Міністерство освіти і науки України
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Навчально-науковий інститут фінансів, економіки, управління та права
Кафедра публічного управління, адміністрування та права

**Кваліфікаційна робота**

на тему: **«УДОСКОНАЛЕННЯ СИСТЕМИ ПУБЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УКРАЇНІ»**

**Виконав:**
студент академічної групи 201м – ДС
освітньо-професійної програми
«Публічне управління та адміністрування»
другого (магістерського) рівня вищої освіти
спеціальності 281
«Публічне управління та адміністрування»
_____ Бондарєв В.В.
**Науковий керівник:**
професор кафедри публічного управління,
адміністрування та права, доктор
наук з державного управління, професор
_____ Лахижа М.І.

Полтава – 2021 рік

**ЗМІСТ**

# ВСТУП

*Актуальність дослідження.* Національна безпека кожної країни в умовах сьогодення більш за все спрямована на протидію інформаційним атакам і загрозам будь-яким в інформаційній сфері, адже це рушій і економіки, і політики і усіх інших сфер. Світ стоїть на порозі побудови глобального інформаційного суспільства. Глобальна інформаційна інфраструктура забезпечує безпрецедентні можливості для спілкування між людьми, їх соціалізації та доступу до інформації. Відповідно, це стає вагомою загрозою для національної безпеки будь-якої країни, особливо нашої, адже воєнний конфлікт з боку Російської Федерації проти України вже триває понад 5 років. І всі ці роки наша держава стикається з інформаційними викликами, які становлять велику загрозу для нашої національної безпеки.

Це стало значним стимулом для початку переоцінки країнами Європейського Союзу діючих правил та принципів забезпечення безпеки в інформаційній сфері. Особливо це помітно на прикладі країн Центральної та Північної Європи, які зважаючи на своє географічне положення та геополітичні цілі вищого керівництва Російської Федерації, знаходяться в зоні постійного впливу з боку Москви. Сьогодні уряди багатьох країн даного регіону намагаються адаптувати систему національної безпеки до нових викликів, зокрема інформаційних, що наявні в сучасних умовах.

Зростання темпів впровадження інформаційно-комунікаційних технологій в галузі державного управління суттєво впливає як на якісні та кількісні показники складових елементів інформаційних процесів, так і на саму інформацію. Використання цифрових технологій та технічних засобів комунікації виявляє не тільки переваги, а й відкриває нові проблеми, пов’язані із організацією питань безпеки інформаційних процесів, в першу чергу, таких, як: отримання, передавання, оброблення та зберігання інформації.

У сучасних умовах система забезпечення інформаційної безпеки України, яка склалася раніше, не відповідає новим принципам Стратегії національної безпеки України й не може ефективно протидіяти новим інформаційним загрозам. Проблема провадження інформаційної безпеки в сучасних умовах агресії проти України з боку Російської Федерації зумовлена особливою роллю інформації у функціонуванні всіх сфер суспільного життя, оскільки саме інформаційні фактори набувають більшої значущості в контексті захисту національних інтересів.

В процесі розбудови цифрового суспільства виникають важливі питання щодо організації та гарантування безпеки інформації на всіх етапах її використання та користування при здійсненні інформаційних процесів. А це може забезпечити тільки держава, яка має для цього усі необхідні інструменти, важелі та можливості.

Тому проблематика удосконалення системи публічного управління інформаційною безпекою є важливою та необхідною.

*Стан наукового дослідження.* Проблематика правового забезпечення інформаційної безпеки України у різний час розглядалася багатьма вченими різних правових наук, зокрема: Ю.О. Бондар, О.В. Глазовим, В.Ю. Світличною, О.О. Грицун, І.І. Залевською, С.В. Шавановим та ін. Інформаційну безпеку з точки зору науки державного управління розглядали В.М. Дрешпак, О.С. Зозуля, І.В. Клименко, В.К. Кожах, К.О. Линьов, О.А. Панченко, А.І. Семенченко, Г.П. Ситник, А.В. Турчак, С.А. Чукут та інші.

*Мета й завдання дослідження*. Мета дослідження полягає в детальному дослідженні сучасного організаційно-правового забезпечення інформаційної безпеки та виробленні на основі здійсненого аналізу узагальнень щодо його удосконалення.

Для досягнення зазначеної мети поставлені наступні завдання:

– встановити поняття та принципи інформаційної безпеки;

– здійснити ретроспективний огляд історії формування та розвитку інформаційної безпеки в Україні;

– охарактеризувати сучасний стан правового регулювання інформаційної безпеки в Україні;

– розкрити поняття та види загроз національної безпеки;

– охарактеризувати особливості існування інформаційної безпеки в умовах глобалізації

– виокремити основні напрямки забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

– зробити висновки та узагальнення по досліджуваній темі та запропонувати власні пропозиції та рекомендації щодо удосконалення організаційно-правових механізмів забезпечення інформаційної безпеки України

– запропонувати пріоритетні напрямки оптимізації державних інформаційних ресурсів в контексті реалізації державної політики в сфері інформаційної безпеки;

– визначити перспективні шляхи вдосконалення щодо забезпечення інформаційної безпеки органів влади в умовах цифровізації.

*Об'єктом дослідження* є суспільні відносини, що складаються у сфері організаційно-правового забезпечення інформаційної безпеки в Україні.

*Предметом дослідження* виступає публічне управління інформаційною безпекою в Україні.

*Методи дослідження.* Методологічним підґрунтям дослідження є діалектичний метод наукового пізнання, що відображає взаємозв'язок теорії та практики, а також концептуальні положення правової науки. У процесі здійснення цього дослідження застосовувалися загальнонаукові та спеціальні методи дослідження, зокрема: системно-структурний – для розбудови внутрішньої структури інформаційної безпеки; функціональний – для аналізу динаміки розвитку правового регулювання та окремих елементів інформаційної безпеки; формально-логічний – для визначення та аналізу проблемних аспектів вказаної проблематики; аналізу та узагальнення – для аналізу та узагальнення матеріалу із зазначеної теми.

*Теоретичну основу дослідження* становлять праці вчених та дослідників науки державного управління, а також юридичної та економічної науки.

*Правову базу дослідження* становлять Конституція України, закони України, підзаконні нормативно-правові акти.

*Наукова новизна дослідження* полягає у систематизації та узагальненні проблематики публічного управління інформаційною безпекою через призму сучасної літератури та законодавства та детальному розкритті сучасного організаційно-правового забезпечення інформаційної безпеки як складової національної безпеки України з виробленням ефективних шляхів його вдосконалення. Зокрема:

– запропоновано авторське визначення інформаційної безпеки під якою пропонується розуміти комплекс умов, при яких можлива захищеність життєво важливих інтересів держави, суспільства та окремого індивіда в інформаційній сфері, яка відображається в чотирьох аспектах: ціннісному (відсутність негативного впливу на громадську думку), технологічному (кібербезпека); правовому (розвиненість законодавства, що регулює правовідносини в інформаційній сфері); соціально-політичному (відсутність політичної цензури, вільний доступ до публічної інформації);

– удосконалено визначення інституту міжнародної інформаційної безпеки як міжгалузевого інституту, що представляє собою особливий і відокремлений комплекс норм, який регулює міжгалузеву сферу відносин;

– запропоновано авторське визначення загрози національній безпеці як можливої небезпеки, що має здатність причинити будь-яку шкоду, призвести до збитків, втрат (матеріальних і людських) або інших негативних наслідків;

– наведена авторська класифікація загроз національної безпеки за двома критеріями: 1) за джерелом виникнення на зовнішні та внутрішні загрози; 2) за сферою дії на загрози національній безпеці в політичній, технологічній, економічній, екологічній і т. д. сферах;

– пропонується авторське розуміння інформаційних загроз як систему зовнішніх та внутрішніх чинників, що чинять згубний вплив на інформаційну безпеку, зачіпаючи життєво важливі інтереси держави, суспільства та людини в інформаційній сфері;

– доведена доцільність створення окремої структури, діяльність якої буде направлена на включення представників такого органу в управлінський процес, використання їх «інтелектуального та експертного ресурсу» для досягнення безпекових цілей в інформаційній сфері, аналітичний супровід політики уряду.

*Практичне значення одержаних результатів.* Викладені в роботі висновки і пропозиції можуть бути використані у науково-дослідницькій роботі, зокрема для подальшого розвитку досліджень публічного управління інформаційною безпекою в Україні. Матеріали дослідження було презентовано автором на VIII Всеукраїнській науково-практичній конференції за міжнародною участю 29 квітня 2021 року (Додаток А).

*Структура та обсяг роботи.* Робота складається із вступу, трьох розділів, дев’яти підпунктів, висновків, списку використаних джерел до кожного розділу, а також додатків. Загальний обсяг роботи складає 137 сторінки. Список використаних джерел розміщений на 12 сторінках та містить 104 найменування.

# РОЗДІЛ 1
# ОРГАНІЗАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

## 1.1. Поняття та принципи забезпечення інформаційної безпеки

Відповідно до положень Закону України «Про національну безпеку України», національна безпека України це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [67].

З даного визначення стає зрозумілим, що подолати будь-яку систему безпеки, зокрема національну, можливо трьома основними способами: 1) посилити тиск за напрямами, проти яких спрямована система безпеки; 2) знайти та створити такі загрози, проти яких система безпеки не спрацює; 3) змінити систему інтересів, а відповідно і комплекс загроз, щоб нейтралізувати дії системи безпеки.

Ю.О. Бондар з цього приводу слушно зазначає, що система забезпечення національної безпеки не є самостійним об'єктом інтересу з боку зовнішніх або внутрішніх загроз. Потужність системи національної безпеки у спроможності протистояти загрозам [7].

Національна безпека і її складова – інформаційна безпека, являють собою складний суспільний процес, що постійно розвивається, залежно від стану і характеру суспільства, суспільних відносин, діючих концепцій, існування протилежних точок зору. Однак, чітко прослідковується взаємозалежність: чим більш розвиненим є суспільство, тим стабільнішою, стійкішою до загроз є система національної безпеки в інформаційній сфері.

Особливості національної безпеки держави розкривають зміст функціонування суспільства і держави, визначають сучасний стан і тенденції до змін суспільства.

Питання інформаційної безпеки як складової національної безпеки викликано розвитком інформаційних технологій, техніки та збільшенням кількості конфліктів між державами. Ще за часів так званої «холодної війни» інформація, та інформаційні системи залишилися дієвим інструментом впливу одних держав і народів на інші.

Найбільш цілісним, з нашої точки зору, є розуміння безпеки як стану, при якому суб'єкт не піддається дії зовнішніх та внутрішніх загроз, що можуть мати негативний вплив на нього; це надійний захист від небезпечних чинників.

Якщо розглядати категорію національної безпеки, то в сучасних умовах доцільно виділяти три цілісних підходи щодо визначення національної безпеки держави. Представники першого підходу акцентують свою увагу на розумінні національної безпеки як системи захист у цінностей суспільства. Серед базових суспільних цінностей вони виділяють суверенітет, сталий економічний розвиток, дотримання прав людини та громадянина, справедливість тощо. Більше того, безпека розглядається не тільки як стан захищеності цінностей, але і як процес їх поширення.

Другий підхід полягає у вивченні національної безпеки у розрізі захисту національних інтересів.

Третій підхід вказує на стійкий взаємозв'язок між категоріями суспільних цінностей та національних інтересів, потребі розуміння їх взаємообумовленості у вивченні сутності та природи національної безпеки держави [12, с.45-46].

Вважаємо доцільним брати за основу третій підхід, поза як національні інтереси як базова категорія в системі національної безпеки держави і захист суспільних цінностей є взаємодоповнюючими елементами загального концепту безпекової політики держави. Забезпечення національних інтересів (воєнно-політичний суверенітет, сталий соціально-економічний розвиток, збереження економічний розвиток, збереження конституційного ладу) та збереження цінностей соціуму (які власне і зберігають його цілісність та можливість розвиватися в подальшому) є ключовою метою державного керівництва в модерному глобалізованому світі.

Розгляд основних підходів дав змогу провести групування наявних визначень інформаційної безпеки.

Перш за все слід чітко визначити основні ракурси з яких варто розглядати дане поняття:

По-перше, інформаційна безпека сприймається як захист інформаційного простору країни від зовнішніх негативних чинників на всіх рівнях (індивідуальному, суспільному, державному).

По-друге, як стан не тільки інформаційного, а й соціально-політичного простору, коли дотримується безпека індивіда, соціальних груп та країни у цілому. В даному контексті мова йде в основному про захист суспільства від пропаганди, маніпуляцій громадською думкою, поширення агресивних та провокаційних гасел / ідей / лозунгів і т. д.

По-третє, як право на отримання необхідних інформаційних ресурсів [80].

Сьогодні, в наукових колах умовно сформовані три підходи до трактування сутності інформаційної безпеки:

1)правовий – визначає сутнісну природу інформаційної безпеки з точки зору її позиціювання в законодавчих актах та нормативних документах;

2)доктринальний – аналізує сутність інформаційної безпеки, зважаючи на наявні в науковій думці теоретичні концепти та дослідницький доробок вітчизняних та зарубіжних вчених;

3)енциклопедичний – грунтується на формалізованому розумінні інформаційної безпеки зважаючи на її трактування в енциклопедичних матеріалах та словниках [81, с. 97].

Виділення правових основ інформаційної безпеки (так само, як і їх вироблення та застосування) ґрунтується на правовому та науковому визначенні самого цього поняття. Аналізуючи не лише дефініції, що відображенні у науковій, науково-методичній та енциклопедичній літературі, а й у правових документах (міжнародного та національного масштабів), ми побачимо величезну кількість визначень інформаційної безпеки, які відображають багатоаспектність та складність цього поняття. Одні правничі наукові школи зосередженні на

розумінні та правозастосуванні інформаційної безпеки як частини інформаційних відносин, інший підхід апелює до безпекових студій та військової науки, розглядаючи інформаційну безпеку як частину загальної безпеки держави (Рис.1.1)


Рис 1.1- Сфери застосування інформаційної безпеки державного управління (побудовано автором на основі законодавства)

Представляючи перший підхід, В. Цимбалюк характеризує інформаційну безпеку як «стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації» [94, с. 204]. Доповнює розуміння Р. Калюжний, який вбачає у цій категорії «вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності» [37, с. 234-235].

Дослідники Л. Задорожня, М. Коваль В. Брижко, наголошуючи на актуальності проблеми законодавчого врегулювання питань інформаційної безпеки визначають: «Інформаційну безпеку можна розуміти, з одного боку, як безпосередньо захист інформації, і особливо – захист таємниці, комерційної інформації, інформації з обмеженим доступом, персональних даних тощо, з

іншого – як захист інформаційних систем, які фактично є засобом передачі інформації» [32, с. 27].

На противагу ним, Л. Харченко, В. Ліпкан, О. Логінов визначають, що інформаційна безпека постає як «складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України» [92, с. 65]. Інформаційна безпека України, згідно тотожної позиції І. Громико та Т. Саханчук, також виступає, як захищеність державних інтересів, за якої забезпечується запобігання, виявлення і нейтралізація внутрішніх та зовнішніх інформаційних загроз, збереження інформаційного суверенітету держави і безпечний розвиток міжнародного інформаційного співробітництва [18, с. 130-134].

Прибічники широкого розуміння проблем інформаційної безпеки розглядають цю сферу діяльності не тільки крізь призму інформаційних відносин, а і через систему державно-управлінської діяльності. Так, В. Ліпкан в процесі аналізу системи забезпечення інформаційної безпеки констатує, що «основу даної системи складають органи, сили та засоби забезпечення інформаційної безпеки, які використовують систему адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління» [47, с. 219-220]. Дослідниця А. Нашинець-Наумова також зауважує, що «інформаційна безпека українського суспільства як важлива складова національної безпеки передбачає системну превентивну діяльність органів державної влади по наданню гарантій інформаційної безпеки особі, соціальним групам і суспільству в цілому і спрямована на досягнення достатнього для розвитку державності та соціального прогресу рівня духовного та інтелектуального потенціалу країни» [54, с.125].

М. Дмитренко, як і багато інших дослідників сучасної держави, звертає увагу на те, що нині жодна сфера життя не тільки окремих суспільств і держав, але і усього світового співтовариства не може функціонувати без розвинутої

інформаційної структури, що в процесі формування інформаційного суспільства, яке є не тільки основою процвітання а також, що саме через інформаційне середовище генеруються та втілюються загрози національній безпеці держави. Зазначається, що ефективно протистояти інформаційним загрозам у сучасних умовах може лише добре організована державна система забезпечення інформаційної безпеки, що повинна здійснюватися при повній взаємодії всіх державних органів, недержавних структур і громадян [29, с. 391].

Науково-правові дослідження не виробили загальноприйнятого механізму визначення та структуризації забезпечення інформаційної безпеки. У такій структурі могли би бути визначальними напрями, механізми та шляхи забезпечення. Однак, на думку О. Тихомирова, «саме розуміння забезпечення інформаційної безпеки як комплексного виду діяльності дозволяє гармонізувати термінологію і здійснювати не лише структурний, а й глибокий змістовний аналіз, повною мірою застосовуючи потенціал діяльнісного підходу» [88, с. 165].

Юридична енциклопедія за редакцією Ю. Шемшученка представляє подібний агрегований синтетичний підхід до інформаційної безпеки. Так, дослідник визначає її «як один з різновидів національної безпеки і функцію держави, котрі сумарно означають: «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»; «підтримку 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»; «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 з іноземними державами»; «законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України» [44, с. 714-715].

Отже, інформаційна безпека є феноменом, що одночасно належить до сфери правової регламентації державної інформаційної політики та сфери нормативного регулювання політики в галузі безпеки держави. Цілком виправданим видається і правове розуміння державної інформаційної політики України − на засадах правової держави, демократичного устрою, розробки та, як зазначає Л. Наливайко, «реалізації відповідних національних доктрин, стратегій, концепцій та програм згідно із чинним законодавством» [53, с.62].

Тому інформаційна безпека як об’єкт правового регулювання та охорони конституційних прав і законних інтересів зазначених суб’єктів спрямована на одночасне забезпечення: конституційних прав і свобод людини, громадянина, єдності їх прав і обов’язків; і на захист духовних, морально-етичних, культурних, історичних, інтелектуальних та матеріальних цінностей суспільства, його інформаційного і природного середовища; конституційного ладу, суверенітету, територіальної цілісності держави; політичної, економічної, соціокультурної, науково-технологічної, оборонної і державної безпеки, екологічної, власне інформаційної сфер тощо складових національної безпеки [53, с. 65]. Загалом кожен із вказаних напрямків потребує і організованої системи протидії інформаційним загрозам, і напрацювання системи власного інформаційного простору, і відповідної інфраструктури, тобто широких інформаційних ресурсів, доступних для держави, суспільства, громадян.

Необхідність забезпечення інформаційної безпеки вченими, такими як Л. Наливайко, цілком справедливо пов'язується з: 1) «потребою забезпечення національної безпеки України як цілісності, що передбачає й інформаційну складову»; 2) «існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам»; 3) «врахуванням того, що за допомогою інформації можна впливати на зміну свідомості людей, їх поведінкові моделі» [53, с.62].

Безумовно відповідний політологічний аналіз розпочинаємо з Основного Закону держави. Забезпечення інформаційної безпеки визначене нормами ч. 1 ст. 17 Конституції України як «найважливіша функція держави» і саме остання виступає головним суб'єктом політики інформаційної безпеки [40]. Згідно зі ст. 2 Закону України «Про національну безпеку України», правову основу в сфері національної безпеки, окрім Конституції, визначають і «закони України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України» [67], а також видані на виконання Конституції та законів України інші нормативно-правові акти.

Тим не менш, вважаємо за доцільне констатувати, що, з нашої точки зору, даний комплекс підходів до визначення не відображає усіх аспектів поняття «інформаційна безпека». З цієї причини, в свою чергу, слід представити комплексну дефініцію, що дасть змогу відобразити увесь спектр елементів, які включає дане поняття.

Спираючись на усе вище викладене, пропонуємо під інформаційною безпекою розуміти комплекс умов, при яких можлива захищеність життєво важливих інтересів держави, суспільства та окремого індивіда в інформаційній сфері, яка відображається в чотирьох аспектах: ціннісному (відсутність негативного впливу на громадську думку), технологічному (кібербезпека); правовому (розвиненість законодавства, що регулює правовідносини в інформаційній сфері); соціально-політичному (відсутність політичної цензури, вільний доступ до публічної інформації). Дане визначення пропонуємо закріпити

у загальних положеннях Доктрини інформаційної безпеки України та ст.1 Закону України «Про національну безпеку України».

Згідно Доктрини в інформаційній сфері України вирізняються наступні життєво важливі інтереси держави: 1) «недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур»; 2) «ефективна взаємодія органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері»; 3) «побудова та розвиток інформаційного суспільства»; 4) «забезпечення економічного та науково-технологічного розвитку України»; 5) «формування позитивного іміджу України»; 6) «інтеграція України у світовий інформаційний простір» [61].

В цьому ж документі було визначено наступні принципи забезпечення інформаційної безпеки України: 1) «свобода збирання, зберігання, використання та поширення інформації»; 2) «достовірність, повнота та неупередженість інформації»; 3) «обмеження доступу до інформації виключно на підставі закону»; 4) «гармонізація особистих, суспільних і державних інтересів»; 5) «запобігання правопорушенням в інформаційній сфері»; 6) «економічна доцільність»; 7) «гармонізація українського законодавства в інформаційній сфері з міжнародним»; 8) «пріоритетність національної інформаційної продукції» [61].

У 1999 році на 54-ій сесії ГА ООН було прийнято оновлений проект резолюції (A/RES/54/49) «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки», який вперше вказав на загрози міжнародної інформаційної безпеки відносно не тільки до цивільної, але і до військової сфер. Поряд із зазначеним, за результатами роботи сесії було опубліковано проект «Принципів, що стосуються міжнародної інформаційної безпеки» (A/55/140У). Принципи є свого роду робочим варіантом кодексу поведінки держав в інформаційному просторі, створюючи для них відповідні моральні зобов’язання, що також закладають основу для широких міжнародних переговорів під егідою ООН і інших міжнародних організацій з проблем міжнародної інформаційної безпеки (МІБ). У них міститься необхідна понятійна база з предмету МІБ,

наводяться основні визначення: міжнародної інформаційної безпеки, погроз інформаційній безпеці, інформаційної зброї, інформаційної війни, міжнародного інформаційного тероризму та злочинності [6, с.75].

У цьому ж розділі зауважимо, що кращі безпекові стратегії та практики, які успішно захищають сучасний інформаційний простір, побудовані на трьох визначальних принципах: ієрархічності; державної координованості; взаємодії. Ці три принципи мають виражений суб'єкт-об'єктний характер, адже йдеться про необхідність побудови системи інформаційної безпеки з керівними і дорадчо-консультативними органами, відповідальне здійснення управління такою системою, координування діяльності та взаємодії її структурних підрозділів. Сучасна країна, що стає об'єктом постійного зовнішнього інформаційного впливу, в контексті самозбереження та розвитку має відповідно й постійно працювати над власною суб'єктністю. У цьому вбачається одна з головних закономірностей політичного життя. В одному й тому ж інституті може бути закладена як діяльнісна активність у світі політики, так і пасивна, виконавська функція. Однак ефективність державних органів від поєднання таких суперечливих початків не повинна втрачатися, адже ці структури мають бути наділені відповідними функціями та засобами для реалізації спільних цілей та дуже конкретних завдань.

В Україні система інформаційної безпеки працює за схожою моделлю центральних суб'єктів, серед яких також варто враховувати діяльність Служби безпеки України, Служби зовнішньої розвідки, інших міністерств і відомств (Міністерства культури та інформаційної, політики, Міністерства освіти та науки України, та ін.). Очевидно, що такі державні структури, які задають напрям та динаміку сфери інформаційної безпеки, мають вибудовувати свою діяльність за принципами координованості, в межах встановлених норм, загальних програм, стратегій та планів, не повторювати повноважень, уникати невластивих функцій та надміру концентрації владного контролю. Вітчизняний законотворець підкреслює також як засадничі принципи інформаційної політики, зокрема «додержання прав і свобод людини і громадянина», «повагу до гідності особи,

захист її законних інтересів, а також законних інтересів суспільства та держави», «забезпечення суверенітету і територіальної цілісності України», про які йдеться у відповідному указі президента [61]. У поєднанні принципів інформаційної політики демократичної системи та принципів інформаційної безпеки суб'єкта цивілізованих міжнародних відносин вбачаємо дійсний шлях розвитку сучасних політичних інститутів. І у розробці стратегій, і у процесі реалізації запланованих програм саме держава дбає про необхідні матеріальні ресурси, кадрове забезпечення, міжнародне співробітництво у сфері інформаційної безпеки.

Сьогодні основні для розуміння забезпечення міжнародної інформаційної безпеки міжнародно-правові норми закріплені у Статуті ООН, а також інших міжнародних нормативно-правових актах, що формують правовий базис для розв'язання збройних конфліктів, визначають засади міжнародного гуманітарного права, а також регулюють процес упередження та боротьби з міжнародним тероризмом. Таким чином, серед основних правових принципів, що пов'язані з міжнародними інформаційними відносинами в частині гарантування інформаційної безпеки називають такі: «принцип суверенної рівності держав у сфері використання інформаційних ресурсів, забезпечення інформаційного суверенітету держави та рівноправної участі в переговорних процесах щодо встановлення і кодифікації міжнародно-правових документів у сфері інформаційної безпеки»; «принцип невтручання у внутрішні справи інших держав, неприпустимість інформаційної інтервенції з метою проведення спеціальних інформаційних кампаній, ворожої пропаганди та поширення деструктивної чи спеціально спрямованої інформації» [91, с. 111]; «принцип заборони застосування сили або загрози силою, який забороняє використання інструментів інформаційного впливу проти територіальної цілісності чи політичної незалежності будь-якої держави»; «принцип мирного врегулювання міжнародних спорів, який зобов'язує держави до превентивної дипломатії або переведення збройного конфлікту на переговорний рівень за допомогою інструментів інформаційного впливу» [42, с. 18]; «принцип територіальної цілісності та непорушності кордонів, який стосується визначення меж

національного інформаційного простору та заходів захисту від несанкціонованого втручання ззовні»; «принцип дотримання фундаментальних прав і свобод людини, який визначає конституційні та спеціальні норми, а також норми міжнародних договорів щодо свободи слова та вільного обігу інформації, незалежності і плюралізму міжнародних мас-медіа, свободи вираження, заборони цензури та захисту конфіденційності інформаційних ресурсів» [91, с. 111]; «принцип самовизначення народів і націй, який встановлює права національних меншин на культурну самобутність та інформаційну діяльність; принцип міжнародного співробітництва, який зобов'язує держави співпрацювати задля зміцнення миру та міжнародного взаєморозуміння, розвитку глобальної інфраструктури з метою досягнення інтересів людства» [42, с. 18]. Отже, це комплекс політичних, економічних і соціокультурних принципів, важливих для міжнародного порозуміння.

Впродовж майже 40 років висловлювались різні погляди, ідеї і концепції щодо його визначення, складу, перспектив розвитку та його місця в загальній структурі міжнародної безпеки. Одним із ключових питань дослідження є визначення поняття інституту міжнародної інформаційної безпеки.

Зважаючи на доволі довгий період відсутності однозначного сприйняття інституту міжнародної інформаційної безпеки в міжнародному праві, варто розглянути погляди, що висловлювались в його доктрині, концептуальні підходи і визначення, що пропонувались при розробці і прийнятті міжнародних угод. Це надасть можливість комплексно поглянути на розуміння інституту міжнародної інформаційної безпеки та визначити його місце в загальній системі міжнародної безпеки.

Одним із перших науковців, хто розкрив своє бачення концепції міжнародної інформаційної безпеки, став В. А. Василенко. Він висловив думку про те, що інформаційна безпека займає особливе місце у всеохоплюючій системі міжнародного миру та безпеки. На його думку, концепція міжнародної інформаційної безпеки включає в себе: «1) відмову від стереотипів «холодної війни»; 2) рівноцінний міжнародний обмін різноманітною та повною

інформацією з метою напрацювання політики, що не наносить нікому шкоди; 3) виховання в широких мас населення всіх країн світу нового політичного мислення, що відповідає реаліям ядерної доби в умовах сучасного етапу науково-технічної революції; 4) заборону пропаганди воєнної, екологічної, економічної, культурної, психологічної агресії в будь-якій формі; 5) засудження колоніалізму, національної, расової та релігійної ненависті, дискримінації, ворожнечі та насилля [9, с. 271-272].

Талімончик В. П. також відстоює позиції розгляду МІБ як частини всеохоплюючої міжнародної безпеки. Досліджуючи питання інформаційної безпеки, в якості класифікатора автор використовує сферу суспільних відносин, на які поширюється інформаційна безпека, а саме – міжнародні та внутрішньодержавні суспільні відносини. Відповідно до цієї класифікації, вона чітко розмежовує поняття міжнародної інформаційної безпеки та внутрішньодержавної інформаційної безпеки. Талімончик В. П. розглядає міжнародну інформаційну безпеку як «властивість системи міжнародних відносин в сфері інформації, що забезпечує її стабільний стан та захищеність від негативних зовнішніх факторів». Крім того, вона зазначає, що МІБ можна також трактувати як «сукупність вимог, що пред'являються до функціонування системи міжнародних відносин в сфері інформації, які забезпечують її захищеність від негативних зовнішніх факторів». Варто зазначити, що Талімончик В. П. звертає увагу й на той факт, що відносини, які виникають у процесі реалізації вимог міжнародної інформаційної безпеки, неоднорідні за своїм складом, а тому, спричиняють комплекс питань як міжнародного публічного, так і міжнародного приватного права [86, с. 231].

Ще одним важливим напрацюванням в розробці термінології у сфері міжнародної інформаційної безпеки став Словник-довідник з інформаційної безпеки для Парламентської Асамблеї Організації Договору про колективну безпеку 2014 року. У вступній частині до словника наголошується на тому, що понятійний апарат в різних галузях законодавства обумовлюється характером відносин, що регулюються. У словнику міжнародна інформаційна безпека

розуміється як «стан глобального інформаційного простору, в якому виключено можливості порушення прав особистості, суспільства та прав держав в інформаційній сфері, а також можливості деструктивного та протиправного впливу на елементи національної критичної інформаційної інфраструктури» [82, с. 39].

На нашу думку, не можна оминути увагою розуміння інформаційної безпеки Міжнародною організацією з питань стандартизації (ISO) як однієї з провідних інституцій, що формує спеціалізовану систему всесвітньої стандартизації. Групі міжнародних стандартів щодо систем управління інформаційною безпекою присвоєно номер 27000 з відповідною подальшою нумерацією відповідно до кожної окремої підгрупи стандартів. Ці стандарти було розроблено Міжнародною організацією з питань стандартизації та Міжнародною електротехнічною комісією. Вони визначають вимоги до систем управління інформаційною безпекою, управління ризиками, а також ключові принципи щодо їх впровадження. Відповідно до Стандарту 27000, інформаційна безпека – це «збереження конфіденційності, цілісності та доступності інформації». Варто зауважити, що в роз'ясненні до цього визначення додаються ще такі властивості інформації, як «автентичність, прозорість, неспростовність та достовірність» [104].

Як бачимо, різні науковці та експерти міжнародних організацій по-різному підходять до визначення поняття міжнародної інформаційної безпеки.

Складність визначення правової природи інституту міжнародної інформаційної безпеки полягає в тому, що він на сьогоднішній день перебуває в стані постійного розвитку, що викликаний перманентним розвитком інформаційно-комунікаційних технологій. На нашу думку, інститут міжнародної інформаційної безпеки виступає в якості міжгалузевого інституту, що представляє собою особливий і відокремлений комплекс норм і регулює міжгалузеву сферу відносин. Зокрема, інститут міжнародної інформаційної безпеки охоплює відносини в таких галузях міжнародного права, як: право

міжнародної безпеки, міжнародне кримінальне право, міжнародне інформаційне право та міжнародне гуманітарне право.

Зупинимось детальніше на аналізі існуючих конвенцій у сфері міжнародної інформаційної безпеки, що відображають різноманітні підходи до розуміння міжнародної інформаційної безпеки.

Угода про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації від 01 червня 2001 року стала першим міжнародним регіональним документом з питань міжнародної інформаційної безпеки. Цим документом держави-учасниці визначили та закріпили список діянь в інформаційній сфері, що тягнуть за собою кримінальну відповідальність, а також основні форми співробітництва держав, порядок призначення компетентних органів держав-учасниць, порядок надання запитів про сприяння, виконання таких запитів, врегулювала питання конфіденційності інформації та порядок вирішення спорів. Держави визначили для себе такі фори співробітництва: 1) виконання запитів про проведення оперативно-розшукових заходів та процесуальних дій у цій сфері; 2) обмін інформацією про злочини у сфері комп'ютерної інформації, про форми і методи розслідування злочинів у цій сфері та про національне законодавство і міжнародні договори, що регулюють ці питання; 3) планування та проведення скоординованих заходів щодо попередження, виявлення та розслідування комп'ютерних злочинів, надання сприяння в підготовці підвищення кваліфікації кадрів; 4) проведення спільних наукових досліджень; 5) створення інформаційних систем задля забезпечення виконання завдань по виявленню, запобіганню і розслідуванню комп'ютерних злочинів; 6) обмін нормативно-правовими актами та інше [90].

16 червня 2009 року в рамках Шанхайської Організації Співробітництва було прийнято документ, що регулює усі три аспекти міжнародної інформаційної безпеки – військово-політичний, антитерористичний та кримінально-правовий. «Загроза інформаційній безпеці» визначена як «фактор,

що створює небезпеку для особистості, суспільства, держави та їх інтересів в інформаційному просторі» [89].

Міжнародні організації, науковці, експерти не лише використовують різні терміни: «міжнародна інформаційна безпека» та «міжнародна кібербезпека», а й включають до сфери регулювання інституту міжнародної інформаційної безпеки різні відносини, що складаються в межах зазначеного інституту.

На основі проведеного дослідження ми доводимо раціональність широкого підходу до розуміння інституту міжнародної інформаційної безпеки, що передбачає поєднання 3 аспектів у структурі міжнародної інформаційної безпеки: військово-політичного, антитерористичного та кримінально-правового, а також наявність змістовного (інформаційного) та технічного (комунікаційного) елементів у структурі кожного з аспектів міжнародної інформаційної безпеки.

Тому на нашу думку, міжнародну інформаційну безпеку слід визначати як стан, що забезпечується загальновизнаними і спеціальними принципами та нормами міжнародного права, який виключає порушення міжнародного миру і безпеки як окремих держав, так і світового співтовариства в цілому у сфері інформації і комунікації.

Інститут міжнародної інформаційної безпеки пропонуємо розглядати як міжгалузевий інститут, що представляє собою особливий і відокремлений комплекс норм, який регулює міжгалузеву сферу відносин. Зокрема, мова йде про охоплення інститутом міжнародної інформаційної безпеки відносин в таких галузях міжнародного права, як: право міжнародної безпеки, міжнародне кримінальне право, міжнародне інформаційне право та міжнародне гуманітарне право.

### 1.2. Історія формування та розвиток системи інформаційної безпеки України

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

на нашу думку, не слід говорити про її появу – адже безпека, як умова існування і розвитку людини, завжди була однією з базових її потреб.

Початок історії захисту інформації вчені пов'язують з появою можливості фіксації інформаційних повідомлень на твердих носіях, тобто з винаходом писемності, а першим видом інформації, що підлягала захисту, вважають державну таємницю. Практично одночасно з народженням писемності виникли перші методи захисту інформації, як шифрування і приховування. Один з найстаріших шифрованих текстів з Месопотамії (2000 рр. до н. Е..) Являє собою глиняну табличку, що містить рецепт виготовлення глазурі в гончарному виробництві, в якому ігнорувалися деякі голосні і приголосні і вживалися числа замість імен. З розвитком суспільства удосконалювалися і способи добування необхідної інформації. До IV століття до н. е. Схід значно випередив Захід в мистецтві розвідки. Сунь Цзи писав: «Те, що називають передбаченням, не може бути отримано ні від духів, ні від богів ... ні за допомогою розрахунків. Воно повинно бути видобуто від людей, знайомих з положенням противника» [85, с.112].

Бажанню здобувати конфіденційну інформацію завжди протиставлялось не менше бажання протилежного боку захистити цю інформацію. Стародавні способи захисту інформації по суті перетривали до сучасності, удосконалюється лише техніка їх реалізації. Наприклад, з метою приховування самого факту наявності інформації у Стародавньому Римі повідомлення, написане на дошці, приховували від сторонніх очей, заливши його воском. У Стародавній Греції обривали раба, писали на його голові і, коли волосся відростало, відправляли до адресата. У середні віки винайдено тайнопис і повідомлення приховували за допомогою невидимих хімічних засобів. В сучасних умовах поширені такі стеганографічні методи, як приховування змісту повідомлень в малюнках, телевізійних і аудіосигналах тощо [11, с. 40]. Паралельно розвивалися методи шифрування і кодування (криптографічні методи), історія яких починається з часів виникнення писемності в Стародавньому Єгипті та Китаї.

Історія інформаційної безпеки на території сучасної України також сягає ще додержавних часів. Першим видом інформації, яку потрібно було охороняти, була військова інформація. Спочатку охорону такої інформації забезпечував князь, потім особа, яку він призначав особисто. Війна була на той час головним і загальновизнаним способом ведення зовнішньої політики будь-якої держави, тому захист військової інформації був головним у політиці князів Олега, Ігоря, Святослава, Ярослава та княгині Ольги. Князі, йдучи в похід, намагалися приховати інформацію про кількість війська і напрям головного удару. Ворог не міг адекватно реагувати на небезпеку, а заздалегідь поширені чутки, перебільшення і дезінформація призводили до паніки [56, с. 11].

Для забезпечення конфіденційності інформації, що передається використовувалися різні методи. Найбільш важливі повідомлення заучувалися гінцем напам’ять. При цьому часто використовувалися натяки, умовні слова. Суть методу полягала в тому, що зміст переданого повідомлення могла зрозуміти тільки посвячена людина. Надалі, в криптографії такий спосіб забезпечення секретності отримав назву «жаргонного коду» і застосовується досі. Так, наприклад, на жаргоні багатьох розвідок слово «хворіти» означає «арешт» або «взяття під варту»; ЛІКАРНЯ – в’язниця; «лікар» - контррозвідка [5, с. 42].

В Речі Посполитій пошуком і знешкодженням шпигунів з метою захисту інформації займалися призначені королем відповідальні особи з його найближчого оточення.

В Російській імперії було встановлено кримінальну відповідальність за розголошення такого виду інформації як державна таємниця. Зокрема, у «Соборному Уложении» (1649 р.) була стаття, що визначала смертну кару за такі дії [56, с.27]. Водночас, централізованої системи охорони державної таємниці не існувало. Найбільш розвиненою була система захисту військової інформації. Її основними напрямами були створення і вдосконалення системи контррозвідувальних органів; організація комплексної системи захисту інформації, що містить військову таємницю; вдосконалення системи фельд’єгерського зв’язку; організація військової цензури.

Наступний період (з середини XIX ст.) пов’язують з появою технічних засобів обробки інформації та передачі повідомлень за допомогою електричних сигналів і електромагнітних полів (наприклад, телефон, телеграф, радіо). У зв'язку з цим виникли проблеми захисту від технічних каналів витоку. На початку XIX століття криптографія збагатилася чудовим винаходом - система шифрування «дисковим шифром», автором якого вважається екс-президент США Томас Джефферсон.

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

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

Сучасний період свідчить про найбільш інтенсивний розвиток засобів захисту інформації починається у зв’язку з масовою інформатизацією суспільства. Проте, наприкінці 20 ст. математично було доведено, що забезпечити повну безпеку інформації в системах її обробки неможливо [93].

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

Перший період інформаційного протиборства охоплює античні часи, епоху Середньовіччя та частину Нового часу до XVIII ст. включно. Перші письмові згадки про інформаційний вплив на суспільство у Стародавньому Китаї. У вже згаданому Трактаті про мистецтво війни китайського полководця Сунь цзи [29] наводиться опис і яскраві приклади застосування прийомів і методів психологічного впливу, які давали змогу досягати перемоги без битв або з мінімальними втратами. Важливе місце, зокрема, відводиться дезінформуванню противника, психологічній обробці власних населення і війська з метою досягнення єдності в суспільстві напередодні і під час війни, здійснення інформаційних диверсій для розладнання військових союзів ворожої держави з іншими державами тощо.

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

На початку XVI ст. в концепції державної влади, що висунув і обґрунтував Н. Макіавеллі у книзі «Державець» вперше сформулював основні принципи ведення інформаційного протиборства в політичній сфері. Він висунув тезу про те, що політик повинен поєднувати в собі риси лева і лисиці. Володіючи якостями цих тварин, він буде здатний, з одного боку, діяти рішуче, із застосуванням сили, з іншого - маніпулювати масами за допомогою хитрості, спритності, обману. Брехня на благо суспільства визнавалася допустимою і навіть необхідною, а в роботі з підданими - «насильство для тіла і брехня для душі».

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

Наполеон активно використовує можливості поліцейського відомства у справі ідеологічно-психологічного впливу на населення і контролю за ним для збереження власної диктатури. Він був одним із перших можновладців Європи, хто дійсно оцінив роль преси у формуванні громадської думки. «Чотири газети зможуть заподіяти ворогові більше шкоди, ніж стотисячна армія». Усвідомлюючи повною мірою силу вплив преси на формування громадської думки, Наполеон диференційовано підходив до діяльності органів друку усередині країни та за кордоном. У Франції він газет заборонив писати про внутрішню та зовнішню політику і скоротив кількість газет з 73 до 13. А у кожній окупованій країні засновував офіційний друкований орган: «Тазетт де Мадрид», «Газетт де Берлін», «Журналь дю Капітоль» тощо, на сторінках яких широко використовувались методи замовчування і дезінформації [59, с. 62].

Характерною рисою фашистської пропагандистської діяльності було ґрунтовне використання наукових розробок у цій сфері. Активно використовувалися напрацювання з психології підсвідомого. Відповідаючи на питання, чому Гітлер не приваблює іноземців, К. Юнг зазначав: «... для будь-якого німця Гітлер є дзеркалом його підсвідомого, у якому не для німця, звичайно, нічого не відображається. Він рупор, настільки посилюючий неясний шепіт німецької душі, що його може почути вухо його підсвідомого». Розроблені німецькими пропагандистами прийоми впливу на маси, до сьогодні використовуються в політтехнологіях. Це передусім театралізовані партійні з'їзди, масові зустрічі на стадіонах, радіотрансляції виступів лідерів на масові аудиторії тощо. Але основною характеристикою фашистської інформаційної політики, безумовно, є інформаційний монополізм.

З кінця 1940 до середини 1980-х рр., в епоху так званої холодної війни, протистояння двох супердержав - СРСР і США - спричинило подальше вдосконалення форм і методів пропаганди та психологічної війни. У 1970-х рр. остання інформаційна революція пов'язана з винаходом комп'ютера висунула на перший план нову галузь - інформаційну індустрію, яка пов'язана зі створенням технічних засобів, методів, технологій для нових знань.

На межі тисячоліть гостро повстало питання про міжнародну інформаційну безпеку, а також кібербезпеку у складі інформаційної безпеки. Негативним ефектом застосування сучасних технологій у військово-політичній сфері стали все ширші можливості застосування інформаційної зброї. Тим не менш, на кожному з вищезгаданих етапів інформаційна безпека людини залишалась і залишається вторинним питанням.

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

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

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

У результаті проведеного аналізу можемо підсумувати, що інститут інформаційної безпеки людини в Україні і світі є наймолодшим, порівняно з

інформаційною безпекою держави чи суспільства. Протягом багатьох тисячоліть інформаційна безпека розглядалась, насамперед, з перспективи інтересів держави. Згодом інтенсифікація процесів інформатизації в усіх сферах, а особливо, зростання значення технічного захисту інформації зумовило становлення правового забезпечення захисту інформації як невід'ємної складової безпеки підприємств, установ та організацій, а також окремих галузей господарства. На межі тисячоліть гостро повстало питання про міжнародну інформаційну безпеку, а також кібербезпеку у складі інформаційної безпеки. Негативним ефектом застосування сучасних технологій у військово- політичній сфері стали все ширші можливості застосування інформаційної зброї. Водночас, базовою цінністю кожного виду інформаційної безпеки, на нашу думку, є людина, оскільки кожна загроза інформаційній безпеці в той чи інакший спосіб спрямована на її права, свободи і законні інтереси, впливає на її життя і можливість задоволення своїх потреб.

### 1.3. Правове регулювання інформаційної безпеки України

Проблематика інформаційного права в цілому та його безпекових аспектів зокрема набуває останнім часом неабиякої актуальності в контексті глобалізації та інформаційного суспільства, як нової ери існування людства, а також з огляду на появу нового типу відносин, що пов'язані із використанням та обігом інформації. Інформаційний простір, на думку численних дослідників є ареною зіткнень і боротьби різновекторних національних інтересів в умовах глобальної інтеграції та жорсткої міжнародної конкуренції головною.

Погоджуємося з думкою, що при цьому сучасні інформаційні технології дають змогу досягти реалізації власних інтересів без застосування воєнного інструментарію, послабити або навіть зруйнувати конкуруючу державу, не застосовуючи сили, за умови якщо ця держава не усвідомить реальних та потенційних загроз негативних інформаційних впливів і не створить дієвої системи захисту і протидії цим загроза [3, с. 95].

Крім того, події в Україні протягом останніх років роблять тему інформаційної політики держави, її безпеки та протидії інформаційним загрозам не просто актуальною, а й життєво-значущою. Тому не дивно, що питання інформаційного права та безпеки стає об'єктом наукових розвідок вітчизняних та західних вчених, однак ця тематика залишає ще велике поле для аналізу, зважаючи на відносну новітність у політичній та правовій науці, постійну еволюцію правової регламентації, а також шалену швидкість практичних зміну у сфері інформаційних технологій. Важливим підґрунтям для розроблення та вивчення проблематики інформаційної, передусім державної, політики є доробки наукових шкіл з інформаційного права, представниками яких виступають, для прикладу, І. Арістова, О. Баранов, Л. Задорожня, Р. Калюжний В. Ліпкан, В. Олійник, А. Пазюк, І. Сопілко, В. Цимбалюк, та М. Швець. Вивченням ролі держави у формуванні інформаційного суспільства та забезпеченні інформаційної безпеки займаються такі вчені як, Г. Почепцов, Ф. Медвідь, О. Литвиненко, Д. Лук'яненко, І. Рамоне, О. Соснін та ін.

З метою розвитку глобальної культури кібербезпеки та мотивації держав щодо вдосконалення національного законодавства у сфері забезпечення кібербезпеки МСЕ було розроблено Глобальний індекс кібербезпеки, що являє собою комплексне дослідження показників рівня розвитку кібербезпеки окремих країн відповідно до 5 сфер: юридичної, технічної, організаційної, розвитку потенціалу та міжнародного співробітництва. Насамперед, хотілося б звернути увагу на те, що відповідно до вищезазначеного дослідження Україна посідає 17-те місце в глобальному рейтингу рівня забезпечення національної кібербезпеки та 4-те місце в рейтингу регіону Співдружності Незалежних Держав із зауваженням, що одну й ту саму позицію можуть займати кілька держав одночасно [102, с. 3,13].

Україна усвідомлює нагальну необхідність у розробці прогресивного національного законодавства у сфері інформаційної безпеки та ключову роль, яку вона відіграє на міжнародному та регіональному рівні щодо протистояння загрозам в інформаційному просторі, особливо з огляду на агресію Російської

Федерації щодо України. Тому, за останні кілька років Україна розробила ряд принципових документа в сфері забезпечення інформаційної безпеки.

Законодавчий рівень інформаційної безпеки є основою для побудови системи захисту інформації, оскільки дає базові поняття предметної області та є регулятором взаємовідносин в цій сфері. Цей рівень відіграє координуючу і спрямовуючу роль в усіх ланках формування системи захисту інформації та в усіх сферах життєдіяльності країни і суспільства. Як слушно підкреслює П. Орлов, в сучасних умовах інформаційна сфера фактично постає системоутворюючим фактором життя суспільства, що активно впливає на стан політичної, економічної, оборонної та інших складових безпеки України, тому ці особливості повинні враховуватися при нормативно-правовому забезпеченні цих сфер суспільного життя [57, с.96].

На жаль, на законодавчому рівні залишається не врегульованим питання покарання за злочини щодо порушення інформаційної безпеки, здійснювані як в середовищі кібербезпеки, так і в офлайн спосіб. Законодавство України потребує внесення змін для формування цілісного комплексу заходів щодо нормативно-правового регулювання сфери інформаційної безпеки держави.

Сфера інформаційної безпеки регулюється рядом Законів України, нормативно-правових актів, прийнятих Кабінетом Міністрів України, рішень Ради Національної безпеки та оборони України, та іншими нормативно-правовими актами щодо захисту інформації. Сюди також відносяться державні стандарти (в тому числі галузеві) щодо технічного захисту інформації.

Загалом, ще донедавна одним з основних правових регуляторів інформаційних відносин в Україні був Закон України «Про інформацію», де, зокрема, основними принципами визначалися:

– гарантованість права на інформацію;

– відкритість, доступність інформації й свобода обміну інформацією;

– об’єктивність, вірогідність інформації;

– повнота й точність інформації;

– законність отримання, використання, поширення й зберігання інформації [65].

З часу прийняття цього закону загальний стан справ і ситуація довкола питання забезпечення захисту інформації (власне інформаційної безпеки) радикальним чином змінилися, з огляду на нові виклики, які отримала Україна з початком військової збройної агресії в 2014 р. з боку Російської Федерації. Розв'язана так звана «гібридна війна» значною мірою перемістилася в площину інформаційного простору, відтак постала нагальна потреба правового врегулювання інформаційної захищеності аби протистояти маніпулятивним впливам з боку ворога та захистити стратегічні національні інтереси в галузі захисту інформації.

Більш розширеними, у розрізі безпекових цілей, є положення Концепції Національної програми інформатизації, схвалена Законом України «Про Концепцію Національної програми інформатизації» від 04.02.1998 р. № 5/98-ВР, мета якої визначається синтез двох стратегічних завдань: забезпечення прав та свобод громадян України у доступі до своєчасної та достовірної інформації (при використанні інформаційних технологій), досягнення цілей інформаційної безпеки [66].

Базовими елементами корекції профільного Закону «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII є: визначення напрямків та форм державно-громадської взаємодії в межах цілей національної безпеки, зокрема в інформаційній сфері; визначення сфер реалізації політики національної безпеки (за зразком Закону «Про основи національної безпеки України» 2003 року), а також визначення цілей безпекової політики відповідно до наявних сфер, класифікації існуючих та потенційних загроз у визначених сферах [67].

Відповідно до чинного законодавства основні принципи, напрямки та методи реалізації безпекової політики в інформаційній сфері базуються на ключових нормах «Стратегії національної безпеки України», а державно-громадська взаємодія розглядається з точки зору забезпечення ефективної конфігурації системи протидії існуючим та потенційним інформаційним

загрозам національній безпеці [74]. Проте, в документі відсутній комплексний підхід до розробки способів протидії цим загрозам. Також, використовуючи термін «кібербезпека» документ фактично звужує сферу його дії лише до комунікаційного аспекту трьох елементів інформаційної безпеки, виключаючи їх змістовну компоненту, що в контексті агресії Росії проти України має найпринциповіше значення.

У 2016 році рішенням Ради національної безпеки і оборони України було затверджено Доктрину інформаційної безпеки України. В документі визначено актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері [72], однак про це більш детально піде мова у наступному розділі даної роботи. Важливо наголосити, що при цьому документ не містить визначення понять: «інформаційна безпека» та «інформаційний простір», а також не розмежовує загрози на воєнно-політичні, терористичні та кримінальні, що суттєво звужує предмет її регулювання.

Крім того, наразі існує Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII. Закон чітко визначає, що його положення не поширюються на відносини та послуги, пов’язані зі змістом інформації, тобто змістовний аспект інформаційної безпеки знову залишається поза межами регулювання зазначеного нормативно-правового акту [72].

Постановою Правління Національного Банку України від 26.11.2015 р. № 829 було затверджено Постанову «Про затвердження нормативно-правових актів з питань інформаційної безпеки» [63].

Проаналізувавши основні документи у сфері забезпечення інформаційної безпеки, що відображають концептуальне розуміння цього поняття законодавцем, приходимо до висновку, що усі ці документи мають суттєві недоліки в контексті використаної там термінології та її змістовного навантаження, а також з позиції логіки і побудови, а тому потребують суттєвого доопрацювання.

Попри це, варто зазначити, що Україна впевнено крокує до створення повноцінної системи інформаційної безпеки держави, як з правової, так і з

технічної точок зору, беручи активну участь у міжнародних ініціативах на універсальному і регіональному рівнях та вносячи свій вклад у розбудову глобальної системи міжнародної інформаційної безпеки [15, с. 204-206].

У рамках співробітництва з ООН щодо досягнень в сфері інформатизації та телекомунікацій в контексті міжнародної безпеки Україною було підготовлено та направлено три доповіді Генеральному Секретарю у відповідь на однойменну резолюцію.

Україною було запропоновано розглянути можливість реалізації таких заходів міжнародного співробітництва: введення в практику консультативних механізмів співробітництва у сфері кіберзахисту; створення системи обміну інформацією щодо моніторингу кіберпростору та системи оперативного оповіщення про початок кібератак; співробітництво з метою усунення негативних наслідків кібератак, напрацювання технічних рішень та організаційних рекомендації з цього питання. Важливо наголосити, що крім зазначених, Україна виступила з ініціативою розробки міжнародно-правових актів щодо погодження єдиної термінології та правил, наприклад, Кодексу поведінки в Інтернеті [21, с. 20-21].

Крім того, в рамках ООН Україна бере участь у роботі групи експертів всебічного дослідження проблеми кіберзлочинності, що проводяться з 2011 року. Під час останнього засідання групою експертів розглядались пропозиції та зауваження до проекту всебічного дослідження проблем кібербезпеки, державами було здійснено обмін інформацією та думками щодо національного законодавства, практики, технічної допомоги та міжнародного співробітництва. Під час засідання також порушувалось питання створення нового міжнародно-правового документа з питань кібербезпеки, проте експертам не вдалось дійти консенсусу з цього питання [22, с. 10].

Україна бере активну участь у роботі МСЕ, вносить пропозиції до рекомендацій МСЕ та активно захищає національні інтереси, зокрема, під час проведення у 2015 році Всесвітньої конференції радіозв’язку Україна виступила із заявою щодо порушення Російською Федерацією правил експлуатації

передавальних засобів у межах офіційних кордонів України та незаконного використання українських радіочастот. Україною було також запропоновано провести в Україні тематичні заходи щодо забезпечення кібербезпеки правомірного використання радіочастот [25], [26].

Активну позицію Україна займає щодо поглиблення співпраці в рамках Ради Європи. Наразі імплементуються положення Конвенції про кіберзлочинність щодо забезпечення строків збереження комп'ютерних даних, збирання і вилучення доказів в електронній формі в кримінальних справах. Україні надається постійна експертна підтримка в рамках спільного проекту Ради Європи та ЄС «Кіберзлочинність та Східне партнерство III», що спрямований на вдосконалення правових методів співробітництва публічного та приватного сектору у сфері боротьби з кіберзлочинністю та електронних доказів [27]. Також, Україна є членом Комітету з питань Конвенції Ради Європи про кіберзлочинність, а тому бере участь в обговоренні підготовку проекту 2 додаткового протоколу до Конвенції РЄ з метою погодження питань розмежування юрисдикцій та сприяння захисту електронних доказів.

Необхідно зауважити, що з метою реалізації курсу України на вступ до НАТО, однією з найрозгорнутіших сфер співробітництва є співпраця України з Альянсом. Так, розроблено Річну національну програму співробітництва Україна - НАТО на 2020 рік [73].

За умови сучасної ситуації, коли глобальних та регіональних інформаційних протистоянь, деструктивних впливів, зіткнення різноманітних національних інтересів, поширення інформаційної експансії та агресії, захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними стратегічними завданнями сучасних держав у системі глобальних інформаційних відносин. При зростанні технічного прогресу та цінності інформації буде все частіше ставитись питання щодо інформаційної безпеки людини, суспільства та держави. Закон України «Про національну безпеку України» від 21 червня 2018 року запроваджує комплексний підхід до

планування у сферах національної безпеки та оборони, в тому числі і у питаннях інформаційної безпеки.

Звертаємо увагу, що чіткого визначення поняття інформаційної безпеки в Законі неможливо знайти. Проте наявні лише перелічені загрози та напрями державної політики у вищезазначеній сфері. Як бачимо, навіть у ключових юридичних документах, які певним чином формулюють проблему інформаційної безпеки держави та нації, є певні суперечності, які не сприяють ефективній політиці безпеки держави в інформаційній сфері.

Потрібно констатувати, що на сьогоднішній день законодавець визначає три стратегічних документи, а саме стратегію, доктрину та концепцію. Про відповідні повноваження СБУ у сфері контррозвідки та інформаційної безпеки ми можемо також знайти інформацію. Закон передбачає, що планування національної безпеки та оборони поділяється на довгострокове, середньострокове та короткострокове. При цьому зовсім нічого знову повноцінно не врегульовано щодо стратегії інформаційної безпеки не визначається самостійно.

Аналізуючи зміст Закону та Стратегій, зазначимо, що Закон не передбачає змін до стратегії інформаційної безпеки України, а також доручень Кабінету Міністрів України щодо приведення своїх нормативних актів у відповідність із цим Законом. В свою сергу, Міністерство інформаційної політики, шо повинно мати на меті врегулювання спірних питань щодо вдосконалення інформаційної безпеки не тільки документально, а і на практиці не здійснює своїх повноважень майже ніяк, що дає нам підстави зробити наступний висновок.

Отже, попри наявність великої кількості наукових та законодавчих джерел розуміння сутності інформаційної безпеки, на практиці маємо значний ряд недоліків. Так, на нашу думку, одним із важливих завдань, що стоять перед законотворцем є розробка разом із Міністерствами відповідних Стратегій, методологічних баз, завдань і врегулювання спірних питань, шляхом прийняття правових положень але із обов’язковим теоретичним обгрунтуванням. Це, в свою чергу, сприятиме  регулюванню питання інформаційної безпеки України.

Таким чином, вважаємо за доцільне наголосити, що для ефективної реалізації національної політики у сфері забезпечення інформаційної безпеки необхідно: 1) привести у відповідність існуючі правові норми у сфері забезпечення інформаційної безпеки сучасним досягненням; 2) сформувати єдиний підхід до розуміння інформаційної безпеки з огляду на її триелементну структуру та наявність технічної і змістовної компоненти кожного з них; привести законодавство України у відповідність до цього підходу; 3) гармонізувати існуючі правові норми у сфері забезпечення інформаційної безпеки з метою уникнення дублювання різними нормативними актами функцій органів державної влади держави в сфері забезпечення інформаційної безпеки, а також ліквідації прогалин щодо регулювання окремих її аспектів; 4) створити технічний потенціал для протидії загрозам в інформаційному просторі; 5) заохочувати розробку програмного забезпечення національного виробництва з метою мінімізації ризиків використання програмного забезпечення з вбудованими шкідливими програмами; 6) сприяти впровадженню національної культури інформаційної безпеки та підвищенню обізнаності громадян і всіх зацікавлених сторін у цій сфері; 7) заохочувати розвиток державно-приватного партнерства у сфері інформаційної безпеки.

Для нормативно-правового регулювання інформаційної безпеки України властива певна дезорієнтованість, фрагментарність, розпливчастість, недосконаліть чинного законодавства, що яскраво виявили анексія Криму Російською Федерацією у 2014 р. та стимуляція розвитку сепаратизму, пряма агресія на сході України і тривала війна України з маріонетковими структурами ЛНР та ДНР, фінансованими та підтримуваними Росією.

Складність законодавчого регулювання у інформаційній сфері пов’язана також з тим, що об’єктами такого забезпечення одночасно є особистість, суспільство та держава. Їхні інтереси збігаються лише частково. При чому забезпечення інформаційної безпеки особистості під контролем і державних органів, і правозахисних організацій, і міжнародних структур, натомість регламентація державної безпеки в інформаційній сфері переважно самої лише

держави [15]. Тому захист інформаційної безпеки держави так потребує внутрішньої консолідації, об'єднання різних політичних сил, соціальних груп, окремих громадян для спільного позиціонування на міжнародній арені.

Проблеми правового регулювання інформаційних відносин в Україні пов'язанні як з інформаційною безпекою держави, так і з можливостями її швидкої подальшої інтеграції у міжнародну спільноту демократичних, модернізованих країн. Загалом правова політика України в інформаційній сфері ще за багатьма ознаками залишається декларативною, розпорошеною, змістовно невизначеною, несистемною, бюрократизованою. Великий вплив на неї мають закріплена система фінансово-промислових інтересів, застарілих комунікацій, інерційних суспільних мас. Однак на шляху до демократії, європейської інтеграції, у боротьбі з російською агресією, ця політика зазнає помітних реформ. На цьому складному шляху часто вирішення складних тактичних завдань, необхідність швидкого реагування на вкрай небезпечні інформаційні виклики, що загрожують навіть цілісності країни та суб'єктності держави, збагачує безцінним досвідом наше суспільство, консолідує довкола спільних цілей та стратегічних орієнтирів, які потенційно стануть важливою основою якісного політико-правового забезпечення інформаційної безпеки українських громадян, соціуму, держави. Такий досвід унікальний, він може скласти важливу частину загальноєвропейського, тож не варто також і недооцінювати потенціал вітчизняної політико-правової системи.

Підсумовуючи усе вище викладене у розділі, зазначимо наступне:

1.Відсутність офіційного визначення інформаційної безпеки є прогалиною у сучасному правовому регулюванні інформаційної безпеки в Україні. Запропоновано авторське визначення інформаційної безпеки під якою пропонується розуміти комплекс умов, при яких можлива захищеність життєво важливих інтересів держави, суспільства та окремого індивіда в інформаційній сфері, яка відображається в чотирьох аспектах: ціннісному (відсутність негативного впливу на громадську думку), технологічному (кібербезпека); правовому (розвиненість законодавства, що регулює правовідносини в

інформаційній сфері); соціально-політичному (відсутність політичної цензури, вільний доступ до публічної інформації).

2.Наразі в сучасному міжнародному праві ще остаточно не сформовано уніфіковане її поняття, а існування великої кількості термінологічних розбіжностей лише ускладнює цей процес. У переважній більшості випадків, використовуючи термін «міжнародна інформаційна безпека», йдеться про змістовний (інформаційний) та технічний (комунікаційний) аспекти інформаційної безпеки, а термін «міжнародна кібербезпека» звужує таке її розуміння лише до технічного аспекту. Проте, нерідко автори використовують ці терміни для визначення одного й того самого поняття. Оскільки кожен з цих термінів має своє змістовне навантаження, пропонується авторське визначення міжнародної інформаційної безпеки як стану, що забезпечується загальновизнаними і спеціальними принципами та нормами міжнародного права, який виключає порушення міжнародного миру і безпеки як окремих держав, так і світового співтовариства в цілому у сфері інформації і комунікації. Інститут міжнародної інформаційної безпеки пропонується розглядати як міжгалузевий інститут, що представляє собою особливий і відокремлений комплекс норм, який регулює міжгалузеву сферу відносин. Зокрема, мова йде про охоплення інститутом міжнародної інформаційної безпеки відносин в таких галузях міжнародного права, як: право міжнародної безпеки, міжнародне кримінальне право, міжнародне інформаційне право та міжнародне гуманітарне право.

3.Інститут інформаційної безпеки людини в Україні і світі є наймолодшим, порівняно з інформаційною безпекою держави чи суспільства. Протягом багатьох тисячоліть інформаційна безпека розглядалась, насамперед, з перспективи інтересів держави. Згодом інтенсифікація процесів інформатизації в усіх сферах, а особливо, зростання значення технічного захисту інформації зумовило становлення правового забезпечення захисту інформації як невід’ємної складової безпеки підприємств, установ та організацій, а також окремих галузей господарства. На межі тисячоліть гостро повстало питання про міжнародну

інформаційну безпеку, а також кібербезпеку у складі інформаційної безпеки. Негативним ефектом застосування сучасних технологій у військово- політичній сфері стали все ширші можливості застосування інформаційної зброї. Відзначено, що наукові дискусії щодо проблематики інформаційної безпеки особливо у інформаційно розвинених країнах світу особливо актуалізувались в останні роки XX сторіччя. В Україні наукове осмислення проблематики інформаційної безпеки людини є в процесі становлення і відбувається як вторинне по відношенню до інформаційної безпеки держави.

4.Сфера інформаційної безпеки передбачає системну превентивну діяльність органів державної влади з надання гарантій інформаційної безпеки особі, соціальним групам та суспільству в цілому і спрямована на формування відповідного рівня довіри до держави, достатнього для подальшого соціального прогресу та належного розвитку інтелектуального потенціалу країни. Україна усвідомлює нагальну необхідність у розробці прогресивного національного законодавства у сфері інформаційної безпеки та ключову роль, яку вона відіграє на міжнародному та регіональному рівні щодо протистояння загрозам в інформаційному просторі, особливо з огляду на агресію Російської Федерації щодо України. Акцентовано, що Україна займає активну позицію щодо поглиблення співпраці зі своїми партнерами в рамках міжнародних універсальних та регіональних організацій в сфері забезпечення МІБ, приймаючи участь в діалозі на рівні ООН та ініціативах МСЄ. Акцентовано, що наша держава вдосконалює національне законодавство у сфері інформаційної безпеки, про що свідчить прийняття таких важливих документів, як Доктрина інформаційної безпеки України та Стратегія кібербезпеки України.

5.Внутрішнє законодавство України потребує суттєвого доопрацювання, як з позиції використаної там термінології та її змістовного навантаження, так і з точки зору логіки і побудови. Тому для ефективної реалізації національної політики у сфері забезпечення інформаційної безпеки пропонується: 1) привести у відповідність існуючі правові норми у сфері забезпечення інформаційної безпеки сучасним досягненням; 2) сформувати єдиний підхід до розуміння

інформаційної безпеки з огляду на її триелементну структуру та наявність технічної і змістовної компоненти кожного з них; привести законодавство України у відповідність до цього підходу; 3) гармонізувати існуючі правові норми у сфері забезпечення інформаційної безпеки з метою уникнення дублювання різними нормативними актами функцій органів державної влади держави в сфері забезпечення інформаційної безпеки, а також ліквідації прогалин щодо регулювання окремих її аспектів; 4) створити технічний потенціал для протидії загрозам в інформаційному просторі; 5) заохочувати розробку програмного забезпечення національного виробництва з метою мінімізації ризиків використання програмного забезпечення з вбудованими шкідливими програмами; 6) сприяти впровадженню національної культури інформаційної безпеки та підвищенню обізнаності громадян і всіх зацікавлених сторін у цій сфері; 7) заохочувати розвиток державно-приватного партнерства у сфері інформаційної безпеки.

# РОЗДІЛ 2
# АНАЛІЗ ОСОБЛИВОСТЕЙ ТА СКЛАДОВИХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

## 2.1. Аналіз головних складових та загроз інформаційній безпеці України

Збільшення інтенсивності науково-технічного прогресу та посилення «електронного співробітництва» між країнами призводить до зростання такої залежності. Так зокрема, М. Галамба переконаний, що «інформаційна складова не може існувати поза цілей загальної національної безпеки, так само, як і національна безпека не буде всеохоплюючою без інформаційної безпеки» [24, с. 220].

Крім того, в контексті інформаційної безпеки доцільно згадати такий фактор, як вплив ЗМІ, інформаційних агентств, телевізійних каналів на формування суспільної свідомості. Всі вищеперераховані елементи закріпили за собою реноме «четверта влада». Як показує практика (в тому числі і українська) за допомогою таких інструментів можна здійснювати визначальний вплив на всі сфери життєдіяльності суспільства, зокрема на політичну.

Разом з тим, кібербезпека та інформаційна безпека на соціально-побутовому рівні сприймаються, в першу чергу, як захист від інформаційних загроз.

Щодо загроз національної безпеки, то їх найчастіше розуміють як можливу небезпеку, що має здатність причинити будь-яку шкоду, призвести до збитків, втрат (матеріальних і людських) або інших негативних наслідків.

Згідно положень п.6 ст.1 чинного Закону України «Про національну безпеку України», загрози національній безпеці України – це явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [2].

Саме тому, з нашої точки зору, доречно всі загрози національній безпеці класифікують за двома критеріями:

1.За джерелом виникнення виділяють зовнішні та внутрішні загрози.

2.За сферою дії виділяють загрози національній безпеці в політичній, технологічній, економічній, екологічній і т. д.

Під інформаційними загрозами слід розуміти систему зовнішніх та внутрішніх чинників, що чинять згубний вплив на інформаційну безпеку, зачіпаючи життєво важливі інтереси держави, суспільства та людини в інформаційній сфері.

У Стратегії національної безпеки, затвердженої Указом Президента України від 14.09.2020 р., загрози національній безпеці та національним інтересам України визначені з урахуванням зовнішньополітичних та внутрішніх умов та поділені та поточні та прогнозовані. З інформаційних загроз виділено інформаційну та гібридну війну, яка ведеться з боку Російської Федерації, відсутність цілісної інформаційної політики держави та кібертероризм [67].

Положеннями Доктрини інформаційної безпеки України, затвердженої Указом Президента України від 25.02.2017 р. № 47/2017 визначено актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері [61].

Виходячи з вище викладеного, пропонуємо виділити та проналізувати найбільш небезпечні на нашу думку загрози в інформаційній сфері за сучасних умов сьогодення: 1) ведення інформаційної та гібридної війни з боку Російської Федерації; 2) кібертероризм.

Переходячи до висвітлення першої інформаційної загрози, першочергово зазначимо, що інформаційна війна – це комплекс цілеспрямованих дій, початок яких пов'язаний із досягненням політичних цілей та інформаційної переваги суб’єктом шляхом здійснення негативного впливу на сектори, що базуються на використанні інформації та інформаційних технологій противника. Вважаємо, що дану дефініцію необхідно брати за основу в ході наукового дослідження [51].

У продовження даної думки зазначимо, що фахівці називають таку війну різновидом бойових дій, де зброєю є засоби і методи опрацювання інформації. Такі засоби дозволяють швидко, цілеспрямовано та таємно здійснювати вплив на військові й цивільні інформаційні системи ворога з метою підриву його економічного стану, політичної стабільності, боєготовності та, врешті решт, – національної безпеки. Залежно від цілей і характеру поставлених завдань інформаційна зброя може бути такою, яка впливає: на засоби захисту інформації, системи, що атакуються; впливає на збережену, оброблену в атакованій системі інформацію [69, с. 80].

У порівнянні з застосуванням інших видів зброї, організація нападу на інформаційні мережі не вимагає значних матеріальних ресурсів. Хімічну або біологічну зброю називають зброєю масового ураження не через обсягу руйнівної енергії, що виділяється при їх застосуванні, а через кількість спричинених ними втрат і не вибірковості дії. Широкомасштабне застосування звичайних озброєнь також викликає серйозної шкоди. Незважаючи на природу інформаційної атаки, яка потребує докладання значних сил, руйнування систем цифрового контролю атомної електростанції може мати настільки ж масштабні наслідки. Важливість запобігання інформаційних атак такого роду відчутна і безперечна.

У даному контексті необхідно розуміти, що саме ресурси ЗМІ і соціальних медіа (соціальні мережі, онлайн-чати тощо) активно використовуються протиборчими сторонами в соціально-політичному конфлікті. Початковою фазою інформаційного протистояння виступає збільшення матеріалів та інших форм інформаційної активності (нагнітання обстановки) з метою залучення уваги до виникає протиріччя або проблемної ситуації. Наступним етапом виступає «завоювання аудиторії» або консолідація споживачів інформаційного продукту навколо розглянутого протиріччя. Третій етап полягає в масованої інформаційної обробці аудиторії, насиченні інформаційного простору матеріалами та відомостями, що дозволяють залучити частину аудиторії на свою сторону. Заключним етапом є керована стороною конфлікту реакція аудиторії,

спрямована протиборчої стороною в необхідне русло з метою забезпечення панування в інформаційному просторі.

Наголошуючи на різноманітності форм інформаційних війн, Мартін Лібікі, один з перших теоретиків у цій галузі, зазначає, що «інформаційна війна має два варіанти:

1) інформаційна блокада – цей вид війни дослідник розглядає в контексті того, що сьогодні формується залежність держав від інформаційних потоків подібно залежності від матеріального постачання, яке існувало в попередній період, для успіху блокади країна повинна бути залежною від зовнішніх інформаційних потоків;

2) інформаційний імперіалізм (інформаційне домінування) – переваги в створенні, маніпуляції і використанні інформації, достатньої для воєнного домінування [96, с. 135].

На нашу думку, виділяти види інформаційної війни необхідно в залежності від спрямованості інформаційних впливів, а саме: інформаційно-психологічного і інформаційно-технічного з використанням відповідного виду зброї. Кошти, виділені види інформаційної війни мають на увазі організацію двох груп заходів. Перша має на меті вплив на системи формування громадської думки і прийняття управлінських рішень, а також свідомості військовослужбовців і цивільного населення для його «перепрограмування». Друга орієнтована на поразку інформації та інформаційно-управлінських систем противника. Засоби, що використовуються при реалізації цих заходів різноманітні: психологічні операції з метою впливу на політичне та військове керівництво, військовослужбовців, а також цивільне населення противника; дезінформація і т. п. в першому, радіоелектронна війна, фізичне знищення елементів інформаційних систем противника, інформаційна атака і т. п. в другому.

Таким чином, інформаційна війна є «самим інтелектуальним варіантом військового протиборства, оскільки і суб’єкт, і об’єкт впливу тут є людським розумом. Якщо звичайна війна націлена на тіло людини, то інформаційна або смислова - на його розум. Інформаційна війна, по суті, тотальна в тому сенсі, що

дійсно є війною не армій, а націй та вимагає мобілізації всіх ресурсів держави, а також ведеться в глобальному інформаційному просторі і використовує найруйнівніші види зброї - слово і інформацію.

Нині Росія веде проти України гібридну війну, надаючи особливого значення застосуванню різноманітних методів з арсеналу інформаційно-психологічної війни, намагаючись не просто вплинути на загальний морально-бойовий стан українських збройних сил, а й деморалізувати найширші верстви населення, а, за можливості, зруйнувати саму національну ідентичність українців.

В геополітичному контексті гібридна війна являє собою відносно нове явище. Методи гібридної війни використовуються головним чином в сфері операцій спеціальних сил, вони поєднують в собі досвід жорстких протистоянь загрозам міжнародній безпеки і уроки, отримані в боротьбі з екстремізмом державних і недержавних суб'єктів. Гібридна війна ведеться як сила- ми, що діють усередині країни або регіону і прагнуть послабити або повалити уряд, так і силами, що діють ззовні. Наслідки спрямовані на надання сприяння повстанцям у вербуванні прихильників і їх підготовці, оперативної та тилової підтримки, а також впливають на економіку і соціальну сферу, координують дипломатичне зусилля, а також проводять окремі силові акції. Для цих цілей залучаються спеціальні підрозділи, розвідка, а також організовують злочинні групи, крім того здійснюється масштабний інформаційний психологічний вплив на населення, особистий склад збройних сил і правоохоронних органів, владні структури з використанням усього спектру інформаційно-комунікаційних технологій. Як приклад можна привести систему інформаційного тероризму ісламістських терористичних угруповань і організацій. Радикальні ісламісти розгорнули в соціальних мережах вербування, агентурну і мобілізаційну роботу. При цьому вони не створювали чогось нового, а просто використовували вже відпрацьовані технології кольорових революцій, одним з найважливіших елементів яких якраз і було створення таких структур в інтернеті.

Отже, по суті гібридна війна не є ні тактикою, ні стратегією, представляючи собою результат соціально-культурного побудови гібридного суспільства. Для глибокого розуміння особливостей гібридної війни потрібно враховувати історичні, соціальні, культурні, політичні, економічні та військові аспекти. Розуміння гібридної війни передбачає наявність знань про суспільство, в якому з'явилися гібридні збройні сили і відповідна стратегія. Без таких знань буде важко зрозуміти схему війни і її деталі, і, відповідно, складніше виробити ефективні методи протидії.

Однією з найбільш застосовуваних дій і водночас загроз національній безпеці держави виступає кібертероризм як ефективний засіб впливу на психіку. У загальному контексті інформаційної війни і створення інформаційної зброї проблема вивчення їх психологічного впливу стає важливим питанням. Вплив за допомогою інформації на людей, що приймають рішення, ґрунтуючись на конкретній інформації в сьогоднішній реальності стає пріоритетним об’єктом інформаційно-психологічного впливу в інформаційній війні. Найбільш традиційною і потужною інформаційною зброєю є пропаганда.

Термін кібертероризм, як правило, відноситься до дій в дезорганізації інформаційних систем, які створюють загрозу життю людей, заподіяння значної майнової шкоди чи настання інших суспільно небезпечних наслідків, якщо вони зроблені з метою порушення громадської безпеки, залякування населення або впливу на рішення влади, а також погрози вчинення таких актів [30, с.133].

Агентство національної безпеки США, що має доступ до запису телефонних розмов та Інтернет-даних створено виключно для боротьби з тероризмом і серйозними злочинами, однак відповідно до документів, оприлюднених Сноуденом, моніторинг здійснюється за усіма громадянами. Межа між захистом національної безпеки в інформаційній сфері і шпигунством як методом отримання інформації від посадових осіб інших держав виявляється дуже тонка. До того ж, працівника ЦРУ Сноудена визнано терористом по відношенню до США, адже розповсюдження цієї таємної інформації і документів, переданих ним у червні 2013 року газеті The Guardian кваліфіковано

як терористичний акт проти національної безпеки США. Однак, оприлюднені документи підтверджують використання інформаційних технологій для перехоплення комунікацій високопосадовців не лише США, а й інших делегацій G20. У сфері інформації у згаданій вище справі використано такі методи, що можуть у подальшому трактуватись як загрози національній безпеці держави, які можна попередити:

– налаштування Інтернет-кафе, де використовували програму електронної пошти перехоплення і програмне забезпечення - ключ ведення журналу, щоб отримувати інформацію при користуванні делегатами комп’ютерами;

– проникаючі безпеки на BlackBerrys делегатів, щоб контролювати повідомлення електронної пошти і телефонних дзвінків.

В результаті застосування даних методів можна було дізнатись будь-яку інформацію, наприклад політику та плани турецького міністра фінансів.

Загрозу становило у переважній більшості розкриття інформації, що містилась на технічних пристроях - комп'ютерах та телефонах делегатів. Для досягнення поставленої мети, як подано у документах, поширених Сноуденом, використано технологію «активного збору з поштової скриньки інформації, програмою, що копіює поштові повідомлення, не видаляючи їх з віддаленого сервера», фактично це означає «читання електронної пошти людей, перш ніж вони це роблять» [103].

Основною ж формою кібертероризму залишається інформаційна атака на комп'ютерну інформацію, комп'ютерні системи, обладнання передачі даних, а також інші компоненти інформаційної інфраструктури, що здійснюються окремими особами або групами. Ця атака дозволяє йому проникнути в цільову систему для перехоплення контролю або придушення засобів мережі обміну інформацією, виконувати інші деструктивні дії.

Таким чином, найбільшою загрозою і небезпекою в інформаційній сфері є кібертероризм, за допомогою якого можна отримувати таємну інформацію пов’язану із забезпеченням національної безпеки держави (наприклад, таку, якою володіє розвідка й інші правоохоронні органи) та її використання для

досягнення деструктивних для цієї держави цілей, що може призвести до війн, економічних криз, краху банківської системи. Основні дії по забезпеченню і попередженню кібертероризму полягають у забезпеченні інформаційної безпеки, шляхом створення відповідних органів із захисту інформації на рівні держави (у більшості країн світу вони вже існують), розкриттю та виявленню кібер-терористів, створення програмного забезпечення що знаходить технічні засоби атаки в інформаційній сфері.

Національному інформаційному простору держави може загрожувати новий вид війни, а саме інформаційна війна. Проблема захисту національного інформаційного простору від атаки противника полягає в тому, що він є невидимим, тому боротьба носить специфічний характер.

Як вважають фахівці, зокрема І. Боднар, «головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни» [6, с. 69], спроба втрутитися у інформаційні ресурси суспільства, деформувати свідомість особистості, заради нав’язування власних цінностей, поглядів, інтересів у життєво важливих сферах, заради управління поведінкою, рішеннями і розвитком тощо. Власне йдеться про комплекс загроз суверенітету країни на інформаційному рівні з використанням окремого, стратегічного та принципово нового виду протистояння – інформаційного, що без застосування зброї у класичному її розумінні, досягає потрібних цілей у сучасних конфліктах і війнах.

Крім того, в жодному з нормативних актів, що регулюють інформаційні відносини в нашій державі, ми не можемо зустріти поняття «інформаційної зброї», що дійсно ускладнює правозастосовну діяльність судів за її використання та є перепоною для правоохоронних, оборонних, безпекових структур у попередженні та вирішенні конфліктних ситуацій, встановлення складу злочину проти територіальної цілісності та державного ладу. Серед таких засобів інформаційної зброї є ті, що вже апробовані часом (наприклад, спеціальні психологічні операції), а також відносно нові (наприклад, специфічні комп'ютерні засоби боротьби), водночас вчені помічають у них спільну ознаку –

«усі вони засновані на ідеї опосередкованого впливу на матеріальний світ через світ інформаційний» [6, с.75].

Інформаційну зброю часто розуміють як деяку сукупність технічних, політичних, організаційних і інших засобів, за допомогою яких реалізуються інформаційні загрози. О. Литвиненко, підсумовуючи напрацювання американських фахівців, вказує, що існує багато видів інформаційної зброї, які можна об'єднати в чотири основні типи: 1) «засоби впливу на інформаційну інфраструктуру»; 2) «засоби розвідки, отримання інформації з інформаційних, телекомунікаційних і подібних систем»; 3) «засоби впливу на інформацію, яка обробляється в інформаційних системах, наприклад, на програмно-математичне забезпечення цих систем»; 4) «засоби впливу на суспільну свідомість» [48, с. 47].

Чимало засобів реалізації загроз для інформаційної безпеки, відтак можна розглядати як прояви використання інформаційної зброї, адже йдеться і про дезінформування, приховування інформації, порушення чинного порядку та перевірених каналів інформаційного обміну, і про несанкціонований доступ до інформаційних ресурсів держави й суспільства, і про чи необґрунтоване обмеження доступу до суспільно важливих джерел інформації, і про крайні прояви інформаційного тероризму, зумисне ушкодження інформаційного простору держави, розповсюдження комп’ютерних вірусів тощо.

За давніми пересторогами Г. Лазарева, дійсним результатом негативних інформаційних впливів є деформація інформації, що відтак спотворює інформаційне середовище держави, соціуму, їхніх інформаційних ресурсів, ускладнює та заплутує функціонування важливих державних, виробничих, наукових, фінансових систем, зрештою порушує національний інформаційний суверенітет [46, с. 81].

Мусимо також констатувати, що законодавством фактично не класифікуються та не пояснюються ані самі загрози інформаційній безпеці, що допомогло б завадити негативним інформаційним впливам, ані регламентуються правові легітимні механізми протидії ним. Водночас протидія загрозам в інформаційній сфері мала би передбачати: 1) моніторинг інформаційної сфери,

тобто системний аналіз чинників і агентів впливу на інформаційну сферу; 2) ранжування загроз, тобто встановлення пріоритетності загроз, реальних і потенційних небезпек; 3) профілактика і попередження негативного впливу загроз; 4) безпосередня протидія загрозам.

Отже, інформаційні загрози сфері слід визначати як систему зовнішніх та внутрішніх чинників, що чинять згубний вплив на інформаційну безпеку, зачіпаючи життєво важливі інтереси держави, суспільства та людини в інформаційній сфері.

Підсумовуючи викладене, зауважимо, що сьогодні в Україні питання її інформаційної безпеки є відкритим для обговорення, адже наявні в інформаційному просторі загрози постійно змінюються та активізуються, в основному у зв'язку з розвитком сучасних інформаційних технологій, які розширюють можливості для швидкого та об'ємного обміну інформацією як між окремими особами в Україні та за її межами, так і безпосередньо поміж країнами світу. Загрози інформаційній безпеці України є перепоною для належного інформаційного обміну, тому вважаємо, що одним із важливих напрямів щодо цього є вдосконалення вітчизняного законодавства, яким врегульовуються як правові, так і організаційні засади забезпечення інформаційної безпеки України.

## 2.2. Аналіз інформаційної безпеки держави в умовах глобалізації та кібербезпеки

У визначенні поняття «інформаційної безпеки як різновиду безпеки національної, який орієнтований на забезпечення прав і свобод людини, зокрема в питаннях вільного доступу до інформації, на створення і запровадження безпечних інформаційних технологій, на захист права власності всіх учасників інформаційної діяльності», слід мати на увазі, що означена категорія має глобальний характер, а тому й потребує розгляду в системі глобального (світового) інформаційного простору. Зупинимось на цьому детальніше.

Сучасна цивілізація характеризується специфічним основним ресурсом її глобального розвитку − інформацією. Це, з одного боку, надає людству, окремим спільнотам та індивіду нові можливості для розвитку й творчості, але з іншого − формує нові виклики та ризики, подолання яких вимагає від усіх суб'єктів загальноцивілізаційного, національного, державного, громадського розвитку докладання додаткових зусиль, спрямованих на посилення ефективності саме інформаційного виміру безпеки. У наших інших розвідках ми констатували, що наскрізна інформатизація всіх «сфер життєдіяльності суспільства і людини вимагає сьогодні особливо уважного ставлення з боку філософів, політологів, науковців до специфіки глобального характеру проблеми інформаційної безпеки» [34, с. 87]. Ми погоджуємося з дослідниками, які вбачають на межі століть зміни в самому сприйнятті інформації сучасним суспільством, коли соціальне значення комунікаційних технологій суттєво оновило наше розуміння світового розвитку, а «всепроникаюча у всі сторони життєдіяльності інформація» буквально трансформувала наші колишні уявлення про безпеку та пріоритети політичного життя. Це, приміром, знаходимо у зауваженні В. Ананьїна, який стверджує, що «в умовах тотальної інформатизації суспільства значну роль відіграють питання інформаційної безпеки» [4, с. 194].

Цікаво, що «перед сучасною людиною і суспільством постає в цьому аспекті складна дилема: з одного боку, інформатизація та глобальний інформаційний простір дають нам безліч нових можливостей до подальшого розвитку в різних сферах суспільної життєдіяльності, а з іншого – через інтенсивність самих інформаційних потоків та бурхливий розвиток технологій інформаційного обміну постійно виникають нові загрози безпеці людини і суспільства» [34, с. 88]. Відповідно, виникає запитання про те, «як вирішувати цю дилему за умов, коли ми вже не можемо відмовитися від процесів інформатизації та глобалізації?» [34, с. 88]. До того ж це вочевидь різні рівні осмислення проблематики для молодих демократій і тих, що вже утвердили свій демократичний вибір та орієнтацію на плідну міжнародну співпрацю (європейську інтеграцію, економічне співробітництво, культурний обмін тощо).

Якісне й ефективне забезпечення інформаційної безпеки держави залежить від низки факторів, які часто походять зі зовнішніх і навіть багатосторонніх джерел, тож тут складно говорити про рівні можливості чи універсальні правила політичної гри.

Питання гостро постало й для дослідників сучасних соціальних і політичних комунікацій, які також вивчають процеси глобалізації, що супроводжуються інтенсивним використанням у економіці, культурі, політиці сучасних досягнень високих технологій. Науковці, наприклад О. Ющук, зазначають, що саме «розвиток інформаційних технологій призвів до зростання відносної важливості окремих аспектів суспільного життя». Річ у тому, що «внаслідок інформаційної революції основною цінністю для суспільства взагалі й окремої людини зокрема поступово стають інформаційні ресурси». Тому, продовжує вчений, «організація соціуму почала трансформуватися у напрямку перерозподілу реальної влади від традиційних структур до центрів управління інформаційними потоками, зросла впливовість засобів масової інформації» [100, с. 224].

Згадані фактори, як ми констатуємо в інших працях, «зумовлюють актуальність концептуально-теоретичного аналізу глобального характеру проблеми інформаційної безпеки» [34, с. 188]. Так, «з одного боку, такий характер дозволяє розробляти певні універсальні форми та механізми захисту конкретного інформаційного простору. З іншого − саме глобальний інформаційний простір, що схильний до надвисокої динаміки розвитку, дуже часто ставить перед національними системами безпеки виклики, на які важко відповідати таким локальним та регіональним суб’єктам, як держави, соціуми, місцеві громади» [34, с. 188].

Саме тому, «актуальність і висока значимість поставленої нами проблематики визначається тим, що сьогодні на всіх рівнях суспільного функціонування необхідно проводити постійний пошук доволі хиткого балансу між тими можливостями, що надає нам глобальна інформаційна цивілізація, і тими ризиками, що з’являються через неможливість контролювати тенденції і

процеси інформаційно-соціального та інформаційно- технологічного розвитку» [34, с. 189]. Тобто сьогодні важливо розуміти як позитивні, так і негативні прояви цифрового світу, постійно розширювати горизонти залучення високих технологій в політичний процес, але прогнозувати і попереджати потенційні небезпеки, які можуть паралельно змінювати політичну картину світу.

На цю ж особливість, але у правовому аспекті звертають увагу вітчизняні правознавці, коли безумовно згадують сучасні переваги, наприклад, швидшої передачі інформації, збільшення її обсягів, можливостей для оперативного її опрацювання. Однак паралельно з тим, коли вони, зокрема Ю. Максименко, висловлюють тривогу з приводу «поширення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків та баз даних, порушення технологій обробки інформації, запуску програм-вірусів, знищення та модифікація даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку, маніпулювання суспільною та індивідуальною свідомістю тощо» [2, с. 13]. Відповідно, глобальний характер таких загроз ускладнює вироблення механізмів їх нівелювання, адже сьогодні щодня виникають нові технологічні виклики, на які не можна відреагувати за допомогою застарілих методів захисту. Саме тому глобальний характер проблеми інформаційної безпеки постійно актуалізує дослідження різних вимірів даної проблематики, а тому і в нашому дослідженні доцільно детальніше проаналізувати переваги та ризики переміщення інформації у глобальному інформаційному середовищі, що формується під впливом інформаційної революції.

Ми вважаємо, що насамперед, необхідно підкреслити абсолютно новий статус, що отримала інформація в рамках нової глобальної цивілізації. Адже інформаційний простір сьогодні не є виключно технологічним, віртуальним, контрольованим», а в сучасній цивілізації «перетворився на прості форми реальної суспільної життєдіяльності». Причому «ми не використовуємо

інформаційний простір, а живемо в ньому, підпорядковуючись абсолютно новим закономірностям розвитку, новим правилам поведінки, новим принципам виробництва і управління. В даний час особливо цінним є політико-філософський погляд на проблему, зокрема у форматі зауваження, яке робить С. Ягодзінський, що «інформаційні простори за своїми властивостями вже не збігаються з просторами віртуальної реальності», адже «їх не можна вимкнути, вийти з них». Тому, продовжує вчений, «інформаційний простір − це частина соціальної реальності, а отже він визначає параметри соціального простору і соціального часу» й «у такому розрізі феномен інформаційної реальності є предметом філософського та політологічного аналізу» [101, с. 77]. При цьому, ми вважаємо, що такий аналіз також має проводитися з врахуванням нових реалій, виявляючи абсолютно нові за своєю сутністю можливості, ризики і суперечності, що визначають тенденції світового, національного і особистісного розвитку.

Переваги інформаційного суспільства сьогодні відчутні у більшості сфер суспільного життя, у політичному сенсу це шлях до прозорості урядів, демократичності рішень, полілогічності політичних дискусій тощо. Сучасні вчені, зокрема О. Золотар, навіть вбачають «своєрідну трансформацію інформації, яка в наш час ототожнюється з простором реальної взаємодії суб'єктів соціальної життєдіяльності» [36, с. 106]. В той же час, ми констатуємо, що «непристосованість до нових реалій несе в собі безліч ризиків, що призводять до складних суперечностей як в житті окремої людини, так і у життєдіяльності цілих соціальних спільнот, включаючи нації та держави, політичні утворення різного рівня, а також глобальну людську цивілізацію в цілому.

Як наслідок цього, ми аналітично констатуємо, що саме через різноманітність та динамічну змінність тих викликів і суперечностей, що постійно виникають внаслідок розвитку інформаційного суспільства, сьогодні надзвичайно актуалізується концептуально-теоретичний аналіз глобального характеру проблеми інформаційної безпеки. Відповідно, винятково в такому її вимірі, з нашої точки зору, уможливлюється реальний пошук дієвих механізмів

її забезпечення. Новітні інформаційні та телекомунікаційні технології у сфері політики загалом та міжнародних відносин зокрема знову ж тісно пов’язують політичний і правовий контексти. Це одночасно формування нового глобального інформаційного середовища, та збереження вже встановлених ціннісних орієнтирів, загальнолюдських сенсів і норм, підважування яких руйнує основи світової стабільності.

Тому для політології тут також важливі чіткі правові означення, які у системі інформаційної безпеки вбачають можливість для налагодження широкого міжнародного співробітництва, але також і протидію активізації раніше невідомих видів злочинності, попередження інформаційного протиборства між країнами. Тобто у контексті міжнародної безпеки та розвитку науковці, зокрема Р. Алямкін, пишуть «про розв’язання проблеми захисту інформаційних ресурсів, а також підвищення надійності та стабільності функціонування електронних засобів зв’язку, передовсім мережі Інтернет» [3, с. 91].

Саме внаслідок цього ми стверджуємо, що при дослідженні проблеми інформаційної безпеки важливо враховувати її міжнародний і глобальний характер. Окрім того, варто говорити про можливості формування ефективної системи державної чи національної інформаційної безпеки без партнерства в цій сфері з іншими суб’єктами міжнародних відносин, державами, транснаціональними корпораціями, міжнародними організаціями.

Отже, нормативно-правові аспекти також збагачують власне політологічні візії проблематики. У цьому слід відзначити, що сьогодні ключові геополітичні гравці глобального світу всіляко намагаються виробити ефективні правила співробітництва і партнерства з метою повноцінного використання переваг та нівелювання ризиків, що створюються завдяки переміщенню інформації у глобальному інформаційному просторі, що формується та розвивається під впливом інформаційної революції.

Політологічний аналіз орієнтує на інституційне забезпечення, регулятивне розмежування, а також загалом геополітичне, концептуальне розуміння основ

міжнародного співробітництва під впливом сучасного інформаційного простору. Політологи пишуть про потребу «якісно нового бачення архітектури міжнародної безпеки», що у сьогочасних реаліях зазнає інформаційних спотворень і маніпуляцій, деструктивних комунікаційних атак, інформаційного тероризму, та й загалом перебуває у полі невизначеності, перманентних змін, подвійних стандартів [79, с. 3].

Ці реалії міжнародної інформаційної безпеки безумовно позначаються й на потенціалі та межах національних систем, коли розвиток технологій випереджає державні потужності і ресурси для адекватного реагування на них, а міжнародні стандарти часто лише формуються та мають здебільшого декларативний характер. Водночас ми констатуємо, що для України особливо актуальною проблемою є те, що в глобальному інформаційному просторі особливо підсилюється роль глобальних гравців, а менш впливові суб'єкти міжнародних відносин просто потрапляють в поле їх інформаційних впливів, перетворюючись на об'єкти. Відповідно, ми постулюємо питання в аспекті національної інформаційної безпеки України про те чи існує можливість запобігання цьому негативному виміру глобального інформаційного простору?

Шукаючи відповідь на нього, зазначаємо, що одним з ключових викликів і ризиків, що постають перед Україною в контексті глобального характеру проблеми інформаційної безпеки, є втрата власної національної ідентичності, державного суверенітету, особливо інформаційного суверенітету, який визнається сьогодні ключовою ознакою державної самостійності та правосуб'єктності.

З цього приводу погоджуємося з О. Дубасом, який всебічне вивчення можливостей, потреб і специфіки інформаційного розвитку в сучасному світі та в Україні бачить дійсним і важливим напрямком для збереження національних культурних і політичних особливостей, інструментом зміцнення діалогу культур, більше того – вагомим підготовчим етапом національної держави для «адекватної відповіді викликам і соціальним небезпекам, які таїть у собі

глобалізація» [23, с. 3]. Науковий потенціал у забезпеченні національної системи інформаційної безпеки сьогодні несправедливо недооцінюється.

Таким чином ми констатуємо, що одним з ключових вимірів проблематики інформаційної безпеки сьогодні є пошук адекватного балансу між впливами глобального характеру, що ґрунтуються на інтенсифікації переміщення інформації в глобальному інформаційному середовищі, та потребами окремих людей та соціальних спільнот, в тому числі держав і націй, що не є провідними суб'єктами, здатними впливати на глобальні цивілізаційні тенденції та процеси. Причому, не можна відкидати і переваги, що створюються завдяки більш вільному та швидкому переміщенню інформації у глобальному інформаційному середовищі, що формується під впливом інформаційної революції. Річ у тому, що одна з таких переваг полягає в тому, що гарна поінформованість розвиває громадянські якості, що сприяє інтенсифікації розвитку громадянського суспільства в різних країнах і регіонах світу. Вчені пишуть, що так звані «громадяни цифрового світу» порівняно менш байдужі у соціальних і політичних справах, вони не відсторонюються від інших, усвідомлюють значимість ефективних інститутів і функціональної системи; вони є частиною онлайн-світу, і саме його здатність поєднувати пасивних абсентеїстів і політично активних громадян дозволяє долати прояви неуцтва [68, с. 67]. Ми ж вважаємо, що в Україні також необхідно повноцінно використати громадянський ресурс глобальної інформаційної цивілізації», адже «такий ресурс може бути дуже корисний при реалізації різноманітних громадянсько-просвітницьких та освітніх проектів. Особливо на тлі того факту, що «саме розвиток громадянських якостей людей, однією з яких є вміння фільтрувати складні інформаційні потоки, може стати в пригоді при протидії ризикам інформаційних впливів і агресивних дій.

В той же час, слід помітити, що на фоні активізації громадянської активності, що відбувається завдяки простішому переміщенню інформації, створюються передумови і для значних негативних ефектів, одним з яких є загроза втрати національно-культурної ідентифікації. Відповідно, користуючись новітніми інформаційними технологіями, людина отримує безліч можливостей

занурюватися в глобальне середовище цінностей і смислів, що повністю втратили національно-культурне коріння. Соціологи в Україні, приміром Т. Рудницька, вже застерігають, що «користувачі Інтернету становлять модернізовану групу, яка за своїми соціокультурними характеристиками значно ближча до представників інших культур у глобальному інформаційному просторі, ніж до українського населення, не охопленого Інтернетом» [79, с. 8]. Таким чином, ми аргументуємо, що важливо в будь-якому аспекті дослідження проблематики інформаційної безпеки звертати увагу на такий подвійний вплив інформаційної революції, коли люди, отримуючи нові корисні можливості, втрачають важливий зв'язок з традиціями, що визначають їх національну, суспільно-групову, особистісно-духовну ідентичність.

Продовжуючи цю логіку, ми зазначаємо, що в аспекті переваг та ризиків переміщення інформації у глобальному інформаційному середовищі, що формується під впливом інформаційної революції, проблематика інформаційної безпеки має розглядатися в якості концептуального ядра, навколо якого вибудовується вся система сучасних соціальних, економічних, політичних, національно-безпекових відносин. Суголосні нашим є міркування вчених, які в інформаційній безпеці вбачають елемент, з якого по суті вибудовується цілісна система національної безпеки. Так, Н. Крилова стверджує, що в інформаційному суспільстві канали, мережі і системи інформації та комунікації стають, так би мовити, і нервовою, і серцево-судинною системою суспільства водночас», а тому «розробка та поширення інформаційних засобів впливу та мирні моменти співіснування відбуваються одночасно у межах інформаційної протидії. Саме через це, продовжує вчена, «збереження стану рівноваги у стосунках, скоріше за все, і буде визначником інформаційної безпеки» [45, с. 427]. Завдячуючи цьому висновку, ми помічаємо, що в умовах глобального характеру сучасних безпекових механізмів неможливо виносити інформаційну безпеку людини, соціуму, держави за межі глобально-цивілізаційних тенденцій», адже «ті суб'єкти, які готують інформаційні загрози, операції, війни, повноцінно використовують глобальний характер сучасного інформаційного середовища,

застосовуючи всі можливі інформаційно-технологічні та психологічні можливості впливу.

Підсумовуючи, ми наполягаємо, що важливо розуміти, що всі переваги та ризики переміщення інформації у глобальному інформаційному середовищі, що формується під впливом інформаційної революції, безпосередньо пов'язані між собою. Відповідно, для того «щоб скористатися перевагами, яких дійсно багато, необхідно вибудовувати таку систему інформаційної безпеки, яка б дозволила максимально нівелювати всі можливі ризики, реальні загрози та суперечності. Причому серед переваг глобалізованого інформаційного простору традиційно, як вважає Н. Глебова, називають «науково-технічний і суспільний прогрес, міжкультурне співробітництво, підвищення рівня життя» [13, с. 26], кожна з цих позицій заслуговує окремого напрямку політичної активності, самостійного урядового порядку денного, розгорнутих і багатосторонніх суспільних комунікацій, які суттєво збагачують якість та зміст національної політики. Часто ми недооцінюємо або ж навпаки переоцінюємо наслідки інформаційних здобутків, коли ж натомість найефективнішим видається збалансований та максимально об'єктивний погляд на комплекс проблем.

Важливо, що тут не завжди доречним виглядають спроби масштабування цих проблем аж до загроз «втрати національної та соціальної автентичності», позбавлення свободи, «нової форми тоталітаризму», але цілком виправданими видаються вимоги виробляти спільні позиції, оновити підходи, напрацювати організаційно-правові, суспільно-економічні і комунікаційно-технологічні норми регулювання інформаційної сфери як у планетарному, так і в національному масштабах [13, с. 26]. У цьому процесі особливо цінними є такі політичні принципи та засоби як оперативність, розмежування рівнів комунікаційного контролю, чітке маркування джерел інформації, відкритість, але також і усування вразливостей до ворожих інформаційних потоків, стратегічна орієнтованість, організованість та координованість дій і взаємодій з глобальним інформаційним простором.

Враховуючи все це, Україна має затвердитися в глобальному цивілізаційному середовищі в якості конкурентоспроможного суб'єкта. Ми наполягаємо, що для цього дуже важливо використовувати всі інструменти ефективного розвитку, що надаються технологічним простором інформаційного суспільства. Водночас, на нашу думку, необхідно облаштувати надійну національну систему інформаційного захисту від безлічі інформаційних загроз, що йдуть від внутрішніх і зовнішніх впливів, а також з боку глобальних факторів небезпеки, притаманних самій структурі інформаційної цивілізації.

Все це дозволяє аргументувати, що перед українською державою на сучасному етапі державотворчих трансформацій постає складне завдання: максимально використати інформаційно-технологічні, соціально-структуруючі, масово-інформаційні можливості, що надаються інформаційної цивілізацією, і при цьому захистити власних громадян та державний організм від ураження з боку руйнівних і загрозливих зовнішніх і внутрішніх інформаційних впливів.

Ми погоджуємося з вченими, які серед обов'язків кожної держави називають і забезпечення вільного та незалежного функціонування засобів масової комунікації, і, як помічає Ю. Горбань, дотримання стандартів свободи слова, інформаційних прав і свобод громадян [14, с. 40], і захист національних інформаційних ресурсів, і створення розвинутого та сучасного інформаційного простору, конкурентоспроможного на світовому та національному ринках. Таким чином, ми з впевненістю наполягаємо, що успішність та конкурентоспроможність нашої держави безпосередньо залежить від того, наскільки ефективну систему інформаційної безпеки вона вибудує на фоні значного зростання переваг та ризиків інтенсифікації циркуляції інформації у глобальному інформаційному середовищі, що формується під впливом інформаційної революції та глобалізованої цивілізації.

Попри це формулювання стратегії інформаційної безпеки держави дійсно залежить від активності держави стосовно напрацювання контрольованих нею інформаційних потоків. Саме активність державних організацій у справі створення власного конкурентоспроможного інформаційного продукту визначає

здатність досягати своїх цілей у глобальному інформаційному середовищі. Вчені наголошують, що визначальним у сучасній «інформаційній і комунікаційній ері» є медіа, а також більш широка проблематика виробництва, поширення, володіння, маніпулювання інформаційними технологіями. Заміщувати неконтрольовані інформаційні виклики, витісняти шкідливі впливи, випереджати загрозливі атаки – усе це комплекс реакційних тактичних заходів і завдань зі стратегічного бачення інформаційної безпеки, натомість заповнювати інформаційне середовище щонайбільшою кількістю контрольованих та суспільно важливих обмінів – ознака максимально збалансованої та продуманої стратегії держави у цій галузі. Активна позиція відрізняє лідерів інформаційного простору на міжнародному ринку, а також успішні держави у глобалізованому світі.

Успішні стратегії у цій галузі відрізняє розуміння інформації як управлінського ресурсу, як корисного інструменту взаємодії (при чому як у глобальному світі, так і на внутрішньому суспільно-політичному ринку). Таке розуміння, а найголовніше – його практичне втілення у політиці передбачає, що інформація має відповідно збиратися, аналізуватися, продукуватися та зрештою організовуватися. Структурована та функціонально розподілена вона стає потужним статусним інструментом політичної влади та державної безпеки, вона унормовує відносини і процеси в політиці, збагачує політичний світогляд та політико-правову культуру суспільства. Сучасне державне управління, місцеве самоврядування, політичне адміністрування складно організувати без здійснення впорядкованої, системної, чітко орієнтованої політики, що базується на принципах грамотної роботи з інформацією та інформаційної безпеки. До того на рівні держави і громадянського суспільства це система розгалужена, коли контрольовані інформаційні обміни додають ефективності, взаємної користі та стабільності партнерським відносинам.

Стратегічне бачення Україною інформаційних загроз сьогодні залежить і від наукових, фундаментальних визначень пріоритетів у цій політиці, і від фактичних дій та практик, які застосовує держава в умовах ведення справжньої

інформаційної війни, в якій постійно перебуває. Те саме стосується й інших суб'єктів політики, які окремо поза державною стратегією інформаційної безпеки ризикують втратити і власну суб'єктність у політичному житті суспільства, і навіть цілковито увесь цей простір незалежного функціонування.

Глобалізація інформаційного середовища стосується не лише держави, адже цей всеохопний процес привносить та змінює більшість суб'єктів і об'єктів сучасної політики, серед яких важливу рол відіграють засоби масової інформації. Проблема, безумовно, міждисциплінарного характеру, тож нашу увагу привернуло дослідження А. Юричка, який вивчає інформаційні маніпуляції у світовій періодичній пресі з позицій сучасної журналістики. Зокрема він зазначає, що такі маніпулювання (через ЗМІ) набули сьогодні масового характеру, більше того, коли медіа використовують сучасні технології інформаційно-психологічного впливу – це найчастіше пов'язано з утвердженням певного політичного впливу та виконанням конкретних політичних завдань. Це очевидно з його позиції про те, що «політичне маніпулювання інформацією, що реалізується через зарубіжні ЗМІ, зокрема, в Україні, є серйозною загрозою, як головним засадам розбудови демократичного суспільства і зміцненню незалежності України, так і особистій інформаційно-психологічній безпеці громадян» [99, с. 3].

Глобалізаційні процеси однаково вражають у якості об'єктів інформаційної війни як великі держави, нації, міжнародні організації та їх союзи, так і комерційні компанії, громадські організації локального рівня, партійні осередки чи просто авторитетних і впливових політичних діячів.

Провокують подібні акти інформаційної агресії зазвичай технологічно та ресурсно потужні структури, серед яких і транснаціональні корпорації, і держави-лідери, що водночас зрідка прямо визнають свою суб'єктність у започаткуванні інформаційних воєн, але активно діють через посередників, беруть участь у відповідних публічних дискусіях, прийнятті рішень тощо.

Нові технології в інформаційній війні пов'язанні не лише зі збільшенням швидкості та обсягів передачі інформації, це також осучаснення та

пристосування маркетингових заходів до цілей інформаційної агресії. Якщо фізичне насильство засуджується усією цивілізованою глобальною спільнотою, то можливості та прояви насильства інформаційного, яке часто пов'язане з технологіями агресивного маркетингу, поки ще мало вивченні, слабко контрольовані та майже не надаються офіційним оцінкам. Ініціатори інформаційних воєн часто користуються можливостями сучасного відкритого глобального інформаційного простору, тією відносно легкою доступністю до свідомості пересічних громадян та активних політиків. У цьому контексті загальна переконливість, емоційність інформаційних повідомлень, першість у їх донесенні, технології самопозиціонування і рекламування ваговитіші за аргументовані та підкріплені раціональним фактажем відомості. Сучасні споживачі інформації мають можливість (хоча далеко не завжди нею користуються) отримувати повідомлення з різних джерел, від кожної сторони-супротивника інформаційної війни. Це може призводити і до різних наслідків: від перетворення споживача інформації у войовничого прихильника однієї зі сторін конфлікту до цілковитого розчарування, сумнівів, аполітичності людей тощо. У будь-якому разі йдеться про боротьбу за громадську думку, яка є важливим об'єктом інформаційної війни.

Трансформація сучасного українського суспільства в процесі загальнодержавного курсу на побудову цифрової економіки та суспільства обумовлює вирішення комплексу соціально-економічних, політичних та ресурсних завдань.

Однією з проблем вироблення державної політики України є відсутність необхідних цифрових (електронних) стандартів діяльності органів публічної влади. Тому формування державної політики у сфері кібернетичної безпеки є важливим стратегічним завданням, від успішного вирішення якого залежать зростання економічного потенціалу країни, якості життя населення, національної безпеки та міжнародного співробітництва.

Ефективна діяльність всіх важливих сфер країни в середовищі кіберпростору означає вихід на якісно новий рівень розвитку індустріалізації, за

умови якщо в якості основного ресурсу суспільного розвитку виступає інформація. Для України лише нещодавно середовище кіберпростору, а, відтак, гарантування кібербезпеки стали актуальними викликами в сфері дотримання і забезпечення національних інтересів. Сфера інформаційної (кібер) безпеки потребує суттєвих ресурсів і системних напрацювань для здійснення її належного контролю і гарантування на всіх рівнях діяльності органів публічної влади.

Необхідність вироблення державної політики у сфері кібербезпеки на етапі переходу до нового типу організації суспільства, його політичних і соціально-економічних систем, що ґрунтується на пріоритетах цифровізації, які пов'язані з формуванням нової управлінської парадигми і необхідністю розвитку нових демократичних механізмів. Для України реалізація політики цифровізації формує перспективи суспільного розвитку, які перебувають у площині розбудови цифрової економіки як моделі сервісної держави з розвиненими демократичними інститутами і механізмами взаємодії основних суб'єктів державно-управлінського процесу.

Кібербезпека як цілеспрямована діяльність створює, насамперед, умови захищеності від фізичних, фінансових, політичних, професійних, психологічних, та інших типів впливів або наслідків аварії, ушкодження, помилки, іншої шкоди або будь-якого іншого втручання чи події в кіберпросторі, які можна потрактувати небажаними та загрозливими. Таким чином, за умови провадження безпеки в цьому середовищі, всі складові кіберпростору повинні бути захищені від максимально можливої кількості загроз та небажаних наслідків.

Сфера кібербезпеки складається з стандартів, норм, стратегій, принципів формування, засобів реалізації, інструментів управління, та запобігання ризиків, що в комплексі формує системний інструментарій (механізмів державного управління) здійснення захисту інформації та даних в кіберсередовищі. В межах окремо взятої організації система захисту спрямовуватиметься на безпосередні ресурси, які складаються:

– з цифрових засобів та інфраструктури інформаційної мережі, яку вони утворюють;

– комунікаційних систем зв’язку, що забезпечують передавання, поширення та збереження інформації;

– запропоновано персоналу, який обслуговує цю інфраструктуру та здійснює операції та сервіси у сфері кібербезпеки.

Тому важливо все ж наголосити, що кібербезпека більшою мірою все ж включає людський ресурс з належним рівнем підготовки. В Україні ще недостатньо досвіду в підготовці фахівців такого рівня, що негативно впливає на кадрове забезпечення відповідних органів влади, оскільки білвшість фахівців, які задіяні у системі реалізації кібербезпеки не відповідають встановленим компетентісним вимогам [31, с. 123], що, в свою чергу, актуалізує розробку фахових програм з підготовки та використання міжнародного досвіду для забезпечення належного професіоналізму в сфері кібербезпеки.

На сьогоднішній день, національну систему кібербезпеки формують ряд державних інституцій як центрального так і місцевого рівня, військові структурні підрозділи, установи, заклади та організації, які задіяні в галузі комунікацій, опікуються питаннями захисту інформації та мають в своєму розпорядженні об'єкти критичної інформаційної інфраструктури.

Серед визначених пріоритетних напрямів провадження кібербезпеки можна назвати такі, як:

– цілісне формування державної політики у сфері кібербезпеки, що досягається за рахунок сумісності з міжнародними стандартами Євросоюзу та НАТО;

– опрацювання вітчизняної нормативно-правової бази у сфері кібербезпеки, та її узгодженість з нормативними документами у сфері захисту інформації та кібербезпеки, цифрових комунікацій відповідно до прийнятих міжнародних стандартів;

– розвиток інфраструктури електронних комунікацій, в тому числі доступу до інтернету;

– посилення міжнародного співробітництва у сфері кібербезпеки, долучення до міжнародних ініціатив в даних питаннях шляхом співпраці з ЄС та НАТО [28].

Також важливими напрямами діяльності в сфері кібербезпеки є формування конкурентного середовища електронних комунікацій з можливістю надання послуг із захисту інформації; проведення навчань щодо усунення надзвичайних ситуацій у кіберпросторі; розвиток та удосконалення системи державного контролю щодо захисту інформації, а також системи незалежного аудиту інформаційної безпеки [97].

Звичайно, Стратегія кібербезпеки визначає лише загальні принципи та окреслює орієнтовні напрями дії в питанні забезпечення кібербезпеки в Україні. Фактично вперше в українському законодавстві сферу кіберпростору визнано важливою ділянкою національних інтересів, проте це потребує ще вагомого доопрацювання в напрямку законодавчо-нормативного та правового вдосконалення і регулювання кібербезпеки в контексті загального провадження інформаційної безпеки країни, з огляду на взаємопов’язаність різних галузей економіки, банківського сектору, державного управління, оборони тощо.

Задля реалізації окреслених напрямів захисту в сфері кібербезпеки було утворено спеціальний Національний координаційний центр кібербезпеки, що фактично є робочим органом Ради національної безпеки і оборони України (Указ Президента України від 7 червня 2016 року № 242/2016). Основними завданнями і повноваженнями центру визначено аналіз та моніторинг стану кібербезпеки, захист державних інформаційних ресурсів, а також заходи, спрямовані на упередження кіберзлочинів та прогнозування появи [70].

У 2017 р. в Україні прийнято Закон «Про основні засади кібербезпеки України» [72], в якому визначено критично важливі об’єкти інфраструктури – «… підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або

порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей» [72].

За результатами дослідження встановлено, що у Законі України «Про основні засади кібербезпеки України» є певні недоліки. Зокрема, поданий Закон України не визначає підстави віднесення організацій (незалежно від форми власності) до суб'єктів критичної інформаційної інфраструктури і, як наслідок, інформаційні системи, інформаційно-телекомунікаційні мережі та автоматизовані системи управління, які належать цим організаціям, виходячи із Порядку формування переліку об'єктів критичної інформаційної інфраструктури, також не зазначені. Така невизначеність уповільнює ідентифікацію критичних інформаційних систем і знижує рівень ефективності забезпечення безпеки [38, с.13].

В системі кібербезпеки України задіяно декілька силових інституцій та їх структурних підрозділів, зокрема Міністерство оборони України (серед спеціальних підрозділів - Головне управління розвідки), Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, Міністерство внутрішніх справ України (Департамент кіберполіції), Служба зовнішньої розвідки України.

Питання провадження інформаційної та кібербезпеки, створення національної системи кібербезпеки відображені також в Концепції розвитку сектору безпеки і оборони України, затвердженій Указом Президента України від 14 березня 2016 р. № 92/2016. Зокрема визначено, що ця проблематика, з огляду на триваючу збройну агресію з боку Російської Федерації, є одним із основних завдань сектору безпеки і оборони, забезпечення якого можливе з використанням ресурсів цього сектору та спрямовуватиметься для боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю [49, с.132].

Для посилення діяльності в сфері захисту інформації та кібербезепки відповідно до Постанови Кабінету Міністрів України від 13 жовтня 2015 р. [41] було утворено спеціальний Департамент кіберполіції в структурі Національної поліції України, спеціалізацією якого визначено попередження, виявлення, припинення та розкриття кримінальних правопорушень, пов'язаних зі злочинами в кіберсередовищі (зокрема з використанням комп'ютерів, телекомунікацій та комп'ютерної мережі інтернет). Такий структурний підрозділ було утворено в рамках реформування та розвитку підрозділів МВС України і створення на їх базі Національної поліції. В свою чергу, це спонукало здійснення підготовки фахівців відповідного напряму в експертних, оперативних та слідчих підрозділах поліції, задіяних у протидії кіберзлочинності.

У рамках міжнародного співробітництва Державна служба спеціального зв'язку та захисту інформації України в 2014 р. уклала угоду про співпрацю з компанією Microsoft, де, зокрема, передбачалося, отримання доступу до інформації, що акумулюється в центрі Безпекового реагування Microsoft щодо кіберзагроз, джерела мережевих атак. Відповідно до Програми безпекової кооперації, що є окремим додатком, урядові організації спільно з Microsoft мають можливість реагувати на комп'ютерні інциденти та запобігати наслідкам кібератак. Такий крок є важливим в питанні розвитку кібербезпеки, що відкриває нові можливості для розвитку інформаційного захисту в державному секторі України.

Зазначимо, що головними тенденціями розвитку кіберзагроз у сучасних інформаційних протиборствах є:

– збільшення кількості кібератак, спрямованих на нанесення широкомасштабної шкоди інфраструктурам великих корпорацій, важливим промисловим об'єктам, а також інформаційним системам органів державної влади;

– зростання рівня складності кібератак, які реалізуються поетапно та адаптовані спеціальними інструментами протидії захисту від супротивника;

– тотальність впливу на всі цифрові (електронні) технології, зокрема мобільні (мережеві) пристрої, які є апріорі максимально вразливими з точки зору інформаційної безпеки;

– комплексне застосування в геополітичному просторі новітніх технологій кібернападу одних країн на інші (інформаційна війна реалізується на міждержавному рівні).

Тому, необхідність побудови дієвої системи кібернетичної безпеки України обумовлена наявністю протиріччя між необхідністю більш широкого впровадження цифрових технологій в усі сфери людської діяльності та підвищенням рівня їхньої безпеки.

Кібер інфраструктура державних органів влади в Україні досі залишається уразливою і не в останню чергу через надмірно широке використання комерційних програмних продуктів та використання матеріально-технічної бази іноземного виробництва.

Крім того, важливу роль у протистояннях в глобальному кіберпросторі, й передусім у відстеженні та подальшому аналізі кібератак, відіграють різноманітні приватні безпекові організації, які часто поєднують свою основну діяльність з виробництвом антивірусних продуктів. Серед таких компаній відзначимо McAfee, Avast, Kaspersky Lab, ESET, F-Secure та ін. Саме вони завдяки більшій свободі у своїй діяльності все частіше стають викривальниками масштабних кібероперацій, у т.ч. таких, як Stuxnet, Flame, Red Octobr [31, с.124]. В Україні фактично не існує потужної організації подібного масштабу, а чи не єдиним антивірусом національного виробництва є «Zillyal», який лише починає освоювати український ринок програмного забезпечення.

Події останнього часу, пов’язані з вірусними кібератаками, ще раз підкреслили важливість цієї сфери для країни та показали уразливість всієї системи національних інформаційних комп’ютерних мереж. Так, в травні 2017 р. численна кількість комп’ютерів в понад 150 країнах світу зазнали атак від вірусу «№вимагача» під назвою «Wanna Cry», що являв собою шкідливе програмне забезпечення, яке поширювалося через електронну пошту. Програма

«WanaCryptOr 2.0» атакує комп’ютери на яких встановлено операційну систему «Windows». Програмою було використано так звану «діру» в системі безпеки Microsoft Security Bulletin MS 17-010, про існування якої раніше було невідомо.

Зазначимо, що так звані віруси «шифрувальники» є особливо шкідливими, оскільки зашифровують файли ураженого комп’ютера за допомогою унікального ключа, розшифрування якого потребує значних обчислювальних потужностей, що фактично унеможливлює його знешкодження (лікування пересічними користувачами).

Згодом відбулася інша хакерська атака за допомогою вірусу «Petya», від якої постраждали комп’ютери нафтових, енергетичних, телекомунікаційних, фармацевтичних компаній та державних органів Данії, Франції, Великобританії та США. Глобальна атака віруса «здирника» модифікації «Petya.A» вразила інформаційні системи компаній багатьох країн світу, проте, особливої шкоди він завдав електронній інфраструктурі органів державної влади України. Українські органи влади та приватні компанії через електронний документообіг масово одержали вірус «шифрувальник» завдяки вразливості програмного забезпечення «M.E.doc». При чому, ураження комп’ютерів відбувалося здебільшого під час оновлення згаданого виробника програмних продуктів. Від ураження вірусом постраждали як урядові органи, так і великі підприємства, зокрема деякі обленерго, мережеві супермаркети, аеропорт «Бориспіль», компанія «Нова Пошта».

Другий етап вірусної атаки «Petya» було вже упереджено зусиллями кіберполіції та СБУ. На думку військових експертів та аналітиків, простежується причетність до розробки та поширення цього вірусу російських спецслужб Російської Федерації. Атака на електронну інфраструктуру органів державної влади України розглядається як елемент кібервійни проти України в рамках ведення гібридної війни.

Після інтервенцій вірусів «Petya» / «Petya.A» представники ОБОЄ та посольства Великої Британії передали підрозділам кіберполіції Національної поліції України 194 одиниці спеціального обладнання для боротьби з

кіберзагрозами [55]. Втім, така акція не може подолати всіх проблем України в питанні протидії кіберзагрозам та своєчасного їх упередження. Реалізація ефективного провадження інформаційної безпеки потребує комплексного підходу, з огляду на існуючий досвід зарубіжних країн та постійний моніторинг ситуації в даній сфері.

Слід зазначити, що найбільшої кількості нападів і загроз зазнають стратегічно важливі комунікаційні мережі, які забезпечують функціонування держави в цілому, її оборонний, фінансовий, банківський сектори. Саме на такі об’єкти критичної інфраструктури і спрямовуються кібератаки, що мають на меті перешкодити повсякденній діяльності органів державної влади України шляхом виведення з ладу технічних засобів та порушення штатного режиму функціонування.

Вчинення умисного втручання (інтервенції) в системи національних комунікаційних мереж з боку зловмисних суб'єктів, безперечно зачіпає важливі соціально-політичні та фінансово-економічні інтереси країни та дає підстави вважати це злочином. Оскільки здійснення подібних дій можливе тільки з використанням комп’ютерних систем і в кіберпросторі, то такий вид злочину називається кібернетичною війною або кібернетичною інтервенцією (кіберінтервенцією) [16, с. 237].

Аналізуючи загрози інформаційній безпеці України з точки зору зовнішніх викликів і розв’язаної збройної агресії, що переросла в гібридну (в тому числі інформаційну) війну, необхідно відзначити негативну тенденцію до збільшення різноманітних інформаційних матеріалів із відвертою антиукраїнською спрямованістю та упередженим висвітленням фактично всіх внутрішніх і зовнішніх подій, які відбуваються як в Україні, так і за її межами та за участі міжнародної спільноти. Російські мас-медіа, які підконтрольні кремлівській владі є безпосередніми учасниками (і засобами) зовнішньо політичної агресивної політики, забезпечують інформаційну підтримку дій її керівництва щодо України та її інтересів.

Така гібридна війна постійно супроводжується інформаційно-психологічними атаками, фейками, викривленим поданням інформації. Інформаційні операції для забезпечення медійної переваги з боку Росії постійно вдосконалюються та набувають нових форм за рахунок блокування українських теле-, радіо-каналів, особливо, на окупованих територіях [16, с. 328].

Можливість здійснення такої інформаційної інтервенції пояснюється недостатнім рівнем кібербезпеки в українському інформаційному середовищі.

Обумовлено це відсутністю чіткого правового регулювання національної державної політики в сфері кібербезпеки, а також відсутністю єдиної державної структури управління (принаймні нею могла б стати Державна служба спеціального зв'язку та захисту інформації України), яка б координувала протидії кіберзлочинам чи кібератакам (вирішення таких питань на рівні Департаменту кіберполіції Національної поліції України є недостатнім), внаслідок чого існує постійна загроза критичній інфраструктурі держави. Проблеми стосовно ключових питань інформаційного захисту на всіх рівнях спричиняючи зростання комп'ютерного шахрайства, кіберзлочинів у сфері обігу персональних даних, зі зламуванням певної інформації. Водночас, використання сучасних інформаційних технологій в безпековій сфері, як, наприклад, створення єдиної автоматизованої системи управління Збройними силами України, сприяючи посиленню рівня безпеки перед кіберзагрозами.

Серед інших загроз в сфері кібербезпеки можна виокремити кібертероризм та кібершпигунство, кібервійну (в тому числі інформаційну гібридну), невід'ємними складовими яких є безпосередні кіберінтервенції, що складаються з кібератак та інших втручань. Так само на рівні повсякдення все звичайнішою практикою в житті пересічних громадян стають злочини із застосуванням сучасних інформаційно-комунікаційних систем і мереж, засобів зв'язку.

З огляду на активізацію упровадження цифрових технологій у всі сфери життєдіяльності людини та держави, протистояння у кіберпросторі шляхом проведення кібератак виходити на новий загрозливий рівень. Крім того, це призводити до змін у реалізації державної політики більшості провідних країн у

бік здійснення жорсткого контролю за власним кіберпростором та посиленням обмежувальних заходів [43, с. 181].

Так увага до реалізації кібербезпеки та створення засобів ведення боротьби у кіберпросторі змушує органи державної влади багатьох країн переглядати й внутрішню політику, що було обумовлено зростанням кількості випадків використання розвідувальними службами та спеціальними військовими підрозділами функціональних можливостей та технічних потужностей транснаціональних кримінальних груп, які спеціалізуються у сфері кіберзлочинності.

Кіберзлочинність, як явище з'явилось практично одночасно з розвитком мережі інтернет. А оскільки інтернет продовжує розвиватись, то відповідно і кіберзлочинність набуває все нових форм і охоплює нові території. Варто зазначити, що саме середовище мережі інтернет є сприятливим для вчинення протиправних дій (анонімність, глобальність і т.п).

Першим зафіксованим інтернет-зломом, було злочинне діяння, вчинене групою неповнолітніх підлітків, які називають себе «група 414». Упродовж дев'яти днів «група 414» взломала більше 60 ПК, серед яких були комп'ютери Лос-Аламоської національної лабораторії, що займається дослідженням ядерної зброї. Саме після цього випадку в найкоротші терміни було створено Центр дослідження Інтернет безпеки CEЯT, для фіксування і дослідження нового виду злочинності. У вісімдесятих роках минулого століття спостерігається яскравий сплеск зростання кібератак. Якщо в 1988 р. їх було зафіксовано всього б, то в 1989 р. - 132, а в 1990 р. - 252, за 2017 р. лише в Україні кількість кібератак зросла з 10 млн. до 100 млн. [19].

Таке збільшення кількості атак пов'язують з прогресом у сфері цифрових технологій, які не завжди є досконалими, чим успішно користуються зловмисники. Також кіберзлочинці постійно вдосконалюють свою тактику, проводячи польові випробування шкідливих програм, блокують засоби контролю і управління. Вони використовують шифрування і легальні інтернет-сервіси, щоб приховувати свою діяльність і подолати традиційні системи

захисту. Хакери застосовують мережні віруси-здирники, задіюють шифрування та усе те, що ІТ-компанії використовують для захисту, але з іншою метою [35] .

З розвитком кіберпростору активно розвивається і Інтернет цифрових речей, будь-яка побутова техніка, що має зв'язок з мережею інтернет є потенційним об’єктом для атаки з боку кіберзлочинців.

Зазвичай, люди не замислюються над тим, кому вони можуть надати доступ до своїх персональних даних, та до яких наслідків це може призвести. Так, підключаючись до безкоштовного wi-fi у публічному місці (кафе, супермаркеті, вулиці тощо) користувач автоматично надає доступ до своїх цифрових даних, історії пошуку, паролів, та персональних фото та відео-контенту. Така інформація, потрапляючи до злочинців, надає можливість здійснити так звану «крадіжку особистості». Наприклад, зараз для отримання багатьох послуг та навіть банківських позик, не обов’язкова особиста присутність їх одержувача. Всі фінансові операції можна здійснити у режимі он-лайн, а отже будь-хто у кого, хто володіє персональними даними користувачів, може використати їх у корисних або злочинних цілях.

За даними досліджень найбільш вразливими до крадіжок особистості є громадяни США, де за 2016 рік зафіксовано 791 мільйон вкрадених персональних записів, а друге місці у світі посідають громадяни Франції, де зафіксовано 85 мільйонів злочинів у цій сфері [8, с.175]. В країнах, що розвиваються, зокрема в Україні, таких масових випадків крадіжок особистості не фіксують, однак, це не означає що вони відсутні, і що громадяни в цих країнах не потерпають від діяльності кіберзлочинців.

Виділяють декілька видів крадіжок особистості, серед яких поширеною є крадіжка бази з даними користувачів для їх подальшого перепродажу, використання отриманих відомостей для виготовлення фальшивих документів з метою отримання кредитів та оформлення он-лайн покупок на чуже прізвище. Також дуже поширені випадки злому сторінок в соціальних мережах або створення клонів, потім від імені жертви розсилаються повідомлення друзям з проханням відправити гроші на зазначені шахраями реквізити. З поміж іншого,

зловмисники скоюють і інші протиправні дії, у результаті яких жертви кіберзлочинів одержують судові позови або штрафи для оплати. Наприклад, після викрадення номеру соціального страхування в США, з його допомогою можна отримати медичну допомогу, яка буде оплачена з страхового рахунку жертви зловмисника. На другому місці крадіжка даних з метою зміни особистості. До такого способу прибігають особи, хто або бажає зберегти анонімність, або переховуються від поліції, кредиторів, імміграційних служб тощо.

Наступним злочином за частотою скоєння є створення клонів відомих особистостей. Так, сторонні особи створюють у різних соціальних мережах сторінки акторів, музикантів або спортсменів для отримання слави або використання популярності у власних цілях, а також з метою отримання прибутку. Однак, створення клону не вважається кримінальним злочином, допоки власник такого фейкового аккаунту не почне використовувати його для одержання прибутку.

Об’єктами кібератак здебільшого стають компанії, які працюють з великими обсягами персональних даних. Відсутність законодавчих актів та належних знань щодо необхідності захисту персональних даних від кібератак (відсутність цифрових компетенцій або навіть нерозуміння важливості дотримання правил цифрової гігієни), низький рівень технологічної захищеності існуючих електронних систем призводить до того, що більшість громадян України потрапляють у зону ризику.

Переважна більшість провідних ІТ-спеціалістів у світі говорять про те, що необхідно краще зберігати та захищати персональні дані користувачів. Однак на нашу думку цього недостатньо, адже більшість пересічних громадян не розуміють наскільки важливо оберігати свої персональні дані від несанкціонованого доступу до них, а тому необхідно проводити просвітницьку роботу серед населення, підвищуючи якісний рівень цифрової компетентності громадян через впровадження навчальних курсів з цифрової гігієни для всіх, незалежно від віку та професій, хто працює інформаційними технологіями.

Визначимо базові принципи цифрової гігієни в контексті убезпечення персональних даних користувачів цифрових технологій та мереж:

– створення паролю високого рівня складності для створення аккаунтів (реєстрації) на будь-яких цифрових-ресурсах (пароль повинен містити цифри, букви та спеціалізовані символи);

– здійснення періодичного контролю банківських рахунків (перевірка виписок, налаштування сервісу Sms-оповіщення з метою відстежування будь-яких змін, оплат, переказів тощо);

– налаштування сервісу безпеки персональних акаунтів в соціальних мережах (максимального захисту від проникнення), визначення (обмеження) цільової аудиторії для перегляду контенту персональних сторінок, розміщення мінімуму особистої інформації, яка непов'язана з професійною діяльністю;

– невикористання підозрілого контенту (посилань, файлів), які надходять користувачам через електронну пошту, соціальні мережі та месенджери (навіть у разі довіри до джерела надходження).

– обмеження користуванням безкоштовним інтернетом через Wi-Fi у публічних місцях перебування (ресторани, заклади харчування, вокзали, аеропорти, готелі, вулиці тощо);

– періодичне оновлення програмного забезпечення та використання відкритих програмних продуктів;

– убезпечення приватних, державних та корпоративних Wi-Fi мереж, особливо у разі наявності великої кількості працюючої Smart-техніки [43].

У цьому контексті, однією з головних задач для забезпечення належного рівня провадження кібербезпеки суспільства, держави та кожного громадянина є налагодження ефективної роботи не тільки Національного координаційного центру кібербезпеки, а насамперед спеціалізованого структурного підрозділу Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України «CERT-UA», який здійснює реагування на надзвичайні ситуації в кіберпросторі країни; Зокрема, внаслідок існуючих хакерських атак необхідно ретельне вивчення способів і принципів дії

для подальшого їх упередження, розробки превентивних заходів та практичних керівництв для убезпечення від таких дій в подальшому.

Значення кібербезпеки в суспільних і управлінських процесах актуалізується з огляду на цифрові трансформації публічного врядування, що дозволяє зробити висновок, що основною умовою досягнення сучасних цілей реформування державного управління є цифровізація всіх його структур.

Завдяки такому підходу створюються умови для формування інформаційного (цифрового) простору органів державної влади в середовищі єдиного кібер-простору, як першого кроку на шляху забезпечення відкритості, підконтрольності діяльності з боку громадських інститутів і забезпечення ефективної комунікативної взаємодії всіх суб'єктів державно-управлінського процесу. Крім того, цифровізація діяльності цих органів дозволяє реалізувати модель раціональної управлінської структури на основі сервісного підходу, що в цілому слугуватиме втіленню концепції «цифрового врядування» як інноваційної основи зміцнення демократичних інститутів громадянського суспільства.

### 2.3. Аналіз забезпечення безпеки інформації в інформаційно-телекомунікаційних системах

Концепція розвитку цифрової економіки та суспільства України на 2018–2020 рр. (у принципі 7 цифровізації «Цифровізація повинна супроводжуватися підвищенням рівня довіри і безпеки») [77] передбачає, що «інформаційна безпека, кібербезпека, захист персональних даних, недоторканність особистого життя та прав користувачів цифрових технологій, зміцнення та захист довіри у кіберпросторі є, зокрема, передумовами одночасно-го цифрового розвитку та відповідного попередження, усунення та управління супутніми ризиками». Це аспект знайшов відображення у Плані заходів щодо реалізації Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр., а також враховано Кабінетом Міністрів України у 2021 р. в контексті розвитку цифрових інфраструктур, враховуючи розвиток національного сегмента мережі Інтернет.

16.12.2020 р. КМУ затвердив Порядок функціонування Національної телекомунікаційної мережі та Правила надання послуг, які надаються з використанням Національної телекомунікаційної мережі. У Порядку функціонування Національної телекомунікаційної мережі зазначено, що «… 33. Взаємодія Національної телекомунікаційної мережі з телекомунікаційною мережею загального користування здійснюється через шлюзи (граничні маршрутизатори), на яких створено комплексну систему захисту інформації відповідно до вимог законодавства у сфері захисту інформації, кіберзахисту та охорони державної таємниці. 34. Взаємодія Національної телекомунікаційної мережі з Інтернетом здійснюється через захищені вузли доступу до Інтернету, на яких створено комплексну систему захисту інформації відповідно до вимог законодавства у сфері захисту інформації, кіберзахисту та охорони державної таємниці» [28].

У свою чергу, 08 лютого 2021 року КМУ було прийнято Постанову № 92 «Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» зі змісту якої вбачається, що Підключення систем, у яких обробляється службова інформація та інформація, що становить державну таємницю, до глобальних мереж передачі даних здійснюється з використанням засобів криптографічного захисту інформації, які допущені до експлуатації для криптографічного захисту інформації відповідного ступеня обмеження доступу, та/або апаратних, апаратно-програмних засобів технічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації та реалізують функції безпеки односпрямованої (односторонньої) передачі даних та/або двоспрямованої передачі даних з урахуванням їх змістовного аналізу. В апаратно-програмних засобах технічного захисту інформації, які реалізують функції односпрямованої (односторонньої) передачі даних та або міжмережевого екранування (фільтрації) даних, що забезпечують захист службової інформації та інформації, що становить

державну таємницю, рівень гарантії коректності надання функціональних послуг безпеки повинен бути не нижче третього [58].

Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (забезпечує проведення єдиної державної політики з питань державного регулювання у сфері телекомунікацій, інформатизації та розвитку інформаційного суспільства, користування радіочастотним ресурсом, надання послуг поштового зв'язку; здійснює державне регулювання та нагляд у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом, надання послуг поштового зв'язку, використання інфраструктури з метою максимального задоволення попиту споживачів на послуги зв'язку та інформаційні послуги, створення сприятливих умов для залучення інвестицій, збільшення обсягів послуг та підвищення їх якості, розвитку та модернізації телекомунікаційних та інформаційно-телекомунікаційних мереж з урахуванням інтересів національної безпеки; забезпечує ефективне користування радіочастотним ресурсом і функціонування ринку телекомунікаційних, інформаційно-телекомунікаційних, інформаційних послуг та послуг поштового зв'язку на основі збалансування інтересів суспільства, суб'єктів господарювання та споживачів цих послуг; сприяє розвитку конкуренції та підприємництва, забезпечення рівних умов діяльності суб'єктів господарювання всіх форм власності, вдосконалення механізму регулювання ринкових відносин у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом та надання послуг поштового зв'язку; забезпечує системність, комплексність і узгодженість розвитку інформатизації та інформаційного суспільства в державі) [71].

Таким чином, на сучасному етапі боротьби держав за сфери впливу акцент із явного застосування сили усе помітніше зміщується на використання більш гнучких засобів, основним із яких є контроль і керування інформаційними ресурсами.. Під виглядом офіційних листів надсилаються електронні повідомлення із вкладеним шкідливим програмним забезпеченням, яке рекомендується встановити. Зокрема, СБУ неодноразово звертала увагу

керівників державних органів влади та установ, а також співробітників IT-департаментів на необхідність посилення заходів з недопущення несанкціонованого встановлення програмного забезпечення чи його оновлення, аби не допустити хакерського проникнення на державні інформаційні ресурси.

Підсумовуючи усе вище викладене у розділі, зазначимо наступне:

1.Під загрозою національній безпеці слід розуміти можливу небезпеку, що має здатність причинити будь-яку шкоду, призвести до збитків, втрат (матеріальних і людських) або інших негативних наслідків. Класифіковано всі загрози національної безпеки за двома критеріями: 1) за джерелом виникнення на зовнішні та внутрішні загрози; 2) за сферою дії на загрози національній безпеці в політичній, технологічній, економічній, екологічній і т. д. сферах. Запропоноване авторське розуміння інформаційних загроз як систему зовнішніх та внутрішніх чинників, що чинять згубний вплив на інформаційну безпеку, зачіпаючи життєво важливі інтереси держави, суспільства та людини в інформаційній сфері. Акцентовано, що загрози інформаційній безпеці України є перепоною для належного інформаційного обміну, тому вважаємо, що одним із важливих напрямів щодо цього є вдосконалення вітчизняного законодавства, яким врегульовуються як правові, так і організаційні засади забезпечення інформаційної безпеки України.

2.Глобальний характер таких загроз ускладнює вироблення механізмів їх нівелювання, адже сьогодні щодня виникають нові технологічні виклики, на які не можна відреагувати за допомогою застарілих методів захисту. Враховуючи все це, Україна має затвердитися в глобальному цивілізаційному середовищі в якості конкурентоспроможного суб’єкта. Наголошено, що для цього дуже важливо використовувати всі інструменти ефективного розвитку, що надаються технологічним простором інформаційного суспільства. Водночас, так само необхідно облаштувати надійну національну систему інформаційного захисту від безлічі інформаційних загроз, що йдуть від внутрішніх і зовнішніх впливів, а також з боку глобальних факторів небезпеки, притаманних самій структурі інформаційної цивілізації. Аргументовано, що перед українською державою на

сучасному етапі державотворчих трансформацій постає складне завдання: максимально використати інформаційно-технологічні, соціально-структуруючі, масово-інформаційні можливості, що надаються інформаційної цивілізацією, і при цьому захистити власних громадян та державний організм від ураження з боку руйнівних і загрозливих зовнішніх і внутрішніх інформаційних впливів.

3.На сьогоднішній день, національну систему кібербезпеки формують ряд державних інституцій як центрального так і місцевого рівня, військові структурні підрозділи, установи, заклади та організації, які задіяні в галузі комунікацій, опікуються питаннями захисту інформації та мають в своєму розпорядженні об'єкти критичної інформаційної інфраструктури. Головними тенденціями розвитку кіберзагроз у сучасних інформаційних протиборствах виокремлені наступні: 1) збільшення кількості кібератак, спрямованих на нанесення широкомасштабної шкоди інфраструктурам великих корпорацій, важливим промисловим об’єктам, а також інформаційним системам органів державної влади; 2) зростання рівня складності кібератак, які реалізуються поетапно та адаптовані спеціальними інструментами протидії захисту від супротивника; 3) тотальність впливу на всі цифрові (електронні) технології, зокрема мобільні (мережеві) пристрої, які є апріорі максимально вразливими з точки зору інформаційної безпеки; 4) комплексне застосування в гео політичному просторі новітніх технологій кібернападу одних країн на інші (інформаційна війна реалізується на міждержавному рівні). Доведена необхідність побудови дієвої системи кібернетичної безпеки України. Основною умовою досягнення сучасних цілей реформування державного управління є цифровізація всіх його структур. Завдяки такому підходу створюються умови для формування інформаційного (цифрового) простору органів державної влади в середовищі єдиного кібер- простору, як першого кроку на шляху забезпечення відкритості, підконтрольності діяльності з боку громадських інститутів і забезпечення ефективної комунікативної взаємодії всіх суб’єктів державно-управлінського процесу.

4.На сучасному етапі боротьби держав за сфери впливу акцент із явного застосування сили усе помітніше зміщується на використання більш гнучких засобів, основним із яких є контроль і керування інформаційними ресурсами. Українські правоохоронці постійно нагадують, що злочинці намагаються зламати інформаційні мережі й поштові сервери державних установ. Під виглядом офіційних листів надсилаються електронні повідомлення із вкладеним шкідливим програмним забезпеченням, яке рекомендується встановити. Зокрема, СБУ неодноразово звертала увагу керівників державних органів влади та установ, а також співробітників ІТ-департаментів на необхідність посилення заходів з недопущення несанкціонованого встановлення програмного забезпечення чи його оновлення, аби не допустити хакерського проникнення на державні інформаційні ресурси.

# РОЗДІЛ 3
# НАПРЯМКИ УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

## 3.1. Удосконалення організаційно-правових механізмів забезпечення інформаційної безпеки України

Інформаційна безпека осмислюється нами у контексті викликів сучасної демократизації і політичної модернізації, тобто як вид безпеки національної, орієнтованої на демократичні права і свободи людини мати вільний доступ до інформації, на створення і впровадження безпечних інформаційних технологій, на вільну журналістську діяльність, на захищені права інтелектуальної власності, на орієнтування у глобальному просторі можливостей інформаційного суспільства тощо. Однак сучасні українські реалії передбачають також розгляд можливих диверсій у цю сферу. Українське суспільство за багатьма вимірами - інституційними, політико-правовими, ціннісно-культурними - виявилось непідготовленим до протидії внутрішнім і зовнішнім інформаційно-деструктивним впливам. Водночас інформаційна війна, яку розгорнув агресор проти України, зобов’язує до активної, цілеспрямованої, стратегічної протидії атакам і війнам в інформаційному полі.

Нагальним питанням сьогодні постає питання щодо оптимізації структури власності суб'єктів інформаційної діяльності, якнайшвидший розвиток суспільного сектора, особливо в галузі електронних мас-медіа. Створення організаційно-правової бази цих змін, згідно з нашими поглядами, - це ще одне нагальне завдання всіх гілок української влади. Крім цього, забезпечення інформаційної безпеки України і захист національного медіа-ринку вимагає перегляду основних принципів регулятивної політики на засадах інформаційної відкритості й підтримки власних медіа-виробників. Головним об'єктом такої підтримки має стати український зміст інформаційної продукції.

Доповнюємо такі ідеї зауваженням, що державна політика забезпечення інформаційної безпеки повинна бути відкритою і передбачати інформування

суспільства про діяльність державних органів і суспільних інститутів у сфері інформаційної безпеки з урахуванням обмежень, встановлених чинним законодавством України. Тому стверджуємо, що вона має виходити з принципу безумовної правової рівності всіх суб'єктів інформаційних відносин незалежно від їхнього політичного, соціального та економічного статусу, ґрунтуватися на обов'язковому забезпеченні прав громадян і організацій на вільне створення, пошук, отримання, накопичення, зберігання, перетворення і поширення інформації у будь-який законний спосіб.

Увиразнюємо ми це тим фактом, що сьогодні найбільш гострою проблемою в Україні є відсутність у переважної більшості громадян довіри до державної влади, впевненості в тому, що всі гілки і структури влади, всі її посадові особи працюють в інтересах суспільства, а не в інтересах самої влади або своїх особистих. Тому вістря державної інформаційної політики має бути, перш за все, спрямоване на усунення «дефіциту довіри до влади», який перешкоджає просуванню по шляху реформ.

У цьому сенсі, вважаємо ми, ключовим завданням є створення відкритого інформаційного середовища, включаючи забезпечення інформаційної прозорості державної влади, необхідної для формування громадянського суспільства і досягнення взаємодії між суспільством і владою на принципах довіри, взаєморозуміння та ділового партнерства.

Річ у тому, що збалансоване функціонування системи інформаційної безпеки забезпечується за рахунок постійного обміну інформаційними потоками як усередині держави, так і між державами. С. Мошковська з цього приводу зазначає: «Будь-яка держава є відкритою системою, яка задіяна в кругообігу інформації. І якщо не буде відбуватися природний обмін в інформаційному просторі, то система руйнується» [52, с. 119]. Тому завдання політики на інформаційному рівні керування процесом обміну. Останній не є хаотичним і підпорядковується цілком визначеним законам, один з яких можна сформулювати таким чином: інформація не викидається в інформаційний

простір довільним способом, а посилається передусім туди, де вона необхідна і її здатні сприйняти.

Ми також зазначаємо, що для створення відкритого інформаційного простору в Україні, перш за все, необхідно запустити механізм практичної реалізації конституційного права на свободу одержання інформації. Правовою основою такого механізму повинні стати законодавчо закріплені чіткі правила, умови і порядок отримання громадянами та інституційними структурами суспільства інформації в органах державної влади і місцевого самоврядування, від інших державних і недержавних юридичних осіб, а також прямого доступу до державних і недержавних інформаційних ресурсів.

Як зазначає з цього приводу М. Гуцалюк, органи (служби) інформаційної безпеки можуть створюватися (на законодавчих засадах) і в недержавних структурах для захисту своїх потреб в забезпеченні необхідною інформацією. Дані органи на основі укладення відповідних угод можуть бути приєднані до єдиної державної системи інформаційної безпеки. На теперішній час окремі елементи системи інформаційної безпеки створені та функціонують (органи зовнішньої розвідки, інформаційні служби різноманітних міністерств, система технічного та криптографічного захисту інформації держави і т. н.). Проте для їхнього функціонування ще недостатня правова база. Зміст діяльності органів інформаційної безпеки також ще не в повній мірі відповідає покладеним на них завданням. Це пояснюється в першу чергу недостатнім опрацюванням питань, що стосуються форм і способів забезпечення інформаційної безпеки [20, с. 3].

Тому для ефективної реалізації державної політики, щодо побудови відкритого правового інформаційного простору України потрібно виконати ряд головних вимог. Більшість дослідників одностайні щодо переліку таких вимог. Так, наприклад А. Ф. Грицик зазначає: 1) в системі органів державної влади має бути сформована єдина структура, функцією якої є проведення державної інформаційної політики. Ця структура повинна охоплювати всі гілки і рівні державної влади і включати як спеціалізовані органи влади, що забезпечують регулювання інформаційної сфери, так і підрозділу в інших органах влади,

відповідальні за інформаційні аспекти діяльності в сфері їх компетенції; 2) державне управління інформаційною сферою має бути планомірно забезпечене фінансовими і матеріальними ресурсами за рахунок бюджетного фінансування - природно, виходячи з реальних можливостей держави за статтею витрат на державне управління; 3) проведення державної інформаційної політики має координуватися з єдиного центру на рівні вищого керівництва країни при персональній відповідальності одного з вищих посадових осіб держави за вирішення цього завдання [17, с. 211]. Адже право самостійно виражати свої власні думки та накопичувати, отримувати і розповсюджувати інформацію, як і кожне інше право, має свої власні обмеження.

Одним з найважливіших елементів управління суспільством є державний контроль над інформацією. Система контролю і дозування інформації існує в кожній державі. Але головне питання, яке так чи інакше постає в цьому контексті: в чиїх інтересах здійснюється такий контроль [33, с. 44].

Наш висновок полягає у тому, що, на жаль, в даний час не тільки жодна з перелічених вище вимог у повному обсязі не виконується, але і на рівні вищого українського керівництва проведення цілеспрямованої інформаційної політики не розглядається в ряду першочергових завдань державного управління. Подібне неадекватне ставлення до створення відкритого і контрольованого інформаційного простору призводить до негативних наслідків, істотно відображаючись на розвитку України. Варто зауважити, що таке ставлення державної влади до інформаційної політики не тільки призвело до інформаційної війни, в стані якої перебуває Україна, а й створило можливості для успішної реалізації Росією інших елементів гібридної війни.

З урахуванням динамічного розвитку національного інформаційного простору, нормативно-правове регулювання інформаційної безпеки повинно складатися з двох рівнів і включати:

– комплексну нормативно-правову регламентацію процесів управління забезпеченням інформаційної безпеки, закріплену в актах законодавства, підготовлених на основі всебічного наукового розгляду і обґрунтування стадій,

методології та системи відносин, що складаються в процесі адміністративно-правового регулювання діяльності суб'єктів забезпечення у визначеній сфері;

– нормативно-правову регламентацію діяльності Національної поліції за окремими напрямами забезпечення інформаційної безпеки, що складається з галузевих нормативно-правових актів Національної поліції, документів інших органів (наприклад, Міністерства інформаційної політики України, Державної служби спеціального зв'язку та захисту інформації України [76]), що забезпечують реалізацію державних функцій у сфері інформаційної безпеки.

Взаємозв’язок законодавчого та відомчого нормативного регулювання доцільно розділити відповідно до характеристики об'єкта управління та предмета управлінсько-правового регулювання, що відповідатиме на питання, які правовідносини поза управлінських меж оформляються (або повинні оформлятися) за допомогою нормативних приписів. Відправним при цьому є теоретичне уявлення про предмет регулювання як про суспільні відносини, що складають об'єкт управлінського впливу, який здійснюється за допомогою правових норм, втілених у законодавстві. Вони адресуються учасникам управлінських відносин, визначають межі можливої та належної поведінки, впливаючи, тим самим, на волю та свідомість відповідних суб’єктів.

На сьогоднішній день рівень відомчого регулювання складають спільні нормативно-правові акти МВС України (Національна поліція, Департамент інформатизації Міністерства внутрішніх справ України), Міністерства інформаційної політики України, Міністерства оборони України, Державної служби спеціального зв'язку та захисту інформації України, Національної комісії, що здійснює державне регулювання у сфері зв’язку та інформатизації. У процесі відомчого адміністративно-правового регулювання забезпечення інформаційної безпеки повинна бути вибудувана певна ієрархія індивідуальних інтересів. У цьому зв'язку можна визначити наступні групи інтересів: первинні інтереси, пов’язані із забезпеченням життєдіяльності індивідів; вторинні інтереси, продиктовані забезпеченням необхідного рівня функціонування

інформаційно-комунікаційних систем; інтереси, спрямовані на реалізацію соціальних перспектив фізичної і юридичної особи в інформаційній сфері.

Комплексну нормативно-правову регламентацію процесів управління забезпеченням інформаційної безпеки доцільно здійснювати за рахунок систематизації і уніфікації адміністративного законодавства в галузі інформаційної безпеки за допомогою кодифікованого нормативного правового акта, який встановить вихідні засади адміністративно-публічного забезпечення інформаційної безпеки в Україні.

В якості такого нормативно-правового акту можна запропонувати спільний наказ Міністерства інформаційної політики України, МВС України, Державної служби спеціального зв'язку та захисту інформації України «Про основи адміністративно-правового забезпечення інформаційної безпеки в Україні», в якому доцільно вирішити такі завдання:

– створення однакового понятійно-категорійного апарату, який гранично ясно та чітко розкриває сутність, структуру та зміст інформаційної безпеки у сфері адміністративно-правового регулювання в Україні, співвідносно з виробленими юридичною наукою категоріями;

– створення в Україні єдиної системи спеціалізованих органів виконавчої влади та виконавчо-розпорядчих органів місцевого самоврядування, які наділяються повноваженнями з питань забезпечення виконання загальнообов'язкових умов та вимог інформаційної безпеки, пов'язаними з безпосереднім втручанням даних органів в адміністративно-господарську, організаційно-розпорядчу та іншу діяльність фізичних і юридичних осіб;

– систематизація та уніфікація адміністративно-правових методів діяльності органів виконавчої влади та виконавчо-розпорядчих органів місцевого самоврядування, які будуть забезпечувати виконання загальнообов'язкових умов і вимог інформаційної безпеки при безпосередньому втручанні в адміністративно-господарську, організаційно-розпорядчу та іншу діяльність фізичних та юридичних осіб;

– формальне визначення функцій адміністративно-правового забезпечення інформаційної безпеки, що передаються органам місцевого самоврядування органами державної влади України в якості аутсорсингу;

– створення оптимальної системної моделі взаємодії методом планомірної та послідовної зміни окремих системних якісних показників на підставі скорочення можливості прямого втручання у сферу технологічних і цивільно-правових відносин, що зумовлює відповідні зміни у колі та характері суспільних відносин, які охороняються адміністративним правом.

Наступним важливим кроком є подолання проблеми організаційної та інституційної слабкості взаємодії між громадянським суспільством та державою в питаннях інформаційної безпеки. Тут чітко простежується необхідність своєчасних системних змін у роботі виконавчих структур, наприклад у принципах діяльності Міноборони. В першу чергу на базі Директиви Міністра оборони України «Про вдосконалення співпраці органів військового управління з громадськими організаціями» [60] та Наказу Міністра оборони України «Про забезпечення участі громадськості у формуванні та реалізації державної політики у військовій сфері» [62] необхідним є формування нових принципів роботи міністерства, які будуть передбачати, по-перше, аналітичне та експертне супроводження з боку громадянського суспільства, по-друге, створення умов для постійного залучення експертів провідних «think tanks» України (таких як Центр Разумкова та інші), до спільної інформаційно-аналітичної роботи із Департаментом воєнної політики та стратегічного планування МОУ.

Зважаючи на інституційну неоформленість взаємодії між громадянським суспільством та державою, важливим кроком є створення консультативного органу, який б забезпечував існування комунікацію між двома суб’єктами (наприклад, Державна служба забезпечення інформаційної безпеки України). При чому важливо розмежувати компетенцію даного органу із компетенцією громадських рад, що включають в свій склад громадські організації та спілки. Досвід зарубіжних країн, зокрема вже розглянутих в роботі США, показує, що такі органи на відміну від громадських об’єднань надають більш фахову та

професійну допомогу державним структурам особливо в сфері національної безпеки.

Разом з тим, вважаємо за доцільне відзначити необхідність створення структури, діяльність якої буде направлена на включення представників такого органу в управлінський процес, використання їх «інтелектуального та експертного ресурсу» для досягнення безпекових цілей в інформаційній сфері, аналітичний супровід політики уряду. Це, в свою чергу, передбачає розробку нормативних та програмних підстав для створення даної структури шляхом: 1) внесення змін в Положення «Про Міністерство інформаційної політики України»; 2) внесення змін в Доктрини інформаційної безпеки України (а саме до розділу 6 «Механізм реалізації Доктрини»); 3) включення пункту про створення такого органу в План діяльності Міністерства інформаційної політики України на 2022 рік.

Структурно такий орган має включати в своєму складі дві групи учасників: не менше половини членів мають складати представники вітчизняних експертів, науково-дослідних інститутів, університетів, а також експерти в сфері інформаційної безпеки; іншу частину повинні складати представники державних інституцій (державних аналітичних центрів та науково-дослідних інститутів).

До основних напрямків роботи запропонованого органу слід відносити наступне: 1) розробка стратегічної програми контрпропагандистських заходів, зокрема у аспекті «розвінчання міфів» про так звані злочини української влади проти мирного населення Донбасу, які поширює офіційна російська пропаганда; 2) формування стандартів та рекомендацій по забезпеченню кібербезпеки інформаційних ресурсів Кабміну та інших центральних органів виконавчої влади і т. д.; 3) аналітичної роботи в сфері інформаційної безпеки, її моніторинг з метою виявлення імовірних ризиків та проблем, а також формування пропозицій щодо вдосконалення стратегічної політики в сфері безпеки та оборони України; 4) реалізації наукових-дослідних ініціатив та проектів спільно із державними аналітичними центрами, науково-дослідними інститутами при університетах, науковцями та фахівцями в сфері інформаційної безпеки; 5) формування

аналітичних доповідей та звітів із актуальних проблем в сфері інформаційної безпеки;

Загалом, ефективність аналітичної та експертної підтримки, яку вітчизняні «мозкові центри» мають можливість надавати уряду і безпековим структурам, може бути підвищена тільки шляхом проведення відповідних змін в діючому механізмі співпраці між громадянським суспільством та державою. Мова йде не про окремі локальні кроки, а про комплексні реформи, що створять умови для підвищення продуктивності спільної роботи обох суб'єктів. Тому вважаємо запропоновані кроки доцільними та ефективними.

### 3.2. Оптимізація державних інформаційних ресурсів в контексті реалізації державної політики в сфері інформаційної безпеки

Головні напрями реалізації безпеки інформації включають нормативно-правову складову, що зорієнтована на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, а також на рівні підприємства або організації чи окремої особистості. Під реалізацією державної політики у сфері інформаційної безпеки слід розуміти сукупність нормативно-правової, організаційно-інституційної діяльності органів публічної влади, спрямованої на досягнення стану захищеності потреб громадян, суспільства та держави в одержанні, обробленні, збереженні, поширенні та захисті інформації.

На нашу думку, для ефективного й оперативного вирішення питань у сфері провадження інформаційної безпеки України, слід опиратися на системний та ситуаційний підходи при виробленні державної політики. Системний підхід дасть змогу об'єднати суб'єкти та механізми реалізації сфери інформаційної безпеки у цілісну систему підтримки прийняття рішень для оперативного та стратегічного управління складовими підсистемами держави, дозволить представити державу як модель відкритої системи, входами якої буде перелік внутрішніх та зовнішніх загроз, методів реалізації захисту, а виходами

результати протидії та стан складових та держави як системи в цілому. Такий підхід дасть змогу:

– визначити основні зовнішні та внутрішні зміни, які впливають на державу, а саме конкретний набір факторів, котрі створюють ситуацію у конкретний момент;

– розробити та впровадити тільки ті специфічні прийоми, які як найшвидше впливають на нейтралізацію або стабілізацію ситуації в державі, або щодо держави.

Створення безпечного інформаційного простору державного управління здійснюється шляхом формування цілісної системи інформаційної безпеки органів державної влади, для чого необхідним є вирішення таких пріоритетних завдань:

– створення єдиного репозитарію програмного забезпечення у сфері інформаційної безпеки з метою належного використання органами державної влади та органами місцевого самоврядування;

– організація ефективної комунікації, убезпечення передачі інформаційних потоків в кіберсередовищі держави;

– цифровізація управлінських та технологічних процесів державного управління;

– централізоване здійснення моніторингу та контролю систем інформаційної безпеки державного управління;

– забезпечення захисту інформації, яка одержується із зовнішнього середовища органами публічної влади;

– гарантування належного рівня безпеки і захисту інформаційно-комунікативної інфраструктури органів державної влади.

Зазначимо, що застосування координованої системи ситуаційних центрів у практичну діяльність органів влади у сфері інформаційної безпеки України забезпечить:

– оперативне залучення осіб, які безпосередньо приймають державно-управлінські рішення стосовно необхідності захисту інформації або персональних даних;

– удосконалення сервісних процедур управління через залучення керівництва не тільки до прийняття, але й до формування державно-управлінських рішень;

– відбір державно-управлінських рішень, які ухвалюються шляхом експертного оцінювання можливих наслідків та моделювання ситуацій за допомогою сучасних цифрових технологій;

– підвищення якості аналізу/синтезу інформації та державно-управлінських рішень із залученням цифрових сервісів, що в комплексі забезпечить ефективну інтеграцію засобів комунікаційного зв’язку, аналітичної обробки та візуалізації будь-яких даних.

На сьогодні стратегічними пріоритетами реалізації державної політики в Україні є: створення умов для реалізації прав на забезпечення законодавчо закріплених потреб громадян та суспільства; гарантування законних інтересів та захисту прав користувачів державних сервісів; забезпечення рівноправності кожного на одержання послуг у сфері інформаційної безпеки за єдиними процедурами; забезпечення рівного доступу до одержання послуг публічної влади для всіх громадян, з урахуванням економічної спроможності різних верств громадян.

Для забезпечення реалізації пріоритетів державної політики у сфері інформаційної безпеки першочерговими завданнями держави є:

– нормативно-правове регулювання сервісної діяльності, в тому числі процедур надання послуг органів влади з інформаційної безпеки;

– делегування управлінських послуг соціально відповідальним суб’єктам недержавного сектору;

– адаптація та дотримання стандартів послугу сфері кіберзахисту;

– запровадження сучасних інноваційних форм та цифрових технологій для зручного одержання послуг користувачем та спрощення процедур сервісної діяльності органів публічної влади.

Таким чином, проблема удосконалення державної політики у сфері інформаційної безпеки вимагає комплексного вирішення, яке може здійснюватися на засадах інтеграції механізмів її реалізації, з огляду на окреслені напрями цифрового розвитку країни, суспільства, держави, громадянина.

### 3.3. Забезпечення інформаційної безпеки органів влади в умовах цифровізації

Оскільки інтернет є найбільш динамічно що розвиваються інформаційним простором, інформаційно-психологічний вплив здійснюється сьогодні переважно на його основі.

На сьогоднішній день систему інформаційного протиборства з тероризмом в мережі Інтернет можна визначити таким чином: 1) законодавча заборона організації; 2) реалізація заборони - боротьба з екстремістськими матеріалами; 3) боротьба з незаконним фінансуванням в мережі Інтернет; 4) протидія вербування; 5) профілактичні заходи (інформаційно-просвітницька робота).

З метою протидії використанню мережі Інтернет терористами, експерти пропонують п’ять напрямків діяльності: 1) постійне вдосконалення захисту мереж з метою унеможливити доступ до його вразливих компонентів зловмисників на скільки це можливо; встановити жорстку правову відповідальність в якості стримуючого фактора для осіб, які приймають участь у агресивних терористичних актах, використовуючи мережу Інтернет; проведення постійного аналізу кіберпростору задля кращого розуміння існуючих та можливих загроз та вразливих місці; тісний обмін розвідувальними даними між відповідними органами щодо протидії загрозам використання кіберпростору в терористичних цілях; обмежити публічне висвітлення успішно проведених кібертерористичних атак з метою позбавити терористичні угрупування досягнення ними політичних цілей [2, с.23].

На нашу думку, для того, щоб ефективно протистояти реальній загрозі використання мережі Інтернет терористичними угрупуваннями необхідно прийняти відповідні заходи як на міжнародному, так і на національному рівнях. На національному рівні рекомендується: 1) застосовувати існуючі норми законодавства, передбачені Конвенцією Ради Європи про кіберзлочинність щодо процедури направлення запитів про взаємну допомогу за відсутності відповідних міжнародних угод; 2) застосовувати існуючі норми законодавства про боротьбу з тероризмом до випадків кібертероризму, зокрема положення Конвенції Ради Європи про запобігання тероризму, що стосуються публічного підбурювання до вчинення терористичного злочину, а також прийняти спеціальні правові норми, спрямовані на боротьбу із використанням Інтернету в терористичних цілях.

У системі захисту інформації і загалом функціонування та захисту електронних сервісів важливу роль відіграють хмарні технології зберігання та доступу до інформації. Хмарні сервісні системи були вперше запропоновані Дж. МакКарті та Дж. Ліклайдером у 1960-х роках, як концептуальна альтернатива придбанню власних потужних обчислювальних комплексів, програмних продуктів та технологій зберігання даних. Було запропоновано принцип спільного використання вказаних ресурсів на підставі їх віртуалізації. Розвиток хмарних гетерогенних систем пов’язують і з комерційними ініціативами компаній Amazon та Google у 2006 році. У цей період з’являються терміни «хмара» (cloud) та «хмарні обчислення» (cloud computing). Переваги концепції хмарних обчислень очевидні: економія капітальних та експлуатаційних витрат клієнтів, підвищення надійності та безпечності зберігання і передавання клієнтських даних. Більшість хмарних систем є інтелектуальними сервісними мережами з динамічно змінною функціональністю та структурою вузлів [83, с.3].

Застосування принципу цифрової взаємодії за допомогою хмарного сервісу дає змогу залучати до неї більшу кількість користувачів з відносно невеликими матеріальними затратами. На сьогодні більшість сервісів, які застосовуються у системах е-уряду функціонують на основі хмар. Для

входження будь-якого користувача у свій особистий кабінет на єдиному порталі послуг і отримання відповідної послуги, не потрібне ніяке додаткове програмне забезпечення на власному комп'ютері. У межах електронної взаємодії всі системи здійснюють інформаційний обмін з використанням веб-сервісів. Більшість цих систем також не вимагають встановлення на робочому місці додаткового програмного забезпечення, оскільки теж функціонують на основі інтернет-браузера. Одним із прикладів використання хмарних технологій у державних органах України є надання Державною фіскальною службою України (ДФС) електронних послуг платникам податків засобами «Електронного кабінету платника податків (ЕКПП)» у складі інформаційної системи «Податковий блок».

На сьогодні у світі провідними неурядовими установами, що займаються питаннями продукування безпеки в «хмарі», є Агентство з питань мережевої та інформаційної безпеки ЄС (ENISA), яке є експертним центром з питань кібербезпеки в Європі, а також Національний інститут стандартів та технологій США (NIST). Кожною із зазначених інституцій було створено відповідний документ (стандарт) щодо класифікації всіх існуючих загроз інформаційної безпеки в хмарі.

Вітчизняні науковці М. Вітер та Х. Засадна визначають наступні базові моделі надання послуг на основі хмарних технологій (Service Models) [10, с.342]: інфраструктура як послуга (Cloud Infrastructure As a Service, IAAS); платформа як послуга (Cloud Platform As a Service, PAAS); програмне забезпечення як послуга (Cloud Software As a Service, SAAS). А також відповідні чотири моделі розгортання хмарних сервісів в інтернет-середовищі Deployment Models): приватна хмара (Private Cloud); хмара співтовариства або загалвна хмара (Community Cloud); публічна хмара (Public Cloud); гібридна хмара (Hybrid Cloud).

Незважаючи на зручність і оптимальність використання хмарних сервісів в умовах функціонування державних цифрових (електронних) сервісів, існуючи і недоліки хмарних застосувань, а саме: проблемність вразливості хмарних

технологій з точки зору безпечності; необхідність швидкісного інтернет-провайдингу; обмеженість перенесення всіх даних до хмарного середовища, з оглядну на обмеженість інструментів; для довготривалого використання хмарної моделі в сервісах доцільним може бути розміщення локального (традиційного) сервера, зокрема, у хмарної технології SAAS; у більш дешевого хмарного провайдера можливими можуть бути затримки у функціонування чи тривалий час відновлення працездатності хмари, наприклад, після збою.

Відтак, враховуючи всі переваги й недоліки технологій у сфері побудови інформаційного захисту, архітектура типової системи управління інформаційною безпекою має включати такі основні компоненти: інтеграційну платформу; апаратно-програмні засоби моніторингу і аудиту; апаратно-програмні засоби захисту інформації; сховище інформації про інциденти інформаційної безпеки; аналітичні інструменти і засоби генерації звітів. Апаратно-програмні засоби моніторингу і аудиту - засоби, що реалізують функції з протоколювання, збору, накопичення та обробки інформації функціонування інформаційно-комунікативної системи. Вони складають підсистему збору інформації про інциденти інформаційної безпеки. Результатом їх роботи є дані, на основі яких системою приймається рішення щодо настання інциденту.

Апаратно-програмні засоби захисту в контексті системи управління інформаційною безпекою включають засоби, які забезпечують локалізацію інцидентів або зниження збитку. Ці засоби мають механізми, що дозволяють проводити швидку і дистанційну зміну своєї конфігурації або мати в своєму складі наперед розроблені автоматизовані сценарії дій з мінімізації можливого збитку від інцидентів інформаційної безпеки [87].

Важливим пріоритетом для функціонування цифрових технологій реалізації інформаційної безпеки є, насамперед, їх інтероперабельність та взаємодія структурних одиниць об’єктів, що полягають в інтеграції протоколів функціонування на основі веб-сервісів. М. Вітер [10, с.345] в даному аспекті виокремлює такі рівні: інтеграцію корпоративних додатків (Enterprise

Applications Integration) - технології, орієнтовані на вирішення проблем інтеграції різних систем, додатків і даних всередині окремої організації; інтеграцію між організаціями (міжвідомчу) (Business-to-Business Integration); технології, орієнтовані на інформаційний обмін між різними організаціями та їхніми інформаційними системами; управління бізнес-процесами (Business Process Management) - технології, орієнтовані на інтеграцію даних міжвідомчого середовища через єдині бізнес-процеси.

Основою веб-інтеграції інформаційних мереж при застосуванні сервісного принципу надання інформаційних безпекових послуг є сервіс-орієнтована архітектура (SOA - Service Oriented Architecture), в якій компоненти (сервіси), маючи узгоджені загальні інтерфейси, використовують єдині правила (контракти) для визначення того, як вони будуть взаємодіяти один з одним.

Головна ідея SOA полягає в тому, щоб убезпечити інформаційну інфраструктуру від зміни поколінь IT та інтегрувати між собою різноманітні успадковані технології. У цьому разі важливим є компонент SOA як так звана “шина сервісів”, що має головною метою технологічну інтеграцію систем, що підключаються, а також надання інтегрованого підходу до системного обліку операцій та засобів забезпечення безпеки. У межах концепції SOA така «сервісна шина» може бути представлена як набір паралельних шин, що відповідають різним принципам [98, с.314].

На світовому рівні провідні IT-компанії, як IBM, Microsoft, Oracle, Sun, RedHat приділяють значну увагу проблематиці розвитку та ефективного використання концепції SOA при впровадженні інтегрованої IT-архітектури в утворювані інформаційні сервісні системи органів державної влади [98, с.312], натомість в Україні й досі не існують жодного з проектів, який було б впроваджено у систему державного управління.

SOAP (Simple Object Access Protocol) являє собою фактично відкритий протокол, який визначає на основі XML загальний формат для комунікаційного зв’язку між будь-якими інтернет-додатками і сервісами.

Заснований на інтернет-стандартах XML і HTTP, протокол SOAP дає змогу взаємодіяти один з одним будь-яким новим або наявним програмам. Веб- вузли, що підтримують SOAP, можуть стати веб-сервісами, доступними лише програмним шляхом і не потребують участі людини. Згідно з технічними вимогами стандарту SOAP, конверт, заголовок та тіло повідомлення повинні бути представлені в незашифрованому вигляді. Окрему роль для забезпечення безпеки в межах такої архітектури відіграють цифрові підписи, які дають змогу перевірити цілісність окремих блоків даних та розпізнавати маніпуляції з повідомленнями (заміна, видалення або зміна даних). З метою підтвердження автентичності всього повідомлення потрібно забезпечити єдність окремих його блоків за допомоги їх криптографічного зв'язку, що не залежать від їх положення всередині повідомлення.

Програмні комплекси, розроблені за сервіс-орієнтованою архітектурою, зазвичай реалізуються як набір веб-служб (веб-сервісів), які взаємодіють за протоколом SOAP (Simple Object Access Protocol), хоча існують й інші способи реалізації: CORBA (Common Object Request Broker Architecture - загальна архітектура брокера об’єктних запитів); REST (Representational State Transfer - передача репрезентативного стану). Веб-сервіс (web service) - програмна система зі стандартизованими інтерфейсами, яка ідентифікується веб-адресою. Веб-сервіси можуть взаємодіяти один з одним і зі сторонніми додатками за допомогою повідомлень, заснованих на відповідних протоколах.

Веб-сервіси - це функціональність і дані, що надаються для використання зовнішніми додатками, які працюють із сервісами за допомогою стандартних протоколів і форматів даних. Веб-сервіси повністю незалежні від мови і платформи реалізації. У рамках формування інтеграційної державної інфраструктури відомчі системи можуть бути реалізовані у вигляді відповідних веб-сервісів або можуть зробити свої інтерфейси доступними у вигляді веб-сервісів [10, с.348].

Серед основних завдань безпеки, які необхідно вирішити для веб-сервісів, можна виділити такі: забезпечити безпечний вхід користувача в особистий

кабінет на видаленому сервері. При цьому треба перевірити достовірність як користувача, так і сервера; реалізувати можливість безпечного формування і перевірки електронного підпису для забезпечення юридичної значущості електронної взаємодії; забезпечити конфіденційність даних, що передаються по каналу зв’язку.

При використанні крипто провайдер а для вирішення певних завдань виникають проблеми наступного характеру: від користувачів потрібні навички установки і налаштування спеціального програмного забезпечення (ПЗ) для роботи з додатками; необхідна прив’язка користувачів до конкретного ПК, на якому встановлений криптопровайдер і наявність прав локального адміністратора операційної системи; при перевстановленні операційної системи вимагається наново проводити установку і налаштування програмного забезпечення [14, с.13].

У процесі інтеграції інформаційної системи з усіма елементами та об’єктами інформаційної інфраструктури важливе місце займає поняття «інтероперабельність» інформаційної системи. Під інтероперабельністю розуміється здатність інформаційної системи взаємодіяти одна з одною. Взаємодія може проявлятися як у вигляді звичайного обміну інформацією, так і у виконанні розподілених завдань. Необхідність забезпечення інтероперабельності виникає при об’єднанні процесів різних організацій, узгодження роботи існуючої інформаційної системи з прийнятими стандартними рішеннями. Інформаційно-орієнтована інтеграція застосовується, в основному, коли необхідний обмін інформацією між декількома інформаційними системами. Даний вид інтеграції є найбільш простим порівняно з іншими, оскільки дані просто передаються з однієї системи в іншу за допомогою перетворення в необхідний формат.

Однією з кращих систем управління інформаційною безпекою серед присутніх на вітчизняному ринку є програмний продукт для обробки подій - netForensics nFX Open Security Platform, яка призначена для роботи з гетерогенним середовищем продуктів забезпечення інформаційної безпеки і

реалізує безперервний збір, обробку та відображення подій безпеки. Система може працювати на платформах Windows, Linux або Solaris, використовуючи в якості сховища даних повнофункціональну систему управління безпекою Oracle. Ця система має широкі можливості щодо роботи в розподіленому режимі, підтримку різних відмовостійких конфігурацій тощо. Система netForensics реалізована на базі технології Java за модульним принципом. Основними модулями системи є сервер додатків (реалізує основну логіку обробки подій, представлення даних, взаємодії з користувачами); база даних (забезпечує зберігання інформації, що надходить до системи); модуль кореляції (здійснює кореляцію зібраних даних); модуль автоматизації УІІБ (здійснює автоматизацію процесів управління інцидентами інформаційної безпеки); агенти (збирають інформацію безпосередньо з пристроїв).

Таким чином, векторами подолання технологічних проблем на шляху оптимізації сервісного підходу в сфері інформаційного захисту мережевих електронних структур в контексті впровадження цифровізації органів державної влади є пошуки загальних принципів інтегративності, сумісності та доступності для користувачів в межах інформаційно-комунікативних систем на основі інтераперабельності.

Однією із ключових умов переходу України до стану розвинутого інформаційного суспільства є реалізація необхідного і достатнього рівня інформаційної безпеки. Основне завдання запровадження цифрових технологій функціонування системи державного управління - оптимізація діяльності всіх органів влади і її переорієнтування на сервісну модель реалізації. Як вже підкреслювалося, державний апарат, побудований за ієрархічним принципом не може бути в повній мірі ефективним в умовах цифрової економіки та суспільства, оскільки децентралізація управління компенсується посиленням горизонтальних зв’язків, що здійснюють взаємодію між однорідними структурами системи.

Головними векторами розвитку сервісно-орієнтованої моделі державного управління та провадження її безпеки повинні стати:

– створення системи визначення і контролю рівня реальної захищеності суспільства від проявів тероризму та шахрайства в інформаційній сфері, що забезпечувало б безперервне отримання відомостей про стан об’єктів інфраструктури;

– створення і підтримка вітчизняних технологій збереження і обробки великих масивів інформації, а також створення захищених функціонали них сервісів і технологічних компонентів;

– розвиток і інтеграція міжвідомчих інформаційних систем єдиного банку даних з проблем інформаційної безпеки;

– розробка спеціалізованих програмно-апаратних комплексів з урахуванням вимог інформаційної безпеки;

– розробка національної програмної платформи на основі єдиних технологій, що дозволяють розробляти нові програмні продукти методом компонування і налаштування вже готових модулів і протоколів;

– створення вітчизняної системи управління базами даних;

– розробка нових та узгодження існуючих архітектурних стандартів та типових компонентів для суміщення програм між собою;

– формування територіально розподіленої інфраструктури технічної підтримки програмного забезпечення;

– формування відкритих стандартів взаємодії інформаційних систем, в тому числі розробка і підтримка профілю відкритих стандартів архітектури державних інформаційних систем, форматів і протоколів обміну даними, що забезпечуючи сумісністю державних інформаційних систем і їх компонентів.

Особливостями уніфікації інформаційної безпеки української держави, влади та суспільства повинні стати: розробка типових стандартів та вимог щодо захисту інформації в єдиній цифровій інфраструктурі органів державної влади; імплементація світових стандартів та досвіду впровадження і функціонування цифрових сервісних пакетів кібербезпеки, запровадження єдиного стандарту цифрового підпису.

Попри окреслені напрями в Україні на сьогодні не існує сформованої системи моніторингу розвитку електронного урядування та діяльності відповідних державних сервісів, що дозволяло би провести багатосторонню оцінку сфери інформаційної безпеки. Відтак, така система повинна бути зорієнтована не тільки на облік реалій сьогоднішнього дня, а й на виявлення тенденцій розвитку відповідно до загальносвітових векторів розвитку, зокрема, в процесі переходу до нових моделей сервісного обслуговування, обумовлених розвитком мобільних та «хмарних» технологічних платформ.

У зв’язку з цим, актуальним постає питання інформаційної безпеки, насамперед, в інтернет-мережі, тобто у форматі фактично «кіберзахисту» (що взагалі є притаманним для більшості розроблених стратегій національної інформаційної безпеки).

Підсумовуючи усе вище викладене у розділі, зазначимо наступне:

1.Державна політика забезпечення інформаційної безпеки повинна бути відкритою і передбачати інформування суспільства про діяльність державних органів і суспільних інститутів у сфері інформаційної безпеки з урахуванням обмежень, встановлених чинним законодавством України. Тому стверджуємо, що вона має виходити з принципу безумовної правової рівності всіх суб'єктів інформаційних відносин незалежно від їхнього політичного, соціального та економічного статусу, ґрунтуватися на обов'язковому забезпеченні прав громадян і організацій на вільне створення, пошук, отримання, накопичення, зберігання, перетворення і поширення інформації у будь-який законний спосіб.

Для створення відкритого інформаційного простору в Україні пропонується запустити механізм практичної реалізації конституційного права на свободу одержання інформації. Правовою основою такого механізму повинні стати законодавчо закріплені чіткі правила, умови і порядок отримання громадянами та інституційними структурами суспільства інформації в органах державної влади і місцевого самоврядування, від інших державних і недержавних юридичних осіб, а також прямого доступу до державних і недержавних інформаційних ресурсів.

Комплексну нормативно-правову регламентацію процесів управління забезпеченням інформаційної безпеки доцільно здійснювати за рахунок систематизації і уніфікації адміністративного законодавства в галузі інформаційної безпеки за допомогою кодифікованого нормативного правового акта, який встановить вихідні засади адміністративно-публічного забезпечення інформаційної безпеки в Україні. В якості такого нормативно-правового акту можна пропонується спільний наказ Міністерства інформаційної політики України, МВС України, Державної служби спеціального зв'язку та захисту інформації України «Про основи адміністративно-правового забезпечення інформаційної безпеки в Україні».

Так само доведена доцільність створення окремої структури, діяльність якої буде направлена на включення представників такого органу в управлінський процес, використання їх «інтелектуального та експертного ресурсу» для досягнення безпекових цілей в інформаційній сфері, аналітичний супровід політики уряду. Це, в свою чергу, передбачає розробку нормативних та програмних підстав для створення даної структури шляхом: 1) внесення змін в Положення «Про Міністерство інформаційної політики України»; 2) внесення змін в Доктрини інформаційної безпеки України (а саме до розділу 6 «Механізм реалізації Доктрини»); 3) включення пункту про створення такого органу в План діяльності Міністерства інформаційної політики України на 2022 рік. Структурно такий орган має включати в своєму складі дві групи учасників: не менше половини членів мають складати представники вітчизняних експертів, науково-дослідних інститутів, університетів, а також експерти в сфері інформаційної безпеки; іншу частину повинні складати представники державних інституцій (державних аналітичних центрів та науково-дослідних інститутів).

2.Для ефективного й оперативного вирішення питань у сфері провадження інформаційної безпеки України, слід опиратися на системний та ситуаційний підходи при виробленні державної політики. Системний підхід дасть змогу об’єднати суб’єкти та механізми реалізації сфери інформаційної безпеки у цілісну систему підтримки прийняття рішень для оперативного та стратегічного

управління складовими підсистемами держави, дозволить представити державу як модель відкритої системи, входами якої буде перелік внутрішніх та зовнішніх загроз, методів реалізації захисту, а виходами результати протидії та стан складових та держави як системи в цілому.

Для забезпечення реалізації пріоритетів державної політики у сфері інформаційної безпеки першочерговими завданнями держави є: 1) нормативно-правове регулювання сервісної діяльності, в тому числі процедур надання послуг органів влади з інформаційної безпеки; 2) делегування управлінських послуг соціально відповідальним суб'єктам недержавного сектору; 3) адаптація та дотримання стандартів послугу сфері кіберзахисту; 4) запровадження сучасних інноваційних форм та цифрових технологій для зручного одержання послуг користувачем та спрощення процедур сервісної діяльності органів публічної влади.

3.Для того, щоб ефективно протистояти реальній загрозі використання мережі Інтернет терористичними угрупуваннями необхідно прийняти відповідні заходи як на міжнародному, так і на національному рівнях. На національному рівні рекомендується: 1) застосовувати існуючі норми законодавства, передбачені Конвенцією Ради Європи про кіберзлочинність щодо процедури направлення запитів про взаємну допомогу за відсутності відповідних міжнародних угод; 2) застосовувати існуючі норми законодавства про боротьбу з тероризмом до випадків кібертероризму, зокрема положення Конвенції Ради Європи про запобігання тероризму, що стосуються публічного підбурювання до вчинення терористичного злочину, а також прийняти спеціальні правові норми, спрямовані на боротьбу із використанням Інтернету в терористичних цілях.

4.Доведена доцільність використання хмарних технологій зберігання та доступу до інформації. Архітектура типової системи управління інформаційною безпекою має включати такі основні компоненти: інтеграційну платформу; апаратно-програмні засоби моніторингу і аудиту; апаратно- програмні засоби захисту інформації; сховище інформації про інциденти інформаційної безпеки; аналітичні інструменти і засоби генерації звітів. Апаратно-програмні засоби

моніторингу і аудиту - засоби, що реалізують функції з протоколювання, збору, накопичення та обробки інформації функціонування інформаційно-комунікативної системи. Вони складають підсистему збору інформації про інциденти інформаційної безпеки. Результатом їх роботи є дані, на основі яких системою приймається рішення щодо настання інциденту. Апаратно-програмні засоби захисту в контексті системи управління інформаційною безпекою включають засоби, які забезпечують локалізацію інцидентів або зниження збитку. Однією з кращих систем управління інформаційною безпекою серед присутніх на вітчизняному ринку є програмний продукт для обробки подій - netForensics nFX Open Security Platform. Пропонується її впровадити у діяльність органів державної влади в Україні.

# ВИСНОВКИ ТА ПРОПОЗИЦІЇ

У результаті проведеного дослідження було досягнено поставленої на початку мети, яка полягала у детальному дослідженні сучасного організаційно-правового забезпечення інформаційної безпеки та виробленні на основі здійсненого аналізу узагальнень щодо його удосконалення. На основі здійсненого аналізу, вироблені наступні удосконалення та пропозиції:

1.Відсутність офіційного визначення інформаційної безпеки є прогалиною у сучасному правовому регулюванні інформаційної безпеки в Україні. Тому нами запропоновано авторське визначення інформаційної безпеки під якою пропонується розуміти комплекс умов, при яких можлива захищеність життєво важливих інтересів держави, суспільства та окремого індивіда в інформаційній сфері, яка відображається в чотирьох аспектах: ціннісному (відсутність негативного впливу на громадську думку), технологічному (кібербезпека); правовому (розвиненість законодавства, що регулює правовідносини в інформаційній сфері); соціально-політичному (відсутність політичної цензури, вільний доступ до публічної інформації).

В сучасному міжнародному праві ще остаточно не сформовано уніфіковане її поняття, а існування великої кількості термінологічних розбіжностей лише ускладнює цей процес. У переважній більшості випадків, використовуючи термін «міжнародна інформаційна безпека», йдеться про змістовний (інформаційний) та технічний (комунікаційний) аспекти інформаційної безпеки, а термін «міжнародна кібербезпека» звужує таке її розуміння лише до технічного аспекту. Проте, нерідко автори використовують ці терміни для визначення одного й того самого поняття. Оскільки кожен з цих термінів має своє змістовне навантаження, пропонується авторське визначення міжнародної інформаційної безпеки як стану, що забезпечується загальновизнаними і спеціальними принципами та нормами міжнародного права, який виключає порушення міжнародного миру і безпеки як окремих держав, так і світового співтовариства в цілому у сфері інформації і комунікації.

Інститут міжнародної інформаційної безпеки необхідно розглядати як міжгалузевий інститут, що представляє собою особливий і відокремлений комплекс норм, який регулює міжгалузеву сферу відносин. Зокрема, мова йде про охоплення інститутом міжнародної інформаційної безпеки відносин в таких галузях міжнародного права, як: право міжнародної безпеки, міжнародне кримінальне право, міжнародне інформаційне право та міжнародне гуманітарне право.

2.Інститут інформаційної безпеки людини в Україні і світі є наймолодшим, порівняно з інформаційною безпекою держави чи суспільства. Протягом багатьох тисячоліть інформаційна безпека розглядалась, насамперед, з перспективи інтересів держави. Згодом інтенсифікація процесів інформатизації в усіх сферах, а особливо, зростання значення технічного захисту інформації зумовило становлення правового забезпечення захисту інформації як невід'ємної складової безпеки підприємств, установ та організацій, а також окремих галузей господарства. На межі тисячоліть гостро повстало питання про міжнародну інформаційну безпеку, а також кібербезпеку у складі інформаційної безпеки. Негативним ефектом застосування сучасних технологій у військово- політичній сфері стали все ширші можливості застосування інформаційної зброї. Відзначено, що наукові дискусії щодо проблематики інформаційної безпеки особливо у інформаційно розвинених країнах світу особливо актуалізувались в останні роки XX сторіччя. В Україні наукове осмислення проблематики інформаційної безпеки людини є в процесі становлення і відбувається як вторинне по відношенню до інформаційної безпеки держави.

3.Сфера інформаційної безпеки передбачає системну превентивну діяльність органів державної влади з надання гарантій інформаційної безпеки особі, соціальним групам та суспільству в цілому і спрямована на формування відповідного рівня довіри до держави, достатнього для подальшого соціального прогресу та належного розвитку інтелектуального потенціалу країни. Аналіз стану сформованості нормативно-правової бази дає підстави стверджувати, що в Україні загалом сформовані всі необхідні правові, адміністративні та економічні

умови для розвитку інституту надання послуг з гарантування захисту і реалізації безпеки інформації. Україна усвідомлює нагальну необхідність у розробці прогресивного національного законодавства у сфері інформаційної безпеки та ключову роль, яку вона відіграє на міжнародному та регіональному рівні щодо протистояння загрозам в інформаційному просторі, особливо з огляду на агресію Російської Федерації щодо України. Так само Україна займає активну позицію щодо поглиблення співпраці зі своїми партнерами в рамках міжнародних універсальних та регіональних організацій в сфері забезпечення МІБ, приймаючи участь в діалозі на рівні ООН та ініціативах МСЄ. Наша ндержава вдосконалює національне законодавство у сфері інформаційної безпеки, про що свідчить прийняття таких важливих документів, як Доктрина інформаційної безпеки України та Стратегія кібербезпеки України.

Внутрішнє законодавство України потребує суттєвого доопрацювання, як з позиції використаної там термінології та її змістовного навантаження, так і з точки зору логіки і побудови. Тому для ефективної реалізації національної політики у сфері забезпечення інформаційної безпеки пропонується: 1) привести у відповідність існуючі правові норми у сфері забезпечення інформаційної безпеки сучасним досягненням; 2) сформувати єдиний підхід до розуміння інформаційної безпеки з огляду на її триелементну структуру та наявність технічної і змістовної компоненти кожного з них; привести законодавство України у відповідність до цього підходу; 3) гармонізувати існуючі правові норми у сфері забезпечення інформаційної безпеки з метою уникнення дублювання різними нормативними актами функцій органів державної влади держави в сфері забезпечення інформаційної безпеки, а також ліквідації прогалин щодо регулювання окремих її аспектів; 4) створити технічний потенціал для протидії загрозам в інформаційному просторі; 5) заохочувати розробку програмного забезпечення національного виробництва з метою мінімізації ризиків використання програмного забезпечення з вбудованими шкідливими програмами; 6) сприяти впровадженню національної культури інформаційної безпеки та підвищенню обізнаності громадян і всіх зацікавлених

сторін у цій сфері; 7) заохочувати розвиток державно-приватного партнерства у сфері інформаційної безпеки.

4.Під загрозою національній безпеці пропонується розуміти можливу небезпеку, що має здатність причинити будь-яку шкоду, призвести до збитків, втрат (матеріальних і людських) або інших негативних наслідків. Класифіковано всі загрози національної безпеки за двома критеріями: 1) за джерелом виникнення на зовнішні та внутрішні загрози; 2) за сферою дії на загрози національній безпеці в політичній, технологічній, економічній, екологічній і т. д. сферах. Пропонуємо авторське розуміння інформаційних загроз як систему зовнішніх та внутрішніх чинників, що чинять згубний вплив на інформаційну безпеку, зачіпаючи життєво важливі інтереси держави, суспільства та людини в інформаційній сфері. Оскільки загрози інформаційній безпеці України є перепоною для належного інформаційного обміну, тому вважаємо, що одним із важливих напрямів щодо цього є вдосконалення вітчизняного законодавства, яким врегульовуються як правові, так і організаційні засади забезпечення інформаційної безпеки України.

5.Глобальний характер таких загроз ускладнює вироблення механізмів їх нівелювання, адже сьогодні щодня виникають нові технологічні виклики, на які не можна відреагувати за допомогою застарілих методів захисту. Враховуючи все це, Україна має затвердитися в глобальному цивілізаційному середовищі в якості конкурентоспроможного суб’єкта. Для цього дуже важливо використовувати всі інструменти ефективного розвитку, що надаються технологічним простором інформаційного суспільства. Водночас, так само необхідно облаштувати надійну національну систему інформаційного захисту від безлічі інформаційних загроз, що йдуть від внутрішніх і зовнішніх впливів, а також з боку глобальних факторів небезпеки, притаманних самій структурі інформаційної цивілізації. Перед українською державою на сучасному етапі державотворчих трансформацій постає складне завдання: максимально використати інформаційно-технологічні, соціально-структуруючі, масово-інформаційні можливості, що надаються інформаційної цивілізацією, і при

цьому захистити власних громадян та державний організм від ураження з боку руйнівних і загрозливих зовнішніх і внутрішніх інформаційних впливів.

6.На сьогоднішній день, національну систему кібербезпеки формують ряд державних інституцій як центрального так і місцевого рівня, військові структурні підрозділи, установи, заклади та організації, які задіяні в галузі комунікацій, опікуються питаннями захисту інформації та мають в своєму розпорядженні об'єкти критичної інформаційної інфраструктури. Головними тенденціями розвитку кіберзагроз у сучасних інформаційних протиборствах виокремлені наступні: 1) збільшення кількості кібератак, спрямованих на нанесення широкомасштабної шкоди інфраструктурам великих корпорацій, важливим промисловим об’єктам, а також інформаційним системам органів державної влади; 2) зростання рівня складності кібератак, які реалізуються поетапно та адаптовані спеціальними інструментами протидії захисту від супротивника; 3) тотальність впливу на всі цифрові (електронні) технології, зокрема мобільні (мережеві) пристрої, які є апріорі максимально вразливими з точки зору інформаційної безпеки; 4) комплексне застосування в гео політичному просторі новітніх технологій кібернападу одних країн на інші (інформаційна війна реалізується на міждержавному рівні). Доведена необхідність побудови дієвої системи кібернетичної безпеки України. Основною умовою досягнення сучасних цілей реформування державного управління є цифровізація всіх його структур. Завдяки такому підходу створюються умови для формування інформаційного (цифрового) простору органів державної влади в середовищі єдиного кіберпростору, як першого кроку на шляху забезпечення відкритості, підконтрольності діяльності з боку громадських інститутів і забезпечення ефективної комунікативної взаємодії всіх суб’єктів державно-управлінського процесу.

7.На сучасному етапі боротьби держав за сфери впливу акцент із явного застосування сили усе помітніше зміщується на використання більш гнучких засобів, основним із яких є контроль і керування інформаційними ресурсами. Українські правоохоронці постійно нагадують, що злочинці намагаються

зламати інформаційні мережі й поштові сервери державних установ. Під виглядом офіційних листів надсилаються електронні повідомлення із вкладеним шкідливим програмним забезпеченням, яке рекомендується встановити. Зокрема, СБУ неодноразово звертала увагу керівників державних органів влади та установ, а також співробітників ІТ-департаментів на необхідність посилення заходів з недопущення несанкціонованого встановлення програмного забезпечення чи його оновлення, аби не допустити хакерського проникнення на державні інформаційні ресурси.

8.Державна політика забезпечення інформаційної безпеки повинна бути відкритою і передбачати інформування суспільства про діяльність державних органів і суспільних інститутів у сфері інформаційної безпеки з урахуванням обмежень, встановлених чинним законодавством України. Тому стверджуємо, що вона має виходити з принципу безумовної правової рівності всіх суб'єктів інформаційних відносин незалежно від їхнього політичного, соціального та економічного статусу, ґрунтуватися на обов'язковому забезпеченні прав громадян і організацій на вільне створення, пошук, отримання, накопичення, зберігання, перетворення і поширення інформації у будь-який законний спосіб.

Для створення відкритого інформаційного простору в Україні пропонується запустити механізм практичної реалізації конституційного права на свободу одержання інформації. Правовою основою такого механізму повинні стати законодавчо закріплені чіткі правила, умови і порядок отримання громадянами та інституційними структурами суспільства інформації в органах державної влади і місцевого самоврядування, від інших державних і недержавних юридичних осіб, а також прямого доступу до державних і недержавних інформаційних ресурсів.

Комплексну нормативно-правову регламентацію процесів управління забезпеченням інформаційної безпеки доцільно здійснювати за рахунок систематизації і уніфікації адміністративного законодавства в галузі інформаційної безпеки за допомогою кодифікованого нормативного правового акта, який встановить вихідні засади адміністративно-публічного забезпечення

інформаційної безпеки в Україні. В якості такого нормативно-правового акту можна пропонується спільний наказ Міністерства інформаційної політики України, МВС України, Державної служби спеціального зв'язку та захисту інформації України «Про основи адміністративно-правового забезпечення інформаційної безпеки в Україні».

Так само доведена доцільність створення окремої структури, діяльність якої буде направлена на включення представників такого органу в управлінський процес, використання їх «інтелектуального та експертного ресурсу» для досягнення безпекових цілей в інформаційній сфері, аналітичний супровід політики уряду. Це, в свою чергу, передбачає розробку нормативних та програмних підстав для створення даної структури шляхом: 1) внесення змін в Положення «Про Міністерство інформаційної політики України»; 2) внесення змін в Доктрини інформаційної безпеки України (а саме до розділу 6 «Механізм реалізації Доктрини»); 3) включення пункту про створення такого органу в План діяльності Міністерства інформаційної політики України на 2022 рік. Структурно такий орган має включати в своєму складі дві групи учасників: не менше половини членів мають складати представники вітчизняних експертів, науково-дослідних інститутів, університетів, а також експерти в сфері інформаційної безпеки; іншу частину повинні складати представники державних інституцій (державних аналітичних центрів та науково-дослідних інститутів).

9.Для ефективного й оперативного вирішення питань у сфері провадження інформаційної безпеки України, слід опиратися на системний та ситуаційний підходи при виробленні державної політики. Системний підхід дасть змогу об’єднати суб’єкти та механізми реалізації сфери інформаційної безпеки у цілісну систему підтримки прийняття рішень для оперативного та стратегічного управління складовими підсистемами держави, дозволить представити державу як модель відкритої системи, входами якої буде перелік внутрішніх та зовнішніх загроз, методів реалізації захисту, а виходами результати протидії та стан складових та держави як системи в цілому.

Для забезпечення реалізації пріоритетів державної політики у сфері інформаційної безпеки першочерговими завданнями держави є: 1) нормативно-правове регулювання сервісної діяльності, в тому числі процедур надання послуг органів влади з інформаційної безпеки; 2) делегування управлінських послуг соціально відповідальним суб'єктам недержавного сектору; 3) адаптація та дотримання стандартів послугу сфері кіберзахисту; 4) запровадження сучасних інноваційних форм та цифрових технологій для зручного одержання послуг користувачем та спрощення процедур сервісної діяльності органів публічної влади.

Для того, щоб ефективно протистояти реальній загрозі використання мережі Інтернет терористичними угрупуваннями необхідно прийняти відповідні заходи як на міжнародному, так і на національному рівнях. На національному рівні рекомендується: 1) застосовувати існуючі норми законодавства, передбачені Конвенцією Ради Європи про кіберзлочинність щодо процедури направлення запитів про взаємну допомогу за відсутності відповідних міжнародних угод; 2) застосовувати існуючі норми законодавства про боротьбу з тероризмом до випадків кібертероризму, зокрема положення Конвенції Ради Європи про запобігання тероризму, що стосуються публічного підбурювання до вчинення терористичного злочину, а також прийняти спеціальні правові норми, спрямовані на боротьбу із використанням Інтернету в терористичних цілях.

Так само доведена доцільність використання хмарних технологій зберігання та доступу до інформації. Архітектура типової системи управління інформаційною безпекою має включати такі основні компоненти: інтеграційну платформу; апаратно-програмні засоби моніторингу і аудиту; апаратно-програмні засоби захисту інформації; сховище інформації про інциденти інформаційної безпеки; аналітичні інструменти і засоби генерації звітів. Апаратно-програмні засоби моніторингу і аудиту - засоби, що реалізують функції з протоколювання, збору, накопичення та обробки інформації функціонування інформаційно-комунікативної системи.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1.Адаптивні підходи до забезпечення кібербезпеки розподілених та ієрархічних систем управління. *Безпека інформації*. 2016. Т. 22. № 3. С. 255-260.

2.Актуальні питання протидії тероризму у світі та в Україні: аналіт. доповідь / [Резнікова О.О., Місюра А.О., Дрьомов С.В., Войтовський К.Є.]; за заг. ред. О.О. Резнікової. К.: НІСД, 2017. 60 с.

3.Алямкін Р. Правове забезпечення національної інформаційної безпеки. *Наукові записки Інституту законодавства Верховної Ради України*. 2013. № 4. С. 91–96.

4.Ананьїн В., Пучков О. Інформаційна безпека як складова національної безпеки України. *Гілея: науковий вісник: зб. наук. пр*. 2014. Випуск 85 (6). С. 194−197.

5.Архипова Є. О. Інформаційна безпека: соціально-філософський вимір: дис. … кандидата філософ. наук: 09.00.03. Київ, 2012. 199 с.

6.Богуш В. Інформаційна безпека держави. Київ: МК-Прес, 2005. 432 с.

7.Бондар Ю. Зміцнення та захист національного інформаційного простору України: проблеми та шляхи забезпечення. Український науковий журнал «Освіта регіону політологія психологія комунікації». URL: http://socialscience.com.ua/article/61. (дата звернення: 05.08.2021).

8.Бурда О.М. Досвід США щодо запобігання крадіжкам у мережі роздрібної торгівлі. *Право і суспільство*. 2019. № 2. С.172-177.

9.Василенко В. А. Основи теорії міжнародного права / В. А. Василенко. К.: Вища школа, 1988. 288 с.

10.Вітер М. Б. Використання хмарних технологій у системі інформаційної взаємодії державних органів. *Наук, вісн. НЛТУ України*. 2014. - Вин. 24.9. С. 341-347.

11.Гапеєва О.Л. Історіографічний аналіз проблеми інформаційної безпеки на пострадянському просторі. *Історико-культурні студії*. 2016. Вип.3. С.37-41.

12.Глазов О. В. Національна безпека: сутність, ознаки, концепція та геополітичні чинники. *Науковий вісник Чорноморського державного університету імені Петра Могили «Наукові праці» Сер.: Політологія*. 2011. Т. 155, Вип. 143. С. 42-46.

13.Глебова Н. Формування свободи й відкритості в глобальному інформаційному просторі. *Соціологічні студії.* 2013. № 2 (3). С. 22−27.

14.Горбань Ю. Сучасні виклики інформаційного простору для демократичної держави. *Актуальні проблеми державного управління, педагогіки та психології: збірник наукових праць*. 2013. Випуск 2. С. 36−41.

15.Грицун О. О. Україна на шляху до створення національної системи інформаційної безпеки. URL: http://www.iir.edu.ua/uploads/files/Publikacii. (дата звернення: 05.08.2021).

16.Грицюк Ю. І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання. *Наук. вісн. НЛТУ України*. 2016. Вип. 26.8. С. 327-337.

17.Грицик А. Правова відповідальність за зловживання свободою інформації. Україна в системі глобального інформаційного обміну: теоретико-методологічні аспекти дослідження і підготовки фахівців: всеукраїнська наукова конференція (Львів, 27 травня 2011 р.). Львів: «Львівська політехніка». 2011. С. 209-215.

18.Громико І. Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам. *Право України*. 2008. № 8. С. 130–134.

19.Група 414. URL: http://e-koncept.ru/2016/96090.htm. (дата звернення: 05.08.2021).

20.Гуцалюк М. Інформаційна безпека України: нові загрози. *Бизнес и безопасность*. 2003. № 5. С. 2-3.

21.Доклад Генерального секретаря Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. URL: http://undocs.org/ru/A/67/167. (дата звернення: 05.08.2021).

22.Доклад о работе совещания Группы экспертов для проведения всестороннего исследования проблемы киберпреступности. URL:

http://www.unodc.org/documents/organized-crime/cybercrime/CybercrimeApril2017/Cybercrime_report_2017/Report_Cyber_R.pdf. (дата звернення: 05.08.2021).

23.Дубас О. Інформаційний розвиток сучасної України у світовому контексті: політологічний аналіз: автореф. дис. ... канд. політ. наук: 23.00.02. Київ. 2004. 23 с.

24.Залевська І. Інформаційна безпека: нові підходи до визначення поняття. *Український науковий журнал «ОСВІТА РЕГІОНУ».* 2010. № 4. С. 216-224.

25.Звіт про відрядження делегації України для участі у роботі Всесвітньої конференції радіозв'язку Міжнародного союзу електрозв'язку (м. Женева, Швейцарська Конфедерація). URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=241214&cat_id=9726. (дата звернення: 05.08.2021).

26.Звіт щодо України, підготовлено Офісом Програми з кіберзлочинності. URL : https://rm.coe.int/ 16806f3743. (дата звернення: 05.08.2021).

27.Делегація Держспецзв'язку та Microsoft підписали угоду про співробітництво у сфері безпеки. URL: https://www.kmu.gov.ua/news. (дата звернення: 05.08.2021).

28.Деякі питання функціонування Національної телекомунікаційної мережі: Постанова Кабінету Міністрів України від 16 грудня 2020 р. № 1358 URL: https://zakon.rada.gov.ua/laws/show/1358-2020-%D0%BF#Text. (дата звернення: 05.08.2021).

29.Дмитренко М. Політична система України: розвиток в умовах глобалізації та інформаційної революції: монографія. Видання 2-ге з доп. та змінами. Київ:Університет «Україна», 2011. 820 с.

30.Дрожчана О.У., Родик Р.В. Кібертероризм, як нова форма тероризму. Енерго- та ресурсозберігаючі технології та машини в аграрному виробництві: матеріали ІІІ Всеукраїнської науково-практичної інтернет-конференції. (м. Полтава, 03-05 грудня 2018 р.). Полтава: ПДАА. С. 131-134.

31.Дубов Д. В. Стратегічні аспекти кібербезпеки України. *Стратегічні пріоритети.* 2013. № 4 (29). С. 119-126.

32.Задорожня Л. Питання вдосконалення законодавства України у сфері інформації та інформатизації. Додаток до наук. журналу «Правова інформатика». Київ: Академія правових наук. 2005. 31 с.

33.Захаренко К. Відкритість інформаційного простору та контроль за доступністю інформації. *Проблеми соціальної роботи: філософія, психологія, соціологія.* 2020. Вип. 14. С. 46-55.

34.Захаренко К. Глобальна природа інформаційної безпеки. *Політологічний вісник*. 2015. Вип. 79. С. 181-189.

35.За рік кількість кібератак в Україні зросла вдесятеро. URL: https://www.depo.ua/ukr/life/za-rik-kilkist-kiberatak-v-ukrayini-zrosla-vdesyatero-20180307739148. (дата звернення: 05.08.2021).

36.Золотар О. Класифікація загроз інформаційної безпеки. *Інформація і право.* 2013. № 3 (9). С. 105−112.

37.Калюжний Р. Інформаційне право України: концептуальні основи формування. *Науковий вісник Дніпропетровського юридичного інституту МВС України.* № 3 (6). 2001. С. 234–244.

38.Ковалів В. О. Огляд нормативно-правових засад кібербезпеки в Україні. *Актуальні задачі та досягнення у галузі кібербезпеки: матеріали Всеукр. наук.-практ. конф., 23-25 листоп. 2016 р., м. Кропивницький.* Кропивницький : [б. в.]. 2016. С. 13-15.

39.Ковалів М. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України. *Traektoriâ Nauki = Path of Science*. 2021. Vol. 7. № 4. S. 2011-2018.

40.Конституція України. Відомості Верховної Ради України. 1996. № 30. С. 141.

41.Концепція інформаційної безпеки: Проект Міністерстві інформаційної політики від 09.06.2015 р. URL: https://ips.ligazakon.net/document/NT1607. (дата звернення: 05.08.2021).

42.Копійка М. Інституціональний концепт інформаційної безпеки України. Деокупація і реінтеграція інформаційного простору Криму: міжнародно-правові та медіакомунікативні інструменти: матеріали міжнародної науково- практичної конференції. м. Київ: 18 квітня 2019 року. Київ. 2019. С. 17–22.

43.Косогов О. М. Сучасна політика безпеки кіберпростору в умовах його мілітаризації. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2015. № 3(24). С. 181-186.

44.Кравець Є. Інформаційна безпека держави. Юридична енциклопедія: У 6 т. / Ред. кол.: Ю. Шемшученко (голова редкол.) та ін. Київ: Укр. Енцикл., 1998–1999. Т. 2. С. 714–715.

45.Крилова Н. Підходи до визначення і розуміння поняття «інформаційна безпека» в рамках національного безпекознавства. *Гілея: науковий вісник: зб. наук. пр. 2010.* Вип. 36. С. 423−428.

46.Лазарев Г. Защита информации в информационно-телекомуникационных системах. *Національна безпека і оборона.* 2001. № 1. С. 80–83.

47.Ліпкан В. Національна безпека України: навч.посібник. 2-ге вид. Київ: КНТ, 2009. 576 с.

48.Литвиненко О. Інформація і безпека. *Нова політика*. 1998. № 1. С. 47−49.

49.Лук’янчук Р. В. Державне стратегічне планування у сфері забезпечення кібербезпеки: реалії сьогодення. *Вісн. НАДУ*. 2016. № 3. С. 131-137.

50.Максименко Ю. Теоретико-правові засади забезпечення інформаційної безпеки України: автореф. дис. ... канд. юрид. наук: 23.00.01. Київ. 2007. 22 с.

51.Малик Я.Й. Інформаційна війна і Україна. URL: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3. (дата звернення: 05.08.2021).

52.Мошковська С. Передумови входження України у глобальний інформаційний простір в контексті вимог міжнародної інформаційної безпеки. Україна в системі глобального інформаційного обміну: теоретико-методологічні

аспекти дослідження і підготовки фахівців: всеукраїнська наукова конференція (Львів, 27 травня 2011 р.). Львів: «Львівська політехніка». 2011. С. 118-122.

53.Наливайко Л. Інформаційна безпека та інформаційна політика в Україні: конституційно правовий аспект. *Вісник Запорізького державного університету. Сер.: Юридичні науки.* 2003. № 1. С. 60–65.

54.Нашинець-Наумова А. Теоретико-правові основи забезпечення інформаційної безпеки українського суспільства. *Вісник Національного технічного університету України «Київський політехнічний інститут». Сер.: Політологія. Соціологія. Право*. 2013. № 4. С. 124–127.

55.ОБОЄ передала українській кіберполіції 194 одиниці обладнання. URL: https://www.ukrinform.ua/rubric-technology/2269227-obse-peredala ukrainskij-kiberpolicii-194-odinici-specialnogo- obladnanna. html. (дата звернення: 05.08.2021).

56.Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посіб. Стоцький А.Б., Тимошенко О.І., Гуз А.М. та ін. К. : Європ. ун-т, 2006. 232 с.

57.Орлов П. Правове забезпечення інформаційної безпеки / П. Орлов // Вісн. Харків, нац. у-ту внутріш. справ. Вип. 15. С. 96-99.

58.Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 08 лютого 2021 року № 92. URL: https://zakon.rada.gov.ua/laws/show/92-2021-%D0%BF#Text. (дата звернення: 05.08.2021).

59.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

60.Про вдосконалення співпраці органів військового управління з громадськими організаціями: Директива Міністерства оборони України від 27.04.2009 р. № Д-13. URL: https://zakon.rada.gov.ua/rada/show/v0013322-09#Text. (дата звернення: 05.08.2021).

61.Про Доктрину інформаційної безпеки України: Указ Президента України від 08 липня 2009 р. Верховна Рада України: офіційний сайт. URL: http://zakon2.rada.gov.ua/laws/show/514/2009. (дата звернення: 05.08.2021).

62.Про забезпечення участі громадськості у формуванні та реалізації державної політики у військовій сфері: Постанова Кабінету Міністрів України від 03.11.2010 р. № 996. URL: https://zakon.rada.gov.ua/laws/show/996-2010-%D0%BF#Text. (дата звернення: 05.08.2021).

63.Про затвердження нормативно-правових актів з питань інформаційної безпеки: Постанова Правління Національного банку України від 26.11.2015 р. № 829. URL: https://zakon.rada.gov.ua/laws/show/v0829500-15#Text. (дата звернення: 05.08.2021).

64.Про затвердження Положення про Департамент інформатизації Міністерства внутрішніх справ України : Наказ МВС України від 31.01.2018 р. № 70. URL: http://parusconsultant.com/?doc=0AZG0FB928&abz=KB7HR. (дата звернення: 05.08.2021).

65.Про інформацію: Закон України від 2 жовт. 1992 р. № 2657-XII. URL: http://zakon2.rada.gov.ua/laws/show/2657-12. (дата звернення: 05.08.2021).

66.Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. № 75/98-ВР. *Відомості Верховної Ради України*. 1998. № 28. Ст.182.

67.Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

68.Проноза І. І. Засоби масової інформації і комунікації в інформаційній війні як сучасна політична практика. *Політикус : наук. журнал.* 2020. № 3. С. 65–70.

69.Проноза І. І. Інформаційна війна: сутність та особливості прояву / І. І. Проноза. Актуальні проблеми політики : зб. наук. пр. / редкол.: С. В. Ківалов (голов. редкол.), Л. І. Кормич (голов. ред.), А. В. Полухіна (відп. ред.) [та ін.] ; НУ «ОЮА», Південноукр. центр гендер. проблем. Одеса : Фенікс, 2018. Вип. 61. С. 76-84.

70.Про Національний координаційний центр кібербезпеки: Указ Президента України від 07 черв. 2016 р. № 242/2016. URL: http://www.president.gov.ua/documents/2422016-20141. (дата звернення: 05.08.2021).

71.Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації: Положення затверджене Указом Президента України від 23 листопада 2011 року № 1067/2011. URL: https://zakon.rada.gov.ua/laws/show/1067/2011#Text. (дата звернення: 05.08.2021).

72.Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст.403.

73.Про Річну національну програму під егідою Комісії Україна – НАТО на 2020 рік: Указ Президента України від 26.05.2020 р. № 203/2020. URL: https://www.president.gov.ua/documents/2032020-3386. (дата звернення: 05.08.2021).

74.Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037. (дата звернення: 05.08.2021).

75.Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 берез. 2016 р. № 96. URL: http://zakon3.rada.gov.ua/laws/show/96/2016. . (дата звернення: 05.08.2021).

76.Про створення міжвідомчої робочої групи Адміністрації Державної служби спеціального зв'язку та захисту інформації України і Міністерства внутрішніх справ України : Спільний наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Міністерства внутрішніх справ України від 08.05.2015 р. № 256/545. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=E26EA615EF0

1E8A00DDF183B87CE5FE9.app2?art id=148413&cat id=121207. (дата звернення: 05.08.2021).

77.Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text. (дата звернення: 05.08.2021).

78.Про утворення територіального органу Національної поліції: Постанова Каб. Міністрів України від 13 жовт. 2015 р. № 831. URL: http://zakon3.rada.gov.ua/laws/show/831-2015-n. (дата звернення: 05.08.2021).

79.Романчук Ю. Міжнародне співробітництво у сфері інформаційної безпеки: концептуальний та регулятивний аспекти: автореф. дис. ...канд. політ. наук: 23.00.04. Київ. 2009. 16 с.

80.Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL: http://www.journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php. (дата звернення: 05.08.2021).

81.Світлична В. Ю. Інформаційна безпека: сутність та порядок реалізації. *Молодий вчений*. 2014. №11. С. 97-100.

82.Словарь-справочник по информационной безопасности для Парламентской Ассамблеи ОДКБ / под общ. ред. М. А. Вуса и М. М. Кучерявого. СПб.: СПИИРАН. Изд-во «Анатолия». «Полиграфические технологии», 2014. 96 с.

83.Стрихалюк Б. М. Структурний та функціональний синтез гетерогенних сервіс но-орієнтованих телекомунікаційних мереж : автореф. дис. ... д-ра техн. наук : 05.12.02. Львів, 2015. 40 с.

84.Суббот А. Інформаційна безпека суспільства. *Віче.* 2015. № 8. С. 29-31.

85.Сунь-цзи. Мистецтво війни. К.: Арій, 2014. 128 с.

86.Талимончик В. П. Международно-правовое регулирование отношений информационного обмена / В. П. Талимончик. СПб. : Издательство «Юридический центр-Пресс», 2011. С. 230-231.

87.Теоретичні основи побудови та функціонування систем управління інцидентами інформаційної безпеки. *Захист інформації*. 2012. № 1. С.1-10.

88.Тихомиров О. Класифікації забезпечення інформаційної безпеки. *Вісник Запорізького національного університету. Сер.: Юридичні науки*. 2011. № 1. С. 164–168.

89.Угода між урядами держав-членів ШОС про співробітництво в сфері забезпечення міжнародної інформаційної безпеки: Міжнародний документ від 16.06.2009 р. URL: http://base.spinform.ru/show_doc.fwx?rgn=28340. (дата звернення: 05.08.2021).

90.Угода про співробітництво держав-учасниць Співдружності Незалежних Держав в боротьбі зі злочинами у сфері комп'ютерної інформації: Міжнародний документ від 01.06.2001 р. URL: https://zakon.rada.gov.ua/laws/show/997_353#Text. (дата звернення: 05.08.2021).

91.Фань Ч. Правове забезпечення інформаційної безпеки в системі сучасної міжнародної співпраці. *Наукові праці МАУП*. 2012. Вип. 4 (35). С. 110–115.

92.Харченко Л. Інформаційна безпека України: Глосарій. Київ: Текст, 2004. 136 с.

93.Хронологія розвитку засобів і методів захисту інформації. URL: http://kspu.kr.ua/index.php. (дата звернення: 05.08.2021).

94.Цимбалюк В. Інформаційне право (основи теорії і практики): монографія. Київ: Освіта України, 2010. 388 с.

95.Цифрова адженда України: проект 2020. URL: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf. (дата звернення: 05.08.2021).

96.Шаванов С. В. Соціальна психологія сучасних інформаційних війн. *Молодий вчений*. 2014. № 4 (07). С. 133–136.

97.Шайхет С. О. Інформаційна безпека як сервіс належного врядування. *Актуальні проблеми державного управління : зб. наук. пр. ОРІДУ*. 2016. Вип. 3(67). С. 97-101.

98.Шевцов О. Технологічні аспекти впровадження концепції сервіс-орієнтованої архітектури у сфері державних електронних послуг. *Вісн. Нац. акад. держ. упр*. 2012. № 39. С. 311-319.

99.Юричко А. Інформаційні маніпуляції у повідомленнях світової періодичної преси в контексті інформаційної безпеки України: стан та шляхи протидії: автореф. дис. ...канд. філолог наук: 10.01.08. Київ. 2007. 18 с.

100.Ющук О. Інформаційна безпека користувачів мережі Інтернет. *Наукові записки. Серія «Культура та соціальні комунікації».* 2009. Вип. 1. С. 224−231.

101.Ягодзінський С. Інформаційний простір глобальних мереж: соціально-філософський аспект. *Вісник Національного авіаційного університету. Серія: Філософія. Культурологія: Збірник наукових праць*. 2013. Вип. 1 (17). С. 77−80.

102.Global Cybersecurity Index & Cyberwellness Profiles : report. Geneva : ITU, 2015. 516 p.

103.GCHQ intercepted foreign politicians' communications at G20 summits / The Guardian. URL: http://www.theguardian.com/uk/2013/jun/16/gchq-interceptedcommunicationsg20-Summits. (дата звернення: 05.08.2021).

104.International Standard ISO/IEC 27000 Third edition. URL: http://www.pqm-online.com/assets/files/pubs/translations/std/iso-mek-27000-2014.pdf. (дата звернення: 05.08.2021).

# ДОДАТКИ

**Додаток А**

Міністерство освіти і науки України
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»
Азербайджанський державний економічний університет (UNEC)
Білостоцький технологічний університет (Польща)
ISMA University (Латвійська республіка)
University North (Хорватія)
Varna Free University «Chernorizets Hrabar» (Болгарія)
Національний університет «Чернігівська політехніка»
Дніпропетровський регіональний інститут державного управління
Національної академії державного управління
при Президентові України
Інститут підготовки кадрів державної служби зайнятості України
Західноукраїнський національний університет
Хмельницький університет управління та права імені Леоніда Юзькова
Херсонський національний технічний університет
Черкаський національний університет імені Богдана Хмельницького

# ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ ПУБЛІЧНОГО УПРАВЛІННЯ В УКРАЇНІ

**Матеріали VIII Всеукраїнської науково-практичної Інтернет-конференції за міжнародною участю**

29 квітня 2021 року

Полтава
2021

УДК 35.073:34(477)
О64





**Організаційно-правові аспекти публічного управління в Україні :** Матеріали VIII Всеукраїнської науково-практичної Інтернет-конференції за міжнародною участю, 29 квітня 2021 р. – Полтава : Національний університет імені Юрія Кондратюка, 2020. – 196 с.

У збірнику матеріалів VIII Всеукраїнської науково-практичної Інтернет-конференції за міжнародною участю розглядаються теоретичні та правові аспекти модернізації публічного управління України з урахуванням іноземного досвіду, шляхи та методи оптимізації діяльності органів влади на регіональному рівні, іноземний досвід впровадження сучасних систем та методів управління в діяльність органів влади, організаційні та фінансові аспекти забезпечення діяльності органів виконавчої влади та місцевого самоврядування, розвиток лідерства в публічному управлінні, підготовка та підвищення кваліфікації кадрів державної служби та служби в органах місцевого самоврядування.
Розрахований на фахівців публічного управління, працівників органів державної влади та місцевого самоврядування, науковців, викладачів, слухачів та студентів.

УДК 35.073:34(477)

## ЗМІСТ

ред. В.Д. Бакуменка. О.О. Краснорyцького. Харків. ХНТУСГ ім. Петра Василенка. 2019. 105 с.
2. Експертна аналітика державного управління: аспекти інноватики, самоорганізації : монографія / Бакуменко В.Д., Іжа М.М., Попов М.П., Попов С.А., Краснорyцький О.О., Білорусов С.Г., Червякова О.В., ; за. заг. ред. В.Д. Бакуменка, М.М. Іжі, С.А. Попова. – Одеса : ОРІДУ НАДУ, 2020. – 220 с.
3. Експертна аналітика розвитку механізмів державного управління: міжрівнева взаємодія, системна організація та самовпорядкування: Монографія. Бакуменко В.Д., Краснорyцький О.О., Дончик Н.П., Усаченко О.О., Гацько А.Ф., Прокопенко В.Ю., Родченко І.Ю., Бєлоусова О.С., Бобловський О.Ю., Краля В.Г., Подольська О.В., Сагачко Ю.М., Смігунова О.В. За. заг. ред. В.Д. Бакуменка. О.О. Краснорyцького. Харків : ХНТУСГ ім. Петра Василенка. 2020. 114 с.

*Бондарєв Владислав Віталійович,*
*Національний університет «Полтавська політехніка імені Юрія Кондратюка», магістрант спеціальності «Публічне управління та адміністрування»*

## ВПЛИВ ІНФОРМАЦІЙНИХ ТА ГІБРИДНИХ ВІЙН НА ПУБЛІЧНУ ПОЛІТИКУ ТА ФУНКЦІОНУВАННЯ ПУБЛІЧНОГО УПРАВЛІННЯ В УКРАЇНІ

В умовах ведення інформаційних та гібридних війн рівень інформаційної безпеки помітно коливається та впливає як на рівень політичної, економічної та інших складових безпеки країни, так і на роботу органів публічного управління та функціонування публічної політики зокрема. Так, основні прояви інформаційних та гібридних воєн проявляються у протиправному доступі до конфіденційної інформації, а також у можливостях маніпулювання свідомістю суспільства. Найбільшу небезпеку такі прояви становлять для функціонування органів публічної влади та ведення публічної політики. Як слушно зазначає В. В. Антонюк, реальну внутрішню загрозу інформаційній безпеці України представляє протиправна діяльність організованої злочинності й окремих особистостей, адже основною метою їх діяльності є отримання надприбутку із застосування сфери політики, яка так само входить у коло їхніх інтересів [1, с. 46].

Отже, на сьогоднішній день коло суб'єктів зі здійснення публічного управління із забезпечення інформаційної безпеки в нашій державі є доволі розгалуженим і представляє собою доволі багаторівневу систему, яка складається з таких державних органів України: 1) Президент України; 2) Кабінет Міністрів України; 3) Служба безпеки України; 4) Державна служба спеціального зв'язку та захисту

інформації України; 5) розвідувальні органи України, до яких належать Служба зовнішньої розвідки України, розвідувальний орган Міністерства оборони України, розвідувальний орган спеціально уповноваженого центрального органу виконавчої влади у справах охорони державного кордону.

Багато вчених і дослідників вважають, що наявна система органів публічного управління не є досконалою та повинна бути адекватною щодо загальної системи державного управління [2]. Ми погоджуємось з таким твердженням і вважаємо, що ця система має бути максимально чітко територіально розподіленою із визначенням усіх координаційних елементів. Відтак, система публічних органів в Україні поки що не здатна ефективно протидіяти проявам інформаційних і гібридних воєн, а залишається лише частиною правових механізмів щодо забезпечення інформаційної безпеки в державі.

За сучасних умов, Україна усвідомлює нагальну необхідність у розробці прогресивного національного законодавства у сфері інформаційної безпеки та ключову роль, яку вона відіграє на міжнародному та регіональному рівні щодо протистояння загрозам в інформаційному просторі, особливо з огляду на агресію Російської Федерації щодо України. Наша держава займає активну позицію щодо поглиблення співпраці зі своїми партнерами в рамках міжнародних універсальних та регіональних організацій в сфері забезпечення МІБ, приймаючи участь в діалозі на рівні ООН та ініціативах МСЄ [3]. Так само, Україна вдосконалює національне законодавство у сфері інформаційної безпеки, про що свідчить прийняття таких важливих документів, як Доктрина інформаційної безпеки України та Стратегія кібербезпеки України. Водночас, внутрішнє законодавство України потребує суттєвого доопрацювання, як з позиції використаної там термінології та її змістовного навантаження, так і з точки зору логіки і побудови.

Тому для ефективної реалізації національної політики у сфері забезпечення інформаційної безпеки пропонуємо: 1) привести у відповідність існуючі правові норми у сфері забезпечення інформаційної безпеки сучасним досягненням; 2) сформувати єдиний підхід до розуміння інформаційної безпеки з огляду на її триелементну структуру та наявність технічної і змістовної компоненти кожного з них; привести законодавство України у відповідність до цього підходу; 3) гармонізувати існуючі правові норми у сфері забезпечення інформаційної безпеки з метою уникнення дублювання різними нормативними актами функцій органів державної влади держави в сфері забезпечення інформаційної безпеки, а також ліквідації прогалин щодо регулювання окремих її аспектів; 4) створити технічний потенціал для протидії загрозам в інформаційному просторі; 5) заохочувати розробку програмного забезпечення національного виробництва з метою мінімізації ризиків використання програмного забезпечення з вбудованими шкідливими програмами; 6) сприяти впровадженню

національної культури інформаційної безпеки та підвищенню обізнаності громадян і всіх зацікавлених сторін у цій сфері; 7) заохочувати розвиток державно-приватного партнерства у сфері інформаційної безпеки.

**Література:**

1.Антонюк В.В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України: дис. ... канд. юрид. наук: 25.00.02 / В.В. Антонюк. – К., 2017. – 218 с
2.Бондар Ю. Зміцнення та захист національного інформаційного простору України: проблеми та шляхи забезпечення [Електронний ресурс]. – Режим доступу: http://socialscience.com.ua/article/61.
3.Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки [Електронний ресурс]. – Режим доступу: http://www.journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.

*Бутенко Михайло Іванович,*
*Головне управління Державної казначейської служби України у Полтавській області, головний спеціаліст відділу обслуговування розпорядників коштів та інших клієнтів місцевого бюджету – управління обслуговування розпорядників коштів та інших клієнтів*

## ЗАВДАННЯ ТА ПРАВОВІ ОСНОВИ МОДЕРНІЗАЦІЇ ДЕРЖАВНОЇ СЛУЖБИ В УКРАЇНІ

Сучасна соціально-економічна і політична ситуація в Україні, реформування державної служби відповідно до завдань правової демократичної держави вимагають відповідних змін в її кадровому забезпеченні, розроблення та освоєння нових підходів і засад підготовки, формування та використання персоналу. Є безпосередня залежність результативності й ефективності функціонування держаних службовців від якості підготовки їх кадрового потенціалу.

Україна прагне до вступу в європейське співтовариство, що зумовлює необхідність адаптації норм вітчизняного законодавства до європейських стандартів, зокрема це стосується трудового законодавства, а також пов'язаного з ним законодавства про державну службу. Реформування державної служби як висококваліфікованої та професійної діяльності уповноважених на виконання функцій держави осіб, зумовлює настання суттєвих змін в інституті державної служби, зокрема зміни стосуються порядку прийняття на державну службу, її проходження та припинення. Закон України «Про державну службу» від 10.12.2015 р. № 889 [1] відповідає Принципам державного управління та спрямований на вирішення основних питань державної служби. Ефективна реалізація зазначеного Закону є найбільшим