп'ютера федерального уряду США та порушення його роботи (Computer Fraud and Abuse Act, 1986 р.)

Важливою ознакою американської моделі правовго 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 сформуванню 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 році 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 Білла Клінтона Presidential

Decision Directive 63 (PDD 63) “Захист критично важливої інфраструктури” 1998 року, 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 року. 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 Інтернет. 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 році 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 року 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 [241].

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 (необхідне відновлення цієї рівноваги і встановлення нових засобів контролю для нових інформаційних відносин); 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 [356,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 року було прийнято кілька Актів про кібербезпеку (The Cybersecurity Act), проте в першому з них було передбачено повноваження Президента США відключати доступ до мережі Інтернет на всій території США у надзвичайних випадках загроз національній безпеці [571].

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 [545].

На початку березня 2010 року Президентом США була затверджена чергова «Ініціатива зі всеосяжної національної кібербезпеки» Ради національної безпеки США у складі розділу Военної 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 році 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 році 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» [474]. 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 році [460]. Під «мережевою та інформаційною безпекою» розумілись здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, аутентичності, 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 висловлений 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.

У програмі «e-Європа 2005» констатувалось, що забезпечення інформаційної безпеки не є суто технологічною проблемою, вона стосується значною мірою людської поведінки, знання та передбачення погроз і засобів захисту [485].

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 року, був створений власне під впливом європейської правової думки. Найбільш близьким за змістом до нього є Кримінальний кодекс ФРН.

Конвенція визначає чотири групи злочинів, пов'язаних з використанням комп'ютерних технологій як інструменту їх учинення. Першу групу становлять злочини проти конфіденційності, цілісності й доступності комп'ютерних даних і систем (протизаконний доступ, протизаконне перехоплення, вплив на дані, вплив на функціонування системи, а також протизаконне використання пристроїв і комп'ютерних програм). Друга група – це злочини, пов'язані з використанням комп'ютерних засобів (підроблення, шахрайство). До третьої групи віднесено злочини, пов'язані зі змістом даних (дитяча порнографія). До четвертої – злочини, пов'язані з порушенням авторського права та суміжних прав. У 2002 році Додатковим протоколом до Конвенції було криміналізовано дії расистського та ксенофобного характеру, вчинених через комп'ютерні системи.

Заслугує на увагу Резолюція Ради ЄС № 2003/С 48/01 від 18 лютого 2003 року про Європейський підхід до культури мережі та інформаційної безпеки, якою запропоновано державам-членам сприяти забезпеченню безпеки, як суттєвому аспекту в управлінні як на державному так і приватному рівні, а саме через розподіл відповідальностей; надавати належну освіту та професійне навчання, а також підвищувати рівень обізнаності щодо питань безпеки, особливо серед молоді; вживати адекватних заходів з метою запобігання та усунення випадків порушення безпеки, а саме через: безперервне вдосконалення ідентифікації і оцінки проблем безпеки та застосування відповідних способів управління ; визначення ефективних способів повідомлення всіх зацікавлених сторін про необхідність у діях через покращення діалогу на Європейському і національному рівнях та, якщо необхідно, на міжнародних рівнях, особливо, серед тих, хто забезпечує технологіями інформаційне суспільство та надає послуги; забезпечувати належний обмін інформацією залежно від

потреб суспільства у поінформованості щодо належних практик у сфері безпеки; заохочувати до співпраці і партнерства наукових з діловими колами з метою розробки технологій безпеки і розробки та затвердження загальноновизнаних 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.

Окрім того, у 2004 році було створено європейське агентство по мережівій і інформаційній безпеці (ENISA) 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 Євросоюзу. Крім того, агентство сприяє розвитку зв'язків між країнами-членами Євросоюзу, інститутами Євросоюзу, господарюючими суб'єктами і приватним бізнесом [82].

У січні 2013 року 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 заповдіює великий збиток фінансовим організаціям і їх клієнтам; поширення дитячої порнографії, кібератаки на ключові інфраструктури і інформаційні системи [108].

У 2016 році Європейський парламент прийняв Директиву ЄС щодо мережевої та інформаційної безпеки, метою якої є встановлення загальних стандартів кібербезпеки та покращення співпраці між країнами ЄС [572]. 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 комп'ютерною безпекою, дуже 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 встановлює загальний рівень мережі та інформаційної безпеки та зміцнює співпрацю між державами-членами ЄС, яка допоможе запобігти майбутнім кібератакам на важливі взаємопов'язані європейські системи, – зазначив доповідач Андреас Шваб з Німеччини. [466]

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. Їм доведеться виконувати зобов'язання, пов'язані з вимогами єдиних стандартів безпеки та звітності. 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 включатиме, наприклад, провайдерів послуг, які мають вирішальне значення для «підтримки критичної соціальної або економічної діяльності», а інциденти, пов'язані з безпекою мережі, «матимуть суттєвий негативний вплив на надання послуги».

Деякі інтернет-провайдери, хоча і не визнаються ключовими (оператори комерційних платформ, пошукових систем і хмарних сервісів), також будуть зобов'язані, хоча й у меншій мірі, забезпечити свою інфраструктуру та повідомляти про серйозні інциденти національним властям. З іншого боку, малі цифрові підприємства будуть звільнені від цих зобов'язань.

Кожна країна ЄС зобов'язана 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. Державам-членам також доведеться налаштувати Комп'ютерні групи з питань реагування на інциденти для комп'ютерів (CSIRTs). Команди обговорюватимуть проблеми транскордонних питань безпеки та шляхи узгодженого реагування. Агенція європейської мережі та інформаційної

безпеки (ENISA) відіграватиме ключову роль у впровадженні цієї Директиви, особливо в координації співробітництва між державами в мережі CSIRT.

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» [587], Директиви ЄС «Зелена Книга. Життя і працевлаштування в інформаційному суспільстві» [503] та Рекомендації «Інформаційна магістраль для глобального суспільства» [544].

У Декларації 1999 року Європейського Союзу було сформульоване бачення «істинно демократичного інформаційного суспільства, засноване 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 році 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» [484], План дій «e-Europe 2005» [485], План дій «e-Government i-2010» [486], а також Цифровий порядок денний для Європи (Digital agenda for Europe) як складова Стратегії Європа 2020. [486]

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 Інтернет; європейський цифровий зміст (контент) для глобальних мереж; розумні транспортні системи.

Резолюція Ради № 2003/С 48/02 від 18 січня 2003 року щодо імплементації Плану дій е-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 року 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 [253,с412-422].

Постійного розвитку зазнавала і концепція електронного урядування. Виходячи від реалізації початкових трьох рівнів реалізації – «Уряд – громадянам», «Уряд – бізнесу» та «Уряд – уряду», в деяких державах почали творити е-демократію, як концепцію за якої значно підвищується ефективність демократичних інститутів, демократичних процесів та поширення демократичних цінностей за умови застосування різноманітних інструментів, що базуються на максимальному використанні інформаційних комп'ютерних технологій [23,с.28-38].

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) тощо⁵¹. [

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 році, проте шлях розвитку є дуже інтенсивним. Переважна більшість існуючих інформаційних систем органів влади і багатьох недержавних установ об'єднані в єдину систему. Наприклад, через Інтернет- банкінг проводиться 98 % банківських операцій країни [215]. 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

⁵¹ Основні програми електронного урядування в ЄС.

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 року 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 року, включаючи картки, що випускаються для електронних резидентів. [558]

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 кібер-команду 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 транспарентності⁵² інформаційної політики і забезпечення інформаційної безпеки. Політика транспарентності є багатовіковою традицією організації

⁵² Транспарентність - забезпечення прозорості та відкритості в оприлюдненні інформації

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 року 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) [145].

Сучасна політика транспарентності спрямована на три ключові області: збільшення фінансової звітності ЄС; зміцнення особистої недоторканності і незалежності інститутів ЄС; введення більш суворого контролю на лобіювання [521].

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, а також інформації, отриманої конфіденційно [380, с.22-28].

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) [473].

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 невиправданої відповідальності; утримання від розкриття інформації при наявності відповідного мандата (якщо розкриття призвело б до порушення юридичних чи нормативних вимог, його слід уникати) [443].

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. [380,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 недоторканості приватного життя [487].

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 відіграє 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 [266]. 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 (Директива про секретність та електронні комунікації);

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 Європейського Співтовариства 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 році було запроваджено незалежний інститут Європейського уповноваженого з захисту даних. Такий інститут було створено відповідно до статті 41 Регламенту 45/2001 Європейського Парламенту і Ради від 18 грудня 2000 року про захист прав приватних осіб щодо обробки персональних даних органами та установами ЄС та про вільний рух таких даних. Функції цього інституту подібні до функцій омбудсмена, але більш вузько спеціалізовані в межах захисту персональних даних. Призначення на цю посаду здійснюється за результатами публічного конкурсу кандидатів. Головним критерієм діяльності Європейського уповноваженого з захисту даних є його незалежність від інших інституцій ЄС, що забезпечується спеціальним механізмом, закладеним в Регламенті [327,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 нашій державі.

Держави-члени ЄС при формуванні національного законодавства про захист персональних даних, хоча й зобов'язані були опиратись на стандарти вищеозначених 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 [54,с.45-57].

Проте навіть наявність такого обсягу не знімає всіх протиріч, що існують у цій сфері. У 2010 році 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 коли мова іде про конфіденційні дані про особу [459,с.55-61].

З 2010 року розпочато тривалу реформу, основні вимоги якої наберуть чинності у 2018 році. 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) [548]”; 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” [546]; 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» [547].

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.

Жодна компанія чи орган влади таким чином, не матиме права збирати дані, за винятком випадків, коли надано однозначну беззаперечну згоду. Так звана «імовірна згода», яка досі частково застосовувалася і забезпечувалася встановленою за замовчуванням «галочкою» на сайтах, більше не дозволяється. Компанії мають право запитувати лише ті дані, які необхідні їм для надання послуг.

Основні принципи обробки персональних даних, які означені у зазначених документах, визначають дотримання наступного: персональні дані повинні оброблятися законно, справедливо і в доступній формі по відношенню до суб’єкта даних (“законність, справедливість і прозорість”);

збиратися для певної, конкретної і законної мети і не піддаватися додатковій обробці, яка несумісна з цією метою; подальша обробка для цілей архівації, з метою наукових, дослідницьких, історичних і статистичних цілей не може бути несумісною з початковою метою (“цільове обмеження”); бути адекватними і обмежуватися тими даними, які відповідають і необхідні для досягнення цілі, для яких вони обробляються (“зведення до мінімуму даних”); бути точними і, при необхідності, постійно підтримуватися в актуальному стані; неточні персональні дані, з урахуванням цілі, для якої вони обробляються, слід видалити або виправляти без затримки (“точність”); зберігаться у формі, що дозволяє ідентифікувати суб’єкта даних не довше, ніж це необхідно для цілі, для якої вони обробляються; персональні дані можуть зберігатися протягом тривалішого періоду виключно для цілей архівації, інтересів наукових, дослідницьких, історичних і статистичних цілей (“обмеження зберігання”); обробляються так, щоб забезпечити належний захист персональних даних, включаючи захист від несанкціонованої або незаконної обробки, випадкової втрати, знищення або пошкодження, з використанням відповідних технічних або організаційних заходів (“цілісність і конфіденційність”) [54,с.45-57].

В регламенті вперше нормативно було закріплено право особи на забуття. Низка рішень ЄСПЛ вже раніше свідчили про таке право, проте Регламентом його розуміння було поширене не лише на пошукові системи, але також і на інші платформи в інтернеті. З травня 2018 року усі користувачі можуть звернутися до інтернет-компаній і попросити їх видалити інформацію, що є неточною, застарілою чи ще якоюсь. Таким чином, передбачається що Google, Facebook, Twitter та інші сервіси, що збирають дані, будуть зобов’язані за вимогою власника видалити аккаунти та особисті дані й більше не мають права передавати їх третім особам. Окрім того, ці веб-сайти повинні інформувати системи пошуку про внесені зміни, аби вони теж видаляли чи блокували всі наявні посилання, пов’язані з видаленою інформацією. Таке нововведення є якраз прикладом реакції на судову практику і суспільну думку, адже дві третини європейців занепокоєні тим, що не мають повного контролю над своїми даними в інтернеті [468].

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 року 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 неспівмірний 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 десь. 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 [471].

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 року 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 розяснює 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 року), 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 стару-добру 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.

Міністр закордонних справ Німеччини Габріель також став мішенню дезінформаційних публікацій, оскільки він привітав Україну з Днем

незалежності, вживши в Твіттері вираз «Слава Україні». У цих словах швидко визнали нібито «добре відомий» нацистський слоган часів Другої світової війни, що стало ще одним прикладом винахідливого історичного ревізйонізму. Насправді вираз «Слава Україні» використовується, як мінімум, з 1919 року і знову набуло популярності після протестів на Майдані в 2013-2014 рр.

Крім того, в деяких виданнях України представили як жертву «підступного Заходу», і це ще один повторюваний мотив в дезінформації. Група хакерів КіберБеркут заявила, що має докази того, що Україна – всього лише випробувальний полігон для секретних експериментів США. Зрозуміло, жодного доказу існування цих сумнівних майданчиків для біологічних випробувань надано не було, це лише заява, яка неодноразово звучала. Раніше та ж сама історія несподівано спливла в Вірменії, як повідомляє в своєму репортажі НВО «Союз поінформованих громадян». У схожій статті чеське видання заявляло, що епідемія кору в Україні була спровокована американськими лабораторіями, що створюють біологічну зброю.

Грузинське і російське видання також опублікували на тому ж тижні нібито сенсаційну новину про те, що колишній глава розвідувальної служби Великобританії MI-6 розкрив плани Заходу по розвалу Росії, в інтерв'ю газеті «The Guardian».

Зрозуміло, це була маніпуляція. Маніпуляцією було згадка плану, розкритого в інтерв'ю (якого насправді ніколи не було і який ніколи не публікувався в «The Guardian»), а використання підставного сайту, щоб хитрістю змусити нас думати, ніби ми читаємо цієї статті «The Guardian». Це фокус, про який ми писали раніше, і він може бути дуже ефективним способом поширення дезінформації, оскільки ймовірність того, що новину підхоплять справжні ЗМІ, куди вище, якщо вона видає себе за вже існуючу в справжніх ЗМІ.

«The Guardian» швидко спростувала інформацію. І все ж через п'ять днів фальшива стаття пробралася-таки на російське телебачення. На статтю послався Володимир 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.» [447]

Країни 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 урочисто відкрита Європейським Союзом у Празі 7 травня 2009 року. Вона стосується шести країн пострадянського простору – України, Білорусі, Молдови, Вірменії, Грузії та Азербайджану. Хоча останнім часом точиться значна кількість дискусій щодо перспектив, наприклад, глава МЗС Польщі Вітольд Вашиковський, коментуючи перспективи «Східного партнерства» заявив, що «програма відводила згаданим державам лише роль буферної зони між Росією та ЄС» [437].

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 року)
- 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 року в Молдові розробляється електронне урядування. У серпні 2010 року створений Урядом Республіки Молдова Центр електронного урядування (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) уряд забезпечує доступ громадян та підприємств і організацій до пакетів даних публічного характеру. Єдина платформа публічних послуг (<https://servicii.gov.md/>) працює як єдиний каталог публічних послуг органів державної влади. Розроблена і впроваджена послуга «мобільний підпис», що дозволяє за допомогою мобільного телефону отримувати доступ до електронних послуг, дозволяючи при цьому ідентифікувати та підтверджувати особу у віртуальному просторі. За допомогою «мобільного підпису» громадяни можуть засвідчувати документи, звіти, декларації, он-лайн заяви. Портал «Реєстр місцевих актів» (www.actelocale.md) надає можливість громадянам

та бізнесу мати доступ до централізованої бази документів, що приймаються всіма органами публічної влади Молдови. Він містить окремі реєстри: органів влади та документів, виданих ними. Для бізнесу Центр електронного урядування пропонує інформацію про послуги «Е-ліцензування», «Швидка декларація», «Електронна декларація». Зокрема, послуга «Швидка декларація» являє собою автоматизований спосіб заповнення та надання документів податкової звітності з використанням технології штрих-коду. Для органів державної влади введено сервіси: «Реєстр персональних даних», «Particip.gov.md», «M-pass». Упровадження платформи «Particip.gov.md» обумовлено тенденцією до впровадження в Республіці Молдова засад 30 партисипативної демократії, що передбачає залучення широкого кола учасників до формування та функціонування політичних і державних інститутів. У такий спосіб долаються недоліки представницької демократії, що часто обмежує участь громадян в управлінні державними справами лише їх виборчою активністю. Затвердження Урядом Республіки Молдова «Плану дій з Відкритого управління» у травні 2012 року поставило низку завдань, для розв'язання яких і використовується платформа «Particip.gov.md». За її допомогою громадяни можуть отримувати консультації (у тому числі в режимі он-лайн) щодо проектів нормативних актів. У межах цього проекту громадяни можуть підписатися на отримання розсилок новин, а також генерувати спеціальний код, який може бути розміщений на будь-якому сайті, завдяки чому автоматично з'являються проекти актів, що являють публічний інтерес. За допомогою платформи громадяни також можуть відслідковувати порядок денний публічних консультацій щодо проектів важливих документів. Ця платформа позиціонується як елемент Програми «Національна стратегія розвитку «Молдова 2020». Послуга «M-pass» забезпечує ідентифікацію осіб, що претендують на доступ до електронних послуг. Це відбувається шляхом ідентифікації цих осіб у кілька способів: через мобільний підпис, цифровий сертифікат, пароль.

Проте системи е-демократії є вразливими з позиції інформаційної безпеки. Хакери атакували урядову автоматизовану інформаційну систему «Вибори» під час референдуму 2010 року. 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. [229]

У Молдові відбувається 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. Що стосується інтелектуальної власності, було запущено розслідування файлообмінного сайту Torrentsmd.com.

Нестійка економіка Молдови створює сприятливі умови для фінансових кіберзлочинів. Мінімальна оплата праці в рік в Молдові складає 595 доларів США. 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 [229].

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, який функціонує досить успішно, в числі інших було розкрито 13 випадків дитячої порнографії в вересні 2013 року [229].

Молдова, як і раніше залишається притулком для піратства і порушень авторських прав – надзвичайно високий рівень поширення піратського програмного забезпечення; за приблизною оцінкою 90 відсотків 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 законних інформаційних прав громадян. Молдова має багаточисельну 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 року 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 жовтні 2012 року парламентом було

прийнято суттєві поправки до кримінально-процесуального кодексу, які ввели процедуру законного перехоплення електронного зв'язку і даних, зібраних провайдерами послуг.

Сьогодні 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.

Також у 2016 році була розроблена нова концепція інформаційної безпеки. [530] 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, завданнями якої є:

- контроль дотримання плюралістичного вираження ідей і думок в програмах, що транслюються під юрисдикцією Республіки Молдова;
- вільна конкуренція;
- справедливий баланс між програмами, пропонованими національними мовниками та тими, що надаються місцевими та регіональними мовниками;
- захист людської гідності і захист прав неповнолітніх;
- захист інформаційного простору, мовної і національної культурної спадщини, в тому числі культури і мов національних меншин;
- прозорість аудіовізуальних засобів масової інформації;
- прозорість власної діяльності.

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 році 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 згодна 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).

Ще у 2014 Рада заборонила ретрансляцію Росія-24, але цим справа і обмежилася. 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 року правоохоронні органи все пробувають «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 тд. Поки що це лише ініціативи, які не підтримав парламент.

Грузія

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 році, 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 року, 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 навіть в таких ліберальних умовах все-таки спостерігається деякий

брак прозорості телекомунікаційної сфери. Склад власників медіакомпаній зачасту 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 відсотків 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 відсотків респондентів дізнаються новини політики онлайн, а ще 12 відсотків вважають інтернет в цілому важливим джерелом інформації [228]. 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 [110].

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 [498]. 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 [163] закріплює такі прав в інформаційній сфері:

- Ст. 28 (право на недоторканність приватного життя): «Кожен має право на захист від незаконного втручання в його особисте життя, в тому числі від посягання на таємницю його кореспонденції, телефонних та інших повідомлень, на його честь і гідність»;

- Ст. 33 (право на свободу думок): «Кожному гарантується свобода думок, переконань і їх вільне вираження. Ніхто не може бути примушений до вираження своїх переконань або відмови від них. Монополізація засобів масової інформації державою, громадськими об'єднаннями або окремими громадянами, а також цензура не допускаються ».

- Ст. 34 (право на загальнодоступну інформацію): «Громадянам Республіки Білорусь гарантується право на отримання, зберігання і поширення повної, достовірної та своєчасної інформації про діяльність державних органів, громадських об'єднань, про політичну, економічну, культурну та міжнародної життя, стан навколишнього середовища. ... Державні органи, громадські об'єднання, посадові особи зобов'язані надати громадянину Республіки Білорусь можливість ознайомитися з матеріалами, що зачіпають його права і законні інтереси. ... Користування інформацією може бути обмежено законодавством з метою захисту честі, гідності, особисте та сімейне життя громадян і повного здійснення ними своїх прав ».

Положення Конституції заклали основу для регулювання інформаційної сфери: Закон «Про інформацію, інформатизацію і захист інформації» (2008) [237] містить положення щодо права на інформацію (Ст. 6); загальнодоступної інформації та її класифікація (Ст. 16); інформації, поширення і (або) надання якої обмежено, та її класифікація (Ст. 17); права на захист інформації про приватне життя фізичної особи та персональних даних (Ст. 18); службової інформації (Ст. 181), а також регулює інтернет-контент щодо широкого спектру питань, від безпеки даних до політик управління.

Існує ряд спеціальних законів, які конкретизують права, закріплені в Конституції і Законі Про інформацію: Закон про архівну справу та діловодство [240] визначає право на доступ до архівних документів; Закон

Про засоби масової інформації – право на інформацію і свободу думок, Закон Аб бібліятечнай справе [1]; Закон Про електронний документ і електронний цифровий підпис, Закон Про авторське право і суміжні права. [239] Регулювання інформації, поширення і (або) надання якої обмежено, здійснюється Законами: «Про державні секрети» [236]; «Про комерційну таємницю»; «Про охорону здоров'я» (норми, що визначають лікарську таємницю); Банківський кодекс (банківська таємниця) [18] та ін.

З 2010 року 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 – Президентський Указ № 60 (2010) охоплює загальні питання інтернету і розвитку ІТ, Президентський указ № 515 (2010) стосується створення телекомунікаційної мережі масштабів країни і Національного центру обміну трафіком, а Указом № 129 «Про затвердження процедури співпраці між операторами зв'язку з органами, які проводять оперативно-розшукову діяльність» (2010) зобов'язано білоруських провайдерів до більш тісної співпраці з державними системами спостереження СОРМ.

Головним виконавчим органом в секторі телекомунікацій є Міністерство зв'язку та інформатизації і йому підпорядковано тринадцять організацій. Структурним підрозділом Міністерства є Республіканське унітарне підприємство з нагляду за електров'язком “БелГІЕ”, 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 році 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 в Білорусі: 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», закон «Про перепис населення».

У Республіці Білорусь законодавче визначення особливо чутливих/вразливих видів інформації відсутнє і 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 » [16]

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.

Вірменія.

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, совести 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 році Радою національної безпеки було схвалено Концепцію інформаційної безпеки. Окрім того, 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 [238]. 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 («медіа», «кібер» та «мобайл») 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 [238].

Інформаційна політика Вірменії пережила значних змін. Обмеження роботи ЗМІ під час президентських виборів 2008 року, яке вплинуло на інтернет-ресурси новин і сайти опозиції, сприяло розвитку блогів і соцмереж.

Висвітлення парламентських виборів 2012 року 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-однорумцями 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. Сектор телекомунікацій останніх 20 років стає все більш конкурентоспроможний в результаті подальшої лібералізації і конкуренції з за кордоном. Провайдери телекомунікаційних послуг значною мірою зосереджені в руках іноземних компаній.

Уряд Вірменії ще в 2001 році сформулював план розвитку сектора ІКТ (Open Net Initiative, «Armenia,» in Access Controlled: The Shaping of

Power, Rights and Rule in Cyberspace, eds. Ron Diebert et al. (MIT Press, 2010). 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 відсотків замість загальнодержавного мінімуму, що становить в даний час 24,4%. [227] Уряд і міністерство економіки продовжують просувати розвиток сектора ІКТ, одночасно працюючи над розвитком електронного уряду в Вірменії і підвищуючи якість послуг зв'язку.

Телебачення, як і раніше є основним джерелом інформації. Однак стрімко розвивається взаємодія через соціальні мережі. Лідером залишаються Однокласники, Facebook на другому місці, але існує також і кілька локальних платформ соціальної взаємодії, найбільш популярнат – це Hayland, що нараховує 156 000 зареєстрованих користувачів. У 2013 році 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 року, Facebook виступив як важлива платформа діалогу і ведення передвиборної кампанії, більшість політиків і їхніх партій вже були присутні в мережі. На думку Тиграна 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. [227]

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 той же час, мають місце злочини в мережевому просторі, за оцінкою поліції 80 відсотків кіберзлочинів в Вірменії відбуваються в соціальних мережах, серед яких найбільш поширені – розкрадання персональних даних та вимагання.Порушники часто створюють підроблені акаунти 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 невіршеним конфліктом з Азербайджаном через Нагірний Карабах. Експерти оцінюють це протистояння як інформаційну війну другого покоління.

Конфлікт супроводжується втручанням третіх сторін, зокрема, свої інтереси в інформаційному протистоянні мають країни регіону-Турція, Іран, Грузія, а також глобальні гравці – Російська Феєрація, США і ЄС. При цьому використовуються широко методи інформаційного впливу (пропаганда), а також кібератаки.

Атаки на сайти загострюються в певні періоди року, часто в місяць здійснюється від 50 до 100 атак на вірменські сайти. За даними фонду «Нораванк» [227], вірменського аналітичного центру, який вивчає проблеми інформаційної безпеки, вірменські сайти часто атакують під час національних свят.

Азербайджан.

Азербайджану в останні роки була властива багатоговекторна 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 відсотків 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 відсотків усіх стаціонарних мереж. Більш того, поширення стаціонарних мереж дещо зросла протягом останніх кількох років, досягнувши 18 відсотків. Азербайджанці добре представлені в соцмережах і дуже активні в місцевій блогосфері. Явним фаворитом серед соцмереж є Facebook, де зареєстровано близько одного мільйона аккаунтів. Приблизно 35 відсотків 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 [226].

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 році, 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 року. 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 року в Баку за допомогою Facebook були організовані протести у відповідь на смерть призовника Джейхану 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 році 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 року, в зв'язку з загибеллю Джейхану Губадова, кілька веб-сайтів, які критикують уряд, включаючи azadliq.az, azadliq.org, musavat.com, qafqazinfo.az, повідомили про успішні DDoS- атаки на них. І «Azadliq», і Йені Мусават впевнені, що за цими DDoS-атаками стоїть уряд.

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 року Азербайджанська Кіберармія (Azerian Cyber Army), група, ймовірно пов'язана з Іраном, атакувала приблизно 40 державних структур в знак протесту проти тісних відносин Баку і Тель-Авіва. МСІТ і Відділ інформаційної безпеки Міністерства національної безпеки розслідували ці атаки і повідомили, 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 році, в підтримку комплексного плану дій щодо запобігання випадків помилкової інформації про тероризм, була введена мобільна реєстрація. Всі мобільні телефони і мобільні пристрої повинні бути зареєстровані відповідно до свого ідентифікаційним кодом IMEI, SIM-картою та номером мобільного мережі з реєстрацією центру мобільних пристроїв. Пристрої, які не зареєстровані до 1 травня 2013 року, були внесені в чорний список.

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 році 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 році [226].

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 року. Бакинський адміністративно-економічний суд №1 зобов'язав компанію ABC Telecom, яка продавала комп'ютери з встановленим неліцензійним програмним забезпеченням Microsoft, відшкодувати збитки компанії Microsoft. [6]

4.3. Перспективи використання іноземного досвіду для вдосконалення законодавства України у сфері інформаційної безпеки людини

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 мінародних 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, апіорі не може розвнатись 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 ситемі міжнародної безпеки пройшла різні етапи становлення. В другій половині ХХ 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 [107,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 [107,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 сформувався 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 інформаційної 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 захист. прав та свобод; фіксують умови щодо застосування прав та свобод людини, одночасно із законними обмеженнями цих прав та свобод [213,с.359].

Проте, інформація та інформаційні технології у сучасному світі є одночасно і основним ресурсом та рушієм прогресу, і однією з найсерйозніших 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 року 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 [494].

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.

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.

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 викорситувати її на власний розсуд (або не використовувати). І таким чином створення самого лише правового поля в цій сфері виявляється недостатнім для досягнення мети – демократизації суспільства і забезпечення реалізації інформаційних прав громадян. Тоді як досвід Сполученого Королівства свідчить, що відкриті дані є не лише відповіддю на суспільний запит, але при ефективному використанні можуть приносити 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 самостійно розбудовувати сервіси на основі цих масивів інформації, якими володіє. Створення належної правової бази означає вирішення таких питань – визначення 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.

Ще одним важливим кроком у напрямку підвищення стандартів захисту інформаційної безпеки людини вбачається створення інституту 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 інформаційний комісар як окрема 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 Мортен Енберг назвав її «ключовою рекомендацією Ради Європи щодо аналізу та розподілу повноважень держустанов у сфері інформаційної політики та медіа в Україні» [324]

Суспільна думка та позиції політикуму щодо цього питання суттєво змінились за останні 10 років. В 2008 році 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 [231].

Проте, вже в 2017 році 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» [143].

Особливістю впровадження такої інституції 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 заді відновлення порушеного права, а також запобіганню подальших незаконних обмежено реалізації інформаційних прав і свобод 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 узалежені 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 рік », виконаному DR Analytica на замовлення Digital.Report. [410]

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 році 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 року № 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 року 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 є 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). [251]

Рекомендація Комітету міністрів державам-членам Ради Європи щодо свободи в інтернеті від 13 квітня 2016 року 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. Наскільки припустимим є це 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 скрайне 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 Олега Гелетканича: «Інтернет створювався як місце свободи, тому повністю обмежити або заблокувати доступ до ресурсу фактично неможливо через саму природу мережі» [432].

Цей досвід вказує 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 невпорядкованість, 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.

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 оцифрування 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 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. Технологічний розвиток відбувається стрімкими темпами, а, отже, вимагає таких же темпів правового і організаційного забезпечення питань, що пов'язані з виникненням нових соціальних відносин.

ВИСНОВКИ

На кожному етапі розвитку людства перед ним неминуче ставало питання про сутність людини і її місце у суспільстві. Розуміння такої сутності і ролі визначало підходи до практики співіснування людини, суспільства і держави, необхідними складовими якої є право і закон.

При цьому, кожна наступна 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 інформаційне⁵³, 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.

Як об'єкт соціальних відносин людина, з одного боку, індивідуально виражає значимі риси певного суспільства, інтегрує соціальні відносини зовнішнього середовища і виробляє своє, особливе ставлення до зовнішнього світу. Інформаційна безпека для сучасної людини є необхідною умовою її ефективного включення в соціум і реалізації її прав, свобод та законних інтересів, оскільки інтегрованість в сучасному суспільстві значною мірою залежить від можливості використання інформаційних технологій.

З іншого боку, правові, економічні, політичні та інші соціальні відносини осмислюються і сприймаються (або ні) особистістю через призму її індивідуальних особливостей, і виявляються в діяльності як особисте ставлення до об'єктивної дійсності. Таким чином, людина виступає як суб'єкт соціальних відносин, який керується в поведінці своїми потребами, інтересами, соціальними установками, ціннісними орієнтаціями. А ці потреби, інтереси, соціальні установки і цінності є значною мірою продуктом соціального середовища, яке на сьогодні є більшою мірою насиченим інформацією ніж будь-коли в історії людства.

Усвідомлені потреби особистості лежать в основі її ціннісного ставлення до навколишнього світу, в основі системи її цінностей і ціннісних

⁵³ Хоча, на думку автора, з огляду на стан суспільства всі означені риси є дискусійними.

орієнтацій. При цьому, в умовах інформаційного суспільства відбувається помітна уніфікація масової свідомості, ставиться під сумнів будь-яка форма ідентичності (національна, релігійна, статева, мовна), відбувається деградація мови і культури, нівелюються морально-етичні принципи, що не може не впливати на правову свідомість. Поширення масової культури, неминучість зіткнення з віртуальною реальністю, в якій складно розрізнити ілюзію і дійсність, створюють не лише психологічні і культурні проблеми, але й правові. Створюючи свій образ у віртуальному просторі, людина втрачає або спотворює сприйняття реального світу, в тому числі правової дійсності. Штучно «розмивається» межа правомірної і протиправної поведінки за рахунок інформаційно-психологічного впливу на індивідуальну і суспільну свідомість.

Як суб'єкт соціальних відносин особистість формується в нових умовах, коли попереднє покоління не завжди спроможне передати базові у нових культурних умовах знання та навички. Інформаційне суспільство вимагає від людини вміння навчатися впродовж життя, критично мислити, ставити цілі та досягати їх, працювати в команді, спілкуватися в багатокультурному середовищі тощо.

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 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.

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.

Новий рівень соціальних відносин призводить особистість до усвідомлення існування віртуальної реальності, яка вимагає переосмислення

форм правового регулювання, а також підходів до забезпечення реалізації прав і свобод людини. Переважна частина 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. Техногенна, інформаційна епоха, в котру живе сучасна людина, розкриває принципово нові сторони та моменти людської сутності, котрі акцентують увагу на нових соціальних ролях людини – комунікативній, творчій та інтелектуальній, а отже за принципово новими моделями взаємодії. Відбувається трансформація не лише соціальних структур, а й людської свідомості, культури, моралі. Але цей процес узалежнений від цілої низки чинників, зокрема, від доступу до необхідної інформації, наявності відповідних компетенцій, а також свободи людини, яка не заключається лише в свободі пересування і вибору видів діяльності, а й у внутрішньому стані свободи – мислити поза нав'язаними стереотипами, обирати форму задоволення власних потреб, вступати у взаємодію з іншими суб'єктами тощо.

За таких умов, обсяг прав і свобод людини в сучасному суспільстві визначається не лише особливостями певного співтовариства людей – національної держави, а й розвитком людської цивілізації в цілому та кожної людини зокрема. Окрім, того ускладнення соціальних зв'язків призводить до появи нових типів правовідносин, а людина, як їх суб'єкт, з однієї сторони набуває все більше яєсно нових прав і обов'язків, з іншої сторони – наражається на нові види небезпек.

Правовий статус людини залежить від сутності соціального ладу, в умовах якого він складається і функціонує, тому становлення інформаційного суспільства обумовлює необхідність юридичного закріплення і державного гарантування правового статусу людини на новому якісному рівні. В інформаційних суспільних відносинах людина може брати участь і як суб'єкт (наприклад, відносини щодо доступу до інформації, право на приватність тощо), може бути їх об'єктом (відносини щодо інформаційної безпеки), а навіть – засобом (відносини щодо маніпуляції свідомістю).

Правовий аспект становлення нового соціокультурного простору інформаційного суспільства і ролі людини в ньому проявляється 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.

В сучасному глобалізованому світі інформаційні права людини неможливо розглядати відокремлено від суспільства і держави. Особистість людини є передумовою й продуктом існування суспільства, держави.

Визначення інформаційно-правового статусу особи в суспільстві і державі вимагає закріплення достатнього обсягу інформаційних прав людини. І власне цим достатнім обсягом в законодавстві окремої країни охоплюються різні права і свободи в залежності від політичного режиму, стану економічного і технологічного розвитку, культурних особливостей та геополітичного становища.

В сучасній науковій думці відсутній однозначний підхід до визначення інформаційних прав людини. Проаналізувавши науковий доробок вітчизняних та зарубіжних вчених, а також законодавство понад двадцяти країн світу, автор під інформаційними правами і свободами розуміє комплекс прав, похідних від свободи інформації, як фундаментального права людини, до яких належать:

1) Інформаційні права, що пов'язані з особою (особистістю)⁵⁴ 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;

⁵⁴ Різниця в застосуванні категорій «особа» і «особистість» в праві та інших соціальних науках розглянута в розділі 1. Йдеться про соціальну природу людини, особливості її взаємодії з іншими людьми, соціальними групами та суспільством в цілому.

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.

При цьому, якщо до розвитку сучасних інформаційно-комунікаційних систем під простором поширення інформації розуміли повітря, космос, водні акваторії океанів і морів, то сучасне розуміння інформаційного простору включає додатково кібернетичні та віртуальні системи.

На сьогодні в англomовному світі поширення набула категорія «цифрових прав і сформувались два підходи до їх розуміння. Перший вбачає, що цифрові права – це розширення і застосування універсальних прав людини до потреб суспільства, заснованого на інформації. У другому, 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.

В усіх згаданих категоріях особливе місце посідає право доступу до інформації, а одним із найбільш поширених сучасних форм є доступ до інформації в інтернеті. Слід розуміти, що право на доступ до інтернету має на меті не лише фізичну можливість доступу до мережі. 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.

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. В свою чергу, цифрові права, на нашу думку, не є самостійною науковою категорією, а становлять частину

інтегральну інформаційних прав і свобод, реалізація яких пов'язана з ІКТ (або цифровими технологіями).

Недопустимим в демократичному суспільстві, на нашу думку, є протиставлення свободи інформації (як фундаментального права людини) та інформаційної безпеки. Тому для визначення належного в демократичному суспільстві стану рівноваги між ними, важливим є розуміння суті інформаційної безпеки людини, її співвідношення з іншими видами безпеки, а також системи її правового забезпечення.

Різноманітність підходів до визначення категорії «інформаційної безпеки», виявлена як в науковій думці, так і в правовому регулюванні, вказує, що інформаційна безпека становить одну з важливих та багатограних концепцій в науці та інших сферах людської діяльності. 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, 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 виконується регулятивна і охоронна функції права, а саме закладаються основи захисту об'єктів інформаційної безпеки і правового регулювання діяльності суб'єктів інформаційної безпеки.

Визначеність логічного змісту інформаційної безпеки залежить від розвитку наукового пізнання, а також від розбудови механізму державного управління. При цьому, метою реалізації інформаційної безпеки вбачається побудова системи забезпечення інформаційної безпеки конкретного об'єкта.

Базуючись на методології, опрацьованій спільно з науковим колективом Науково-дослідного інституту інформатики і права НАПрН України, 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 забезпечення;
- 3) політика інформаційної безпеки;
- 4) засоби і способи забезпечення інформаційної безпеки.

Під час дослідження було 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 щодо соціального світу і людини, 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 невідомої складової безпеки підприємств, установ та організацій, а також окремих галузей господарства. На межі тисячоліть гостро повстало питання про міжнародну інформаційну безпеку, а також кібербезпеку у складі інформаційної безпеки. Тим не менш, на кожному з цих етапів інформаційна безпека людини залишалась вторинним питанням.

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 інформаційного суспільства, у сфері 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 проти Російської Федерації.

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. І це відображає певну системну помилку, закладену в чинному законодавстві.

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. В наступних нормативних актах акцент ще більше зміщено на інформаційну безпеку держави і суспільства, відводячи людині лише місце окремої складової в соціальній системі. Такий підхід нівелює розуміння людини, гарантування її прав і свобод, як мети забезпечення будь-якого виду інформаційної безпеки – чи то суспільства, чи держави, чи міжнародного співтовариства. Це в свою чергу знаходить відображення в державній інформаційній політиці та законодавстві, що регулює конкретні сфери життєдіяльності людини, коли в пріоритет виносяться інтереси держави і суспільства, а не захист прав і свобод окремої людини.

Всі проаналізовані в праці підходи до розуміння інформаційної безпеки людини можна узагальнити в два основні. Перший (подекуди його називають технічним або технологічним) підхід домінує в правових науках та безпекознавстві, і насамперед, наголошує на забезпеченні людині здатності вільно і безперешкодно реалізовувати права та свободи в інформаційній сфері, зокрема право на інформацію – вільно збирати, зберігати, використовувати і поширювати інформацію. Значною мірою акцентуючи на здатності і вмінні передбачати та попереджувати загрози інформації, яка циркулює в технічних системах, і загрози самим системам, цей підхід зосереджений на захисті прав людини на інформацію.

Другий (гуманітарний або психологічний) підхід наголошує на захищеності психіки та свідомості людини від небезпечних інформаційних впливів; маніпулювання, дезінформування, образ, мови ненависті, спонукування до самогубства тощо. Проте він не обмежується лише захистом від небезпечної чи небажаної інформації.

Неможливо відкинути динамічної ознаки інформаційної безпеки людини. Вона, водночас, є процесом, невід'ємною частиною життя, в якому людина постійно перебуває під дією конкретних інформаційних впливів. І значимим з позицій забезпечення інформаційної безпеки людини є врахування особливостей конкретної особистості на основі співвідношення в них біологічного та соціального, а також середовища в якому вона знаходиться. 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.

Водночас, слід звернути увагу, 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, а з позицій психологічної науки результат впливу завжди психологічний, навіть якщо за змістом він є фізичний, хімічний чи соціальний. Таким чином, 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.

Доктриною інформаційної безпеки України захищеність від руйнівних інформаційно-психологічних впливів визначено як життєво важливі інтереси особи в інформаційній сфері України. Проте в жодному правовому акті відсутній перелік або визначення критеріїв, які б дозволяли відносити певні дії до руйнівних інформаційно-психологічних впливів. Відсутній також і правовий механізм захисту від таких 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.

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 увагу присвячено наступним:

1) окремі вікові групи: насамперед, діти, підлітки і молодь, а також люди похилого віку;

2) люди з обмеженими фізичними можливостями, особливостями інтелектуального розвитку та психосоціальними особливостями,

3) люди, що здійснюють діяльність, яка має або може мати значимі 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 АТО – військовослужбовці, які беруть чи брали участь в АТО, їх сім'ї, а також сім'ї загиблих, населення окупованих територій, «сірої» зони, внутрішньо переміщені особи тощо;

б) український народ – не лише як населення країни, що проживає на її території, але скоріш як громадяни України, що мають спільну соціально-історичну спільність та/або ідентифікують себе такими у процесі здійснення своїх прав і обов'язків.

Здійснене дослідження свідчить, що державна інформаційна політика має враховувати специфіку різних категорій населення, які зазнають інформаційно-психологічних впливів з різною інтенсивністю та різними методами.

Проте, першочерговою необхідністю, на нашу думку, є напрацювання 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.

Дослідження існуючого законодавства зарубіжного досвіду регулювання інформаційної безпеки вказує на наступну системну проблему, що

має місце у правовому забезпеченні інформаційної сфери України в цілому, і інформаційної безпеки людини зокрема. Стан українського законодавства у інформаційній сфері свідчить про його невпорядкованість, неузгодженість та безсистемність. Окрім того, слід зазначити, що на сьогодні інформаційна сфера розглядається і як відносно самостійна сфера, і як складова інших видів діяльності. Останнє передбачає, 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.

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.

Особливу увагу 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 оцифрування окремих документів та зміна каналів

отримання інформації. Має відбутись переосмислення всіх процесів і цінностей в демократичному суспільстві.

Окрім того, міжнародний досвід свідить 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.

Ситуація щодо інформаційної безпеки людини в Україні та її правового забезпечення ускладнено не лише гібридною війною, в інформаційну складову якої втягнуто фактично все населення держави, а ще й низкою соціальних, політичних, економічних, історичних передумов, що мають вплив як на окремих людей, так і на суспільство в цілому. Тому 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. З цією метою необхідними також вбачаються певні інституційні зміни на рівні державної влади. По перше, центральний орган державної виконавчої влади, що буде реалізовувати політику держави щодо розбудови приязного для людини інформаційного суспільства в Україні. Зрозуміло, що саме існування відповідного органу не вирішує проблеми (про що свідчить діяльність співзвучного за назвою Міністерства інформаційної політики), і для реалізації будь-якої політичної програми слід її закріпити на законодавчому рівні. Така програма має закріплювати не лише гіпотетичні цілі, а конкретні межі відповідальності 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. І 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.

По друге, на рівні незалежного органу держави має повстати інститут інформаційного комісара, діяльність якого спрямована на захист прав і свобод людини в інформаційній сфері, зокрема, права на доступ до публічної інформації та захист персональних даних. Такому інституту 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 – правозахисні повноваження щодо припинення правопорушень та відновлення порушених прав.

Врегулювання на законодавчому рівні також 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 інформаційного суспільства, особливо у вразливих категорій населення – дітей та молоді, осіб похилого віку, осіб з особливими потребами; цю потребу особливо актуалізує інформаційна війна;

подолання цифрової нерівності в географічному та демографічному (віковому) вимірі та інші.

Якщо більшість з названих проблем мають відносно добре наукове опрацювання і користуються суспільним схваленням, то поруч із ними існують інші, що вимагають етичної оцінки, і тому значно складніше інтегруються у суспільну свідомість, отже і правосвідомість та правову культуру. Зокрема, йдеться про цілу низку питань, пов'язаних із використанням штучного інтелекту та робототехніки, технологій аналізу великих даних, політтехнологій, пропаганди та маніпуляцій суспільною свідомістю, використання генетичної інформації тощо. І всі вони безпосередньо пов'язані не лише з інформаційною безпекою людини, а й з безпекою людини в цілому, як фізичної особи і як члена суспільства.

Таким чином, оскільки головним джерелом добробуту людини стає інформація, то інформаційна безпека людини має на меті забезпечення збереження цілісності особи та її здатності до розвитку як визначальних категорій буття людини, враховуючи реалії становлення інформаційного суспільства.

ВИКОРИСТАНА ЛІТЕРАТУРА І ДЖЕРЕЛА

1. Аб бібліятечнай справе: Закон Рэспублікі Беларусь от 22 сакавіка 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. Преодолевая 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. 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/ (дата звернення: 02.10.2017)
6. Азербайджан: Суд впервые запретил компании использовать нелицензионное ПО. URL: <https://digital.report/azerbaydzhan-sud-vpervyie-zapretil-kompanii-ispolzovat-nelitsenzionnoe-po/> (дата звернення: 19.10.2017)
7. Алещенко В.І., Сербін В.Г. Проблеми захисту від негативного інформаційно-психологічного впливу противника. Мат. машини і системи. 2010. № 1. С. 77-86.
8. Американская компания уже в августе вживит чипы сотрудникам URL: <http://datification.org/article/amerikanskaya-kompaniya-vzhivit-chipy-svoim-sotrudnikam/> (дата звернення: 29.07.2017)
9. Анализ законодательства в Российской Федерации в контексте права человека на информацию. URL: http://www.medialaw.ru/publications/books/inf_right. (дата звернення: 20. 08.2017)
10. Ананьев Б.Г. Психология чувственного познания. М.: Наука, 2001. 279 с.
11. Андрущенко В. Філософія: Підр. Харків: Консум, 2000. 672 с.
12. 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.
13. 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.
14. 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.
15. Архипова Є. О. Інформаційна безпека: соціально-філософський вимір : дис. ... кандидата філософ. наук : 09.00.03 / НТУ України «Київський політехнічний інститут». К., 2012. 199 с.
16. Аскерко А. Комментарий к Закону Республики Беларусь «О регистре населения. URL: <http://www.center.gov.by/article61.html> (дата звернення: 02.10.2017)

17. Балалыкина Э.А. *Метаморфозы русского слова: учебное пособие*. М.: Флинта. Наука, 2012. 524 с.
18. Банковский кодекс: Кодекс Республики Беларусь от 25.10.2000 г. № 441-3. URL: <http://kodeksy.by/static/bankovskiy-kodeks.pdf>
19. Баранов О.А. *Інформаційне право України: стан, проблеми, перспективи*. Київ: СофтПрес, 2005. 316 с.
20. Баранов О.А. *Право власності на інформацію. Права інформатика*. 2008. № 1(17). С.15-19.
21. Баранов О.А. *Інформаційна безпека і економічні перетворення. Поглиблення ринкових реформ та стратегія економічного розвитку України до 2010 року: Мат. міжнародної конференції*. К., 1999. Ч. 2, т. 1. 168 с.
22. Баранов О.А. *Правове забезпечення інформаційної сфери: теорія, методологія і практика: Моногр.* Київ: Едельвейс, 2014. 434 с.
23. Баранов О.А. *Правові проблеми “електронної демократії”*. Інформація і право. 2017. № 1(20). с.28-38.
24. Бауман З. *Глобалізація. Наслідки для людини і суспільства / пер. з англ. І. Андрущенко*. К.: Вид. дім "Києво-Могилянська академія", 2008. 109 с.
25. Бачило І.Л., Лопатин В.Н., Федотов М.А. *Информационное право: Учеб.* СПб.: Юрид. центр Пресс, 2001. 789 с.
26. Бачило І.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 (дата звернення: 11.08.2016)
27. Бачило І.Л. *Информационное право. Основы практической информатики: Учеб. пособ.* М.: Юриформцентр, 2001. 352 с.
28. Беззубов Д.О. *Суспільна безпека: (організаційно-правові засади забезпечення): Моногр.* К.: МП Леся, 2013. 451 с.
29. *Безпека дітей в Інтернеті* URL: <http://mon.gov.ua/ua/activity/education/59/196/korinf19/bezditvinet/> (дата звернення: 02.10.2017)
30. *Безпека дітей в Інтернеті: відомості для батьків і вчителів* URL:<https://support.office.com/uk-ua/article> (дата звернення: 02.10.2017)
31. *Безпека інформації* URL: <http://jrn1.nau.edu.ua/index.php/Infosecurity> (дата звернення: 10.09.2017)
32. Белл Д. *Социальные рамки информационного общества. Новая технократическая волна на Западе*. М.: Прогресс, 1986. С. 330–342.
33. Беляева Е. В. *Метаморфозы нравственности: динамика исторических систем нравственности*. Минск: Экономпресс, 2007. 464 с.
34. Бергсон А. *Творческая эволюция / пер. с фр. В. Флеровой*. М.: Академический проект, 2015. 318 с.
35. Беркмен О. *Зникла межа між віртуальним і матеріальним світами*. URL: <http://>

osvita.telekritika.ua/print/material/2099. (дата звернення: 24.11.2016)

36. Бехтерев В.М. Внушение и его роль в общественной жизни. СПб.: Питер, 2001. 256 с.
37. Беляков К.І. "Віртуальність" в контексті формування аксіоматики інформаційно-правових досліджень . Право та державне управління. Запоріжжя: Класичний приватний університет, 2011. № 4. С. 32–37.
38. Беляков К.І. Понятійні та методологічні основи регулювання нових типів інформаційних відносин : «віртуальні правовідносини». «Lex Portus». Одеса, Національний університет «Одеська юридична академія», 2016. № 2-2016. С. 47-63.
39. Беляков К.І. Правове регулювання "віртуального простору" Наука і правоохорона. К.: ДНДІ МВС України, 2011. № 2 (12). С. 102–109.
40. Беляков К., Ланде Д., Ніконова В. Інформаційне законодавство: новели 2013 року. Юридичний Вісник України. № 52 (965). 28 грудня 2013 року – 3 січня 2014 року. с. 14-15
41. Беляков К.І. Інформація в праві: теорія і практика: Моногр. К.: КВІЦ, 2006. 118 с.
42. 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.
43. Беляков К. І. Інформаційна безпека. Внутрішня безпека України та шляхи її забезпечення: наукове видання. К.: Міжвідомчий наук. дослід. центр, 2005. С. 26–32.
44. 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.
45. Більше половини жителів сіл в Україні вже користуються інтернетом URL:<http://watcher.com.ua/2017/04/13/bilshe-polovyny-zhyteliv-sil-v-ukrayini-vzhe-korystuyutsya-internetom/> (дата звернення: 04.10.2017)
46. Богущ В., Юдін О. Інформаційна безпека держави. К.: «МК-Прес», 2005. 432 с.
47. Боднар І. Інформаційне право країн західної Європи. Підприємництво, господарство і право. № 6. 2011. С. 34-38.
48. Боднар І.Р. Державна політика та інформаційна безпека України: післякризові виклики. Актуальні проблеми післякризового відновлення економіки України: Зб. мат. наук.-практ. конференції викладацького складу і аспірантів навчально-наукового комплексу "Академія". Л., 2013.
49. Бодрук О.С. Структура воєнної безпеки: національний та міжнародний аспекти: Моногор. К.: НІПМБ, 2001. 300 с.
50. 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)
51. Бостром Н. Искусственный интеллект. Этапы. Угрозы. Стратегии / пер. с англ. С. Филина. М.: Манн, Иванов и Фербер, 2016. с.496.

52. Бот — друг или враг юриста? URL:<https://delo.ua/tech/kak-ispolzovat-chat-botov-v-ecommerce-330479/> (дата звернення: 06.11.2017)
53. Брижко В. До питання сучасної інформаційної політики. Вісн. Академії управління МВС. 2009. № 2. С. 32–36.
54. Брижко В. Сучасні основи захисту персональних даних в європейських правових актах. Інформація і право. 2016. № 3(18). С. 45-57.
55. Булеца С. Персональні дані пацієнта розголошує не підлягають URL: http://yurincom.com/ua/legal_practice/analitichna_yurysprudentsiia/personalni_dani_ratsiienta_rozgholosu_ne_pidliagaiut-publication/ (дата звернення: 11.10.2017)
56. 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.
57. 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-regulyvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350 (дата звернення: 15.08.2017)
58. В ЛНР издали детский журнал Вежливые человечки URL: <http://korrespondent.net/ukraine/3630876-v-lnr-yzdaly-detskyi-zhurnal-vezhlyvye-chelovechky> (дата звернення: 12.03.2016)
59. Василенко В.О. Антикризисное управление предприятием: Навч. посібник. К.: Центр навч. л-ри, 2005. 504 с.
60. Великий тлумачний словник сучасної української мови / Уклад. і голов. ред. В.Т. Бусел. Київ, Ірпінь: ВТФ “Перун”, 2005. 1728 с.
61. Вернадский В. Несколько слов о ноосфере. URL: https://www.e-reading.club/bookreader.php/11180/Vernadskii_-_Neskol%27ko_slov_o_noosfere.html (дата звернення: 01.02.2015)
62. Веселуха В. Значення віктимологічної профілактики в системі запобігання злочинам. Право України. 1999. № 10. С. 67–73.
63. Винокуров И., Гуртовой Г. Психотронная война: От мифов — к реалиям, М.: Мистерия, 1993. 366 с.
64. Витяг з протоколу засідань Комісії при Президенті України по підготовці пропозицій про статус, порядок діяльності і структуру Ради національної безпеки 10 лютого 1992 року № 31/92-рп URL: <http://zakon3.rada.gov.ua/laws/show/31/92-%D1%80%D0%BF>
65. 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-prava-na-dostup-do-publichnoii-informatsiui-u-g/> (дата звернення: 04.09.2017)
66. Віртуальний світ – це вже реальність. Секонд лайф. (Новини ТСН, 17.06.07). URL:www.pokrovka.2bb.ru/viewtopic.php?id=15]. (дата звернення: 04.03.2015)
67. Войтович П. П. Проблеми міжнародно-правового регулювання інформаційної

безпеки. Міжнародні читання з міжнародного права пам'яті проф. П.С. Казанського : Матер. третьої міжнар. наук. конф. Одеса, 2–3 листопада 2012 р. Одеса : Фенікс, 2012. С. 42-44.

68. 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.
69. Гарантувати безпеку/ Мова – ДНК нації. URL: <https://ukr-mova.in.ua/library/inshe/garantuvati-bezpeku> (дата звернення: 04.03.2017)
70. Герасимова И. А. Диалог культур и когнитивная эволюция. Эволюция. Мышление. Сознание. М.: Канон, 2004. С. 169 -227.
71. 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/ (дата звернення: 11.10.2017)
72. Глобальний звіт про розвиток інформаційних технологій-2015 URL: <http://edclub.com.ua/analityka/riven-rozvytku-informaciyno-komunikaciyneh-tehnologiyv-ukrayini-ta-sviti> (дата звернення: 24.09.2016)
73. Головатий С. Верховенство права: Моногр. у 3-х кн. Київ: Вид-во «Фенікс», 2006. 1747 с.
74. Головенко Р.Б., Котляр Д.М., Слизьконіс Д.М. Доступ до публічної інформації: посібник із застосування «трискладового тесту». К.: ЦІПСА, 2014. 152 с.
75. 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)
76. Головченко В. Правові механізми формування правосвідомості студентів. Право України. 2006. № 9. С. 100-103.
77. Горбань О.М., Бахрушин В.Є. Основи теорії систем та системного аналізу. Запоріжжя: ГУ ЗІДМУ, 2004. 204 с.
78. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. Вісник Національної академії державного управління при Президентіві України. 2015. № 1. С. 136-141.
79. 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.
80. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу URL:https://dt.ua/internal/gibridna-viyuna-yak-klyuchoviy-instrument-rosiyskoyi-geostrategiyi-revanshu_.html (дата звернення: 04.03.2017)
81. Городенко Л.М. Цифрова та інформаційна нерівність у мережеві комунікації. Інформаційне суспільство. К., 2012. Вип. 16. 64 с.
82. Государственные стратегии кибербезопасности URL: <http://www.bezpeka.com/ru/lib/sec/gen/government-cybersecurity-strategy.html> (дата звернення: 04.03.2017)
83. Грачев Г.В. Мельник И.К. Манипулирование личностью: Организация, спосо-

- бы и технологии информационно-психологического воздействия. М.: Алгоритм, 2002. 228 с.
84. Губерський Л. Філософія: Навч. посіб. для студ. і аспір. вищих навч. закл. К.: Вікар, 2005. 516 с.
 85. Гурковський В.І. Деякі організаційно-правові питання взаємовідносин органів державної влади у сфері інформаційної безпеки. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2002. Вип. 5. С. 87.
 86. 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.
 87. Гуцу С. Ф. Правові основи інформаційної діяльності: Навч. посібник Х.: Нац. Аерокосм. Ун-т «Харк. авіац. ін. -т», 2009. 48 с.
 88. Давидов С. А. Социология: консп. лекцій. М., Изд-во: Эксмо; 2008; 160 с.
 89. Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» від 12.12.2003. URL: http://zakon2.rada.gov.ua/laws/show/995_c57
 90. Дем'яненко М. Електронне декларування: суспільний резонанс і політичні прогнози. Україна: події, факти, коментарі. 2016. № 21. С. 7–15.
 91. Денисенко вважає, що був прийняти «дуже» сирий «закон», який може мати негативні наслідки. URL: <https://ua.112.ua/polityka/nardep-denyshenko-vvazhaie-shcho-e-deklaratsii-mozhut-staty-priamoiu-navodkoiu-dlia-zlochytstiv-334219.html> (дата звернення: 11.09.2016)
 92. Державна інформаційна політика URL:<http://merega.org.ua/law/projects/derzh-polityka>. (дата звернення: 15.11.2016)
 93. 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.
 94. Деякі рекомендації по відродженню інтересу української громадськості до Відкритих даних. URL: <https://www.prostir.ua/?blogs=deyaki-rekomendatsiji-povidrozhennyu-interesu-ukrajinskoji-hromadskosti-do-vidkrytyh-danyh> (дата звернення: 04.03.2017)
 95. Дзьобань О. П. Соціокультурні аспекти інформаційної безпеки Зовнішня торгівля: економіка, фінанси, право. 2013. № 2. С. 171-176.
 96. Дзьобань О.П., Пилипчук В.Г. Інформаційне насильство та безпека: світоглядно-правові аспекти: Моногр. Х.: Майдан, 2011. 244 с.
 97. 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.
 98. 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.
99. Доктрина інформаційної безпеки України – це лише декларація URL:<http://www.radiosvoboda.org/a/28336852.html> (дата звернення: 29.05.2017)
 100. Доктрина інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 514/2009. URL:[://www.president.gov.ua/documents/9570.html](http://www.president.gov.ua/documents/9570.html)
 101. Доктрина інформаційної безпеки України, затв. Указом Президента України від 25 лютого 2017 року № 47/2017 URL: <http://www.president.gov.ua/documents/472017-21374>
 102. Домарєв В.В., Швець В.А., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом: Навч. пос. К.: НАУ, 2006. 108 с.
 103. Донбас Медіа Форум: інформаційний простір та інформаційна політика в умовах війни URL: <http://www.isdpa.org.ua/news/donbas-media-forum-informaciyniy-prostir-tainformaciyna-politika-v-umovah-viyni> (дата звернення: 26.08.2017)
 104. Дослідження проведене соціологічною службою Центру Разумкова з 21 по 26 квітня 2017 року. URL: https://dt.ua/POLITICS/prezidentu-ukrayini-doviryayut-22-gromadyan-uryadu-13-radi-9-242814_.html (дата звернення: 04.08.2017)
 105. 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)
 106. Дубенко Л. Соціальні мережі : реальні загрози віртуального світу. URL: www.ogo.ua/articles/toprint/2011-02-23/26490.html
 107. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: моногр. К.: НІСД, 2014. 328 с.
 108. Европейский центр борьбы с киберпреступностью отчитался за первый год работы URL:<http://www.interfax.ru/world/357250> (дата звернення: 22.07.2017)
 109. Ежевская Т.И. Психологическое воздействие информационной среды на современного человека. Психопедагогика в правоохранительных органах. 2012. №3(27) URL: <https://cyberleninka.ru/article/n/psihologicheskoe-vozddeystvie-informatsionnoy-sredy-na-sovremennogo-cheloveka> (дата звернення: 11.03.2015)
 110. Електронне врядування в Грузії. URL: <http://gurt.org.ua/news/recent/7822/> (дата звернення: 04.08.2017)
 111. 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 (дата звернення: 04.03.2015)
 112. Еріксен Т.Г. Тиранія моменту. Швидкий і повільний час в інформаційну добу / пер. з англ. В. Дмитрука. Л.: Кальварія, 2004. 196 с.
 113. Етимологічний словник української мови : у 7 т. Т. 1. К.: Наукова думка. 1982. 632 с.
 114. Свдоченко 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.
115. Єдиний демографічний реєстр порушує права людини і принципи верховенства права. URL: <http://pravo.org.ua/ua/news/4960-> (дата звернення: 23.07.2017)
 116. Сленський В. Глобальні тенденції релігійного розвитку у XXI столітті URL: https://risu.org.ua/ua/index/studios/studies_of_religions/32037/ (дата звернення: 04.03.2017)
 117. 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
 118. 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.
 119. 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)
 120. Живайкина А.А., Кузнецова М.Н. Интеракция больных с нарушениями психического здоровья на платформе Интернета. Бюллетень медицинских Интернет-конференций. 2016. Т. 6. №1. С.184-187.
 121. 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 (дата звернення: 15.09.2017)
 122. Забара І.М. Міжнародне інформаційне право: актуальні проблеми: Наук. доп. Київ, 2011. 23с.
 123. Загальна декларація прав людини, прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року URL:http://zakon5.rada.gov.ua/laws/show/995_015
 124. Зайчук О.В. Оніщенко Н.М. Теорія держави і права: Акад. курс, підр. К.: Юрінком Інтер, 2006. 688 с.
 125. Закликаємо припинити переслідування журналістів у Криму URL: <https://docs.google.com/document/d/1krMs7UCaB5MTr5hRGbg9jZwaqOV3pdoInTjaPXsgruY/edit> (дата звернення: 04.08.2017)
 126. Залізник В.А. Інформаційна безпека як інститут інформаційного права України . Актуальні проблеми зміцнення державності і національної єдності України: матеріали наук.-практ. конференції. Київ, 2010. С. 46-48.
 127. 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.
 128. Захист інформаційних ресурсів в інформаційно-телекомунікаційних системах: матеріали круглого столу. Київ: [б. в.], 2001. 212 с.
 129. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. Видання офіційне. Київ, Держстандарт України, 1996.

130. Захист інформації. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. Видання офіційне. Київ, Держстандарт України, 1997.
131. Згуровський М.З. Шлях до інформаційного суспільства – від Женеви до Тунісу. Тернистий шлях до відродження. К.: Генеза, 2010. 368 с.
132. Золотар О.О. Віртуальна реальність. Моделі колективної безпеки: інформаційний вимір: Зб. мат. / Упоряди. Ланде Д.В. К.: НДЦП НАПрН України, 2011. С. 63-66.
133. Золотар О.О. Генеза охорони і захисту інформації в Україні: історико-правовий аспект. Державна політика цивільної авіації XXI 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
134. Золотар О.О. Критичне мислення як необхідна умова безпеки людини в інформаційному суспільстві: соціально-правовий аналіз. Інформаційна безпека людини, суспільства, держави. 2017. № 3(23).
135. Золотар О.О. Правова охорона як складова інформаційної безпеки: моногр. – Київ: ТОВ «ПанТот». 2011. 100 с.
136. Золотар О.О. Про поняття “інформаційний шум” у правовідносинах» Інформація і право. 2012. № 1(4). С. 70-74.
137. Золотар О.О. Свобода інформації в контексті концепції природного права. Правова інформатика. 2011. № 1(29). С. 12-16.
138. Золотар О.О., Трубін І.О. Класифікація загроз інформаційній безпеці. Інформація і право. 2013. № 3(9). С. 105-114.
139. Інтернет-залежність. URL: <http://megasite.in.ua/5168-internet-zalezhnist-spravzhnisinka-narkotichna-prihilmist.html> (дата звернення: 04.11.2016)
140. Інформаційна безпека (соціально-правові аспекти): Підр. / Остроухов В.В., Петрик В.М. та ін.; за ред. Є. Д. Скулиша. – Київ : КНТ, 2010. 776 с.
141. Інформаційна безпека України в умовах євроінтеграції: Навч. посіб. / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський. К.: КНТ, 2006. 280 с.
142. Інформаційний вплив: теорія і практика прогнозування : Моногр. / За ред. П.Д. Фролова. К.: Міленіум, 2011. 304 с.
143. Інформаційний комісар: хто захищатиме доступ до інформації . URL: <https://dostup.pravda.com.ua/stories/publications/informatsiinyi-komisar-khto-zakhyshchatyme-dostup-do-informatsii> (дата звернення: 04.03.2017)
144. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. / за заг. ред. А. Баровської. К.: НІСД, 2016. 109 с.
145. Історія доступу по-шведськи: королівський указ про свободу друку 1766 року. URL: <https://dostup.pravda.com.ua/stories/publications/istoriia-dostupu-pro-shvedsky-korolivskyi-ukaz-pro-svobodu-druku-1766-roku> (дата звернення: 04.11.2017)
146. Калюжний К.Р. Сутність інформаційних прав людини в науці інформаційного права. Юридичний вісник. 2012. № 4(25). С. 55–58.

147. Калюжний Р.А., Баєв О.О. Нормативно-правове забезпечення інформаційної безпеки України. *Правова інформатика*. 2009. № 4(24). С. 5-11.
148. Кант І. Критика практичного розуму. К.: «Юніверс», 2004. 240 с.
149. Кастельс М. Галактика Інтернет: Размышления об Интернете, бизнесе и обществе. Екатеринбург: У-Фактория, 2004. 328 с.
150. Кастельс М. Информационная эпоха: экономика, общество и культура. / Пер. с англ. под науч. ред. О.И. Шкаратана. М.: ГУ ВШЭ, 2000. 608 с.
151. Кафтя А.А. Інформаційне законодавство України: стан та тенденції розвитку URL: <http://goal-int.org/informacijne-zakonodavstvo-ukraini-stan-ta-tendencii-rozvitku/> (дата звернення: 21.05.2016)
152. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи. К., ПНБ, НА СБУ, 2004. 472 с.
153. Кібер-булінг: небезпечне віртуальне «бикуння» URL: http://osvita.mediasapiens.ua/mediaprosvita/research/kiberbullin_nebezpechne_virtualne_bikunnya/ (дата звернення: 09.10.2017)
154. Кіберзагрози і кібербезпека: чи здатні фахівці протистояти хакерам? URL: <http://ukr.obozrevatel.com/news/34918-kiberzagrozi-i-kiberbezpeka-chi-zdatnifahivtsi-protistoyati-hakeram.htm> (дата звернення: 19.09.2016)
155. 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.
156. Коваленко І.П. Правова соціалізація особистості як процес формування правової культури. *Культура України*. 2011. № 32. С.110-118
157. Коваленко І.І., Бідюк П.І., Гожий О.П. Вступ до системного аналізу: Навч. посіб. Миколаїв: МДГУ ім. Петра Могили, 2004. 148 с.
158. 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)
159. Конвенция об обеспечении международной информационной безопасности від 18.12.1979 № 995_207. URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptlCk6B6BZ29/content/id/191666?p_p_id=101_INSTANCE_CptlCk6B6BZ29&_101_INSTANCE_CptlCk6B6BZ29_languageId=ru_RU
160. 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
161. Конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.2001 № 994_575. Офіційний вісник України. 2007, 10 вересня. № 65. Ст. 2535.
162. 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
163. Конституція Республіки Беларусь. URL: <http://pravo.by/pravovaya-informatsiya/normativnye-dokumenty/konstitutsiya-respubliki-belarus/>

164. Конституція України від 28.06.96 р. № 254/96 ВР: Відомості Верховної Ради (ВВР) України. 1996. № 30. Ст. 141.
165. Копелєв І.Ю., Живко М.О. Інформаційні загрози: суть і проблеми: Інформаційна та економічна безпека. Системи обробки інформації (INFECO – 2010): мат. III міжнародної НПК. 2010. Вип. 3(84). С.130-131.
166. Копылов В.А. Информационное право. М.: Юристъ, 2002. 512 с.
167. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посіб. К.: Кондор, 2004. 382 с.
168. Кормич Б.А. Інформаційне право: Підр. Х.: БУРУН і К., 2011. 334 с.
169. 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.
170. Косиця О.О. Інституціональний механізм системи інформаційної безпеки Порівняльно-аналітичне право. 2016. № 4. URL: http://www.pap.in.ua/4_2016/45.pdf. (дата звернення: 25.06.2017)
171. Костецька Т.А. Конституційно-правове регулювання інформаційних прав: деякі термінологічні аспекти. Часопис Київського університету права. 2013. № 2. С. 114-117.
172. Котляр Д. Інформація не може бути об'єктом право власності URL: <https://www.youtube.com/watch?v=nTKYEI-5P0M> (дата звернення: 08.12.2017)
173. 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.
174. Кохановська О.В. Цивільно-правові проблеми інформаційних відносин в Україні. Дис. ... д-ра юрид.наук: 12.00.03. Київ, 2006
175. Кравець Є. А. Інформаційна безпека держави. Юридична енциклопедія: в 6 т. К.: Укр. енцикл., 1992. С. 744.
176. Красноступ Г.М. Організаційно-правові аспекти необхідності реформування сучасного інформаційного законодавства. Право України. 2005. № 9. С. 81—83.
177. Кримінальний кодекс України: кодекс України від 05.04.2001 № 2341-III. ВВР України. 2001. № 25-26. Ст.131.
178. Кримінально-процесуальний кодекс України: кодекс України від 13.04.2012 № 4651-VI. ВВР України. 2013. № 9-10. № 11-13. Ст.88.
179. Крутских А.В., Сафонова И.Л.. Международное сотрудничество в области информационной безопасности. URL: <http://www.ict.edu.ruft002472intcoop.pdf> (дата звернення: 11.08.2017)
180. Крымов Г. Всемирная сеть мошенников. Жертвой киберпреступников может стать каждый URL: http://cripo.com.ua/?sect_id=6&aid=115837 (дата звернення: 10.06.2015)

181. Кубі Г.: накидання «гендерної рівності» – це культурне перепрограмування суспільства. URL: <http://credo.pro/2013/05/83148> (дата звернення: 09.10.2017)
182. Лазоренко О.А. Інформаційний складник гібридної війни Російської Федерації проти України: тенденції розвитку. Стратегічні пріоритети. 2015. № 3. С. 124-133.
183. 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.
184. 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.
185. 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.
186. Линник Г.М. Адміністративно-правове регулювання інформаційної безпеки України : автореф. дис. ... канд. юрид. наук : 12.00.07 / Нац. ун-т біоресурсів і природокористування України. Київ, 2011. 20 с.
187. 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.
188. 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)
189. Литвиненко О. Інформація і безпека. Нова політика. 1998. № 1. С. 47-49.
190. Литвиненко О. Проблема інформаційної безпеки в контексті міграційних процесів. URL: http://www.nbu.gov.ua/portal/soc_gum/Ukralm/2012_7/lytvynenko.pdf (дата звернення: 04.03.2015)
191. 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.
192. Лицевая идентификация может помогать преступникам URL: http://www.infox.ru/hi-tech/tech/2011/08/02/Licyevaya_idyentifik_print.phtml (дата звернення: 19.10.2017)
193. Ліпкан В., Максименко Ю. Інформаційні права і свободи людини та громадянина. Підприємництво, господарство і право. 2011. №9. С. 64–68.
194. Ліпкан В.А. Національна безпека України: навч. посіб. К.: КНТ, 2009. 576 с.
195. Ліщинська О.А. Культурна психічна залежність особистості: передумови, чинники, механізми: монографія. Київ: Легко інк, 2008. 266 с.
196. Логінов А. 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.

197. Логінов О.В. Гносеологічний аспект управління інформаційною безпекою України. *Наук. вісн. Юридичної академії МВС України*. 2004. № 2. С. 153-161.
198. 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)
199. Лоренц К. Агрессия (так называемое «зло») URL: <http://lib.ru/PSIHO/LORENC/agressiya.txt> (дата звернення: 19.10.2017)
200. Лукашевич М.П., Мигович І.І. Теорія і методи соціальної роботи: Навч. посіб. К.: МАУП, 2003. 168 с
201. Лызь Н.А. Развитие безопасной личности в образовательном процессе вуза: Моногр. Таганрог: Изд-во ТРТУ, 2005. 305 с.
202. Магда Є.В. Гібридна війна: вижити і перемогти. Х.: Віват, 2015. 304с.
203. Макаренко Є.А. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст. Актуальні проблеми міжнародних відносин. 2011. Вип. 102(1). С. 51-62 .
204. Макарова М.В. Електронна комерція : Посіб. К.: Видавничий центр “Академія”, 2002. 272 с.
205. Максименко Т. Мобильник под запретом. Ущемление прав человека или “закон есть закон”? URL:www.mobiset.ru/articles/text/?id=3280&printer=ok. (дата звернення: 19.10.2017)
206. 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.
207. Малик Я.Й. Інформаційна безпека України: стан та перспективи розвитку. Ефективність державного управління: Зб. наук. праць. 2015. Вип. 44. С. 13-20.
208. 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.
209. Марущак А. І. Інформаційне право України: Підр. К.: Дакор, 2011. 456 с.
210. Марущак А.І. Визначення поняття “інформаційні права людини”. Інформація і право. 2011. № 2(2). С. 21 – 26.
211. Марущак А.І. Інформаційне право: Доступ до інформації: Навч. посіб. К.: КНТ, 2007. 532 с
212. Марценюк О.Г. Теоретико-методологічні засади інформаційного права України: реалізація права на інформацію: дис. ... канд. юрид. наук : 12.00.07. К., 2009. 266 с.
213. Международное право: Учеб. для вузов / Отв. ред. проф. Г.В. Игнатенко и проф. О.И. Тиунов. М.: Изд. группа НОРМА-ИНФРА, 1999. 584 с., с. 359

214. Мельник С.В. Понятійно-категоріальний апарат у системі професійної підготовки майбутніх фахівців з кібербезпеки. Інформаційні технології і засоби навчання. 2016. Т. 55. №5. С. 187–197.
215. 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)
216. 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)
217. Міжнародна інформаційна безпека: Сучасні виклики та загрози / Макаренко Є.А., Рижиков М.М. та ін. Київ: Центр вільної преси, 2006. 916 с.
218. Монтескьє Ш.Л. О духе законов. М.: Мысль, 1999. 672 с.
219. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. Віче. 2007. №12. С. 23-25.
220. Мукомела І.В. Право на доступ до Інтернету: проблеми визначення та забезпечення. Вісник Національної академії правових наук України. – 2016. № 4. С. 77-85.
221. Мурашкевич О.А., Черних О.О. Освіта в сфері прав людини в Інтернеті: Метод. посіб. К.: ВАІТЕ, 2015. 70 с.
222. 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_Spivvidnoshennia_prava_na_svobodu.pdf (дата звернення: 06.09.2017)
223. 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.
224. Наливайко Л.Р. Інформаційна безпека та інформаційна політика в Україні: конституційно-правовий аспект. Вісник Запорізького державного університету. 2003. №1. С. 60-65.
225. Настюк В.Я., Белевцева В.В. Адміністративно-правовий захист інформації: проблеми та шляхи вирішення. Х.: Право, 2013. 128 с.
226. Национальный ИКТ-профайл Азербайджана. Часть 7: Информационная приватность URL: <https://digital.report/azerbaydzhan-informatsionnaya-privatnost/> (дата звернення: 19.10.2017)
227. Национальный ИКТ-профайл Армении. Часть 6: Информационная безопасность и защита информации URL: <https://digital.report/armeniya-informatsionnaya-bezopasnost/>(дата звернення: 19.10.2017)
228. 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)

229. Национальный ИКТ-профайл Молдовы. Часть 6: Информационная безопасность и защита информации. URL: <https://digital.report/moldova-informatsionnaya-bezopasnost/> (дата звернення: 19.10.2017)
230. Некрасов Н.А. Полное собрание сочинений и писем в 15-ти томах. Том 1. Л.: Наука, 1981. 719 с.
231. Нестеренко О. Інформаційний омбудсман в механізмі забезпечення прав людини і основоположних свобод. Бюлетень «Права людини». 2008. № 17. URL: <http://khp.org/index.php?id=1216383271> (дата звернення: 22.04.2015)
232. 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.
233. Німецькі поборники приватності углядели загрозу в соціальній мережі Facebook, а точніше в улюбленій користувачами кнопці like. URL: <http://briz.if.ua/9590.htm> (дата звернення: 08.09.2017)
234. 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)
235. 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.
236. О государственных секретах: Закон Республики Беларусь от 19.07.2010 р. № 170-3. URL: <http://www.kgb.by/ru/zakon170-3/printv>
237. О информации, информатизации и защите информации: Закон Республики Беларусь от 10 ноября 2008 г. № 455-3. URL: <http://pravo.by/document/?guid=3871&p0=h10800455>
238. О некоторых проблемах информационной безопасности. Ереван: НОФ «Нораванк», 2009. 236с.
239. 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
240. 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>
241. Общая политика США в сфере информационной безопасности URL: <http://www.INTUIT.ru>. (дата звернення: 25.12.2016)
242. 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.
243. Олійник О.В. Нормативно-правове забезпечення інформаційної безпеки в Україні. Право і суспільство. 2012. № 3. С. 132-137.
244. Олійник О.В. Теоретико-методологічні засади адміністративно-правового забезпе-

зпечення інформаційної безпеки України. Моногр. К., Вид. підпр-во «Український пріоритет», 2012. 400 с.

245. 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.
246. Орбан-Лембрик Л. Б. Соціальна психологія: Навч. посіб. К.: Академвидав, 2005. 448 с.
247. 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.
248. Осторожно: Кибербуллинг! URL:<http://darkermagazine.ru/page/ostorozhno-kiberbulling> (дата звернення: 18.09.2017)
249. Пазюк А.В. Міжнародно-правовий режим кіберпростору в мирний час Право і суспільство. 2014. № 1.2. С. 313-315.
250. Пазюк А.В. Інтеграція України в Європейське інформаційне суспільство виклики та завдання. К.: ФОП Клименко, 2014. 212 с.
251. Пазюк А.В. Правовий аналіз Указу Президента щодо блокування доступу до ресурсів Інтернету . URL:<http://moe-pravo.com.ua/pravoviy-analiz-ukazu-prezidenta-shhodo-blokovannya-dostupu-do-resursiv-internetu/> (дата звернення: 19.09.2017)
252. Пастернак-Таранушенко Г.А. Економічна безпека держави. Методологія забезпечення: Моногр. К.: Київ. екон. ін-т менедж., 2003. 320 с.
253. Пахнін М.Л. Особливості державної інформаційної політики в розвинених країнах світу. Теорія та практика державного управління. 2014. Вип. 4. С. 414-422.
254. Петрик В. Канарський Ю. Методи гібридної війни Росії проти України. Напрями протидії. Information Technology and Security. 2015. Vol. 3, № 1. С. 30-37.
255. 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.
256. 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.
257. Петрицький А.Л. Інформаційне законодавство України: актуальні проблеми та шляхи їх вирішення. Вісник Маріупольського державного університету. Серія: право. 2013. Вип. 5. С. 64-68.
258. Петров В.П., Петров С.В. Информационная безопасность человека и общества: учеб. пособ. М.: ЭНАС, 2007. 334 с.
259. Петров Є.В. Інформація як об'єкт правовідносин . Вісник Національного Університету внутрішніх справ; Спецвипуск. 2001. С. 249–252.
260. Плачинда С. Словник давньоукраїнської міфології. К.: Велес, 2007. С. 181–182.
261. Погребняк А.В. Технології комп'ютерної безпеки: Моногр. Рівне: МЕНГУ, 2011. 117 с.

262. Політанський В.С. Право на інформацію як фундаментальне право людини : Моногр. Х.: Право, 2017. 208 с.
263. 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)
264. 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)
265. Порухення права на приватність в Україні. URL: <http://forbidentoforbid.org.ua/uk/porushennya-prava-na-privatnist/> (дата звернення: 19.09.2017)
266. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2015. 216 с.
267. 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)
268. Потебня А.А. Эстетика и поэтика. М.,»Искусство», 1976. 614 с.
269. Потий О. Криптография, прошлое и настоящее. Служба безопасности. 2001. № 2-3. С. 30.
270. Почепцов Г. Гібридна війна: інформаційна складова. URL: http://osvita.mediasapiens.ua/trends/1411978127/gibridna_viyna_informatsiyua_skladova/ (дата звернення: 23.12.2017)
271. Права людей з інвалідністю. URL: <https://www.helsinki.org.ua/%2Fwp-content%2Fuploads%2F2016%2F02%2FPrava-lyudej-z-invalidnistyuu-Mojisa.doc&usg=AFQjCN GsLANQQivOhD7KsJh1JwTlgeWdgQ&sig2=w9fvh0rLbIib0-eB1VFj8g> (дата звернення: 19.09.2017)
272. Права людини в Криму. «Крим SOS». URL: <http://crimeamap.krymsos.com/ru/map.html> (дата звернення: 19.11.2017)
273. 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-potrnbno-zaprovadzhuвати-feysbuk-dentifikacyu-advokatv.html>. (дата звернення: 20.12.2016)
274. Правила адвокатської етики, затв. Звітно-виборним з'їздом адвокатів України 9.06.2017 р. URL: http://unba.org.ua/assets/uploads/3ae9a115a40b9a5bc04f_file.pdf (дата звернення: 19.08.2017)
275. Право на доступ до інформації: еволюція підходів Європейського суду з прав людини. URL: http://cedem.org.ua/analytics/pravo-na-dostup-do-informatsiyi-evolyutsiya-pidhodiv-yevropejskogo-sudu-z-prav-lyudyny/#_ftn2 (дата звернення: 19.02.2015)
276. Право на інформацію та реалізація інформаційних прав у сфері особистих немайнових прав людини в Україні / Є.В. Дергачов, О.О. Одинцова. Вісник Нац. техн. ун-ту України «Київський політехнічний інститут». Політологія. Соціологія. Право. 2013. № 2. С. 85-90.

277. Право природи в концепції римських юристів і Цицерона. Древнє право. IVS ANTIQVVM. 2009. № 1 (23).
278. 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)
279. Президент затвердив Доктрину інформаційної безпеки України URL: <http://ru.telekritika.ua/news/2009-07-08/46723> (дата звернення: 19.02.2015)
280. Про авторське право і суміжні права: Закон України від 23 грудня 1993 р. № 3792-12. ВВР України. 1994. № 13. Ст.64.
281. Про бібліотеки і бібліотечну справу: Закон України від 27 січня 1995 р. № 383-18. ВВР України. 2014. № 14. Ст.252.
282. 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.
283. 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.
284. Про внесення змін до Закону України «Про інформацію»: Закон України від 13.01.11 р. Офіційний вісник України. 2011. № 10. Ст. 2.
285. 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
286. Про державну таємницю: Закон України від 21.01.1994 р. ВВР України. 1994. № 16. Ст.93.
287. Про доступ до публічної інформації від 13.01.2011 № 2939-VI. ВВР України. 2011. № 32. Ст. 314.
288. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.1992 р. № 2782-XII. ВВР України. 1993. № 1. Ст. 1.
289. Про електронний цифровий підпис: Закон України від 22.05.2003 р. № 852-IV. ВВР України. 2003. № 36. Ст.276.
290. Про електронні довірчі послуги: Закон України від 5.10.2017 р. № 2155-VIII. ВВР України. 2017. № 45. Ст.400.
291. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. ВВР України. 2003. № 36. Ст.275.
292. 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.
293. Про запобігання корупції: Закон України від 14 жовтня 2014 року, № 1700-VII. ВВР України. 2014. № 49. Ст.2056.
294. Про засади інформаційної безпеки України: проект Закону України від 28.05.2014 р. № 4949. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JG3TH00A.html

295. 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>
296. 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.
297. 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>
298. 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.
299. Про захист дітей від інформації, що завдає шкоду їх здоров'ю та розвитку: Модельний закон від 03.12. 2009 р. № 33-15. URL: <http://jurconsult.net.ua/zakony-stran-sng>.
300. 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-телекомунікаційних системах). ВВР України. 1994. № 31. Ст.286.
301. 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>
302. Про зв'язок: Закон України (втратив чинність) від 16.05.1995 р. №160/95-вр. ВВР України. 1995. № 20. Ст.143.
303. Про інформацію : Закон України від 02.10.92 р. № 2657-12. ВВР України. 1992. № 48. Ст. 650.
304. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. № 75/98. ВВР України. 1998. № 27-28. Ст.182.
305. Про науково-технічну інформацію: Закон України від 25.06.1993 р. № 3322-ХІІ. ВВР України. 1993. № 33. Ст.345.
306. Про національний архівний фонд і архівні установи: Закон України від 24.12.1993 р. №3814-ХІІ. ВВР України. 1994. № 15. Ст.86.
307. Про Національну програму інформатизації: Закон України від 4.02.1998 р. № 74/98. ВВР України. 1998. № 27-28. Ст.181.
308. Про Національну раду України з питань телебачення і радіомовлення: Закон України від 23.09.1997 р. № 538/97. ВВР України. 1997. № 48. Ст. 296.
309. 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>

310. Про освіту: Закон України від 05.09.2017 р. № 2145-19. ВВР України. 2017. № 38-39. Ст. 380.
311. Про основи національної безпеки України : Закон України : від 19.06.2003 р. № 964-IV. ВВР України. 2003. № 39.
312. Про основні засади забезпечення кібербезпеки України: Закон України від 5.10.2017 р. № 2163-VIII. ВВР України. 2017. № 45. Ст.403.
313. 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.
314. Про охорону прав на винаходи і корисні моделі: Закон України від 15.12.1993 р. ВВР України. 1994. № 7. ст. 32.
315. Про радіочастотний ресурс України: Закон України від 1.06.2000 р. № 1770-III. Офіційний вісник України. 2000. № 26. Ст. 1079.
316. Про рекламу: Закон України від 3.07.1996 р. № 270/96-ВР. ВВР України. 1996. № 39. Ст. 181.
317. Про Суспільне телебачення і радіомовлення України: Закон України від 17.04.2014 р. № 1227-VII. Відомості Верховної Ради. 2014. № 27. Ст. 904.
318. Про телебачення і радіомовлення: Закон України від 21.12.1993 р. ВВР України. 1994. № 10. ст. 43
319. Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV. ВВР України. 2004. № 12. Ст.155.
320. Проект Закону про внесення доповнень до Цивільного кодексу України (щодо гарантування права фізичної особи на доступ до Інтернету) URL: http://w1.c1.gada.gov.ua/pls/zweb2/webproc4_1?pf3511=50669. (дата звернення: 19.08.2017)
321. 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.
322. Процик І. Як “витягнути” дитину з віртуального світу URL: <http://www.vn.20minut.ua/news/158911> (дата звернення: 19.06.2017)
323. Рабінович П.М. Межі здійснення прав людини (загальнотеоретичний аспект). Вісник академії правових наук України. 1996. № 6. С. 124–130.
324. Рада Європи рекомендує створити офіс інформаційного комісара в Україні. URL: <http://www.eurointegration.com.ua/news/2017/03/1/7062377/>
325. Рекомендація СМ/Рес(2014)6 Комітету міністрів Ради Європи державам- членам щодо посібника з прав людини для Інтернет-користувачів та пояснювальний меморандум. URL: <https://rm.coe.int/16802e3e96> (дата звернення: 19.10.2015)
326. Рівень розвитку інформаційно-комунікаційних технологій в Україні та світі. URL: <http://edclub.com.ua/analytika/riven-rozvytku-informaciyno-komunikaciynyh-tehnologiy-v-ukrayini-ta-sviti> (дата звернення: 23.10.2017)
327. Різак В.М. Правовий статус уповноваженого органу з питань захисту персональ-

них даних: досвід зарубіжних країн. Форум права. 2012. №3. С. 619-625.

328. Рогожа М. Моральнісні засади сучасності. Людина в лабіринті перспектив. К.: Парапан, 2004. С.119-139
329. Розпізнавання осіб: сховатися від поліції буде все складніше. URL: <https://ukr.media/science/210350/> (дата звернення: 19.10.2017)
330. 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)
331. Руссо Ж.Ж. Об общественном договоре, М.:»КАНОН-пресс», «Кучково поле», 1998. 416 с.
332. Савінова Н.А. Стратегії соціальних комунікацій як спосіб зниження соціальної напруги на макро-, мезо- та макрорівнях. Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. у 2 ч., ч.2. Київ, 18.03.2016 р. К.: Нац. акад. СБУ, 2016. 164 с.
333. Сапожников Е. И. Общество потребления в странах Запада. Вопросы философии. 2007. №10. С. 53-63.
334. Свобода інформації : навчальний посібник для державних службовців / пер. з англ. Р. Тополевського. К.: Тютюкін, 2010. 128 с.
335. 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.
336. Сегодня. Итоговая программа, 2 марта 2014 года URL: <http://www.ntv.ru/peredacha/itogovaya/m22900/o227537/> (дата звернення: 09.05.2014)
337. Сейд М. Концепция образования в исламе. Основы построения исламской философии образования. / пер. с англ. под ред. Кямилева С.Х. М.: Типография МПГУ, 2000. 67 с.
338. Семикіна М.В. Удосконалення підготовки професійних кадрів промисловості на засадах соціального партнерства. Проблема ефективного використання та професійно-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.
339. Сепир Э. Коммуникация. Избранные труды по языкознанию и культурологии. М.: Прогресс, 1993. 656 с.
340. Сергій Жадан: Мова ненависті — це мова слабаків URL: http://osvita.mediasapiens.ua/ethics/standards/sergiy_zhadan_mova_nenavisti_tse_mova_slabakiv/ (дата звернення: 03.10.2017)
341. Сидоренко Е.В. Личностное влияние и противостояние чужому влиянию. Психологические проблемы самореализации личности. СПб. : СПбГУ, 1997. С. 123–142.
342. 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)
343. Система. URL: <https://uk.wikipedia.org/wiki/система> (дата звернення: 13.01.2017)
344. Ситник Г. Безпека як інтегральна характеристика розвитку соціальних систем. Державне управління в Україні: реалії та перспективи: зб. наук. праць. К., 2005. – С. 278-282.
345. Ситник Г. Державне управління національною безпекою України. К.: Вид-во НАДУ, 2004. С. 69.
346. Сіденко В.Р. Нові глобальні виклики та їх вплив на формування суспільних цінностей. Український соціум. 2014. №1(48). С. 7-21.
347. Сіленко А. Цифрова нерівність як глобальна соціально-політична проблема. Політичний менеджмент. 2006. № 3. С. 51-62.
348. Сімочук О. Як видання регулюють поведінку журналістів у соцмережах. Телекритика. URL: <http://ua.telekritika.ua/society/kak-izdaniya-reguliruyut-povedenie-zhurnalistov-v-sotssetyah> (дата звернення: 10.08.2017)
349. Скакун О. Ф. Теорія права і держави: Підр. К.: Алерта; ЦУП, 2011. 524 с.
350. 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 (дата звернення: 04.09.2017)
351. Скляренко А., Ковалевський В. Хто виховує наших дітей? URL: http://www.unk.org.ua/publ/informacijna_bezpeka/khto_vikhovue_nashikh_ditej/34-1-0-251 (дата звернення: 11.04.2015)
352. Словарь философских терминов. Новейший философский словарь. URL: <http://www.philosophi-terms.ru/word/Система> (дата звернення: 09.09.2017).
353. Словник синонімів української мови URL: http://synonyms_uk.enacademic.com/ (дата звернення: 22.10.2017)
354. Собків Я. Класифікація інформаційних прав і свобод людини та громадянина. URL: <http://goal-int.org/klasifikaciya-informacijnix-prav-i-svobod-lyudini-ta-gromadyanina/> (дата звернення: 05.08.2017)
355. Солодка О.М. Щодо окремих організаційно-правових питань забезпечення інформаційної безпеки України URL: <http://stratcom.co.ua/shhodo-okremih-organizatsijno-pravovih-pitan-zabezpechennya-informatsijnoyi-bezpeki-ukrayini/> (дата звернення: 01.09.2017)
356. 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.
357. Соціологія: короткий енциклопедичний словник /під ред. В.І. Воловича ; Соціологічна асоціація України. Київ : Укр. Центр духовної культури, 1998. 736 с.
358. Спам в марте 2014. URL: http://www.securelist.com/ru/analysis/208050840/Spam_v_marte_2014 (дата звернення: 19.05.2015)

359. Спеціальні та галузеві соціології: Навч. посіб. 2-е вид. К.: Каравела, 2004. 350 с.
360. Створення єдиного реєстру фізичних осіб – це можливість для тотального стеження за людиною URL: <https://helsinki.org.ua/articles/stvorennya-jedynoho-rejestru-fizychnyh-osib-tse-mozhlyvist-dlya-totalnoho-stezhennya-za-lyudynoyu/> (дата звернення: 19.11.2017)
361. Стеценко В. Екзистенціалізм як «філософія людини» ХХ сторіччя. Соціо-манітарні проблеми людини. 2010. Вип.4. С.44-54.
362. Столяренко О. Міжнародні трансфери персональних даних. URL: <http://uba.ua/documents/events/2017/20170407/Presentations/StoliarenkoOleksii.pdf> (дата звернення: 19.08.2017)
363. Стратегія кібернетичної безпеки України, затв. Указом Президента України від 15 березня 2016 року № 96/2016. URL: <http://zakon3.rada.gov.ua/laws/show/96/2016>
364. 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)
365. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы. М.: МЦМНО, 2002. 296 с.
366. 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.
367. Сугестивні технологи 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.
368. Сухорольський П. Проблеми забезпечення та розвитку прав людини в умовах інформаційного суспільства. Український часопис міжнародного права. 2013. № 1. С. 21.
369. Талимончик В. П. Международно-правовое регулирование отношений информационного обмена. Спб. : Юридический центр-Пресс, 2011. 382 с.
370. Таран В. О., Зотов В. М., Резанова Н. О. Соціальна філософія: Навч. посіб. К.: Центр учбової літератури, 2009. 272 с
371. Тарнавська Т.В. Генеза поняття «система»: історичний огляд. Духовність особистості: методологія, теорія і практика. 2011. № 6 (47). С.130-139.
372. Татенко В.О. Соціальна психологія впливу: Моногр. К.: Міленіум, 2008. 216 с.
373. Тема номер один для журналістської спільноти – фізична безпека журналістів – Томіленко. URL: <http://procherk.info/resonance/2-cherkassy-news/51677-tema-omer-odin-dlja-zhurnaliststskoyi-spilnoti-fizichna-bezpeka-zhurnalistiv-tomilenko> (дата звернення: 03.09.2017)
374. Тер-Акопов А.А. Безопасность человека: социальные и правовые основы. М.: НОРМА, 2005. 272 с.
375. Тертишник В.М. Кримінальний процес України. Загальна частина: Підруч. Акад. вид. К.: Алерта, 2014. 440 с.

376. Тихий В. П. Поняття безпеки людини і її правове забезпечення. Вісник Асоціації кримінального права України. 2016. № 1(6). С. 21-40.
377. 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.
378. 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.
379. Тихомиров О.О. Інформаційні права людини як цивільно-правова категорія. Юридичний вісник. Повітряне і космічне право. 2015. № 1. С. 104-109.
380. 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.
381. 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)
382. Толковый словарь Ожегова. URL: <http://www.ozhegov-shvedova.ru/19-741515/СИСТЕМА> (дата звернення: 15.09.2017)
383. Толубко В.Б. Рось А.О. Складові інформаційної боротьби. Наука і оборона. 2002. № 2. С. 23 – 28.
384. Тофтул М. Г. Фома Аквінський. Сучасний словник з етики. Житомир: Вид-во ЖДУ ім. І. Франка, 2014. 416 с.
385. Требін М. Інформаційне суспільство. Війни нової епохи. Віче. 2002. № 4. С. 64–68
386. Требін М. П. «Гібридна» війна як нова українська реальність. Український соціум. 2014. № 3. С. 113-127.
387. Труфанов С.Н. Классическая теория познания Вильгельма Гегеля. URL: <http://www.hegel.ru/trufanov1.html> (дата звернення: 03.08.2017).
388. 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 (дата звернення: 19.10.2017)
389. Українська держава не оплачує мовлення в окупованому Криму — Муждабаєв /Перший український інформаційний. URL: <http://www.5.ua/окурасија-krimu/Ukrainskaderzhava-ne-oplachuie-movlennia-v-okupovanomu-Krymu-Muzhdabaiev-107352.html> (дата звернення: 19.10.2017)
390. Урсул А.Д. Устойчивое развитие и проблема безопасности. Информационный сборник «Безопасность». 1995. № 9. С. 47-51.
391. УСЕ. Універсальний словник-енциклопедія / Гол. ред. ради чл.-кор. НАН України М. Попович. К.: Ірина, 1999. 1551 с.
392. Фатьянов А.А. Тайна как социальное и правовое явление. Ее виды. Государство и право. 1998. № 6. С. 14–16.

393. Филипповский В. Сутність людини та її місце в сучасному світі URL: <http://h.ua/story/246400/> (дата звернення: 07.08.2017)
394. Философский энциклопедический словарь. М.:Сов. Энциклопедия, 1983. 840 с.
395. 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://itnopr.ostu.ru> (дата звернення: 03.08.2017)
396. Філософія. Навч. посіб. / За заг. ред. Ю.В. Осічнюка. К.: Атіка, 2003. 464 с.
397. Філософія: конспект лекцій: 3б. праць. К., 2012. 750 с.
398. Філософський словник / За ред. В. І. Шинкарука. К.: Голов. ред. УРЕ, 1986.
399. Фурашев В.М. Законодавче забезпечення інформаційної безпеки України Інформація і право. 2014. №1(10). С. 59-66.
400. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право. 2013. № 2(8). С. 113-119.
401. Халамендик В.Б. Інформаційна гігієна як фактор збереження психічного здоров'я людини. Гум. вісн. Запорізької державної інженерної академії. 2008. Вип. 35. С. 82-89.
402. 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 (дата звернення: 05.11.2016)
403. Хамзатов М.М. Влияние концепции сетецентрической войны на характер современных операций. Военная мысль. 2006. № 7. С. 13–17.
404. Ханін І. Г. Формування міжнародної системи інформаційної безпеки: економічні орієнтири для України URL: <http://www.m.nayka.com.ua/?op=1&j=efektyvna-ekonomika&s=ua&z=4457> (дата звернення: 12.09.2017)
405. Хартия прав интернета / Ассоциация прогрессивных коммуникаций URL: http://www.apc.org/sites/default/files/APC_charter_RU_1_2.pdf (дата звернення: 03.09.2017)
406. Хворост Х.Ю. Інформаційно-психологічний вплив у розрізі безпеки здоров'я. Наука і освіта. 2016. №2-3. с.184-191.
407. Химанен П., Кастелс М. Информационное общество и государство благосостояния. Финская модель М.: Логос, 2002. 224 с.
408. Хотіли як краще... Закон і Бізнес. 2017, 21-27 січ. № 3(1301). URL: <http://zib.com.ua/ua/127261-> (дата звернення: 22.03.2017) [v_ukraini_zakonodavcho_zakriplyuetsya_zvuzhennya_prav_advoka.html](http://zib.com.ua/ua/127261-v_ukraini_zakonodavcho_zakriplyuetsya_zvuzhennya_prav_advoka.html)
409. Хоффман Л.Дж. Современные методы защиты информации [пер. с англ.]. М: Советское радио, 1980. 57 с.
410. Цена свободы и безопасности – Индекс ИКТ-законодательств Евразии за 2016г. URL: <https://www.slideshare.net/VadimDryganov1/2016-73139338> (дата звернення: 03.09.2017)

411. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV. Офіційний Вісник України. 2003. № 11. Ст. 461.
412. 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.
413. Цимбалюк В. С. Суспільна мораль як різновид інформаційної безпеки. Правова інформатика. 2010. № 1(25). С. 23–29.
414. 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.
415. Черних О.О. Права людини в інтернеті як актуальний напрям роботи соціального педагога URL: <https://www.academia.edu/27680968> (дата звернення: 18.08.2017)
416. Чи є блокування інтернету «порушенням прав людини»? ООН вирішила, що так. URL: <http://ua.euronews.com/2016/07/05/un-denounces-disruption-of-internet-access-as-human-rights-violation> (дата звернення: 18.08.2017)
417. Что такое система? Значение и толкование слова sistema, определение термина / Толковый словарь Ушакова. URL: <http://www.onlinedics.ru/slovar/ushakov/s/sistema.html>
418. 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.
419. 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 року. Курськ : ЮЗГУ, 2010.
420. 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.
421. 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.
422. 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)
423. Шевчук С. Судовий захист прав людини. Практика Європейського суду з прав людини у контексті західної правової традиції. К.: Реферат, 2006. С. 424.
424. 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.
425. 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.

426. Шлімакова І. І. Феноменологія категорії впливу у вітчизняній психології. Вісник Чернігівського національного педагогічного університету. Серія : Психологічні науки. 2014. Вип. 121(2). С. 203-206.
427. Шопіна І. М. Адміністративно-правове регулювання управління органами внутрішніх справ України : дис. ... д-ра юрид. наук: 12.00.07 / ДНДІ МВС України. К., 2012. 514 с.
428. Шпенглер О. Закат Европы. Очерки морфологии мировой истории. Т. 1.: Гештальт и действительность. М.: Мысль, 1993. 663 с.
429. Щодня дивляться новини по телевізору 60% українців / Дослідження проводилося компанією R&B в період з 1-10 лютого 2017 року серед 1800 осіб по всій території України за винятком Криму та ОРДЛО. URL: https://dt.ua/UKRAINE/ukrayinci-dovigayaut-televizoru-v-dva-razi-bilshe-nizh-internet-zmi-235601_.html (дата звернення: 16.10.2017)
430. Щодо інформаційно-психологічної складової агресії Російської Федерації проти України (за результатами подій 1-2 березня 2014 року). Аналітична записка Національний інститут стратегічних досліджень URL: <http://www.niss.gov.ua/articles/1476/> (дата звернення: 28.03.2015)
431. Юридична психологія : Підруч. / Д.О. Александров та ін.; заг. ред. Л.І. Казміренко, Є.М. Моїсєєв. К.: КНТ, 2007. 359 с.
432. Юристи розглянули подробиці введення санкцій проти російських сайтів та соцмереж URL: <http://ukr.segodaya.ua/politics/society/yrusty-rassmotreli-podrobnosti-vvedeniya-sankciy-protiv-rossiyskih-saytov-i-socsetey-1021451.html> (дата звернення: 03.10.2017)
433. 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)
434. Ярочкин В.И. Информационная безопасность. М.: Междунар. отношения, 2000. 400 с.
435. Ярочкин В.И. Секьюритология – наука о безопасности жизнедеятельности. М.: Ось-89, 2000. 400 с.
436. Яценко В. А. Щуровський А. М. Національна та державна безпека : діалектика взаємозв'язку. Державна безпека України. 2004. № 1. С. 19-20.
437. «Східне партнерство» закінчилося катастрофою – глава МЗС Польщі URL: <http://www.eurointegration.com.ua/news/2016/01/29/7044114/> (дата звернення: 22.07.2017)
438. «Е-декларації – «наводка» для грабіжників» – голова Ради суддів у Вінниці URL: <http://www.judges.org.ua/dig11269.htm> (дата звернення: 13.10.2017)
439. «Інформаційний вибух» XXI століття, або Горе з розуму. URL: <http://for-ua.com/analytics/2012/11/26/084809.html> (дата звернення: 03.05.2017)
440. «Мова ворожнечі»: чи є протиріччя між професійним та громадянським обов'язком? URL: <http://detector.media/infospace/article/121803/2016-12-27-mova->

vorozhnechi-chi-e-protirichchya-mizh-profesiinim-ta-gromadyanskim-obovyazkom/ (дата звернення: 03.09.2017)

441. «Мова ворожнечі»: як не абсолютизувати ані її уникання, ані правомірного використання під час війни? URL: <http://detector.media/infospace/article/122037/2017-01-08-mova-vorozhnechi-yak-ne-absolyutizuvati-ani-ii-unikannya-ani-pravomirnogo-vikoristannya-pid-chas-viini/> (дата звернення: 03.09.2017)
442. «Мова ненависті» — мова забороненої правди. URL: <http://credo.pro/2016/07/161637> (дата звернення: 03.09.2017)
443. A comprehensive strategy on data protection in the European Union URL: http://epic.org/privacy/intl/eu_data_protection_directive.html. (Last accessed: 26.08.2017).
444. A Declaration on A Culture of Peace, UNESCO, A/Res/53/243. URL: www.unesco.org/cpp/uk/declarations/2000.htm.
445. An algorithm trained on emoji knows when you're being sarcastic on twitter URL: <http://www.businessinsider.com/this-algorithm-knows-when-youre-being-sarcastic-on-twitter-2017-8> (Last accessed: 10.08.2017).
446. Analysis and Implications of Laws / Cyberbullying Research Center URL: <http://cyberbullying.org/cyberbullying-laws>
447. Back to basics. Disinformation Review. 2017, 7 September. URL: <https://euvsdisinfo.eu/> (Last accessed: 09.10.2017).
448. Bailey K. Sociology and the New Systems Theory: Toward a Theoretical Synthesis. Albany: State University of New York Press, 1994. 372 p.
449. Becker K. Tactical Reality Dictionary, Cultural Intelligence and Social Control, Selene Verlag. Wien, New York: Autonomedia, 2002. URL: <http://world-information.org/trd> (Last accessed: 10.08.2017).
450. 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/ (Pobrano: 01.04.2015)
451. Buchanan L. Peter Drucker from A to Z. Inc. magazine. Retrieved 2012, 12 March.
452. Burke R. The Complling dialogue of Freedom. Human rights Quarterly: Human rights at the Bandung Conference. 2006. Vol. 28. s.962.
453. Butlin J. Our common future. Journal of International Development. London, Oxford University Press, 1987. pp. 284–287.
454. Cassirer E. An Essay on Man: An Introduction to a Philosophy of Human Culture, Yale & New Haven, 1944. 294 p.
455. Castells M. Siła tożsamosci. Warszawa, Wydawnictwo Naukowe PWN, 2009. 464 s.
456. Castells M. Społeczeństwo sieci. Warszawa, Wydawnictwo Naukowe PWN, 2013. 556 s.
457. Colvin M. Developing Key Privacy Rights. Oxford, Portland, Oregon : Hart Publishing, 2002. 198 p.
458. Communication from the Commission on a European Programme for Critical

- Infrastructure Protection (COM/2006/786 final). URL: Режим доступу: <http://eur-lex.europa.eu/> (Last accessed: 10.08.2017).
459. 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.
 460. 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/europe/2002/news_library/pdf_files/netsec_en.pdf (Last accessed: 10.08.2017).
 461. Compass: Manual For Human Rights Education With Young People URL: <http://www.coe.int/en/web/compass> (Last accessed: 07.06.2017)
 462. Complak K. Uwagi o godności człowieka oraz jej ochrona w świetle nowej Konstytucji. Przegląd Sejmowy. 1998, № 5 (28). s. 43.
 463. Council Decision 2008/0200 (CNS) on a Critical Infrastructure Warning Information Network (CIWIN), The Council of the EU. October 2008.
 464. 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)
 465. 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)
 466. Cyberbezpieczeństwo: dyrektywa NIS przyjęta, firmy w UE muszą spełnić nowe wymogi. URL: www.rp.pl/Bezpieczenstwo/307069909-Cyberbezpieczenstwo-dyrektywa-NIS-przyjeta-firmy-w-UE-musza-spelnic-nowe-wymogi.html#ap (Last accessed: 03.09.2017)
 467. Cyberbullying Activity: Laws. URL: <http://cyberbullying.org/cyberbullying-laws> (Last accessed: 22.09.2017)
 468. Data protection Eurobarometer URL: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf (Last accessed: 10.08.2017).
 469. 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 (Last accessed: 10.08.2017).
 470. Definition – What does Cyberlaw mean? URL: <https://www.techopedia.com/definition/25600/cyberlaw> (Last accessed: 10.08.2017).
 471. Digital Agenda for Europe 2020 URL: https://europa.eu/european-union/file/1497/download_en?token=KzfSz-C (Last accessed: 02.09.2017).
 472. Digital freedom: the case for civil liberties on the Net URL: http://news.bbc.co.uk/1/hi/special_report/1998/encryption/58154.stm (Last accessed: 10.08.2017).

473. 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).
474. Discussion Draft of the Cybersecurity Information Sharing Act of 2014, 113th Congress, 2d Session, June 11, 2014. S. 2588.
475. Donahoe E. Human Rights in the Digital Age. URL: <https://www.hrw.org/about/people/eileen-donahoe> (Last accessed: 02.04.2017)
476. Drucker P. The Future of Industrial Man. New York: The John Day Company, 1942. P. 205.
477. Drucker P. Landmarks of Tomorrow. New York: Harper & Row, 1957. 186 p.
478. Drucker P. Managing the Non-Profit Organization. New York: Harper Collins, 1990. 224 p.
479. 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-from-nonprofits> (Last accessed: 05.08.2017)
480. Drucker P. The Five Most Important Questions You Will Ever Ask About your Organization. San Francisco: Jossey-Bass, 2008. p. 19.
481. Security. English definition dictionary URL: <http://dictionary.reverso.net/english-definition/to%20provide%20security>
482. Erice Declaration on Principles for Cyber Stability and Cyber Peace, World Federation of Scientists, Aug. 2009. URL: www.ewi.info/system/files/Erice.pdf. (Last accessed: 02.04.2015)
483. 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.
484. EU: eEurope 2002 – An Information Society For All. Action Plan. URL: http://ec.europa.eu/information_society/europe/2002/documents/archiv_eEurope2002/actioplan_en.pdf39
485. EU: eEurope 2005 – An Information Society For All. Action Plan. URL: http://ec.europa.eu/information_society/europe/2005/all_about/action_plan/index_en.htm
486. 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
487. Europe 2005 Security Policies in Brief [Электронный ресурс] – Режим доступа URL: : http://ec.europa.eu/information_society/europe/2005/all_about/security/index_en.htm.
488. 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
489. 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.
490. Evaristo, Adams & Curley. Information Load Revisited: A Theoretical Model URL: <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1061&context=icis1995> (Last accessed: 03.10.2015).
491. 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).
492. Facebook отключил искусственный интеллект после «диалога» ботов на своем языке. URL: <http://www.dsnews.ua/future/facebook-otklyuchil-iskusstvennyy-intellekt-posle-dialoga-botov-01082017132500> (Last accessed: 15.10.2017).
493. 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).
494. Figure of the Week: 50 million euros. URL: <https://euvsdisinfo.eu/figure-of-the-week-50-million-euros/> (Last accessed: 05.03.2015).
495. Frank T. Catsouras v. Department of California Highway Patrol. Point of Law. 2010, May 10.
496. Garlicki L. Polskie prawo konstytucyjne. Warszawa 2003. S. 85.
497. General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) on 2016, 14 April. URL: <https://www.eugdpr.org/>
498. Georgia: Can Democracy Thrive Without Opposition? 2017, April 5. URL: <http://www.eurasianet.org/node/83116> (Last accessed: 15.10.2017).
499. 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).
500. Github URL: <https://github.com/project-open-data/project-open-data.github.io/issues> (Last accessed: 15.10.2017).
501. Glendon M., A Wourld Made New. Eleanor Roosevelt And The Universal Declaration Of Human Rights. New Yoork, 2001. S.15.
502. Green Paper on a European Programme for Critical Infrastructure Protection, The European Commission. Brussels. 2005.
503. Green Paper. Living and Working in the Information Society: People First. European Comission. Brussels. 1996.
504. Gross B. M. The Managing of Organizations. The Administrative Struggle. 1964. Vol. 2. P. 856.
505. Guardchild: Protecting children in the digital age. URL: <https://www.guardchild.com/statistics/>
506. Hartmann F. H. The relations of nations. London: Macmillan, 1962. 710 p.
507. Hemp P. Death by information overload. Harvard Business Review. 2009. № 87(9). Pp. 83–89.

508. Henkin L. Human rights. New York, Foundation Press, 1999. P. 302-306.
509. 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).
510. 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.
511. 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 Інформаційна агресія як невідемна складова ведення гібридної війни] URL: <https://sci.lidubgd.edu.ua/bitstream/handle/123456789/3198/8.pdf?sequence=1&isAllowed=y>.
512. 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-asked-thousands-of-kids-around-the-world-67940> (Last accessed: 15.11.2016).
513. 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-teen-girl-was-pregnant-before-her-father-did/#f13e1ad34c62>
514. Hybrid Warfare URL: <http://www.gao.gov/assets/100/97053.pdf> (Last accessed: 15.10.2017).
515. Ignatieff M. Human rights. The Midlife Crisis. The New York Review of Books. 1999, March 20. S.59.
516. INHOPE: the International Association of Internet Hotlines. URL: <http://www.inhope.org> (Last accessed: 15.10.2017).
517. International Organization for Standardization. URL: <http://www.iso.org> (Last accessed: 15.10.2017).
518. Internet Access Is Now A Basic Human Right. URL: <http://gizmodo.com/internet-access-is-now-a-basic-human-right-1783081865> (Last accessed: 02.03.2017).
519. Izdebski H. Fundamenty współczesnych państw. Warszawa, 2007. S. 28.
520. Justynian. Instytucje. Warszawa, 1986. S. 17.
521. 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).
522. 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.
523. Kolarzowski J. Powszechna Deklaracja Praw Człowieka — historycznym przełomem. Biuletyn Olimpiady Filozoficznej. 1994. № 7. URL: <http://www.racjonalista.pl/kk.php/s,4710> (Pobrano: 24.03.2015)

524. Kowalski R, Limber S., Agatston P. *Cyber bullying: bullying in the digital age*. Oxford: Blackwell Publishing Ltd, 2008. 218 p.
525. Krąpiec M. A. *O ludzką politykę*. Warszawa, 1996. S. 139-140.
526. Kuhse H., Singer P. *Should the Baby Live? The Problem of Handicapped Infants*, Oxford University Press, 1985. 228 p.
527. Kuźniar R. *Prawa człowieka*, Warszawa, 2008. S. 22.
528. 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.)
529. Le Bon G. *Psychologia tłumy / tł. z fr. Bolesław Kaprocki. Kęty : ANTYK*, 2004. 95 s.
530. *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 (Last accessed: 15.10.2017).
531. Lesiński B., Rozwadowski W. *Historia prawa*, wyd. IV. Warszawa-Poznań, 1985. S. 22.
532. Liderman K. *Bezpieczeństwo informacyjne*. Warszawa, Wydawnictwo Naukowe PWN, 2012. 216 s.
533. Liedel K. *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*. Toruń: Wyd-wo Adam Marszałek, 2014. 96 s.
534. Linton S. *Claiming Disability Knowledge and Identity*. New York: New York University Press, 1998. P. 9.
535. Livingstone S. *Young People and New Media: Childhood and the Changing Media Environment*. London: Sage, 2002. 275 p.
536. 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_
537. Maryniarczyk A. *Dekalog a prawo naturalne. Człowiek w kulturze*. 1994. №3. S. 133-150.
538. Masuda Y. *Computopia*. Oxford, 1985. URL: <http://connection.ebscohost.com/c/articles/12608885/vision-computopia> (Last accessed: 15.10.2017).
539. Masuda Y. *Hypothesis on the genesis of homo intelligens*. *Futures*. Guilford, 1985. Vol. 17. № 5. P. 479-494.
540. Masuda Y. *The Information Society as Postindustrial Society*. Wash.: World Future Soc., 1983. 320 p.
541. *Materiały dydaktyczne do przedmiotu: Prawa człowieka*. URL: <http://bip.ms.gov.pl/> (Pobrano: 23 marzec).
542. Mendel T. *Freedom of information: A Comparative legal survey*. Paris, UNESCO Publ., 2008. 176 p.
543. *Merriam-Webster's Collegiate Dictionary*. Eleventh edition. Merriam-Webster, 2003. 1664 p. URL: <http://www.merriamwebster.com/dictionary/system>
544. *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.

545. 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).
546. 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/legalcontent/en/TXT/%3Furi%3DCELEX%253A32016L0680&p rev=search>
547. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) : Reglment (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016. URL: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>
548. 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-eu-pnr-directive/&prev=search>
549. Osiatyński W. Historia i filozofia praw człowieka. URL: <http://www.hfhr.pl/publikacje/czym-sa-prawa-czlowieka/#sthash.yW2nvApZ.dpuf> (Pobrano: 22.03.2015)
550. Osiatyński W. Prawa człowieka i ich granice. Kraków: Znak, 2011. 371 s.
551. Pacem in Terris. URL: http://www.opoka.org.pl/biblioteka/W/WP/jan_XXIII/encykliki/Pacem_In_Terris_11041963.html (Pobrano: 02.04.2015)
552. Pollitt and Bouckaert, Christopher and Geert. Public Management Reform. New York: Oxford University Press, 2011. p. 38.
553. Powszechna encyklopedia filozofii. T. 9. (2008): Se-Ż. S. 1009.
554. Pyżalski J. Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży. Kraków, 2012, 318 s.
555. Rapaczynski A. Popular Sovereignty and the Concept of Representation. The Relevance of American Costitutionalism in Eastern Europe. International Journal of Sociology, Vol. 26. № 4. P. 7-16.
556. 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)
557. 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 (Last accessed: 15.10.2017)
558. 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)
559. Sartre J.-P. Being and Nothingness. N.Y., 1965., p. 529.
560. Sen A. Human Rights and Asian Values. New York, 1997. P. 171-193.
561. Shawn H. WCAG 2.0 is now also ISO/IEC 40500!. World Wide Web Consortium. 2012. October 15.
562. Śmietana T. Początki praw człowieka. URL: <http://www.tolerancja.pl/?historia-praw-czlowieka,257> (Pobrano: 22 marzec 2015)
563. Solove D.J. Understanding Privacy. Cambridge: Harvard University Press, 2008. 272 p.
564. 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).
565. Stone L. Extracting Signal from Noise in Social Networking. – Режим доступа : // www.research.microsoft.com/en-us/um/redmond/events/scs2005
566. Study: 80 percent of children under 5 use Internet weekly URL: <http://content.usatoday.com/communities/technologylive/post/2011/03/study-80-percent-of-children-under-5-use-internet-weekly/1> (Last accessed: 15.02.2014).
567. Stylianidis E. Antyczna cywilizacja grecka a prawa człowieka. Prawa człowieka, geneza, koncepcje, ochrona / red. Banaszak B. Wrocław: Wydawn. Uniwersytetu Wrocławskiego, 1993. S. 122.
568. 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)
569. Szusc J. Three historical Regions of Europe, 1981. [cyt. Osiatyński, W. Prawa człowieka i ich granice Kraków: Znak, s. 25]
570. The Blue Brain Project – A Swiss Brain Initiative URL: <http://bluebrain.epfl.ch/>(Last accessed: 08.10.2017).
571. The Cybersecurity Act of 2009. URL: <https://www.congress.gov/bill/111th-congress/senate-bill/773/summary/00> (Last accessed: 08.04.2017).
572. The Directive on security of network and information systems (NIS Directive) URL: <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive> (Last accessed: 08.10.2017).
573. The Global Information Infrastructure Commission URL: <http://giic.org/about/> (Last accessed: 02.04.2017).
574. 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 (Last accessed: 15.10.2017).
575. The Susan Mbarek Women’s International Peace Movement, The Cyber Peace Initiative. URL: <http://smwipm.cyberpeaceinitiative.org/> (Last accessed: 22.11.2017).
576. Thomae de Aquino. Summa theologiae, I, q. 76, a. 1. URL: <http://www>.

- corpusthomicum.org/sth1075.html (Last accessed: 22.10.2015).
577. Toffler A. *Future Shock*. USA, Random House, 1970. P. 576.
578. Toffler A. *The Third Wave*. N.Y.: William Morrow & Company, 1980. 544 p.
579. *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).
580. 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. (Last accessed: 12.04.2016).
581. UN General Assembly Resolution 217 A (III) 10.12. 1948. Материалы ЮНЕСКО об информационном обществе. ЮНЕСКО, 2003.
582. Verdict in MySpace Suicide Case URL: <http://www.nytimes.com/2008/11/27/us/27myspace.html> (Last accessed: 02.10.2015).
583. Wallerstein I. *Analiza systemów-światów. Wprowadzenie*. Warszawa, 2007. 160 s.
584. Warren S., Brandeis L. *The Right to Privacy*. Harvard Law Review. Dec. 15, 1890. Vol. 4. № 5. P. 193-220.
585. Webster F. *Theories of The Information Society*. London and New York, 1995. P. 22.
586. 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).
587. *White Paper. The Challenges and Ways Forward into the 21s Century*. Brussels, 1993.
588. *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-ceo-explains-its-employee-microchip-implant.html> (Last accessed: 05.08.2017).
589. Willard N. *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*. Champaign: Research Press, 2007. 311 p.
590. Wojtyła K. *Miłość i odpowiedzialność. Seria Człowiek i moralność*. Lublin, 1982. S. 42-43.
591. *World Internet Users and Population Stats*. URL: www.internetworldstats.com/stats.htm (Last accessed: 15.10.2017).
592. Wroczyński K. *O źródłach treści praw człowieka. Człowiek w kulturze*. 1998. № 11. S. 161-176.
593. Wrzoch W. *Wszystko, co musisz wiedzieć o handlu wirtualnymi dobrami w grach*. URL: <http://www.komputerswiat.pl/artykuly/redakcyjne/2013/11/handel-wirtualnymi-dobrami-w-grach.aspx> (Pobrano: 10.05.2015).
594. Zięba R. *Instytucjonalizacja Bezpieczeństwa europejskiego*. Warszawa; Scholar, 2001. 406 s.
595. Zolotar O. *Społeczeństwo informacyjne a bezpieczeństwo: kwestie teoretyczne i polityczno-prawne na przykładzie Polski, Ukrainy i Rosji*. *Wschodnioznawstwo*. 2015. № 1. Ss. 361-374.

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

Ольга Золотар

**ІНФОРМАЦІЙНА БЕЗПЕКА ЛЮДИНИ:
ТЕОРІЯ І ПРАКТИКА**
(Монографія)

Формат 60*84/16

Папір офсетний. Друк цифровий. Гарнітура Times New Roman.

Умовн.-друк.арк.25,92, Обл.-вид.арк. 22,9.

Замовлення № Д-0223-877

Підисано до друку 09.02.2018р.

Виготовлено в друкарні

ТОВ «Видавничий дім «АртЕк»

04050, м. Київ, вул. Мельникова, буд. 63

Тел. 067 440 11 37

artek.press@ukr.net

www.artek.press

Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції –
серія ДК №4779 від 15.10.14р.

АртЕк
видавничий дім