НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

**КУШНІКОВ Вадим Вадимович**

УДК 351:342.57

**ДИСЕРТАЦІЯ**

# УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Спеціальність 281 Публічне управління та адміністрування
Галузь знань 28 Публічне управління та адміністрування

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____Вадим КУШНІКОВ

Науковий керівник: Дєгтяр Андрій Олегович, професор кафедри економіки та публічного управління, доктор наук з державного управління, професор, Заслужений діяч науки і техніки України

Харків – 2026

# АНОТАЦІЯ

***Кушніков В.В.*** **Управління інформаційною безпекою держави в умовах гібридних загроз.** – Кваліфікаційна наукова праця на правах рукопису.

*Дисертація на здобуття наукового ступеня доктора філософії з галузі знань «Публічне управління та адміністрування» за спеціальністю 281 «Публічне управління та адміністрування». Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, 2026.*

У дисертаційній роботі здійснено теоретичне узагальнення та запропоновано вирішення актуального для науки публічного управління та адміністрування науково-прикладного завдання, яке полягає в обґрунтуванні теоретичних засад і розробленні практичних рекомендацій щодо вдосконалення процесів управління інформаційною безпекою держави в умовах гібридних загроз.

З'ясовано сутність інформаційної безпеки як об'єкту публічного управління. Обґрунтовано, що інформаційна безпека держави являє собою стійкий стан інформаційної сфери, котрий спрямований на сприяння гармонізації процесів розвитку інформаційного суспільства через забезпечення своєї цілісності та захисту об'єктів за наявності зовнішніх і внутрішніх впливів несприятливого характеру як результат усвідомлення соціальними суб'єктами своїх життєво важливих інтересів, цінностей та цілей розвитку.

Охарактеризовано сучасний стан механізмів публічного управління інформаційною безпекою в Україні; оцінено поточні виклики та суперечності публічного управління інформаційною безпекою в Україні в умовах гібридних загроз; проаналізовано досвід зарубіжних країн стосовно управління інформаційною безпекою держави. Відмічено, що організаційно-правовий

механізм кіберзахисту в Україні складається з загальнодержавного, галузевого, регіонального (місцевого), приватного та громадського секторів.

Показано, що серед викликів та загроз для національного кіберпростору України слід акцентувати увагу на наступних: активне застосування кіберзасобів у конкурентних процесах на міжнародному рівні; процеси мілітаризації кіберпростору та розповсюдження кіберзброї в умовах повномасштабного російського вторгнення; реорганізація та трансформація суспільних відносин на рівні дистанційного режиму з масштабним застосуванням інформаційно-комп'ютерних систем й електронних сервісів; безсистемне впровадження нових механізмів, технологій та цифрових сервісів.

Обґрунтовано стратегічні орієнтири захисту єдиного інформаційного простору України в умовах гібридних загроз; виокремлено шляхи модернізації механізмів управління інформаційною безпекою держави; здійснено моделювання ризиків для інформаційно-критичних елементів політичної інфраструктури в умовах гібридних загроз.

Запропоновано комплексний механізм протидії інформаційно-політичним ризикам і загрозам різного типу, котрий складається з політичного, організаційного економічного, правового та соціально-психологічного компонентів, та який передбачає застосування різнохарактерних заходів, здатних протидіяти заподіянню шкоди від розповсюдження негативної інформації або нівелюванню цієї шкоди.

Розроблено нову загальну технологію сценарного моделювання інформаційно-політичного впливу (маніпулювання), що враховує інформаційний чинник у процесі формування та розвитку загрози. Ця технологія є взаємопов'язаною реалізацією наступних модельних блоків: «структура інформаційно-політичної загрози», «політична структура», «визначення інформаційно-критичних елементів політичної структури», «операційно-тимчасова модель інформаційно-політичного впливу», «оцінка поточного стану інформаційно-політичного впливу».

**Ключові слова:** публічне управління, інформаційна безпека держави, механізми, гібридні загрози, державна політика.

## ANNOTATION

***Kushnikov V.V. Managing of the state information security in the face of hybrid threats****. – Qualifying scientific work on the rights of manuscripts.*

*Dissertation for obtaining the scientific degree of Doctor of Philosophy in the field of knowledge «Public management and administration» with specialty 281 «Public management and administration», National Aerospace University "Kharkiv Aviation Institute", Kharkiv, 2026.*

The dissertation work provides a theoretical generalization and proposes for a solution of a scientific and applied task relevant to the science of public management and administration, which consists in substantiating of theoretical foundations and developing practical recommendations for improving of the processes of managing of the state's information security in the face of hybrid threats.

The essence of information security as an object of public administration is clarified. It is substantiated that the information security of the state is a stable condition of the information sphere, which is aimed at promoting of the harmonization of the processes of development of the information society by ensuring its integrity and protecting objects in the presence of external and internal influences of an adverse nature as a result of the awareness by social subjects of vital interests, values, and development goals.

The current state of public information security management mechanisms in Ukraine is characterized; the current challenges and contradictions of public information security management in Ukraine in the context of hybrid threats are assessed; the experience of foreign countries concerning managing of the state's information security is analyzed. It is noted that the organizational-legal mechanism of cyber defense in Ukraine consists of the national, sectoral, regional (local), private and public sectors.

It is shown that among the challenges and threats to the national cyberspace of Ukraine, attention should be focused on the following ones: active use of cyber means in competitive processes at the international level; processes of militarization of cyberspace and proliferation of cyber weapons in conditions of a full-scale Russian invasion; reorganization and transformation of social relations at the level of a remote regime with large-scale use of information and computer systems and electronic services; unsystematic introduction of new mechanisms, technologies and digital services.

The strategic guidelines for protecting of the unified information space of Ukraine in the context of hybrid threats are substantiated; the ways to modernize the mechanisms for managing of the state's information security are identified; risk modeling for information-critical elements of the political infrastructure in the context of hybrid threats is carried out.

A comprehensive mechanism for countering of informational and political risks and threats of various types is proposed, which consists of political, organizational, economic, legal, and socio-psychological components, and which involves the use of various measures capable of counteracting harm from the spread of negative information or leveling this harm.

A new general technology for scenario modeling of informational and political influence (manipulation) is developed, which takes into account the information factor in the process of threat formation and development. This technology is an interconnected implementation of the following model blocks: structure of informational and political threat, political structure, determination of informational and critical elements of political structure, operational-temporal model of informational and political influence, assessment of the current state of informational and political influence.

**Keywords:** public administration, state information security, mechanisms, hybrid threats, state policy.

## СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

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

1. Кушніков В. В. Державна політика у сфері забезпечення інформаційної безпеки в умовах гібридних загроз. *Інвестиції: практика та досвід*. 2026. № 3. С. 416–420.

2. Кушніков В. В. Механізми публічного управління у сфері інформаційної безпеки: роль та специфіка формування. *Інвестиції: практика та досвід*. 2025. № 15. С. 311–314.

3. Кушніков В. В. Методи вибору стратегічних напрямів розвитку державної політики України у сфері забезпечення інформаційної безпеки. *Державне управління: удосконалення та розвиток*. 2025. № 7. URL: https://nayka.com.ua/index.php/dy/article/view/6979/7087.

4. Кушніков В. В., Дєгтяр А. О. Забезпечення інформаційної безпеки держави в умовах гібридних загроз як глобальна проблема. *Державне управління: удосконалення та розвиток*. 2025. № 11. С. 9–20. URL: https://nayka.com.ua/index.php/dy/article/view/8019/8150.

*Особистий внесок автора: виокремлено напрями формування глобальної інформаційної безпеки.*

5. Кушніков В. В., Курило А. Г., Механізми розвитку інформаційних технологій в контексті модернізації політики інформаційної безпеки. Вісн. Нац. ун-ту цивільного захисту України. Серія: Державне управління. 2025. Вип. 2(23). С. 59–63.

*Особистий внесок автора: запропоновано шляхи модернізації політики інформаційної безпеки держави.*

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

1. Кушніков В. Інформаційна безпека суспільства і держави. *Управління розвитком соціально-економічних систем: матеріали X Міжнародної науково-практичної конференції* (м. Харків, 05-06 березня 2026 року). Харків: Державний біотехнологічний університет, 2026. С. 223–225.

2. Кушніков В.В. Специфіка дотримання інформаційної етики в межах державної політики інформаційної безпеки. *ІТ-простір сьогодення: тенденції, інновації та перспективи розвитку : збірник тез доповідей ІІ Міжнародної науково-практичної студентської конференції (м. Харків, 15 жовтня 2025 р.)*. Харків : Харківський національний університет імені В. Н. Каразіна, 2025. С. 79–80.

3. Кушніков В.В. Ефективне публічне управління у сфері інформаційної безпеки як запорука забезпечення громадського здоров'я. *Громадське здоров'я в Україні: проблеми та способи їх вирішення «Томілінські читання» : матеріали VIII науково-практичної конференції з міжнародною участю, Харків, 30 жовтня 2025 р.* / Ред. кол.: О. А. Наконечна, К. Г. Помогайбо, В. Г. Нестеренко та ін. Харків, 2025. С. 193–194.

4. Кушніков В.В. Формування державної політики у сфері інформаційної безпеки: теоретико-методологічний аспект. *Інформаційні технології і автоматизація – 2025 : матеріали XVIII міжнародної науково-практичної конференції (м. Одеса, 30–31 жовтня 2025 року)*. Одеса: Видавництво ОНТУ, 2025. С. 293 – 295.

5. Кушніков В.В. Проблеми та перспективи публічного управління щодо забезпечення інформаційної безпеки під час повномасштабного російського вторгнення та у повоєнний період. *Війна в історичній та індивідуальній пам'яті* : *колективна монографія за матеріалами VIII Міжнародної науково-практичної конференції, присвяченої 81-й річниці Визволення України від гітлерівських загарбників, 11-й річниці Великої Національної війни (гібридної), розв'язаної рашизмом XXI століття проти Незалежності України,*

*державного суверенітету та територіальної цілісності 1 березня 2014р. (м. Кривий Ріг, 28 жовтня 2025 року).* Кривий Ріг, 2025, С. 759–761.

6. Кушніков В.В. Цифровізація у воєнній сфері як об’єкт публічного управління. *Виклики і можливості для агробізнесу: наука, практика та цифрове майбутнє : збірник матеріалів Міжнародної науково-практичної конференції (м. Одеса, 4 листопада 2025 року)*. Одеса: ІКОСГ НААН, 2025. С. 24–26.

**ЗМІСТ**

# ВСТУП

**Актуальність дослідження.** Активізація розвитку інформаційних технологій та формування інформаційного суспільства на їх основі сприяли формуванню принципово нових механізмів, що впливають на процеси суспільно-політичного характеру в державі та регіонах. Основою цих механізмів є застосування інформації в межах глобального інформаційного простору.

На рівні всіх сфер життєдіяльності суспільства чітко простежується наявність принципово нових небезпек і загроз, котрі пов'язані із використанням технологічних засобів нового покоління, та можуть бути представлені у вигляді маніпулювання людською свідомістю, підміни способу життя і цілей нав'язаними стандартами, спотворенням інформації, фальсифікацією віртуальними світами існуючої реальності тощо. Це особливо чітко простежується з початку повномасштабного російського вторгнення в Україну та проявляється у вигляді блокування правдивої інформації та поширення великої кількості недостовірної інформації через соціальні мережі, месенджери тощо.

Систематичне зростання масштабності інформаційних технологій та їх повсюдне використання спричинили суттєву трансформацію системи цінностей, що, своєю чергою, призвело до виникнення глобальної ціннісної кризи в сучасному суспільстві. У подібних умовах цілком очевидно, що домінанта інформаційної безпеки держави в умовах гібридних загроз суттєво зростає. Відповідно, однією з фундаментальних наукових проблем, які вирішуються нині, є розробка теоретико-методичних засад забезпечення інформаційної безпеки особистості, суспільства, держави. Вона передбачає наявність підходів, котрі забезпечують протидію впливам деструктивного характеру в межах глобального інформаційного простору та способи ідентифікації змістовних впливових процесів на масову свідомість й особистість, а також ризики й небезпеки, спричинені негативними наслідками

маніпуляції свідомістю. Виходячи з цього, актуальною є модернізація процесів управління інформаційною безпекою держави в умовах гібридних загроз, що дозволить забезпечити ефективне функціонування та успішний розвиток як інформаційної сфери, так і соціуму в цілому. У цьому зв'язку Кабінетом Міністрів України було введено в дію Розпорядження «Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року» від 30 березня 2023 р. № 272-р.

Загальним науково-практичним засадам публічного управління та адміністрування присвятили свої наукові праці такі вчені, як Е. Афонін, О. Амосов, Л. Антонова, В. Бакуменко, А. Васіна, О. Висоцький, В. Воротін, Б. Гаєвський, В. Горник, О. Гуторова, А. Дєгтяр, С. Домбровська, М. Латинін, І. Лопушинський, В. Князєв, О. Коротич, О. Машков, А. Мельник, О. Марухленко, Н. Нижник, В. Олуйко, К. Пастух, Б. Ребкало, В. Сиченко, О. Смоленський, В. Стрельцов, Ю. Сурмін, Т. Тарасенко, М. Туленков, Ю. Шаров та ін.

Питання, пов'язані з інформаційною безпекою, розглядали у своїх роботах Л. Арсенович, Н. Бєлоусова, В. Бурячок, А. Велігура, Т. Воропаєва, В. Гавриляк, С. Гладиш, В. Горбулін, В. Гурковський, В. Дереко, К. Захаренко, О. Золотар, І. Колодій, М. Кравченко, І. Курас, С. Ленков, Є. Макаренко, Ф. Медвідь, А. Момот, В. Остроухов, В. Петрик, В. Політанський, В. Сідак, В. Хорошко та ін.

Дослідження практики публічного управління у сфері інформаційної безпеки здійснювали Т. Биркович, К. Бєляков, О. Бухтатій, М. Дітковська, О. Довгань, Я. Жарков, І. Жиляєв, М. Каращук, Б. Кормич, О. Корнейко, Є. Котух, О. Кохановська, О. Крюков, В. Куйбіда, А. Рурило, С. Луценко, А. Маращук, О. Нестеренко, М. Ожеван, О. Олійник, С. Петров, Г. Почепцов, О. Семенченко, В. Степанов, В. Торічний, С. Чукут, О. Юдін та ін. Проте питання вдосконалення процесів управління інформаційною безпекою держави в умовах гібридних загроз в сучасних умовах залишаються недостатньо висвітленими.

**Зв'язок роботи з науковими програмами, планами, темами.** Дисертаційну роботу виконано на базі Національного аерокосмічного університету «Харківський авіаційний інститут» відповідно до тематики науково-дослідної роботи «Теоретичні та прикладні проблеми економіки та публічного управління в Україні в умовах воєнного стану та повоєнний період» (ДР № 0124U000577, у межах якої здобувачем запропоновано інноваційні напрями розвитку процесів управління інформаційною безпекою держави в умовах гібридних загроз.

**Мета і завдання дослідження.** *Метою* дисертаційної роботи є наукове обґрунтування теоретичних засад і розроблення практичних рекомендацій щодо вдосконалення процесів управління інформаційною безпекою держави в умовах гібридних загроз.

Поставлена мета передбачила необхідність формулювання та вирішення таких *завдань*:

– з'ясувати сутність інформаційної безпеки як об'єкту публічного управління;

– охарактеризувати сучасний стан організаційно-правового механізму управління інформаційною безпекою України;

– оцінити поточні виклики та суперечності публічного управління інформаційною безпекою в Україні в умовах гібридних загроз;

– проаналізувати досвід зарубіжних країн стосовно управління інформаційною безпекою держави;

– обґрунтувати стратегічні орієнтири захисту єдиного інформаційного простору України в умовах гібридних загроз;

– виокремити шляхи модернізації механізмів управління інформаційною безпекою держави;

– здійснити моделювання ризиків для інформаційно-критичних елементів політичної інфраструктури в умовах гібридних загроз.

*Об'єктом дослідження* є управління захистом інформаційного простору держави.

*Предмет дослідження* – управління інформаційною безпекою держави в умовах гібридних загроз.

**Методи дослідження.** Теоретико-методичною основою дослідження виступають фундаментальні положення теорії публічного управління у сфері інформаційної безпеки. Для вирішення завдань дисертаційної роботи було використано такі методи загального та спеціального наукового пізнання:

– гіпотетико-дедуктивний – для уточнення сутності предмета дослідження;

– узагальнюючий і порівняльний – для оцінки діючих механізмів управління інформаційною безпекою в умовах гібридних загроз в Україні та зарубіжних країнах;

– суб'єктно-об'єктний – для розробки комплексного механізму протидії інформаційно-політичним ризикам і загрозам;

– метод рефлексивного управління – для виокремлення стратегічних орієнтирів захисту єдиного інформаційного простору України в умовах гібридних загроз;

– структурно-функціональний підхід – для сценарного моделювання інформаційно-політичного впливу;

– експертне опитування та багатовимірний аналіз – для оцінки значимості інформаційно-критичних елементів у конкретному варіанті політичної структури;

– ризикоорієнтований підхід – для моделювання ризиків для інформаційно-критичних елементів політичної інфраструктури в умовах гібридних загроз.

Інформаційно-аналітичною основою дисертаційної роботи є законодавчі та підзаконні акти України, які регулюють питання, пов'язані з інформаційною безпекою держави, наукові здобутки вітчизняних і закордонних дослідників, статистичні дані органів державної влади та місцевого самоврядування, власні авторські напрацювання.

**Наукова новизна одержаних результатів** полягає в теоретичному обґрунтуванні та наданні практичних пропозицій з удосконалення процесів управління інформаційною безпекою держави в умовах гібридних загроз. Основними науково-теоретичними та практичними результатами дослідження, що зумовлюють його новизну, є такі:

*вперше:*

– побудовано комплексний механізм протидії інформаційно-політичним ризикам і загрозам негативістського й компліментарного характеру, котрий складається з політичного, організаційного, економічного, правового та соціально-психологічного компонентів із вбудованими алгоритмами моніторингу та адаптації, та який передбачає вирішення проблем технічного, організаційного й правового характеру через формування спеціальних інформаційних контурів у діючих інформаційно-критичних елементах політичної структури, націлених на виявлення інформаційних загроз;

*удосконалено:*

– методичний підхід до запобігання явищ інформаційного тероризму в межах інституційної, нормативної, комунікативної, культурно-ідеологічної та функціональної підсистем політичної системи через інформаційно-психологічний вплив на окремі особистості, громадські й соціальні групи та на все населення загалом з метою збереження цілісності організаційних, технічних й інформаційних зв'язків цієї системи;

– теоретичний підхід до модернізації державної політики у сфері інформаційної безпеки через виокремлення в ній нормативно-правової, організаційної, технологічної та кадрової складових, що уможливлює своєчасне виявлення інформаційних загроз безпеці особистості, суспільства і держави та протидію ним, а також реалізацію стратегічних інтересів держави у складному конкурентному інформаційному просторі сьогодення на основі загальновизнаних принципів та норм міжнародного права щодо забезпечення інформаційної безпеки;

– практичний підхід до сценарного моделювання інформаційно-політичного впливу, котрий передбачає взаємопов’язану реалізацію наступних модельних блоків: «структура інформаційно-політичної загрози», «політична структура», «визначення інформаційно-критичних елементів політичної структури», «операційно-тимчасова модель інформаційно-політичного впливу», «оцінка поточного стану інформаційно-політичного впливу», котрий враховує інформаційний фактор у процесі формування й розвитку загрози, та дозволяє визначити основні інформаційно-критичні елементи політичної системи з урахуванням інформаційно-ресурсного потенціалу;

*дістали подальшого розвитку:*

– зміст напрямів створення державної системи реагування на інформаційно-психологічні контентні загрози, яка забезпечує інформаційну та роз'яснювальну роботу органів державної влади та місцевого самоврядування щодо культури інформаційної безпеки та поєднує в собі єдиний реєстр ресурсів, котрі містять протиправну інформацію; систему аналітики інформації на наявність протиправного контенту; програму з використанням контентної фільтрації, та яка уможливлює блокування протиправного контенту;

– стратегічні орієнтири захисту єдиного інформаційного простору України в умовах гібридних загроз, котрі базуються на прогнозуванні, виявленні та оцінці джерел і характеру інформаційно-політичних загроз, основних суб'єктів інформаційно-політичного впливу та інформаційно-критичних елементів політичної системи, що в сукупності забезпечує захист інформаційної інфраструктури України в цілому й інформаційної інфраструктури політичної системи зокрема від негативних інформаційних впливів;

– змістовно-категорійний апарат науки «Публічне управління та адміністрування» через уточнення сутнісної характеристики таких понять: «*інформаційна безпека держави*» в якості стійкого стану інформаційної

сфери, котрий спрямований на сприяння гармонізації процесів розвитку інформаційного суспільства через забезпечення своєї цілісності та захисту об'єктів за наявності зовнішніх і внутрішніх впливів несприятливого характеру як результат усвідомлення соціальними суб'єктами своїх життєво важливих інтересів, цінностей та цілей розвитку; «*інформаційно-критично важливий елемент політичної структури*» як акт маніпуляційного інформаційного впливу, щодо якого порушено (чи припинено) функціонування інформаційної складової, що, своєю чергою, може призвести до втрати керованості в масштабах країни або окремої частини її території, а також до важких дисфункцій в інфраструктурі та економіці на тривалий період.

**Практичне значення одержаних результатів** полягає в обґрунтуванні та розробці пропозицій, орієнтованих на вдосконалення процесів управління інформаційною безпекою держави в умовах гібридних загроз. З наукових праць, опублікованих у співавторстві, використано лише ті положення, які є результатом особистої роботи здобувача, що полягає у дослідженні комплексу питань, пов’язаних з удосконаленням механізмів розвитку інформаційних технологій в контексті модернізації політики інформаційної безпеки.

Розробки, представлені в дисертаційному дослідженні, знайшли практичне застосування в діяльності Департаменту культури і туризму обласного комунального закладу «Харківський організаційно-методичний центр туризму» Харківської обласної військової адміністрації в контексті підвищення результативності функціонування державної системи реагування на інформаційно-психологічні контентні загрози (довідка про впровадження № 26/15 від 21.04.2026 р.), у Національному агентстві акредитації України Міністерства економіки, довкілля та сільського господарства України щодо впровадження теоретичного підходу до модернізації державної політики у сфері інформаційної безпеки (довідка про впровадження № 20-06К від 20.05.2026 р.), а також у Директораті європейської та євроатлантичної інтеграції Міністерства освіти і науки України (довідка про впровадження № 2/43-26 від 22.05.2026 р.) щодо формування державної політики у сфері інформаційної безпеки.

**Особистий внесок здобувача.** Дисертаційна робота є самостійно виконаним науковим дослідженням. Наукові розробки, висновки та пропозиції, що містяться в дисертації, належать особисто автору. З наукових праць, опублікованих у співавторстві, використано лише ті положення, які є результатом особистої роботи здобувача, що полягає у дослідженні комплексу питань, пов'язаних з вдосконаленням процесів управління інформаційною безпекою держави в умовах гібридних загроз.

**Апробація результатів дослідження.** Ключові положення дисертаційної роботи було оприлюднено та обговорено на: XVIII міжнародній науково-практичній конференції «Інформаційні технології та автоматизація – 2025» (м. Одеса, 30–31 жовтня 2025 року), II Міжнародній науково-практичній студентській конференції «IT-простір сьогодення: тенденції, інновації та перспективи розвитку» (м. Харків, 15 жовтня 2025 року), VIII науково-практичній конференції з міжнародною участю «Громадське здоров'я в Україні: проблеми та способи їх вирішення» (м. Харків, 30 жовтня 2025 року), Міжнародній науково-практичній конференції «Виклики і можливості для агробізнесу: наука, практика та цифрове майбутнє» (м. Одеса, 4 листопада 2025 року), VIII Міжнародній науково-практичній конференції «Війна в історичній та індивідуальній пам'яті» (м. Кривий Ріг, 28 жовтня 2025 року) та X Міжнародній науково-практичній конференції «Управління розвитком соціально-економічних систем» (м. Харків, 0506 березня 2026 року).

**Публікації.** Основні наукові положення та здобутки дисертаційного дослідження викладено у 11 публікаціях, із них 5 статті – у фахових журналах і збірниках наукових праць; 6 – тези доповідей на конференціях. Загальний обсяг публікацій становить 3,8 авт. арк.

**Структура та обсяг дисертації.** Дисертаційна робота складається зі вступу, трьох розділів, що містять 9 підрозділів, висновків до кожного розділу, загальних висновків, списку використаних джерел і додатків. Дисертацію викладено на 243 сторінках, із них 209 сторінок основного тексту. Робота містить 23 рисунки, 2 таблиці і 3 додатки (на 4 сторінках). Список використаних джерел налічує 272 найменування (на 30 сторінках).

# РОЗДІЛ 1
# ТЕОРЕТИЧНІ ЗАСАДИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

## 1.1. Інформаційна безпека як об’єкт публічного управління

Поряд із зростанням ролі інформації та її затребуваності в нашому житті, роздержавленням суспільного та приватного життя та формуванням громадянського суспільства відбувається одночасне переосмислення поняття «інформація», її основних видів та властивостей, а також відносин, пов’язаних з нею.

У гносеологічному вимірі пізнання об'єкта як системи, тобто в нерозривній єдності його цілісності та внутрішньої диференційованості, неминуче передбачає виокремлення складових частин і характеру зв'язків між ними. Розкрити структуру об'єкта — означає встановити його елементи та способи, у які вони вступають між собою у взаємодію. Зважаючи на те, що структура може описуватися «кількома відносинами», її визначення потребує цілеспрямованого відбору певних відносин із сукупності внутрішніх зв'язків між частинами об'єкта, а також із зовнішніх відносин, у які він вступає. Відповідь на це питання, як і обґрунтування засад будь-якого «вибору» у природі чи суспільстві, може дати лише дослідження генезису та еволюції об'єктів відповідного типу. Саме тому у цьому контексті доцільно звернутися до короткого історичного огляду проблеми та виокремити для з'ясування сутності інформації та її структури певні відносини й пов'язані з ними методологічні питання, зокрема щодо співвідношення інформації з матерією та знанням. У сучасній науці матерія тлумачиться як «об'єктивна реальність, що існує поза і незалежно від людської свідомості та відображається нею» [28, с. 52]. Матерії притаманні субстанціональність (вона охоплює нескінченну множину реально існуючих об'єктів і систем світу та є субстанціональною основою всіх властивостей і форм руху), загальність (існує лише у своїй

незліченній різноманітності) та абсолютність (є незнищенною, вічною у часі й нескінченною у просторі, нерозривно пов'язаною з рухом і здатною до невпинного саморозвитку), що в сукупності відображає матеріальну єдність світу. Свідомість постає як найвища форма відображення матеріального та є атрибутивною властивістю матерії. Серед невичерпного різноманіття властивостей матерії сучасна наука особливо вирізняє упорядковану системну організацію, що виявляється в таких основних формах існування матерії:

– системи неживої природи (елементарні частинки та поля, атоми, молекули, макроскопічні тіла, космічні системи);

– біологічні системи (біосфера — від мікроорганізмів до людини);

– соціальні системи (суспільство) [28, с. 25]

Визначальна роль інформації у становленні та розгортанні нових форм руху й інформаційних структур, а також єдність і взаємообумовленість внутрішньої та зовнішньої інформації найбільш виразно виявилися на двох переломних етапах еволюції матерії — переході від неживої природи до живої та від вищих тварин до людини й людського суспільства. Формування розгалуженої мережі якісно нових взаємозв'язків і взаємодій стало підґрунтям для виникнення принципово відмінної системи організації — соціальної, уособленням якої є людське суспільство.

Внутрішня інформація являє собою інформацію як характеристику організованості будь-якої системи [58, с. 36]; те, що Аристотель позначав поняттям «ентелехія», сучасні дослідники визначають як міру організації системи та позначають терміном «структурна інформація» [2, с. 32]. Структурна (або зв'язана) інформація є невід'ємною властивістю всіх об'єктів живої та неживої природи як природного, так і штучного походження; вона формується внаслідок відбору, фіксації та закріплення в системі позитивного досвіду її взаємодії із зовнішнім середовищем у вигляді певних структурних перетворень. Зазначена інформація характеризується відносною об'єктною самостійністю. Показовим прикладом цього слугує досвід із квітковим годинником, сконструйованим видатним біологом Карлом Ліннеєм на основі

закономірного почергового розпускання та змикання квіток різних рослин упродовж світлового дня — від шостої години ранку до шостої години вечора. Передумовою для цього стали дослідження французького астронома Жан-Жака Дорту де Мерана, проведені понад 250 років тому: помістивши квітку геліотропа в затемнену кімнату, вчений встановив, що цикл її розкривання та змикання точно відтворював зміну дня і ночі. На підставі цього він дійшов висновку про існування в рослині певного внутрішнього механізму регуляції біологічних ритмів.За дослідженнями вчених для людського організму властиві понад 100 циркадних ритмів, скоординованих із циклом сон-неспання (наприклад, зміна температури тіла протягом кожної доби на 0,6 градусів, у тому числі зниження до мінімуму вночі – між 2 та 5 годинами); інфрадіанні ритми (наприклад, 28-денний жіночий репродуктивний цикл). Порушення цих внутрішніх ритмів може призвести до психічних розладів.

Категорія зовнішньої інформації розкривається через її роль як організуючого начала системи [50, с. 25]. Аристотелівський «кінесис» [2, с. 23] знаходить своє відображення в сучасних наукових поняттях «відносної» та «оперативної (робочої)» інформації, що нерозривно пов'язані з принципом відображення: об'єкт А, зазнавши структурних змін під впливом об'єкта В, перетворюється на носія відомостей про нього [58; 63]. Сонячні та місячні цикли активності наочно демонструють, яким чином подібна інформація впливає на функціонування біологічних систем. Дослідження електромагнітної сигналізації у тваринному світі дозволило виокремити чотири її різновиди [58, с. 34-35]:

– командні сигнали, що забезпечують злагодженість переміщення у птахів, риб, ссавців та комах, які рухаються групами;

– орієнтаційні сигнали, що уможливлюють виявлення особин одного виду на великих просторових дистанціях;

– координаційні сигнали, що регулюють узгодженість фізіологічних і поведінкових процесів у межах угруповань;

– синхронізаційні сигнали, що забезпечують часову узгодженість процесів як на рівні окремого організму, так і на рівні групової взаємодії.

У системах неживої природи зовнішня інформація присутня в латентній формі та тісніше пов'язана з кібернетичними системами, де вона циркулює між об'єктами матеріального світу й задіяна в процесах управління живою природою, технічними системами та людським суспільством. Безпосередній зв'язок інформації з відображенням як універсальною властивістю матерії зумовлює необхідність врахування двох принципово відмінних типів відбиття, що реалізуються на різних рівнях організації матерії, зокрема фізичному, хімічному, біологічному, соціальному та інших, а саме прямого й опосередкованого.

Прямий тип охоплює всі різновиди контактного відбиття, тобто зміни положення, будови, форми, контуру, розміру, швидкості або інтенсивності впливу відбиваючого об'єкта як наслідок його безпосередньої взаємодії з об'єктом відображення. Принциповою особливістю контактного відображення є одночасне виникнення двох взаємних відбитків, коли взаємодіючі об'єкти фіксують сліди одне одного.

За опосередкованого типу взаємодія об'єктів відбувається через проміжне середовище, яким можуть слугувати світлові, звукові хвилі тощо, що виступає водночас і посередником, і носієм відображення. У цьому середовищі формується подібність або ізоморфна відповідність відображуваному об'єкту, прикладом чого може слугувати відповідність між формою предмета та просторовою організацією відбитих від нього світлових променів.

У біологічних та соціальних системах розрізняють три форми інформації, що відповідають трьом фізичним сутностям кібернетичних систем [50]:

– біологічна – усередині живих організмів та між ними (у тому числі генетична, зоопсихологічна);

– машинна –усередині та між машинами;

– соціальна – у людських спільнотах.

При всій якісній різниці у змісті та формах подання зазначені види інформаційних процесів ізоморфні у структурному відношенні, що є об’єктивною передумовою створення штучних інформаційних систем, котрі реалізують функції пам’яті, зворотного зв’язку, імітації реальних фізичних, біологічних, соціальних та інших різних за своєю природою процесів та явищ.

Інформаційна диференціація суспільства є закономірним наслідком того, що зростаючі обсяги накопичених відомостей дедалі активніше залучаються до всіх галузей людської діяльності. Соціальна, науково-технічна, технологічна та статистична інформація перетворилися на ресурс, без якого неможливе створення штучного предметного світу — від виробничих знарядь і побутових речей до наукових відкриттів і мистецьких творів. Саме цей процес лежить в основі становлення ноосфери [239, с. 1155]. Кібернетика як наукова дисципліна вперше надала інформації статусу самостійної категорії, довівши її визначальну роль у процесах пізнання та управління. Будь-яка система, що прагне зберегти стійкість в умовах змінного середовища, змушена постійно збирати й опрацьовувати сигнали ззовні та відстежувати власний внутрішній стан. Результатом цієї діяльності стає формування динамічної інформаційної моделі, яка дозволяє системі адекватно реагувати на нові обставини. Саме тому збирання, накопичення, перетворення та розповсюдження інформації становлять фундаментальну основу управлінських і пізнавальних процесів незалежно від того, чи відбуваються вони в живому організмі, технічному пристрої або в суспільстві загалом, оскільки без цих процесів вироблення ефективних керуючих впливів на керовану систему є принципово неможливим.

Принципова особливість кібернетичного підходу полягає в тому, що всі взаємодії системи із середовищем та між системами розглядаються виключно крізь призму інформаційного обміну, тоді як інші наукові дисципліни аналізують ті самі процеси в іншому аспектуальному вимірі. Це зумовлює специфіку кібернетичного трактування управління: воно визначається через

інформацію як переведення системи в один із потенційно досяжних для неї станів, що здійснюється або самою системою, або зовнішньою системою внаслідок отримання й передачі відповідних сигналів. Ключовим орієнтиром управлінської діяльності з позицій кібернетики вважається збереження та примноження інформації, що надходить до системи, що рівнозначне підтриманню або підвищенню рівня її внутрішньої організованості.

У біологічних та соціальних системах зовнішня інформація використовується для управління та пізнання. Тому в інформаційній структурі розрізняють два контури зворотного зв'язку. У першому контурі циркулює інформація, яка виникає як результат відхилення параметрів системи від заданих під впливом середовища (система управління) або як результат прояву властивостей об'єкта, що досліджується під впливом сигналів суб'єкта пізнання (система пізнання). У другому контурі в результаті семантичної фільтрації інформаційних потоків першого контуру відбувається відбір і накопичення корисної з погляду цільової функції інформації, перетворення її на внутрішню (структурну) і тим самим формування процесу саморозвитку системи на структурному рівні [115]. Здатність до навчання, адаптації та прогнозування майбутніх станів середовища через випереджувальне відображення дійсності є якісно новими властивостями, що виникають у розвинених системах управління і суттєво зміцнюють їхній потенціал виживання та стійкого функціонування. Пізнавальна діяльність уможливлює виявлення закономірностей досліджуваного об'єкта, висування гіпотез, доведення теоретичних положень і побудову цілісних наукових теорій. Поряд з цим, безумовний інтерес представляє і така властивість інформації, як здатність до обмеження в системах, де вона виступає засобом організації, при цьому, чим вищий рівень організованості, тим вищий рівень обмежень. Поняття обмеження дозволяє краще виявити, що існують якісь глибокі зв'язки фундаментальних принципів теорії інформації з поняттями і принципами класичної механіки і взагалі фізики; зв'язки, що не зводяться до формальної подібності математичних виразів.

Таким чином, інформація виконує роль міри організованості та інструменту організації й розвитку будь-якої форми матерії, що дає підстави для висновку про інформаційну природу всієї матерії. Водночас те, що інформація реалізується виключно через матеріальні об'єкти та їхні властивості, свідчить про матеріальний характер будь-якої інформації. Щодо методологічного питання про первинність матерії або інформації, то обидва начала правомірно розглядати як двоєдину першооснову існуючої природи і світу загалом.

Залежно від критерію розрізняють такі види інформації [58; 68]:

– за рівнем розумово-діяльної переробки – синтаксична, семантична, прагматична;

– за модульністю (спрямованістю) повідомлення – у образній сфері, в емоційній сфері, у понятійній сфері;

– за формою фіксації інформації (спосіб сприйняття та переробки інформації) – піктографічна (фотографія, технічний малюнок, креслення, схема, піктограма), ідеографічна (графік, гістограма, діаграма, таблиця, формула, номограма), текстова.

Структура семантичної інформації охоплює три складові: знак, що поділяється на універсальний, акцидентальний і конвенційний різновиди; значення, яке диференціюється на екстенсіональне та інтенсіональне; а також зміст.

Як предмет наукового вивчення інформація потребує аналізу в семантичному, лінгвістичному, прагматичному та технічному вимірах [68, с. 85].

Семантичний вимір зосереджений навколо проблеми точності відтворення змісту повідомлень засобами кодованих сигналів. У кібернетичній системі такий підхід отримав назву інформаційного: він пов'язаний із реалізацією в системі комплексу процесів відображення як зовнішнього середовища, так і внутрішнього стану самої системи через збирання, накопичення та опрацювання відповідних сигналів [68, с. 86].

Лінгвістичний аналіз інформації орієнтований на виявлення знакової системи, необхідної для забезпечення ефективного сприйняття та розуміння інформації в процесі її обміну між системами. У соціальних системах алфавітні та цифрові засоби слугують інструментом вираження смислового навантаження інформації, її фіксації та подальшого логічного застосування. Саме на їхній основі конструюються слова, словосполучення, речення та зв'язні тексти, що забезпечує логічне оформлення відомостей у формі, придатній для сприйняття. Поряд із документованою інформацією існують інші організаційні форми її вираження, зокрема звукова, світлова та біоенергетична, однак логічна система людського мислення наразі опрацьовує їх через письмову знакову систему, оскільки й звуково-мовна форма комунікації ґрунтується на алфавітно-цифровому способі представлення інформації.

Прагматичний вимір дослідження зосереджений на оцінюванні споживчої цінності отриманого повідомлення крізь призму його впливу на подальшу поведінку реципієнта. Цей підхід прийнято називати управлінським, оскільки він охоплює процеси функціонування системи, вектори її руху під дією отриманої інформації та ступінь досягнення нею визначених цілей [68, с. 85].

Технічний вимір охоплює дослідження проблем точності, надійності та швидкості передачі повідомлень, а також питання побудови каналів передачі сигналів, їхнього захисту від перешкод та вдосконалення відповідних технічних засобів і методів [63, с. 25].

Наведене засвідчує багатозначність категорії інформації, а розмаїття її тлумачень відображає надзвичайну складність реального світу, що суттєво ускладнює формування дієвої стратегії забезпечення інформаційної безпеки. З огляду на це, обґрунтованим видається таке трактування поняття інформації, яке інтегрувало б як її внутрішню, так і зовнішню складові з урахуванням усієї сукупності сутнісних ознак і характеристик.

З проведеного аналізу можна назвати такі основні ознаки інформації.

1. Системність інформації – це властивість інформації відображати об'єкти, процеси та явища не ізольовано, а у взаємозв'язку й взаємозалежності між собою, тобто як цілісну структуровану сукупність елементів, де кожен компонент займає визначене місце, виконує конкретну функцію та впливає на загальний стан системи, завдяки чому інформація набуває не лише описового, а й пояснювального та прогностичного характеру, дозволяючи суб'єкту управління або дослідження сприймати реальність як організоване ціле, виявляти закономірності, встановлювати причинно-наслідкові зв'язки та приймати обґрунтовані рішення.

2. Селективність інформації як принцип вибору корелює в теоретичному відношенні з категорією невизначеності. Акти вибору, що в своїй сукупності утворюють процеси селекції, необхідні для конструювання слів і висловлювань, усувають певну частку невизначеності в наперед існуючій або умовно заданій множині елементів, груп елементів чи відносин, виокремлюючи й формуючи в ній утворення з певними, зокрема лінгвістичними, структурами. Якщо елементарну одиницю інформації та одиницю процесу її виникнення звести до акту вибору з певної множини наявних можливостей, то елементом уже накопиченої інформації виступатиме результат відповідних актів, адже поодинокий акт вибору сам по собі не породжує цілісного образу. Поняття вибору або відбору є внутрішнім для теорії інформації та її практичних застосувань також у тому розумінні, що воно використовується при аналізі самої інформації та процесів її накопичення й опрацювання. У біологічних дослідженнях, що спираються на інформаційний підхід, особливо в галузі теорії еволюції, концепція відбору посідає центральне місце. У контексті вивчення різноманітних процесів опрацювання інформації в психічній діяльності поняття активного вибору інформації суб'єктом набуло вагомого методологічного значення.

Становлення інформаційного суспільства постає як органічний результат еволюційного поступу сучасного соціуму, визначальними рисами якого є повсюдне поширення інформаційних технологій і розбудова

глобального інформаційного простору. Усвідомлення інформаційної специфіки цього нового типу суспільного устрою та цілеспрямоване розкриття закладеного в ньому потенціалу є необхідною умовою успішного завершення трансформаційних процесів, спричинених технологічними зрушеннями.

Питання протидії новим видам небезпек і загроз, що набули актуальності на початку третього тисячоліття, перебуває в центрі уваги дослідників сучасного суспільства, а кількість наукових праць із проблематики інформаційної безпеки невпинно зростає [104; 123; 206]. Попри значний масив напрацювань у цій галузі, більшість авторів одностайні в тому, що сформулювати вичерпне визначення інформаційної безпеки надзвичайно складно [109; 213; 215]. Пошук дефініції, здатної чітко й точно відобразити зміст цього феномена, триває, оскільки з'ясування сутності інформаційної безпеки є завданням, що має водночас і теоретичну, і практичну значущість.

Кожне явище, об’єкт чи процес має внутрішній зміст і відповідний йому зовнішній вираз. Поєднання двох зазначених складових дозволяє отримати повне уявлення про предмет дослідження та напрямки використання його результатів.

Перш ніж приступити до дослідження поняття «інформаційна безпека», спочатку цілком логічно визначити, що є безпекою. Епікур бачив безпеку в гармонії людини та природи. Л. Валла пов’язував її з поняттям миру та дружби. Т. Гоббс розумів безпеку у двох чеснотах: вірі та законах. Дж. Локк говорив, що для безпеки необхідна розробка дослідно-практичного та теоретичного знання [29].

Еволюція суспільства змінювала уявлення про безпеку, відповідно, різні філософські напрями у вигляді власних гносеологічних оцінок знання про безпеку наповнювали специфічним змістом.

У сучасній науковій літературі категорія «безпека» отримує кілька інтерпретацій. В одному трактуванні вона постає як сукупність умов і чинників, за яких об'єкт повноцінно функціонує та розвивається відповідно до своїх внутрішніх закономірностей. В іншому підході безпека розуміється як

такий стан об'єкта, за якого відсутні умови та чинники, що становлять загрозу існуванню індивіда чи спільноти. Поширеним є також розуміння безпеки як здатності об'єкта утримувати свої системоутворювальні властивості під впливом деструктивних чинників, що намагаються дезорганізувати його ключові параметри та характеристики, втрата яких рівнозначна втраті самої сутності об'єкта. Крім того, під цим поняттям також мається на увазі система гарантій, що забезпечує нормальний розвиток будь-якого явища [29; 64; 65; 101].

Показово, що переважна більшість наведених визначень зазнає критики як з боку науковців, так і з боку практиків. Головна вада багатьох із них полягає в тому, що при конкретизації поняття «безпека» поза увагою залишається її діалектична протилежність у вигляді небезпеки, без урахування якої розкрити зміст цього терміна повною мірою неможливо. Безпека набуває свого справжнього смислу лише у співвідношенні з небезпекою, будучи похідною від неї категорією. Небезпека, своєю чергою, характеризує такий стан об'єкта, за якого внутрішні або зовнішні деструктивні впливи порушують механізми життєзабезпечення системи, породжуючи загрозу нормальному режиму її функціонування. При цьому варто підкреслити, що не кожна загроза дисфункції заслуговує кваліфікації як небезпека: уваги потребує лише та, що зазіхає на функціональну цілісність системи, адже безпека реалізується саме як подолання небезпеки.

Однак система безпеки, заснована на підході, який враховує стан небезпеки, втрачає сенс, оскільки налаштована не стільки на подолання небезпеки, скільки на виправдання існування власне соціальної системи. Деякі автори навіть констатують, що в даний час не розроблено теоретичне обґрунтування предметної галузі, яка здатна визначати сферу безпеки [29; 64; 101; 127]. Розуміння безпеки під кутом «життєво важливих інтересів особистості, суспільства та держави» містить у собі внутрішню смислову суперечність і є недостатньо коректним у науковому відношенні.

Інші автори зазначають, що інтереси, важливість яких не викликає сумнівів, необхідно формулювати та реалізовувати, забезпечуючи ті чи інші потреби особистості, суспільства та держави у вигляді цілеспрямованої соціально-політичної діяльності [15; 22; 106]. Йдеться не про захист інтересів людей як таких, а про захист базових умов існування людей, держави та суспільства в цілому, закріплених у системі цінностей та життєвих засад. Внаслідок цього сфера безпеки має бути представлена як соціальний простір, що охоплює основи суспільного буття та базові цінності людини.

Узагальнюючи викладене, безпеку правомірно визначати як здатність системи не лише протистояти зовнішнім і внутрішнім небезпекам, а й переходити у своєму розвитку на якісно вищий рівень організації. Підтримання безпечного стану є необхідною передумовою нормального функціонування та поступального розвитку системи. У ширшому контексті безпека постає водночас як базова характеристика життєзабезпечення будь-якого об'єкта і як його іманентна здатність реагувати на деформацію власних цінностей, цілей та інтересів, що становлять підвалини існування цієї системи.

Розкривши змістовне наповнення категорії «безпека», логічним видається звернення до аналізу поняття «інформаційна безпека». Останнє є унікальним феноменом сучасного суспільства, становлення якого має загальноцивілізаційне значення для всього людства, що робить формулювання його об'єктивного й практично орієнтованого визначення нагальною науковою потребою [56, с. 56].

Складність висвітлення проблеми інформаційної безпеки до сьогодні, як зазначають фахівці, пов’язана з відсутністю загальноприйнятого тлумачення термінів, що описують предметну область [53; 74; 221]. Поряд із терміном «інформаційна безпека» активно використовується термін «безпека інформації». Не викликає сумнівів, що дані поняття взаємопов’язані. При цьому дуже важливо внести уточнення, що безпека сама по собі не існує. Зміст поняття «безпека» визначає вибір об’єкта. У разі, якщо об’єктом захисту виступає сама інформація, поняття «безпека інформації» і «інформаційна

безпека» стають синонімами. У той же час, якщо в якості об’єкту захисту розглядається інший об’єкт чи суб’єкт як учасник інформаційної взаємодії, тоді в терміні «інформаційна безпека» слово «інформаційна» уточнює напрямок діяльності, відповідно, поняття «інформаційна безпека» слід трактувати як стан захищеності зазначеного об’єкта (суб’єкта) від загроз різного характеру в інформаційній сфері [71, с. 245].

Окремі дослідники проводять чітку демаркаційну лінію між поняттями «інформаційна безпека» та «безпека інформації», наголошуючи на їхній змістовній відмінності. Зокрема, безпека інформації тлумачиться як захищеність інформації від деструктивних впливів, що можуть виявлятися у порушенні її фізичної або логічної цілісності через знищення чи спотворення, а також у несанкціонованому доступі до неї та її використанні [74, с. 10].

Інформаційна безпека є справді складним феноменом, концептуальне осмислення якого ускладнюється низкою об'єктивних обставин. Серед них доцільно виокремити найбільш суттєві.

1. Інформаційна безпека постає як об'єктивне явище, породжене умовами суспільного розвитку. Її становлення відбувається в нерозривному зв'язку з процесом інформатизації суспільства, який сам перебуває на стадії активного формування і потребує подальшого поглибленого дослідження. Додаткову складність привносить те, що специфіка інформаційної безпеки зумовлена передусім реформуванням системи національної безпеки держави загалом. Сукупна дія зазначених чинників унеможливлює вироблення повноцінного й вичерпного визначення досліджуваної категорії.

2. Труднощі у визначенні поняття «інформаційна безпека» пов'язані також із тим, що цей феномен досліджується в різних наукових площинах: технічній, правовій, психологічній, соціальній та інших. Представники кожної з цих галузей наповнюють поняття «інформаційна безпека» власним предметним змістом, додатково акцентуючи таким чином її багатовимірну природу, що суттєво ускладнює вироблення єдиного універсального визначення. Наслідком цього є переважно спеціалізований характер наявних

досліджень, кожне з яких висвітлює інформаційну безпеку крізь призму конкретної наукової дисципліни.

Окресливши основні перешкоди, з якими стикаються дослідники в процесі з'ясування сутності інформаційної безпеки, доцільно звернутися до характеристики ключових підходів до визначення цього поняття. Наявні в науковій літературі підходи до тлумачення категорії «інформаційна безпека» допускають умовний поділ на два напрями – технологічний і гуманітарний, загальна характеристика яких потребує окремого розгляду.

Зокрема, технологічний підхід до визначення інформаційної безпеки, розглядає це поняття з погляду розвитку індустрії інформатизації, забезпечення безпеки інформаційно-телекомунікаційних систем, забезпечення потреб національного ринку інформаційно-технологічною продукцією та виходом її на світовий ринок.

Так, деякі автори вважають, що інформаційна безпека може бути визначена як неможливість завдання шкоди властивостям об’єкта безпеки, що обумовлюються інформацією та інформаційною інфраструктурою; у вузькому сенсі інформаційна безпека передбачає [63]:

– захист інформації від внесення до неї змін неуповноваженими особами;

– збереження цінних даних;

– надійність роботи комп’ютера;

– збереження таємниці листування в електронному зв’язку.

У контексті вирішення проблем комп’ютерного тероризму інформаційну безпеку можна представити в якості сукупності заходів, методів, механізмів, й інструментальних засобів, що дозволяють виявити і запобігти шляхом оперативного реагування на дії, здатні привезти до:

– несанкціонованого доступу до інформації, що охороняється законом;

– руйнування інфраструктури мережі у вигляді виведення з ладу системи управління нею чи її елементів.

Інформаційна безпека піддається також інтерпретації як комплекс засобів, методів і заходів, спрямованих на унеможливлення розголошення, витоку та несанкціонованого доступу до інформації. У межах цього підходу найбільш лаконічне тлумачення зводить безпеку до забезпечення надійного захисту від впливів як природного, так і штучного походження.

Наведені вище визначення в рамках технологічного підходу яскраво демонструють пріоритетний об’єкт захисту інформаційної безпеки: основна увага сконцентрована виключно на проблемі захисту інформації та інформаційній інфраструктурі. При цьому під інформаційною інфраструктурою передбачається сукупність організаційних структур, технічних засобів, апаратного та програмного забезпечення, призначених для зберігання інформації з метою її подальшої обробки та передачі [38]. Подібний підхід цілком зрозумілий, він визначає одну із сутнісних сторін інформаційної безпеки. З технологічного погляду інформація є «продуктом» інформаційних технологій, відповідно, потребує захисту.

Підхід, що визначає інформацію та підтримувальну її інфраструктуру пріоритетним об'єктом захисту, має однобічний характер, адже залишає поза увагою інші не менш важливі складові інформаційної безпеки. Зокрема, він не враховує суб'єктів інформаційних відносин, серед яких особистість, суспільство і держава, а також інформаційне середовище, що охоплює суспільство, системи формування, поширення та використання інформації. Крім того, соціально-психологічні та соціально-політичні виміри інформаційної безпеки в межах цього підходу фактично не отримують належного концептуального осмислення. Попри зазначені обмеження, він зберігає домінуюче становище серед інших наявних підходів. Технологічна складова інформаційної безпеки розроблена значно ґрунтовніше, тоді як гуманітарний вимір цієї сфери залишається істотно менш дослідженим.

Прихильники гуманітарного підходу до вивчення проблематики інформаційної безпеки обстоюють позицію, згідно з якою цей феномен є соціальним явищем переважно гуманітарно-технічного характеру [186; 205].

У рамках цього напряму ряд авторів обґрунтовує двоїсту природу інформації: з одного боку, інформація існує об'єктивно-фізично, і саме в цьому вимірі її досліджують фізика, математика та технічні дисципліни; з іншого, вона має суб'єктивний вимір, що робить її предметом психологічних, біологічних, філософських і соціально-гуманітарних наук. При цьому природничо-технічний аспект інформаційних процесів розглядається як підпорядкований, тоді як магістральний напрям досліджень зосереджений у площині соціально-політичного та гуманітарного аналізу. Відтак чимало дослідників акцентують міждисциплінарний характер інформаційної безпеки і наголошують на необхідності її комплексного розроблення [53; 221].

Гуманітарний підхід осмислює інформаційну безпеку крізь призму завдань духовного оновлення суспільства та дотримання конституційних прав і свобод громадян у сфері інформаційної діяльності. Коло ключових питань, що охоплюються зазначеним підходом, унаочнено на рисунку 1.1.

Розглядаючи інформаційну безпеку як вимір усіх видів суспільної діяльності, в яких індустрія інформатики відіграє визначальну роль, можна запропонувати таке її тлумачення: інформаційна безпека є здатністю держави, суспільства, соціальної групи та особистості, по-перше, з достатнім ступенем вірогідності забезпечувати захищене інформаційне середовище та соціальну ентропію, необхідні для підтримання життєдіяльності й стійкого розвитку соціуму; по-друге, чинити ефективний опір інформаційним небезпекам і загрозам, деструктивним інформаційним впливам на індивідуальну та суспільну свідомість, психіку людей, а також на комп'ютерні мережі та інші технічні джерела інформації; по-третє, формувати в індивідів і груп навички та вміння безпечної поведінки в інформаційному середовищі; по-четверте, підтримувати постійну готовність до адекватного реагування в умовах інформаційного протиборства; по-п'яте, послідовно й цілеспрямовано інтегрувати штучний інтелект у соціальне середовище за відповідною безпековою програмою. Попри те, що наведене формулювання загалом коректно відображає специфіку інформаційної безпеки, воно має суттєвий

недолік: прагнення охопити всі сутнісні виміри цього явища перетворює його на громіздку конструкцію, що ускладнює її практичне сприйняття та застосування.

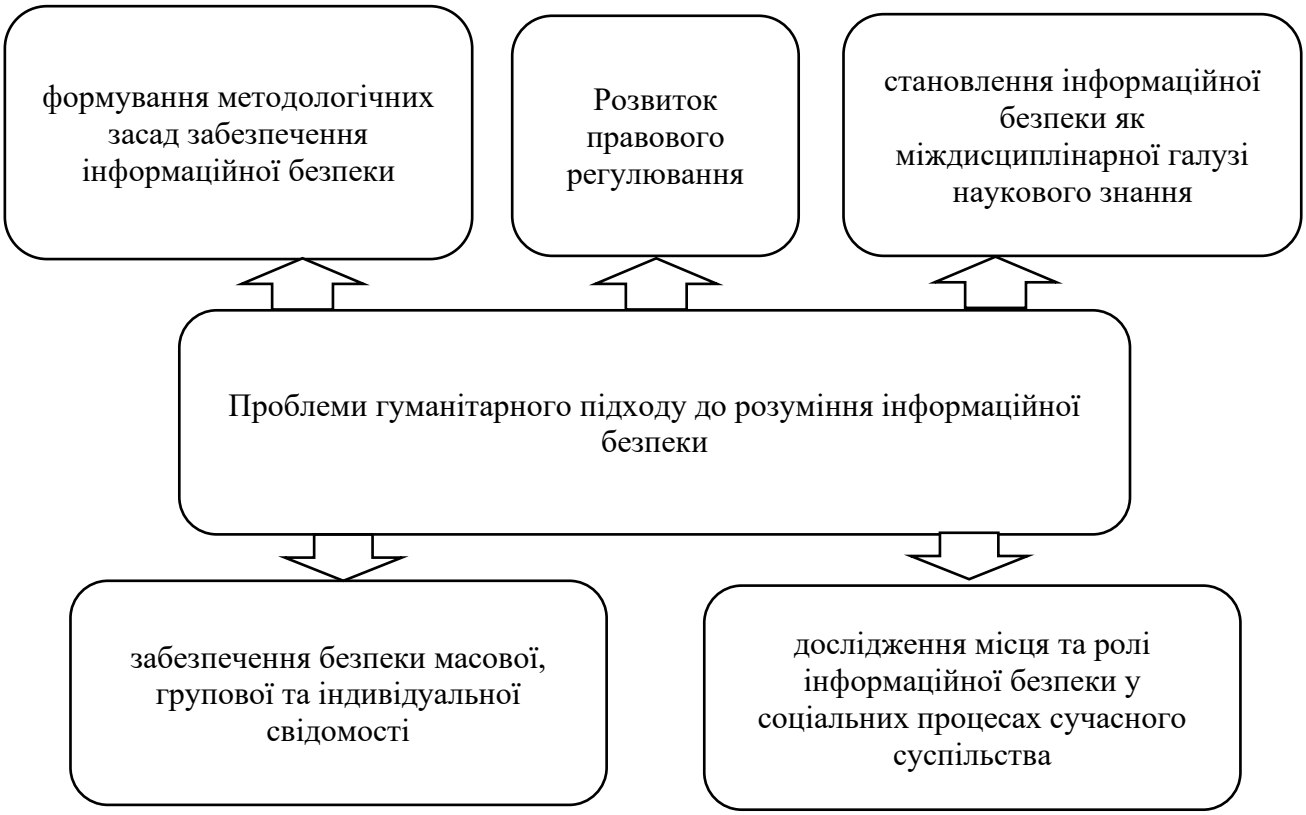


Рис. 1.1. Проблеми гуманітарного підходу до розуміння інформаційної безпеки

*Джерело: складено автором на підставі [53; 186; 221]*

Водночас у науковій літературі представлені дослідження, спрямовані на конкретизацію соціальних, психологічних, політичних, правових, педагогічних та інших аспектів інформаційної безпеки. Однак необхідно відзначити, не всі з перерахованих напрямів пропонують концентроване визначення поняття, що вивчається, в рамках власного бачення проблем в межах певної області знань. З метою реалізації поставлених перед поточним дослідженням завдань слід розглянути підходи до вирішення проблем щодо інформаційної безпеки.

Перший підхід – це нормативно-юридичний, представлений у законодавстві України та інших зарубіжних країн, стосовно регулювання

відносин по забезпеченню інформаційної безпеки [73; 108; 117]. У межах цього підходу інформаційна безпека розглядається як об'єкт правової охорони, що потребує чіткого визначення кола суб'єктів, їхніх прав, обов'язків та відповідальності, закріплених у відповідних нормативно-правових актах. Нормативно-юридичний підхід передбачає формування цілісної системи законодавства, яка охоплює як загальні засади державної інформаційної політики, так і спеціальні норми щодо захисту критичної інформаційної інфраструктури, персональних даних та державної таємниці. Принциповою характеристикою цього підходу є його спрямованість на узгодження національного законодавства з міжнародними правовими стандартами, насамперед із нормативною базою Європейського Союзу у сферах кібербезпеки та захисту інформації, що набуває особливого значення з огляду на курс України на європейську інтеграцію.

Другий, психологічний підхід, акцентує увагу на психологічній складовій інформаційної безпеки [16; 201]. Його принципова відмінність від усіх інших наявних підходів полягає в тому, що він висуває на перший план людину та особистість як суб'єкта інформаційної взаємодії, цілком обґрунтовано наголошуючи на психологічному вимірі як одній із сутнісних сторін інформаційної безпеки. Водночас трактування, що найповніше втілюють логіку цього підходу, є концептуально обмеженими: захист психологічного стану людини від деструктивних інформаційних впливів є необхідним і невід'ємним, проте далеко не єдиним елементом системи інформаційної безпеки.

Варто зазначити, що в останні роки психологічний підхід отримав інтенсивний розвиток, результатом якого стало формування самостійного напряму соціальної практики та наукових досліджень, позначеного поняттям «інформаційно-психологічна безпека».

Третій підхід – соціально-філософський – визначає інформаційну безпеку як результат подолання умов, що породжують відповідну небезпеку, і закріплюється у формах, які дозволяють соціальним суб’єктам зберегти

здатність виробити релевантні об’єктивні потреби цілі та можливості їх досягнення [186; 205]. Дане формулювання відрізняється істотним недоліком, у ньому позиціонується соціальний суб’єкт і властиві йому потреби, цілі, можливості щодо деяких форм і небезпек поза інформаційним середовищем, як наслідок – поняття втрачає специфічні особливості.

Ще одне визначення інформаційної безпеки – стан захищеності суб’єкта, який виражається в безпеці інформації суб’єкта та його інформаційно-психологічної безпеки, що досягається за допомогою рефлексивного визначення та контролю єдності його природного існування та розвитку в ході реалізації інформаційних процесів (створення, передачі, подання, отримання, обробки, зберігання) [56, с. 25]. Наведене визначення вирізняється прагненням інтегрувати максимально повний перелік інформаційних компонентів: об'єкт, суб'єкт, мету, процеси, діяльність і засоби. Однак саме ця всеохопність обертається втратою лаконічності, перетворюючи формулювання на громіздку конструкцію, складну для практичного сприйняття.

Частина дослідників тлумачить поняття «інформаційна безпека» як стан інформаційного середовища, що забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, належний захист самої інформації та убезпечення суб'єктів від деструктивних інформаційних впливів [47; 59; 71]. Попри певні переваги, це визначення характеризується недостатнім рівнем конкретизації, а його змістовне наповнення не охоплює повного обсягу поняття «інформаційна безпека», яке в дійсності є значно ширшим.

Узагальнення результатів аналізу поняття «інформаційна безпека» в межах гуманітарного підходу дозволяє констатувати, що в наявних визначеннях суб'єкти інформаційних відносин та інформаційне середовище як сфера їхньої діяльності, пов'язаної зі створенням і споживанням інформації, набувають статусу інтегрального об'єкта захисту.

Таким чином, спектр визначень інформаційної безпеки широкий, і в роботі наведені найбільш характерні з них відповідно до методологічних підходів авторів. Аналізуючи зазначені визначення інформаційної безпеки,

необхідно відзначити їх основний недолік: дослідники сконцентровані на специфічних аспектах феномена чи навпаки недостатньо конкретні, у результаті важливі моменти смислового наповнення втрачені. Зрештою виникає у певному плані неповне трактування поняття, яке не відбиває повного розуміння досліджуваного феномена. До позитивних характеристик розглянутих підходів необхідно зазначити, що за своєю суттю перелічені трактування не суперечать один одному, вони лише відображають різні грані інформаційної безпеки, що дає підставу досить докладно опрацювати зазначену актуальну проблему.

Спільною рисою більшості дослідників у процесі розроблення визначення досліджуваного поняття було прагнення досягти не лише термінологічної, а й методологічної визначеності в інтерпретації категорії «інформаційна безпека». Зважаючи на те, що сутність безпеки системи розкривається через її здатність зберігати власну цілісність і реалізовувати потенціал розвитку в реальних умовах, зокрема несприятливих, таких як конфлікт, ризик і невизначеність, інформаційну безпеку доцільно розглядати в двох взаємопов'язаних вимірах: як безпеку об'єкта в умовах інформаційного середовища та як безпеку самої інформаційної сфери.

Зокрема, під інформаційним середовищем слід уважати:

– сукупність суб’єктів, що знаходяться в інформаційній взаємодії;

– технології, що забезпечують дану взаємодію.

Інформаційна сфера включає крім сукупності суб’єктів та безпосередньої інформації, призначеної для використання суб’єктами інформаційної взаємодії, інфраструктуру, що забезпечує обробку, зберігання та обмін інформацією, а також відносини, що склалися у зв’язку з формуванням, зберіганням та розповсюдженням інформації.

Узагальнення проведеного аналізу наукових підходів дозволяє виокремити такі ключові змістовні складові поняття «інформаційна безпека»:

– захист інформації від несанкціонованого доступу, спотворення та знищення;

– убезпечення суб'єктів інформаційної взаємодії від деструктивних інформаційних впливів;

– задоволення інформаційних потреб суб'єктів інформаційної взаємодії шляхом підтримання безпечного стану інформаційного середовища.

Проведене дослідження розширює змістовне наповнення категорії інформаційної безпеки, вводячи третю сутнісну ознаку: забезпечення інформаційних потреб суб'єкта в ході його інформаційної взаємодії в умовах захищеного інформаційного середовища.

У найзагальнішому сенсі інформаційна потреба передбачає необхідність інформації, що виявляється у інформаційному запиті.

Вивчаючи питання задоволення інформаційних потреб суб’єктів інформаційної взаємодії, деякі автори зазначають, що в безумовному порядку повинні задовольнятися не будь-які інформаційні потреби, а ті, які визначаються необхідністю забезпечення життєдіяльності суб’єкта, його адаптації до умов навколишнього середовища, що постійно змінюються. Насамперед цього числа слід додати інформацію, що забезпечує формування науково обґрунтованої адекватної картини світу [56; 84; 195]. Далі – інформацію, що відповідає за соціалізацію особистості. Після цього – все, що забезпечує господарську, виробничу та іншу легітимну діяльність суб’єкта. При цьому важливо наголосити, що інформаційні потреби мають виключно персональний характер. Вони залежать як від особливостей поставлених завдань, так і від психологічних, освітніх та інших характеристик суб’єкта, що приймає рішення. Так, необхідна для задоволення інформаційних потреб інформація має бути: достатньою (щодо повного прийняття рішень), достовірною та своєчасною.

У свою чергу, задоволення інформаційної потреби пов’язане з небезпекою: якщо велика кількість низькоякісної інформації не буде виключена, безпека не буде гарантованою. Для того щоб процес задоволення інформаційних потреб не чинив деструктивного впливу та мав позитивний характер для суб’єкта інформаційної взаємодії, інформація має відповідати

основним вимогам: бути достовірною, своєчасною та достатньою. Імовірність прийняття правильного рішення, як правило, визначається якістю інформації та когнітивними здібностями самого суб’єкта.

Розвинену здатність диференціювати контент, аналізувати інформацію та знаходити правильні рішення при реалізації поставленого можна навіть називати «мудрістю» суб’єкта. Відсутність необхідної інформації для прийняття рішень змушує суб’єкта інформаційної взаємодії екстраполювати ситуацію за допомогою попереднього досвіду, що бере до уваги структуру системи, стан зв’язків, поведінку елементів тощо. Вагомим чинником у цьому процесі є накопичений попередніми поколіннями позитивний досвід, що традиційно знаходить своє закріплення в міфах, переказах, моральних нормах і принципах, тобто в культурному надбанні соціуму. У сутнісному відношенні інформаційна безпека являє собою такий стан об'єкта або суб'єкта, за якого інформаційне середовище його функціонування забезпечує збереження можливостей і здатності реалізовувати власні рішення відповідно до цілей прогресивного розвитку. Стан динамічної рівноваги всієї системи, досягнутий за таких умов, кваліфікується як стійкий.

Викладене свідчить про те, що досягнення інформаційної безпеки не зводиться виключно до застосування засобів, методів і заходів захисту інформаційного середовища та убезпечення об'єкта або суб'єкта від деструктивних впливів. Не менш важливим є розвиток у об'єкта або суб'єкта внутрішньої здатності протистояти деструктивному інформаційному впливу та ухилятися від нього. При цьому центральним елементом системи інформаційної безпеки є не комп'ютер, а людина, здатна до прогресивного саморозвитку і діяльності відповідно до власних цінностей та цілей.

Цінності, інтеріоризовані у свідомості соціального суб'єкта, формують його життєві цілі та світоглядні орієнтири, визначають характер потреб. Саме вони задають ключові критерії, що обумовлюють вибір і обґрунтування дій соціального суб'єкта в процесі його функціонування в інформаційній сфері. Включення цінностей до числа визначальних компонентів поняття

«інформаційна безпека» є відмітною рисою запропонованого трактування цієї категорії.

На підставі проведеного аналізу видається доцільним запропонувати авторське визначення інформаційної безпеки. Під інформаційною безпекою пропонується розуміти стійкий стан інформаційної сфери, спрямований на забезпечення її цілісності та захист відповідних об'єктів від несприятливих внутрішніх і зовнішніх впливів як результат усвідомлення соціальними суб'єктами своїх цінностей, потреб як життєво важливих інтересів та цілей розвитку.

Запропоноване визначення у концентрованій формі відображає сутнісний зміст категорії «інформаційна безпека» в єдності її аксіологічного, гносеологічного та онтологічного вимірів. Онтологічний аспект фіксує ситуацію подолання небезпеки, орієнтованої на забезпечення цілісності об'єкта та підтримання стійкого стану інформаційного середовища. Антропологічний вимір розкриває завдання убезпечення суб'єкта інформаційної взаємодії. Аксіологічна складова відображає систему цінностей і цілей, що визначають характер інформаційних потреб суб'єкта.

Підсумовуючи викладене, змістовне ядро поняття «інформаційна безпека» охоплює три взаємопов'язані складові:

– захист інформації від несанкціонованого доступу та деструктивних впливів;

– убезпечення суб'єктів інформаційної взаємодії від негативних інформаційних впливів;

– задоволення інформаційних потреб соціальних суб'єктів шляхом формування та підтримання захищеного інформаційного середовища.

Отже, інформаційна безпека постає як багатовимірний феномен об'єктивного суспільного розвитку, покликаний сприяти гармонійному становленню інформаційного суспільства та забезпечувати його стале функціонування.

## 1.2. Особливості управління інформаційною безпекою держави в умовах гібридних загроз

Визначальною рисою сучасного етапу суспільного розвитку є дедалі вагоміша роль інформаційної сфери, що охоплює сукупність інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збирання, формування, поширення та використання інформації, а також механізми регулювання суспільних відносин, що виникають у цьому процесі. Інформаційна сфера набула статусу системоутворювального чинника суспільного життя, а інформація перетворилася на фундаментальну основу сучасного високотехнологічного та комп'ютеризованого світу, який у науковій літературі отримав назву інформаційного суспільства [49; 136]. Нагромадження різноманітних видів інформації в суспільстві супроводжувалося різким зростанням інтенсивності її споживання в усіх галузях людської життєдіяльності, а розуміння та практичне застосування інформації вийшло на якісно новий рівень. Результатом цих процесів стала «інформаційна революція», що не зводиться до суто технологічних перетворень. Інтенсивний поступ інформаційних технологій справив глибокий вплив на економічну, політичну та духовну сфери суспільства. На межі тисячоліть людство стало свідком фундаментальних суспільних зрушень, спричинених стрімким ускладненням технологій і якісними змінами в системі комунікацій.

Приблизно з середини XX століття у науковому середовищі зміцнюється усвідомлення факту, що інформаційні процеси носять всеосяжний характер. А стрімке проникнення інформаційних технологій у різні сфери життєдіяльності, по суті, призводить до зміни парадигми уявлення про місце та роль інформації в сучасному суспільстві.

Науково-технічна революція в інформаційній сфері дедалі активніше визначає розвиток суспільного прогресу. Серед інших факторів саме інформаційні технології, особливо поширення Інтернету з його відкритістю та

глобальною досяжністю, справили рішучий вплив на бізнес та комунікаційну інфраструктуру в суспільстві.

Інформація починає сприйматися як основа технічного прогресу, джерело та найважливіший ресурс воєн та конфліктів, значний фактор геополітичних змін; як стратегічно важливий ресурс у політиці та управлінні, особлива соціально-економічна цінність і, навіть, – елемент економічного потенціалу, який має в своєму розпорядженні суспільство і держава [8; 104].

Інформація необхідна для прийняття політичних рішень, вона лежить в основі процесів навчання та освіти, та будь-якого іншого процесу. Інформація, що впливає на діяльність людини, а через неї та на навколишній світ, стає гігантською технічною, соціально-економічною, політичною та культурною силою. При цьому суперечки та дискусії про сутність інформації не вщухають досі.

Одне з фундаментальних у сучасній науці поняття інформації походить від латинського information – відомості, роз’яснення, виклад. Спочатку інформація розумілася в сенсі повідомлення про щось і пов’язувалася виключно з комунікативною діяльністю у суспільстві. До кінця 1940-х років під інформацією розумілися відомості, що передаються людьми усним, письмовим та іншим чином [68, С. 84].

Сьогодні інформація визнається багатогранним та дуже широким явищем, яке може одночасно позначати:

– повідомлення про щось;

– відомості, котрі є об’єктом зберігання, переробки та передачі;

– кількісну міру усунення невизначеності, міру організації системи.

Залежно від галузі досліджень інформація має безліч визначень:

– позначення змісту, отриманого від зовнішнього світу у процесі пристосування до нього; з

– заперечення ентропії (Л. Бріллюен);

– комунікація та зв’язок, у процесі якої усувається невизначеність (К. Шеннон);

– передача різноманітності (У. Ешбі);

– міра складності структур (А. Моль);

– ймовірність вибору [68; 118].

Дослідження інформації як наукового об'єкта охоплює три взаємодоповнювальні виміри: технічний, семантичний і прагматичний.

Технічний вимір зосереджений на вивченні проблем точності, надійності та швидкості передачі повідомлень, а також на розробленні засобів і методів побудови каналів передачі сигналів та забезпечення їхньої перешкодозахищеності [63, с. 56].

Семантичний вимір орієнтований на розв'язання проблеми адекватного відтворення змісту повідомлень засобами кодованих сигналів [68, с.85].

Прагматичний вимір розкривається через оцінювання споживчої цінності отриманого повідомлення крізь призму його впливу на подальшу поведінку реципієнта [68, с.86].

У межах системно-кібернетичного підходу інформація розглядається у трьох аспектах (таблиця 1.1).

Категорія інформації в її базовому розумінні передбачає наявність щонайменше трьох елементів: джерела інформації, її споживача та середовища передачі. При цьому інформація не здатна передаватися, прийматися або зберігатися у чистому, незакріпленому вигляді.

Матеріальним носієм інформації слугує повідомлення, яке являє собою кодований еквівалент певної події, зафіксований джерелом інформації та виражений через упорядковану послідовність умовних фізичних символів, що утворюють певний алфавіт. Передача повідомлень між суб'єктами здійснюється за допомогою каналів зв'язку, в яких повідомлення може функціонувати виключно у формі сигналу, єдино прийнятній для конкретного каналу. Сигнал являє собою знак, фізичний процес або явище, що поширюється каналом зв'язку та несе відомості про певну подію, стан об'єкта спостереження або контролю, управлінські команди чи вказівки [115, с. 25].

Таблиця 1.1

Специфіка розгляду інформації у межах системно-кібернетичного підходу

| Аспект системно-кібернетичного підходу | Характеристика |
|---|---|
| інформаційний | пов’язаний з реалізацією в системі певної сукупності процесів відображення зовнішнього світу та внутрішнього середовища системи шляхом збирання, накопичення та переробки відповідних сигналів |
| управлінський | враховує процеси функціонування системи, напрями її руху під впливом отриманої інформації та ступінь досягнення своїх цілей |
| організаційний | характеризує пристрій та ступінь досконалості самої системи управління у термінах її надійності, живучості, повноти реалізованих функцій, досконалості структури й ефективності витрат на здійснення процесів управління в системі |

*Джерело: складено автором на підставі [63; 115]*

У науковій літературі щодо сутності феномена інформації можна виокремити два основні концептуальні підходи. Перший розглядає інформацію як атрибут матерії, тобто як властивість, що уможливлює передачу певного змісту та спричиняє зміни властивостей або стану матеріальних об'єктів. Другий підхід, вужчий за своїм охопленням, але водночас більш релевантний для цілей даного дослідження, отримав назву органічного. В його межах інформація трактується як властивість живої матерії відображати об'єктивну реальність і використовувати результати цього відображення для пристосування до змін навколишнього середовища [56; 68]. Кожна з наведених концепцій висвітлює певний аспект інформації, що робить їх сумісними в рамках єдиного підходу. При цьому атрибутивна концепція акцентує незалежність інформації як атрибуту матеріального об'єкта від процесів її практичного використання, відображаючи тим самим статичний вимір інформації.

Виходячи з наведеного розуміння інформації, цей феномен можна розглядати як:

– явище життя організмів;

– явище життя людини, тому що людина як об’єкт живої природи має не лише здатність адаптації до змін навколишньої дійсності, а й здатність активно впливати на неї з метою задоволення своїх потреб;

– і, нарешті, як явище та умова життя суспільства, оскільки життя суспільства є сукупністю соціальних форм буття людини, зміст яких визначається ставленням індивідів до спільної з іншими діяльності із задоволення індивідуальних та соціальних інтересів. У цьому випадку інформація проявляється у формі відомостей, що передаються тим чи іншим індивідам, та повідомлень, що містять ці відомості. І саме ці відомості та повідомлення часто виступають як об’єкти суспільних відносин, що формують інформаційну сферу суспільства.

Поняття «інформаційне суспільство» з'явилося в науковому обігу в другій половині 1960-х років, а його авторство традиційно приписується професору Токійського технологічного інституту Ю. Хаяші [249, с. 56]. Вихідне концептуальне окреслення основних характеристик «суспільства знання» було здійснено ним у доповідях, підготовлених для японського уряду кількома організаціями: Агентством економічного планування, Інститутом розробки використання комп'ютерів та Радою структури промисловості. У цих документах високоіндустріальне суспільство визначалося як таке, в якому розвиток комп'ютеризації відкриє громадянам доступ до надійних інформаційних джерел і звільнить їх від рутинної праці завдяки масштабній автоматизації виробничих процесів. Передбачалося, що глибокі структурні зрушення торкнуться безпосередньо виробництва, продукт якого набуде виразно вищої «інформаційної ємності», що зумовить суттєве зростання питомої ваги інновацій, дизайну та маркетингу в його вартості. Виробництво інформаційного, а не матеріального продукту, на переконання авторів концепції, має стати визначальним рушієм суспільного розвитку та освіти.

Трохи пізніше, у 1973 році, на світ з’явилася праця американського соціолога Д. Белла «Наступне постіндустріальне суспільство. Досвід соціального прогнозування» [234]. У зазначеній книзі Д. Белл охарактеризував нове суспільство як суспільство нової формації. Він зазначив, що воно відрізняється головним чином зростанням кількості та значення інформації, а також тим, що інформація в кількісному та якісному відношенні є ключовою характеристикою розвитку. На його думку, ядро трансформацій, що переживає сучасний світ, пов’язане з технологіями обробки інформації та комунікацією. Говорячи про інформацію, Д. Белл стверджує, що життя в новому суспільстві «засноване на послугах і є взаємодією з людьми», отже, «головну роль відіграє не груба м’язова сила, не енергія, а інформація» [234, с. 123].

Подальший розвиток електронних засобів масової інформації та інформаційних технологій спонукав дослідників до поглибленого вивчення ролі й функцій інформації в суспільному житті. Вагомий внесок у цьому напрямі зробили канадський мислитель М. Маклюен та американський футуролог Е. Тоффлер. Зокрема, М. Маклюен відводив інформаційним технологіям роль найвагомішого чинника формування соціально-економічного підґрунтя нового суспільства. Розмірковуючи над перспективами еволюції засобів масової комунікації в умовах інформаційного суспільства, він наполегливо звертав увагу на тенденцію до посилення активної ролі мас-медіа у творенні «глобальних обіймів», де всі явища та процеси виявляються надзвичайно тісно взаємопов'язаними [105, с. 127].

Е. Тоффлер, ще один провідний теоретик інформаційного суспільства, запропонував оригінальну концепцію історичного процесу. У праці «Третя хвиля» він виокремив три послідовні етапи розвитку цивілізації:

– перша хвиля – аграрна (до XVIII століття);

– друга хвиля – індустріальна (до 50-х років XX століття);

– третя хвиля – постіндустріальна (починаючи з 50-х років XX століття) [208, с. 98].

На його переконання, наближений історичний злам є настільки ж глибоким, як і перша хвиля перетворень, що розгорнулася десять тисяч років тому із запровадженням землеробства. Друга хвиля була породжена промисловою революцією, тоді як третя стала можливою завдяки інформаційній революції, що набирає дедалі більших обертів. Ціннісні орієнтири сучасності, на думку Е. Тоффлера, ґрунтуються на миттєвому отриманні та передачі даних, ідей і символів, а рушійною силою трансформацій, що переживає сучасний світ, є технології опрацювання інформації та комунікації [208].

Перехід людської цивілізації до Нової епохи зумовлений революцією в інформаційних технологіях, яка в 1970-х роках заклала підвалини якісно нової технологічної системи, що поступово охопила весь світ. Саме інформаційно-технологічна революція слугує відправною точкою для розуміння складнощів становлення нової економіки, суспільства та культури. Паралельно зі змінами в матеріально-технологічній сфері докорінних перетворень зазнала соціальна та економічна архітектура суспільства: відносно жорсткі й вертикально впорядковані інституції поступаються місцем гнучким горизонтальним мережам, через які здійснюється влада та відбувається обмін ресурсами. У концепції М. Кастельса формування міжнародних ділових і культурних мереж та розвиток інформаційних технологій постають як нерозривно пов'язані та взаємозумовлені явища [239]. Зростання обсягів інформації в розвинених суспільствах супроводжується масштабним вивільненням робочої сили зі сфери промислового виробництва та переміщенням її до сфери послуг і інформаційної діяльності, що своєю чергою генерує подальше збільшення інформаційних потоків. У цих умовах формується «нова свідомість», характерна для постіндустріального суспільства: відбувається зсув від «економізуючого» етосу, орієнтованого на максимальне задоволення власних інтересів, до «соціологізованого» способу життя. Остання модель передбачає усвідомлене осмислення суспільних потреб на засадах чітко визначеного

«суспільного інтересу», де знання постають якісно новою основою соціальної системи та її «осьовим принципом».

Іншими словами, за відносно короткий історичний проміжок часу «все — від геополітики великих національних держав до повсякденного життя пересічних людей — виявилося включеним в інформаційний простір і глобальні мережі». Конститутивними ознаками нового інформаційного суспільства стали:

– зростання значущості інформації та знання в усіх вимірах суспільного життя;

– збільшення питомої ваги інформаційних комунікацій, продуктів і послуг у структурі валового внутрішнього продукту;

– розбудова глобального інформаційного простору, що забезпечує ефективну інформаційну взаємодію між людьми, вільний доступ до світових інформаційних ресурсів та задоволення потреб у відповідних продуктах і послугах [49; 184].

При цьому внаслідок нерівномірності світового економічного розвитку стало можливим виділити національні шляхи інформаційного розвитку та побудови інформаційного суспільства. Їх відмінності ґрунтуються на особливостях макроекономічної політики держави та законодавства, специфіці ідеології та національної культури. Нерівномірність світового економічного розвитку призвела до того, що стало можливим виділити американський, азіатський та європейський шляхи інформаційного розвитку та побудови інформаційного суспільства.

На рубежі XX-XXI століть проблематика забезпечення безпеки зачіпає гранично широке коло значущих аспектів: йдеться про військову, політичну, економічну, інформаційну, екологічну, культурну безпеку як складові системи загальнонаціональної безпеки. При цьому особливої актуальності набула інформаційна безпека та різні аспекти її забезпечення: економічний, соціальний, психологічний, кожен з яких претендує в майбутньому на самостійність [109; 123; 213]. Інформаційна безпека сьогодні забезпечує

формування інформаційного середовища суспільства, її використання та розвиток на користь громадян, організацій, держави. Інформаційна безпека охопила політичний, технологічний, економічний, суспільно-правовий аспекти життя держави. І саме безпека в інформаційній сфері сьогодні визначає політику держав, комерційних компаній, відносини громадських організацій, індивідів.

Окремо слід розглянути соціальне партнерство суспільства та держави у забезпеченні державної політики у сфері інформаційної безпеки.

Відповідальне громадянське суспільство є неодмінною передумовою будь-якого суспільного поступу. Громадянська самоорганізація в її різноманітних проявах акумулює колосальний невикористаний ресурс для соціально-економічного та культурного піднесення України. Роль держави в цих процесах принципово переосмислюється: замість функції керівництва добровільними об'єднаннями громадян на перший план виходить їхня підтримка та розширення реальних можливостей для участі в публічному житті.

Вихід із кризового стану української системи інформаційної безпеки лежить у площині об'єднання зусиль усіх суспільних інституцій довкола спільної концепції управління — державного, регіонального та корпоративного рівнів. Її фундаментом мають слугувати довіра між учасниками, готовність до конструктивного діалогу та співпраці, застосування міжсистемної оптики при аналізі та захисті інформації, а також максимально ефективне залучення наявних інформаційних ресурсів [61; 92].

Громадянське суспільство сьогодні виходить за межі пасивного спостерігача і перетворюється на активного учасника формування безпекової політики. Пропозиції щодо вироблення адекватних і універсальних механізмів реагування на терористичні загрози та інші виклики безпеки дедалі частіше надходять від суспільства безпосередньо до керівництва держав, спецслужб і правоохоронних структур. Майданчиком для напрацювання таких рекомендацій слугують конгреси, симпозіуми, конференції, семінари та круглі

столи, що організовуються інститутами громадянського суспільства. Саме через ці форми публічної взаємодії влада отримує практично орієнтовані пропозиції щодо протидії інформаційному тероризму та іншим викликам, породженим входженням країни в інформаційну епоху.

Фактичні дані свідчать про те, що громадяни очікують і від держави, і від громадянського суспільства набагато більшої активності й ефективності, вважаючи за необхідне їхнє рівноправне партнерство.

При цьому на суспільство лягає завдання давати політиці держави оцінку та вносити свої коригування, а також уважно відстежувати та не допускати впливу деструктивних ідей на вироблення та коригування доктрини інформаційної безпеки. Особлива відповідальність лягає на суб'єктів, що виробляють концептуальні підходи та впливають на суспільні та державні рішення.

Залучення громадян до забезпечення інформаційної безпеки має відбуватися на тих самих демократичних засадах, що й інші форми політичної участі. Ключовою передумовою цього є розбудова розгалужених комунікаційних зв'язків, які гарантують реальну доступність громадян до відомостей про процеси вироблення та прийняття політичних рішень [230, с. 177]. Розширення такого доступу здатне суттєво підвищити спроможність громадян та інститутів громадянського суспільства здійснювати дієвий вплив на органи державної влади й місцевого самоврядування.

Нагальною залишається потреба в якісному оновленні діяльності публічних органів влади та трансформації управлінської системи в напрямі вироблення механізму узгодження інтересів тих, хто управляє, і тих, ким управляють. Легітимне підґрунтя таких механізмів має бути закріплено в законодавстві, укорінено в суспільній свідомості та відображено в політичній культурі державних службовців, політиків і пересічних громадян.

Влада, що вибудовує відкритий і системний діалог із суспільством, отримує реальний шанс здобути громадянську довіру до своїх дій і на цій

основі суттєво підвищити результативність усієї системи забезпечення інформаційної безпеки.

При цьому чинником, що визначає таку співпрацю, може бути залучення широкого кола контрагентів (учасників) до процесу. Наприклад, таких як:

– виробники комп'ютерних компонентів та програмного забезпечення, які зазнають тиску ринкового попиту щодо найбільш якісних продуктів;

– страхові компанії, зацікавлені у запобіганні страховим випадкам;

– інвестиційні фонди та приватні стейкхолдери, зацікавлені у стабільності своїх вкладень;

– організації, що займаються сертифікацією та авторизацією, здатні підвищити рівень довіри;

– аудиторські фірми, здатні надавати незалежні та публічні оцінки, тощо [266; 268];

Вони можуть сприяти:

– оптимізації процесу прийняття управлінських рішень на основі широких консультацій із зацікавленими сегментами приватного сектору;

– проведенню аналізу, обговоренню, організації взаємообміну та впровадженню зразків передового досвіду (best practices);

– виробленню ясного розуміння того, що навіть найнадійніші зовнішні стіни не захистять від внутрішніх загроз, пов'язаних з проявами недбалості, несумлінності або прихованого саботажу з боку інсайдерів;

– поширенню інформації про державне сприяння в галузі навчання та підвищення кваліфікації персоналу із залученням широкого експертно-аналітичного співтовариства, академічних структур та приватних консультативних компаній.

Водночас практичне втілення партнерських відносин в умовах інформаційного розвитку українського суспільства потребує врахування реалій, притаманних вітчизняним умовам, зокрема наявної інформаційної асиметрії між центром і регіонами, зумовленої нерівномірністю розвитку інформаційно-комунікаційної інфраструктури на різних територіях країни.

Сучасна Україна переживає глибоку трансформацію суспільних відносин, у ході якої формується якісно нове інституційне середовище і відбуваються докорінні зміни в соціальній структурі. За цих обставин недостатня інтегрованість суб'єктів громадянського суспільства в загальнодержавні процеси постає як додатковий чинник ризику для ефективного забезпечення державної безпеки.

Для вирішення проблем забезпечення інформаційної безпеки потрібно враховувати досвід інших країн та створювати систему громадянської взаємодії, що може суттєво підвищити ефективність відповідної політики. Така соціальна взаємодія держави та суспільства може мати на увазі [54; 55; 216]:

– організацію спільних приватно-державних конференцій, круглих столів;

– проведення заходів із залученням ЗМІ;

– організацію інтерв’ю в друкованих ЗМІ;

– розроблення програми виховання належного ставлення до державно-важливої інформації у молоді, коли за підтримки суспільства буде створено культурно-інформаційні центри, електронні бібліотеки;

– підготовку та навчання комерційними структурами своїх співробітників, які мають доступ до важливої інформації з урахуванням кваліфікації, ієрархії, соціального та психологічного аспекту внутрішньогрупових відносин в умовах забезпечення інформаційної безпеки, системи заборон та обмежень. Необхідне постійне підвищення рівня освіти користувачів у галузі інформатики, підвищення кваліфікації розробників, експертів та обслуговуючого персоналу інформаційних систем. Достатня кваліфікація персоналу та своєчасне її коригування є порівняно недорогим засобом підвищення безпеки інформаційного простору;

– створення обстановки свідомого ставлення до захисту інформації в керівництва, шляхом поєднання профілактичних заходів при посиленні покарання за незначні на перший погляд посадові злочини, пов’язані з

порушенням вимог інформаційної безпеки, але здатні призвести до тяжких наслідків. Особливо, якщо це стосується недбалості чи навмисної бездіяльності перших осіб, вищої та середньої ланки керівництва.

Пріоритетним напрямом залишається формування комплексу заходів із зміцнення партнерської взаємодії між науково-освітньою спільнотою, бізнесом, громадськими організаціями та населенням у реалізації стратегії інформаційного розвитку.

Інструментарій співпраці держави та приватного сектору не є уніфікованим – він може набувати різних конфігурацій залежно від галузі суспільної практики, з якої запозичується. Серед найбільш перспективних механізмів взаємодії публічних органів і структур громадянського суспільства виокремлюються політичні мережі, що консолідують різнорідних учасників довкола спільних інтересів на засадах взаємозалежності, рівноправності та готовності до конструктивної співпраці. Така мережева архітектура управління громадськими справами інтегрує державні, приватні та громадські організації й установи в єдину систему, сполучаючи державу та громадянське суспільство через спільність цілей і взаємну зацікавленість.

Мережевий формат взаємодії виявляється продуктивнішим за інші моделі налагодження зв'язків між державою та громадянським суспільством, оскільки його функціонування спирається на механізми довіри як базового структуроутворювального чинника. Об'єднувальним стрижнем таких утворень слугує спільний кооперативний інтерес акторів, зацікавлених в обміні наявними ресурсами та досягненні взаємовигідних домовленостей. Саме це принципово відрізняє мережу від ринку, де кожен учасник керується насамперед власною вигодою, а не колективними цілями. В організаційному відношенні мережа являє собою договірну конструкцію, що функціонує на основі узгоджених формальних і неформальних комунікаційних правил, пронизаних особливою культурою консенсусу. У більш широкому розумінні вона постає як система державних і недержавних суб'єктів, що діють у певній сфері публічної політики, взаємодіють між собою в умовах ресурсної

залежності та прагнуть досягти узгоджених рішень з питань, що становлять спільний інтерес, застосовуючи при цьому як формальні, так і неформальні регулятивні норми [31; 72].

Невід'ємною складовою ефективної державної політики у сфері інформаційної безпеки є розроблення та запровадження стратегії соціального партнерства. Залежно від масштабу, періодичності та характеру спрямованості такі стратегії диференціюються на державні й регіональні; систематичні та епізодичні; випереджувальні й реактивні [91; 90].

Випереджувальна стратегія охоплює сукупність заходів, покликаних нейтралізувати потенційну загрозу або мінімізувати її деструктивні наслідки ще на етапі, що передує виникненню небезпечної ситуації, або в період прихованого чи слабовираженого вияву тривожних симптомів. Натомість реактивна стратегія передбачає комплекс дій, до яких суб'єкт безпеки вдається безпосередньо після того, як небезпечна ситуація вже виникла та набула виразних ознак [92, с. 10].

Існують різноманітні засоби реалізації запобіжних стратегій. Відповідно, можна виокремити такі тактики:

– тактика попередження – маються на увазі превентивні заходи щодо забезпечення безпеки;

– тактика виявлення – систематичний контроль можливості появи реальних чи потенційних загроз.

Діапазон застосування випереджувальних стратегій охоплює різні цілі та об'єкти впливу, серед яких профілактична діяльність у правовій, організаційно-технічній, економічній та громадській площинах.

Закономірно, що в усіх країнах питання свободи в інформаційній сфері, форм поширення та отримання інформації перебуває в центрі уваги як громадськості, так і державних інституцій. Свобода в цьому контексті не тотожна вседозволеності чи відсутності контролю – вона являє собою виважений баланс між відкритістю та обґрунтованими обмеженнями у сфері доступу до інформації та її використання.

Досягнення такого балансу потребує цілеспрямованого культивування правової культури, а також чіткого нормативного закріплення правового статусу всіх учасників системи інформаційних відносин: громадян, соціальних інститутів, громадсько-політичних організацій, органів державної влади та місцевого самоврядування. Невід'ємним елементом цієї системи є встановлення відповідальності зазначених суб'єктів у межах реалізації конституційного права на свободу інформації [164; 217].

Нарешті, є доцільним виділення в окрему галузь права відносин, що виникають у сфері забезпечення інформаційної безпеки.

Невідкладним завданням залишається також модернізація законодавства за такими напрямами:

– запровадження уніфікованих підстав для обмеження права на доступ до інформації, визначення вичерпного переліку видів інформації з обмеженим доступом та механізмів реалізації відповідних обмежень, а також закріплення принципів і організаційних механізмів доступу до відкритих інформаційних ресурсів органів державної влади, місцевого самоврядування, громадських організацій та суб'єктів господарювання;

– врегулювання відносин у сфері збирання, зберігання та поширення персональних даних, забезпечення захисту особистої та сімейної таємниці, а також гарантування недоторканності приватного життя особи;

– перегляд та уточнення положень законодавства України, що регулює конституційні права і свободи людини і громадянина в інформаційній сфері, з метою конкретизації механізмів юридичної відповідальності за їх порушення та усунення наявних нормативних суперечностей;

– зміцнення правових механізмів охорони об'єктів інтелектуальної власності, зокрема ноу-хау, винаходів, що становлять службову чи державну таємницю, а також фірмових найменувань, із одночасним закріпленням державних прав на відповідні об'єкти;

– деталізація правових механізмів протидії пропаганді та агітації, що розпалюють соціальну, расову, національну та релігійну ненависть і ворожнечу;

– розбудова державної системи контролю за обігом спеціальних технічних засобів негласного збирання інформації;

– нормативне закріплення порядку використання державних інформаційних ресурсів, у тому числі фондів музеїв, бібліотек та архівів, а також формування правового механізму запобігання їх несанкціонованому використанню та його припинення;

– упорядкування відносин у сфері поширення масової інформації через канали радіо- та телемовлення, включаючи запобігання монополізації медіапростору.

Окремої уваги потребує створення дієвих механізмів фінансової підтримки громадянських ініціатив та наукових розвідок у сфері інформаційної безпеки. Пріоритетними в цьому напрямі є цільове фінансування наукових досліджень, запровадження на загальнодержавному рівні системи регулярного і належного стимулювання молодих науковців, а також реалізація програм підтримки молодих фахівців галузі із залученням як державних, так і приватних та комерційних джерел фінансування.

У сфері забезпечення інформаційної безпеки в Україні ключового значення набуває підготовка кваліфікованих кадрів, оскільки спостерігається відсутність достатньої кількості підготовлених фахівців із цих питань в органах законодавчої, виконавчої, судової влади, а також у правоохоронних органах; немає достатньої кількості кваліфікованих цивільних фахівців, які займаються розробкою нових технологій у галузі програмування та обладнання, що забезпечують захист інформації [3; 75]. Також актуальним є створення системи ліцензування цивільних фахівців. Та й загалом необхідним є створення спеціалізованих організаційних структур. Наприклад, для організації взаємодії правоохоронних структур різних країн у галузі

виявлення, попередження та припинення злочинів у сфері високих технологій є вкрай важливим.

Необхідною є організація просвітницької роботи з населенням для розвитку інформаційно-правової культури громадян. Слід, зокрема, звернути увагу на проблему телебачення. Свого часу німецький філософ Ю. Хабермас висунув концепцію публічної сфери, де між громадянами та урядом діють громадські інститути та, зокрема, засоби масової інформації [248, с. 131]. Сьогодні ця публічна сфера багато в чому зайнята саме телебаченням, яке, як уже було зазначено вище, має значний потенціал маніпулювання свідомістю [4; 16]. Для протидії цьому необхідно мати, поряд із комерційним телебаченням, телебачення та радіо, які представляли б суспільні інтереси.

Серед пріоритетів державної політики України вирізняється забезпечення доступу вітчизняної та міжнародної громадськості до достовірної інформації про позицію держави щодо суспільно значущих питань національного та міжнародного порядку денного [114; 190]. Головним інструментом реалізації цього завдання на сьогодні залишається зміцнення потенціалу державних засобів масової інформації та розширення їхніх функціональних можливостей, а також вироблення підходів до формування інформаційної політики державних телерадіомовних організацій та інших підпорядкованих державі медіаструктур.

Провідні експерти наголошують на принциповій відмінності між державним телебаченням як загальнонародним надбанням та телебаченням урядовим, президентським чи відомчим: перше має належати всьому суспільству, а не окремим владним інституціям [114; 190; 204]. Йдеться про серйозні, суспільно значущі канали, орієнтовані не на обслуговування інтересів великих корпоративних структур, а на врахування потреб держави, громадян і громадянського суспільства загалом. Аналогічні вимоги висуваються і до приватного телебачення, діяльність якого має підпорядковуватися суспільному інтересу. Схожа логіка стосується і радіомовлення. Обов'язковим елементом медіапростору мають стати

некомерційні інформаційні канали та просвітницькі програми, покликані задовольняти інформаційні потреби громадянського суспільства.

Нагальною потребою є формування у молодого покоління відповідального ставлення до інформації, що має державне значення [97; 99]. Реалізація цього завдання потребує впровадження спеціальних довгострокових державних проєктів, спрямованих на підвищення громадянської свідомості в питаннях використання інтернет-ресурсів, комп'ютерних баз даних та інших інформаційних інструментів. Паралельно необхідним є охоплення програмами інформатизації всієї системи загальної та спеціальної освіти, включаючи подальші форми підготовки й перепідготовки фахівців, а також підвищення кваліфікації кадрів, задіяних у реалізації цих програм. Інфраструктурною основою для цього мають слугувати культурно-інформаційні центри, публічні електронні бібліотеки та інші відповідні інституції [168; 184].

У межах локалізуючої стратегії, своєю чергою, можливі дії, створені задля виявлення й аналізу причин, які спричинили виникнення збитків, можливостей їх усунення чи ослаблення дії загроз, застосування санкцій до агентів-порушників та до тих, хто їх провокує тощо. Такі заходи можуть мати правовий, соціальний чи економічний характер. Йдеться про досить жорстку систему каральних заходів правового характеру, наприклад, що передбачає позбавлення ліцензії на право випуску друкованої продукції або ведення діяльності в Україні.

Права людини виконують роль своєрідного індикатора зрілості громадянського суспільства та правової держави, вимірюючи їх відповідність цивілізаційним і загальнодемократичним стандартам розвитку. Небезпека криється не лише в порушеннях прав окремих громадян, а передусім у ризику втрати стратегічних орієнтирів при пошуку рівноваги між публічними та приватними інтересами. В умовах демократичного розвитку однаково неприйнятними є обидві крайнощі: абсолютизація «суверенітету» особистості та її самодостатності у відриві від історичних, соціальних і культурних

цінностей суспільства і держави, і протилежний полюс — ідеологія державного патерналізму з її примусовим примусом держави над індивідом. Надмірна опіка з боку держави позбавляє суспільство ініціативи й творчої енергії, стримуючи розвиток громадянських інститутів. Демократична держава покликана не домінувати над особистістю та суспільством, а виступати гарантом реалізації індивідуальних прав і духовно-морального поступу соціуму.

Отже, стратегія забезпечення інформаційної безпеки сучасного суспільства потребує дієвого комплексу організаційних заходів, здатних не лише оперативно й результативно нейтралізовувати наявні загрози, а й упереджувати їх виникнення.

Сьогодні в Україні активно впроваджуються новітні інформаційні та телекомунікаційні технології, залучаються унікальні інформаційні ресурси, органічно формується культура інформаційної епохи. Проте інтеграція до глобального інформаційного простору несе в собі чинники, здатні негативно вплинути на нормальний розвиток країни.

## 1.3. Механізми формування та реалізації державної політики у сфері інформаційної безпеки

В умовах глобалізованого світу інформаційна безпека перетворилася на фундаментальну передумову безпечного існування всієї світової спільноти. Визначальною тенденцією в її змістовному наповненні стає дедалі вагоміша роль гуманістичного виміру, покликаного нейтралізувати ключові небезпеки та загрози інформаційного характеру й забезпечити суспільству безпечне освоєння потенціалу інформаційних технологій.

Вирішення цього питання вимагає попередніх зусиль з метою формування безпечного існування в інформаційному середовищі. Аналіз можливостей технологій завтрашнього дня показує, що інформаційні технології, котрі використовуються суспільством, повинні отримувати

соціальний зміст і втілювати цілі, що виключають антигуманістичне застосування. Розробка та впровадження нових інформаційних технологій, що мають соціально-гуманістичну спрямованість, визначаються не тільки стараннями творців технологій, але, насамперед, суспільства, котре формує сприятливе гуманістично спрямоване соціальне середовище [92, 109].

У даному руслі особливої значущості набуває оцінка інформаційно-технічних винаходів та перспектив використання інформаційних технологій, що впливають на виживання суспільства. Можливість мати достовірну інформацію про наслідки застосування інформаційних технологій сприяє попередженню негативних проявів різного характеру. Неповна чи недостовірна інформація, незнання чи нерозуміння наслідків є глибинною причиною основної кількості катастроф та аварій у майбутньому. Інакше гіпотетичне майбутнє людства має бути визначальним орієнтиром розвитку можливих напрямів системи інформаційних технологій. Від цього усунення пріоритетів у змісті інформаційної безпеки сьогодні неминуче внесе зміни до структури функціонування глобальної безпеки на підтримку загальнолюдських інтересів.

Захист основних прав і фундаментальних свобод людини в інформаційному вимірі передбачає забезпечення максимального різноманіття легітимного контенту в інформаційних мережах, орієнтованого передусім на задоволення тих інформаційних потреб, що сприяють суспільному прогресу. Концепція раціональної інформаційної технології, побудованої на повазі до людських цінностей, виходить із того, що технологічне опанування суспільством знань та інформації має слугувати виключно цілям поступального розвитку.

Розширення соціальної бази суспільства закономірно супроводжується зростанням кількості суб'єктів інформаційної безпеки, що висуває на перший план завдання підвищення рівня освіченості та інформаційної культури як окремих соціальних суб'єктів, так і суспільства загалом. Це завдання охоплює як професійну діяльність у галузі інформаційних технологій, так і будь-яку активність в інформаційному середовищі, консолідуючи навколо себе всіх

учасників інформаційних відносин. Зрештою саме рівень розвитку людського потенціалу як визначальна передумова формування наукового, соціального, економічного, культурного та духовного капіталу суспільства обумовлює реальний стан його безпеки. З огляду на це наука та освіта постають вирішальними чинниками забезпечення інформаційної безпеки як стрижневого елемента національної безпеки держави [88; 101].

Посилення соціального виміру інформаційної безпеки зумовлює усвідомлення потреби у впровадженні принципово нового захисного інструментарію – соціальних заходів забезпечення інформаційної безпеки [195; 207]. Новаторський характер цієї форми захисту визначається її багаторівневою архітектурою, що охоплює різноманітні механізми та поведінкові моделі, покликані в сукупності гарантувати інформаційну безпеку особистості, суспільства і держави.

Комплексне розв'язання проблем інформаційної безпеки потребує системи заходів, що включає [97; 98]:

– цілеспрямований виховний та освітній вплив на різні верстви населення;

– активне поширення та утвердження в масовій свідомості через усі доступні медіаплатформи й із застосуванням найсучасніших інформаційних технологій за безпосередньої участі держави;

– зразків і принципів морально відповідальної поведінки в глобальному інформаційному середовищі;

– засад етичного знання та культури інформаційної етики.

Системний характер соціальних заходів інформаційної безпеки розкривається через їхню рівневу організацію та відповідні напрями захисної діяльності. Структурування цих заходів передбачає виокремлення трьох ієрархічних рівнів [91; 90]:

– загальносуспільного, що охоплює процеси макрорівня;

– організаційно-групового, що функціонує в межах установ та соціальних спільнот на мезорівні;

– особистісного, зосередженого на індивідуальному мікрорівні.

Кожен із зазначених рівнів організації соціальних заходів задає відповідний вектор розвитку та функціонування системи інформаційної безпеки в цілому.

На рівні суспільства в цілому або макрорівні соціальні заходи інформаційної безпеки реалізуються завдяки організації та регулюванню інформаційних потоків, а також поширенню засобів, способів та своєрідних «алгоритмів» оцінки, обробки інформації та застосування інформаційних технологій у процесі соціальної взаємодії від масової комунікації до міжособистісного спілкування. На цьому рівні суб'єктами захисту інформаційної безпеки виступають суспільство та держава у вигляді діяльності конкретних соціальних інститутів, що включають систему поширення соціальних норм, традицій, соціокультурних цінностей, систему освіти, формування сприятливої соціальної атмосфери, систему морального, правового регулювання тощо.

На мезорівні соціальні заходи захисту реалізуються завдяки використанню та поширенню інформаційних джерел та специфічних способів соціальної взаємодії, оцінки та переробки інформації, характерних для конкретних організацій та соціальних груп. Тут можна виділити прийняті у різних соціальних групах чи професійних організаціях етичні норми, правила, регламентації, процедури інформаційної взаємодії та безпечного використання інформаційних технологій. До цього рівня належать такі суб'єкти захисту, як соціальні групи, виробничі структури, політичні, суспільні, релігійні та інші організації та об'єднання.

На мікро- чи індивідуальному рівні соціальні заходи забезпечення інформаційної безпеки здійснюються у процесі навчання та розвитку індивіда у вигляді створення специфічної регулятивної системи чи комплексу механізмів і алгоритмів, котрі визначають поведінку суб'єкта в інформаційному середовищі.

Визначивши структуру та зміст системи соціальних заходів забезпечення інформаційної безпеки, доцільно розглянути докладніше передбачені нею технології захисту.

Реалізація державної політики на макрорівні соціальних заходів забезпечення інформаційної безпеки потребує здійснення таких кроків [73; 90]:

– формування цілісної та внутрішньо узгодженої концепції правового регулювання у сфері інформаційної безпеки;

– утвердження системної практики поширення в суспільстві базових принципів інформаційної безпеки, прав та обов'язків суб'єктів інформаційних відносин;

– розбудова науково-методологічного підґрунтя для розвитку галузі інформаційної безпеки.

У дослідженні соціальних аспектів інформаційної безпеки можна зазначити, що проблеми інформаційної безпеки зі своєї спеціальної області давно перейшли в область соціальну, тобто область захисту прав людини та суспільства [186; 205]. Доцільно наголосити на тому факті, що єдиним гарантом їх дотримання тут стає держава.

Поряд із удосконаленням чинного законодавства у боротьбі зі злочинами, які скоюються за допомогою комп’ютерних технологій, з метою захисту прав людини та суспільства необхідна уніфікація національного законодавства та об’єднання зусиль міжнародного співтовариства у виробленні єдиних підходів щодо питань регулювання світового інформаційного простору. Важливим чинником цього процесу є всебічне дослідження проблем у цій сфері з урахуванням балансу технічних, етичних, культурних та інших аспектів [54; 55; 216].

Невід'ємним напрямом реалізації державної політики у сфері інформаційної безпеки є мобілізація потенціалу засобів масової інформації та освітньої системи для цілеспрямованого утвердження в суспільній свідомості стандартів морально відповідальної поведінки в глобальному інформаційному

середовищі, що закладає міцне підґрунтя для розбудови цілісної системи інформаційної безпеки.

Вивчаючи вплив інформаційних технологій на цінності людини, можна визначити своєрідні щаблі популяризації етичного знання, що сприяють вирішенню проблем застосування технологій сучасного суспільства

Відповідно, слід звернути увагу на історію інформаційної етики, в межах якої вирішуються фундаментальні завдання: захист головних людських цінностей, зокрема, здоров'я, безпека, свобода, знання і використання нових можливостей. Ґрунтуючись на подібному підході, необхідним є вивчення проблем, що виникають у світлі застосування інформаційних технологій на двох різних щаблях, перша з яких базисна. Вона важлива тим, що дає відчути всім представникам суспільної системи той факт, що процес використання інформаційних технологій має соціальні й етичні наслідки. Основні дії на цьому рівні припускають інформування широкого загалу населення про проблеми, що виникають у сфері створення та застосування інформаційних технологій з метою їх популяризації та пропаганди.

Наступний ступінь – «теоретична» інформаційна етика, яка на заданому рівні покликана застосовувати наукові теорії до аналізу соціальних та етичних проблем, що виникають у суспільстві у процесі застосування інформаційних технологій.

У свою чергу, роль держави у забезпеченні зазначених процесів визначається аж ніяк не жорстким контролем кожного етапу чи сфери інформаційної взаємодії; вона скоріше носить особливий допоміжний характер. Основні функції держави у цьому зв'язку мають бути зосереджені на таких діях [31; 32]:

– проголошувати та перекладати на мову права етичні засади, що лежать в основі інформаційного суспільства; відстежувати та контролювати їх ефективне здійснення;

– у разі потреби, при виявленні зловживань або відсутності підтримки проголошених цінностей суб'єктами різної діяльності, вжити заходів регулювання на основі методів прозорості та відкритості.

Понад те, до функцій держави належить обов'язок в якості зразка етичного застосування інформаційних технологій навіяти повагу до прийнятих норм морального регулювання та втілювати їх у життя. Інформаційна етика має призвести соціум до усвідомлення принципів, у межах яких надалі потрібно будувати інформаційне суспільство. Водночас зазначені принципи мають знайти екстраполяцію у затвердженні прав, які обстоюють.

Формування високоморального інформаційного середовища – шлях, прокладений далеко не на примусі, через блокування чи покарання неугодних або тих, хто не дотримується прийнятих правил. Насамперед, це формування виховних моделей, впровадження засобів та розробка методів, призначених для засвоєння людьми етичних цінностей, виховання поваги до них та рефлексії. Очікуваним результатом від зазначених дій мають стати етичне саморегулювання в інформаційному середовищі, а також самоконтроль, що ґрунтується на цінностях солідарності та соціальної відповідальності [266; 268].

Мезорівень соціальних заходів забезпечення інформаційної безпеки включає формування та впровадження захисних механізмів на колективному рівні, що ґрунтуються на ідентифікації індивіда з конкретною соціальною групою, спільністю, об'єднанням. Основною метою дії зазначених механізмів є вміння людини керуватися у процесі застосування інформаційних технологій чи інформаційної взаємодії певними оцінками, нормами, думками, прийнятими у соціальній групі чи професійному середовищі.

У цьому зв'язку необхідно виділити категорії соціальних груп та колективів у галузі застосування інформаційних технологій, які відчувають на сьогоднішній день потребу в моральному регулюванні соціальної взаємодії в інформаційному середовищі.

1. Першу групу складають фахівці, для яких інформаційні технології є галуззю професійної діяльності, та які мають в інформаційному середовищі різноманітні ділові, комерційні відносини.

2. Друга група об’єднує всі категорії користувачів та спільнот користувачів.

3. Третя група представлена засобами масової інформації.

4. У четвертій групі представлені регулювальники контенту в інформаційному просторі Інтернет, для яких етичні кодекси через відсутність правових важелів діяльності покликані служити забезпеченням прозорості в роботі пошукових служб.

Професійне середовище фахівців, які працюють у галузі інформаційних технологій, вже досить тривалий час займається питаннями морального регулювання дій професіоналів у своїй галузі. Сьогодні питання професійної відповідальності фахівців стає дедалі актуальнішим. Ця обставина визначена підвищенням вимог до рівня професіоналів, що пов’язане з обстановкою, котра розгортається в галузі інформаційної безпеки, та розвитком інформаційного суспільства в цілому. Свого часу Р. Броуді ввів поняття «інформаційна наївність» у професіоналів у галузі інформаційних технологій, проводячи фундаментальну різницю між змістом слів «знати про» та «знати» [237].

Визначення «інформаційної наївності» полягає в «стані, який не може бути більшим, ніж реалізація процесу, пов’язаного з виробництвом артефактів» [237, с. 1126]. Виходячи за рамки прийнятого розуміння наївності, тобто не більше ніж недбалість у користуванні, слід залучити також сюди такі характеристики, як низький рівень компетентності та недолік у професійних знаннях.

У боротьбі з подібним станом «інформаційної наївності» необхідно активніше використовувати етичні кодекси в індустрії виробництва інформації та інформаційних технологій, які зобов’язані вимагати високої

професійної компетентності, точності та попередити прояви можливих негативних ефектів [266; 268].

Водночас, проблеми у сфері використання інформаційних технологій не обмежуються питаннями лише у сфері професіоналізму. Глобальна інформаційна мережа, завдяки своєму універсальному середовищу та простоті технічного використання, послужила підґрунтям для утворення різних соціальних та культурних меж, що позиціонують себе як окремі субкультури, котрі мають в арсеналі свою систему цінностей та норми поведінки. Певний рівень розвитку таких Інтернет-спільнот є приводом для формулювання зазначених атрибутів у кодекси та правила етичного регулювання дій членів сформованих груп (хакери, блогери тощо).

У свою чергу, етичні кодекси конкретних спільнот Інтернет-простору є приватними прикладами вирішення етичних проблем поведінки в глобальній інформаційній мережі за допомогою прийняття певних правил. Як більш масштабне рішення нівелювання зазначених проблем дослідники пропонують виділити основні складові мережевої етики: кодекс мережевої етики (регулятор відносин у Мережі) та мережевий етикет (регулятор поведінки у Мережі). Зокрема, у постулатах кодексу мережевої етики декларуються традиційні цінності, які екстраполюються на взаємини користувачів мережі Інтернет. Їхня мета – допомогти людині зберегти в собі людські якості, не втратити свій особистісний початок, свою індивідуальну специфіку в Інтернеті.

Щодо третьої групи користувачів, які потребують регулювання діяльності етичними кодексами, слід зазначити таке. Професійна етика працівників, які функціонують в межах засобів масової інформації, має давню історію, пов’язану зі становленням демократичного, громадянського суспільства. З часом моральні правила, визнані всіма працівниками медіасфери, сформувалися у відповідні етичні канони. Сьогодні принципи міжнародної журналістської етики сфокусовані на професійній чесності та об’єктивності, повазі до приватного життя та гідності, відображенні

суспільних інтересів, загальних цінностей та різноманіття культур, просуванні правди, дотриманні норм інформаційної безпеки, а також особистому переконанні втілювати в життя зазначені принципи [258, с. 124].

Високі моральні норми етичного кодексу працівники медіасфери, друкованих ЗМІ, радіо, телебачення, державного мовлення разом із результатами своєї діяльності зобов'язані проєктувати зі звичайного світу до глобальних інформаційних мереж. Сьогодні, у період небувалого розвитку інформаційно-комунікаційних технологій, коли інформаційні джерела впливають на всі сфери життєдіяльності людини, засоби масової інформації набувають практично необмежених можливостей впливу на суспільний настрій, тому як ніколи важливо пам'ятати і втілювати в життя перелічені вище моральні постулати.

Заключна група, яка потребує обов'язкового запровадження етичних кодексів, становить спільноту регулювальників контенту в інформаційному просторі Інтернет, оскільки, як згадувалося раніше, через відсутність правових важелів подібної діяльності етичні кодекси мають бути забезпеченням прозорості у роботі пошукових служб.

Коло основних питань щодо контролю роботи пошукових служб має бути таким: Кому підзвітні пошукові служби? Які є гарантії етичної діяльності цих підприємств? Якими критеріями керуються служби у процесах блокування та розповсюдження інформаційного контенту? Крім того, до питань відповідальності Інтернет-провайдера необхідно додати такий аспект, як передача незаконного, забороненого, небезпечного чи неетичного контенту в Інтернет-середовищі. Так, ситуація наочно показує гостру необхідність обговорення етичного кодексу для інформаційних посередників, які мають інформувати про принципи і методи, які гарантують конфіденційність інформації, довіреної їм.

Наприклад, Європейська асоціація з інформаційних послуг (англ. – European Association of Information Services – EUSIDIC) пропонує кодекс практики для виробників баз та банків даних [242]. У пунктах етичного

кодексу виробників інформаційних ресурсів чітко простежується спрямованість дотримання принципів інформаційної безпеки: повноти, конфіденційності та доступності. Етичні правила спрямовані на збереження належного рівня відкритості інформаційних потоків, водночас з урахуванням захисту персональних даних, а також забезпечення законних інтересів усіх сторін, які беруть участь у процесі виробництва, зберігання та розподілу інформації. Такі категорії, як відкритість, конфіденційність, точність та справедливість є основою фундаменту у сфері професійної діяльності інформаційних посередників.

Крім того, в рамках питання про можливе регулювання зазначеної вище категорії необхідно привернути увагу зацікавленої громадськості та вчених до етичних аспектів роботи ігрових сервері. Введення певних правил у надання послуг середовища Інтернет має сприяти зниженню загальної кількості випадків розвитку психосоціальних розладів у дітей і підлітків.

Відповідно до Конвенції про права людини, регулювання свободи слова та свободи доступу до інформації в демократичному суспільстві пов’язане з обов’язками та відповідальністю [70]. У цьому зв’язку слід виділити самоконтроль як спосіб ефективного регулювання інформаційної взаємодії. Відповідно, необхідно зазначити і технічні прийоми його реалізації: використання програм фільтрації, застосування функцій модераторів, розробку технічних регламентів як програмне забезпечення для фільтрації та рейтингових процедур. У практиці сьогодні існують поки нечисленні приклади активності кінцевих користувачів у процесах саморегулювання та спільного регулювання. Зразком спільного регулювання контенту в інтернет-середовищі може служити Вікіпедія – вільна загальнодоступна мультимовна універсальна Інтернет-енциклопедія, що займається залученням усієї громадянської інформаційної спільноти в процеси створення контенту, редагування та перевірки фактів. В силу об’єктивних причин ця енциклопедія не може становити кількість наукових видань, водночас вона є одним із найпопулярніших інформаційних джерел у користувачів мережі Інтернет.

У широкому розумінні забезпечення безпеки як процес опанування умовами власного існування є одночасно процесом здобуття свободи суб'єкта, що виявляється в його здатності свідомо керувати обставинами свого буття. Підтримання належного рівня захищеності об'єктів безпеки потребує формування розгалуженої системи правових норм, що регулюють відносини в безпековій сфері, а також окреслення пріоритетних векторів діяльності органів державної влади та місцевого самоврядування у цьому напрямі. Досягнення необхідного рівня захищеності стає можливим завдяки проведенню скоординованої державної політики через комплекс економічних, політичних, організаційних та інших заходів, що відповідають характеру реальних загроз життєво важливим інтересам особистості, суспільства і держави. Дотримання балансу між інтересами цих трьох суб'єктів у межах інформаційної сфери є визначальним принципом, навколо якого вибудовується вся система реалізації державної політики у галузі інформаційної безпеки.

Фундаментом державної політики у сфері інформаційної безпеки України слугують такі основоположні принципи [90; 92]:

– неухильне виконання вимог Конституції України, чинного національного законодавства та загальновизнаних норм міжнародного права в галузі інформаційної безпеки;

– гарантування правової рівності всіх громадян незалежно від їхнього соціального, політичного чи економічного становища на основі конституційного права вільно шукати, отримувати, передавати, виробляти та поширювати інформацію будь-якими законними засобами;

– забезпечення прозорості у здійсненні функцій органами державної влади та громадськими об'єднаннями через систематичне інформування суспільства про їхню діяльність;

– цілеспрямований розвиток вітчизняного сектору інформаційних і телекомунікаційних технологій, нарощування виробництва технічних і програмних засобів, спроможних забезпечити модернізацію національної

телекомунікаційної інфраструктури та її інтеграцію до глобальних інформаційних мереж.

Чинне законодавство закріплює також організаційні засади побудови системи забезпечення інформаційної безпеки.

Під системою забезпечення інформаційної безпеки розуміється інтегрована сукупність органів, методів, сил і засобів, що забезпечують захист інформаційного простору [59, с. 34]. Її призначення полягає у практичному втіленні державної політики у відповідній сфері, а сама вона функціонує як органічна складова загальнонаціональної системи безпеки держави.

Державна система інформаційної безпеки країни в науковій літературі тлумачиться як структурно впорядкована сукупність уповноважених державних органів, сил і засобів, діяльність яких здійснюється на правовій основі під судовим контролем і в межах судового захисту [75; 115].

До кола функціональних завдань зазначеної системи належать [95, с. 193]:

– своєчасне виявлення та прогнозування дестабілізувальних чинників й інформаційних загроз, спрямованих проти життєво важливих інтересів особистості, суспільства і держави;

– здійснення комплексу стратегічних і невідкладних заходів, орієнтованих на нейтралізацію та подолання виявлених загроз;

– формування та підтримання постійної боєздатності сил і засобів, задіяних у системі забезпечення інформаційної безпеки.

Звичайно, органи інформаційної безпеки можуть і повинні створюватися і в недержавних структурах для захисту своїх потреб у забезпеченні необхідною інформацією, її збереження тощо, але виключно на законодавчій основі. Більше того, ці органи шляхом укладання договорів можуть бути включені в єдину державну систему інформаційної безпеки.

Побудова системи забезпечення державної інформаційної безпеки України здійснюється на засадах чіткого розмежування повноважень між законодавчою, виконавчою та судовою гілками влади. Організаційну

архітектуру цієї системи формують два ключові елементи: інституційний, представлений органами державної влади та місцевого самоврядування, і програмно-стратегічний, втілений у державній політиці у сфері інформаційної безпеки.

Змістовна структура державної політики у сфері інформаційної безпеки охоплює чотири взаємопов'язані складові: нормативно-правову, організаційну, технологічну та кадрову [91; 90].

Нормативно-правова складова покликана створити та послідовно вдосконалювати систему правових механізмів протидії загрозам в інформаційній сфері, включаючи інструменти їх практичного застосування.

Організаційна складова окреслює функціональну архітектуру державних органів і громадських організацій, що беруть участь у реалізації відповідних правових норм, унормовує відносини між ними, а також характер їхньої взаємодії з громадянином як ключовим суб'єктом інформаційних відносин.

Технологічна складова забезпечує інструментальну спроможність системи до своєчасного виявлення інформаційних загроз безпеці особистості, суспільства і держави, об'єктивного оцінювання потенційної та завданої шкоди, а також організації дієвої протидії цим загрозам.

Кадрова складова орієнтована на цілеспрямоване нарощування та підтримання людського потенціалу, необхідного суспільству й державі для повноцінного та ефективного функціонування всієї системи забезпечення інформаційної безпеки.

Передумовою результативної державної політики у сфері інформаційної безпеки є поєднання трьох взаємозалежних чинників: стійкої та авторитетної державної влади, професійного апарату управління, укомплектованого компетентними фахівцями, а також відлагодженого механізму вироблення й виконання управлінських рішень. Саме системний підхід до формування та реалізації такої політики відкриває перед державою реальні можливості не лише для нейтралізації актуальних інформаційних загроз, а й для

відстоювання власних стратегічних інтересів у високо конкурентному глобальному інформаційному середовищі сучасності.

Засади та принципи державної політики у сфері інформаційної безпеки мають слугувати орієнтиром для всього комплексу захисних заходів у політичній, економічній, оборонній та інших галузях державної діяльності. До першочергових заходів із реалізації цієї політики належать [89; 90; 92]:

– вироблення та запровадження механізмів регулювання відносин в інформаційній сфері, підвищення якості державного управління діяльністю публічних медіаструктур, проведення активної державної інформаційної політики, а також підготовка концептуальних засад правового забезпечення інформаційної безпеки;

– формування, затвердження та виконання державних програм підвищення правової свідомості та цифрової грамотності населення, розбудова інфраструктури єдиного інформаційного простору України, протидія кіберзлочинності та вдосконалення системи підготовки кваліфікованих кадрів у галузі інформаційної безпеки;

– зміцнення технологічного суверенітету держави в інформаційно-телекомунікаційній сфері, приведення вітчизняних стандартів інформатизації та інформаційної безпеки у відповідність до міжнародних норм і вимог.

У сфері забезпечення інформаційної безпеки держава [177; 175; 179]:

– здійснює комплексне й неупереджене дослідження та прогнозування загроз інформаційній безпеці, напрацьовуючи відповідні механізми їх нейтралізації;

– запроваджує контрольні функції щодо розроблення, застосування, експорту та імпорту засобів захисту інформації через систему сертифікації та ліцензування відповідної діяльності;

– реалізує протекціоністські заходи на підтримку вітчизняних виробників засобів інформатизації та захисту інформації, водночас убезпечуючи внутрішній ринок від надходження неякісної іноземної продукції в цій галузі;

– створює сприятливі умови для отримання фізичними та юридичними особами доступу до глобальних інформаційних мереж і світових інформаційних ресурсів;

– визначає стратегічні пріоритети та забезпечує практичне втілення державної інформаційної політики.

Практика реалізації державної політики у сфері інформаційної безпеки виявляє існування низки суперечностей і парадоксів, що унаочнені на рисунку 1.2.

Вихід із кризового стану системи інформаційної безпеки потребує об'єднання зусиль усіх суспільних інституцій та вироблення концептуальних засад ефективного управління на державному, регіональному й корпоративному рівнях. Фундаментом такого управління мають слугувати взаємна довіра між учасниками, конструктивний діалог і готовність до співпраці, застосування міжсистемної методології в аналізі та захисті інформації, а також раціональне залучення наявного інформаційно-ресурсного потенціалу [61; 92].

Повноправна інтеграція держави до глобального інформаційного суспільства відкриває якісно нові горизонти для підвищення ефективності її функціонування, водночас породжуючи принципово нові вимоги до публічного управління. Пришвидшення інформаційного обміну диктує владним структурам необхідність прискореного реагування на суспільні зміни та вироблення гнучкіших і результативніших управлінських механізмів. Роль каталізатора та координатора в процесі руху до інформаційного суспільства має взяти на себе саме держава, спрямовуючи й узгоджуючи зусилля всіх залучених учасників. Принципи державно-приватного партнерства при цьому мають посісти центральне місце в системі реалізації державної політики у сфері інформаційної безпеки України.

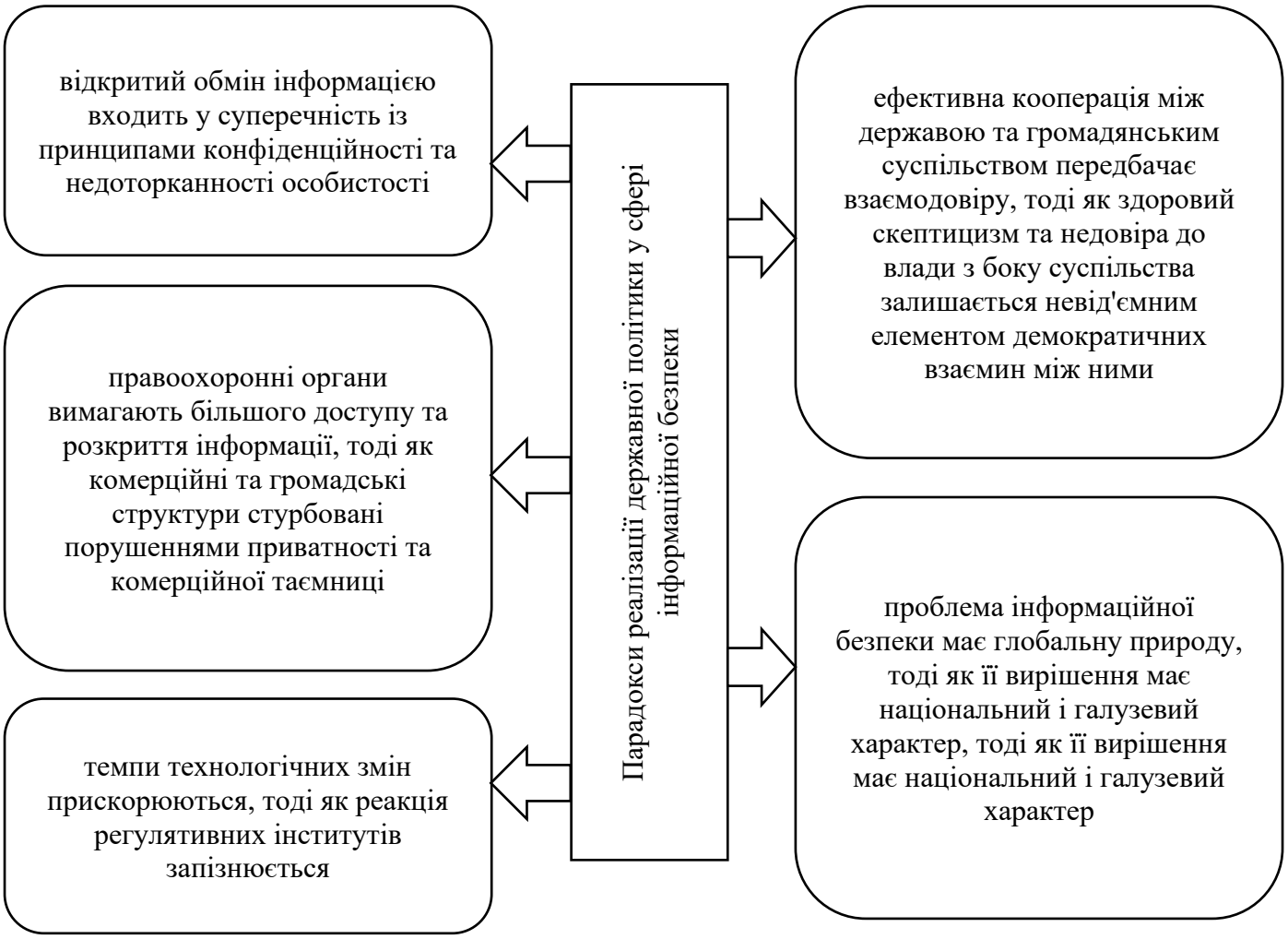


Рис. 1.2. Парадокси реалізації державної політики у сфері інформаційної безпеки

*Джерело: складено на підставі [89; 91; 90; 92]*

Насправді держава на сьогоднішній день фактично позбавлена підтримки інститутів громадянського суспільства через їхню слабкість і нерозвиненість, що помітно послаблює державність.

У цьому необхідно підкреслити, щоб в розробці чинного законодавства, котре регламентує реалізацію державної політики у сфері інформаційної безпеки, було враховано проблеми розвитку українського суспільства, породжені як радянським періодом його історії, так і періодом соціально-економічних і політичних перетворень, котрі наразі продовжуються.

Зважаючи на той факт, що проблема інформаційної безпеки виходить за коло проблем технічного та телекомунікаційного характеру, необхідно наголосити, що завдання інститутів громадянського суспільства полягає сьогодні у тому, щоб виконувати функцію сполучної ланки, котра забезпечує взаємодію громадян з державою та бізнесом як основними ініціаторами процесів інформатизації [112; 135].

Іншими словами, у нашій державі назріла потреба активувати процес взаємодії в забезпеченні інформаційної безпеки.

Завдання державної політики у сфері інформаційної безпеки полягає не тільки в тому, щоб захистити громадян і суспільство від цих загроз, а й реалізувати цю політику в таких формах та методах, які, у свою чергу, не поставили б під загрозу обраний демократичний вектор розвитку. Адекватна запитам часу політика у сфері інформаційної безпеки має спиратися на пріоритети взаємовигідного співробітництва та розвитку громадянської ініціативи, за керівної та спрямовуючої ролі держави. У зв’язку з цим склалися всі передумови до того, щоб стратегії соціального партнерства та громадянської участі посіли гідне місце у процесах вироблення та реалізації комплексної політики інформаційної безпеки.

**Висновки до першого розділу**

1. Обґрунтовано, що інформаційна безпека являє собою стійкий стан інформаційної сфери, спрямований на збереження її цілісності та захист відповідних об'єктів від несприятливих внутрішніх і зовнішніх впливів як результат усвідомлення соціальними суб'єктами власних цінностей, потреб як життєво важливих інтересів та цілей розвитку. За своєю природою інформаційна безпека постає як багатовимірний феномен об'єктивного суспільного розвитку, покликаний сприяти гармонійному становленню інформаційного суспільства.

Встановлено, що змістовне ядро категорії «інформаційна безпека» охоплює три взаємопов'язані складові:

– захист інформації від несанкціонованого доступу та деструктивних впливів;

– убезпечення суб'єктів інформаційної взаємодії від негативних інформаційних впливів;

– задоволення інформаційних потреб соціальних суб'єктів шляхом підтримання захищеного стану інформаційного середовища.

2. Доведено, що вихід із кризового стану системи інформаційної безпеки потребує об'єднання зусиль усіх суспільних інституцій навколо концепції ефективного управління на державному, регіональному та корпоративному рівнях, фундаментом якої є взаємна довіра, конструктивний діалог, готовність до співпраці, міжсистемна методологія аналізу та захисту інформації, а також раціональне використання інформаційно-ресурсного потенціалу. Наголошено, що залучення громадян до процесів забезпечення інформаційної безпеки має відбуватися на тих самих демократичних засадах, що й інші форми політичної участі. Розбудова розгалужених комунікаційних зв'язків, що гарантують реальний доступ громадян до відомостей про механізми вироблення та ухвалення політичних рішень, здатна суттєво зміцнити спроможність як окремих громадян, так і інститутів громадянського суспільства здійснювати дієвий вплив на органи державної влади та місцевого самоврядування.

3. Встановлено, що ефективне розв'язання проблем інформаційної безпеки потребує як вивчення та адаптації зарубіжного досвіду, так і побудови розгалуженої системи громадянської взаємодії, здатної якісно підвищити результативність відповідної державної політики. Механізми такої взаємодії держави та суспільства можуть охоплювати: – організацію спільних публічно-приватних конференцій і дискусійних майданчиків у форматі круглих столів;

– проведення інформаційних кампаній із залученням медіаресурсів;

– реалізацію програм виховання відповідального ставлення до інформації державного значення серед молоді із створенням за суспільної підтримки культурно-інформаційних центрів та електронних бібліотек;

– організацію систематичного навчання комерційними структурами власних працівників, які мають доступ до чутливої інформації, з урахуванням їхньої кваліфікації, службової ієрархії, соціально-психологічних особливостей внутрішньогрупових відносин, а також вимог і обмежень у сфері інформаційної безпеки;

– формування в керівного складу організацій культури свідомого захисту інформації шляхом поєднання профілактичних заходів із посиленням відповідальності за службові порушення у сфері інформаційної безпеки, що можуть спричинити серйозні наслідки.

Окремим пріоритетом залишається зміцнення партнерської взаємодії між науково-освітньою спільнотою, бізнесом, громадськими організаціями та населенням у реалізації стратегії інформаційного розвитку.

Обґрунтовано також доцільність виокремлення відносин у сфері забезпечення інформаційної безпеки в самостійну галузь права.

4. Розкрито сутність системи забезпечення інформаційної безпеки як інтегрованої сукупності органів, методів, сил і засобів, що функціонують у цій сфері. Обґрунтовано, що її призначення полягає у практичному втіленні державної політики інформаційної безпеки, а сама вона є органічною складовою загальнонаціональної безпекової системи держави. З'ясовано, що в науковій літературі система забезпечення інформаційної безпеки держави тлумачиться як структурно впорядкована сукупність уповноважених державних органів, сил і засобів, діяльність яких здійснюється на підставі законодавчих і підзаконних нормативних актів у межах судового контролю та під захистом судової влади.

Визначено, що до кола функціональних завдань цієї системи належать:

– моніторинг і прогнозування дестабілізувальних чинників та інформаційних загроз, спрямованих проти життєво важливих інтересів особистості, суспільства і держави;

– впровадження комплексу стратегічних і невідкладних заходів з метою їх нейтралізації та усунення;

– формування та підтримання постійної боєздатності сил і засобів, задіяних у системі забезпечення інформаційної безпеки.

5. Встановлено, що державна політика у сфері інформаційної безпеки структурно охоплює чотири взаємопов'язані складові: нормативно-правову, організаційну, технологічну та кадрову. Нормативно-правова складова забезпечує розбудову та постійне вдосконалення системи правових механізмів протидії загрозам в інформаційній сфері разом із інструментами їх практичного застосування. Організаційна складова окреслює функціональну архітектуру державних органів і громадських організацій, що задіяні у реалізації відповідних правових норм, унормовує відносини між ними, а також характер їхньої взаємодії з громадянином. Технологічна складова забезпечує інструментальну спроможність до своєчасного виявлення інформаційних загроз, об'єктивного оцінювання завданої і потенційної шкоди та організації дієвої протидії цим загрозам. Кадрова складова орієнтована на нарощування та підтримання людського потенціалу, необхідного для повноцінного функціонування всієї системи інформаційної безпеки.

Акцентовано, що результативність державної політики у сфері інформаційної безпеки зумовлюється поєднанням трьох взаємозалежних чинників: авторитетної та стійкої державної влади, компетентного управлінського апарату та відлагодженого механізму вироблення й виконання рішень. Системний підхід до реалізації такої політики відкриває державі реальні можливості для нейтралізації актуальних загроз і відстоювання власних стратегічних інтересів у висококонкурентному глобальному інформаційному середовищі.

З'ясовано, що фундаментом реалізації державної політики у сфері інформаційної безпеки України слугують такі основоположні принципи:

– неухильне виконання вимог національного законодавства та загальновизнаних норм міжнародного права в галузі інформаційної безпеки;

– гарантування правової рівності всіх громадян незалежно від їхнього соціального, політичного чи економічного становища на основі конституційного права вільно шукати, отримувати, передавати, виробляти та поширювати інформацію будь-якими законними засобами;

– забезпечення прозорості у здійсненні функцій органами державної влади та громадськими об'єднаннями через систематичне інформування суспільства про їхню діяльність;

– цілеспрямований розвиток вітчизняного сектору інформаційних і телекомунікаційних технологій, нарощування виробництва технічних і програмних засобів, спроможних забезпечити модернізацію національної телекомунікаційної інфраструктури та її інтеграцію до глобальних інформаційних мереж.

# РОЗДІЛ 2
# АНАЛІЗ СУЧАСНОГО СТАНУ ТА ТЕНДЕНЦІЙ РОЗВИТКУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

## 2.1. Організаційно-правовий механізм управління інформаційною безпекою України в умовах гібридних загроз

З метою реалізації курсу на цифровізацію держави та розбудови системи цифрових послуг в Україні засновано Міністерство цифрової трансформації України (МЦТУ) – центральний орган виконавчої влади, підпорядкований Кабінету Міністрів України та координований ним [132]. У системі центральних органів виконавчої влади МЦТУ виконує роль провідної інституції, відповідальної за формування та практичне впровадження державної політики в таких сферах:

– цифровізація, цифровий розвиток, цифрова економіка, цифрові інновації та технології;

– електронне урядування та електронна демократія;

– розбудова інформаційного суспільства та інформатизація;

– запровадження електронного документообігу;

– розвиток цифрових компетентностей і цифрових прав громадян;

– відкриті дані, публічні електронні реєстри, національні електронні інформаційні ресурси та їх інтероперабельність, широкосмуговий доступ до мережі Інтернет, електронна комерція та електронний бізнес;

– надання електронних адміністративних послуг населенню;

– електронні довірчі послуги та електронна ідентифікація;

– розвиток вітчизняної ІТ-галузі;

– функціонування та вдосконалення правового режиму «Дія.Сіті».

У своїй діяльності МЦТУ керується Положенням про МЦТУ. МЦТУ реалізує свої повноваження Розпорядженням Кабінету Міністрів України

«Про деякі питання цифрової трансформації» від 2 серпня 2024 р. № 735-р [142].

Паралельно Кабінет Міністрів України затвердив Стратегію цифрової трансформації соціальної сфери (розпорядження КМУ від 28 жовтня 2020 р. № 1353-р [181]), а також продовжив термін реалізації Стратегії цифрового розвитку системи управління державними фінансами до 2025 року (розпорядження КМУ від 13 травня 2025 р. № 464-р [172]). З метою інституційного забезпечення цифрових перетворень постановою Кабінету Міністрів України від 03.03.2020 № 194 [36] у міністерствах, інших центральних органах виконавчої влади та регіональних військових адміністраціях запроваджено посаду заступника керівника з питань цифрового розвитку – головного спеціаліста з цифрової трансформації.

Для прискорення і розширення масштабів цифровізації Міністерство цифрової трансформації України розробило Єдиний державний веб-портал електронних послуг «Дія». Відповідно до Положення, затвердженого постановою КМУ від 4 грудня 2019 року № 1137 [129], портал «Дія» забезпечує реалізацію права кожного на доступ до електронних послуг та інформації про адміністративні й державні послуги, подання звернень до органів виконавчої влади, державних органів, органів місцевого самоврядування, підприємств, установ та організацій, отримання відомостей із національних електронних інформаційних ресурсів, а також моніторинг і оцінювання якості послуг. Крім того, міністерство ініціювало та підтримало низку проєктів: «Дія.Цифрова освіта», «Дія.Бізнес», «Безпека дітей в Інтернеті», «Е-резидентство», «Дія.City», «Європейська інтеграція», «Ноутбук кожному вчителю», «Віртуальні активи», «Дія.Платформа центрів» [87; 212].

Мобільний застосунок «Дія» надає громадянам України можливість користуватися електронними документами безпосередньо зі смартфона. Правова сила цифрових документів закріплена такими нормативно-правовими актами:

– електронні паспорти та ІПН: постанова КМУ від 18 серпня 2021 року № 911 [159];

– електронне свідоцтво про народження: постанова КМУ від 23 вересня 2020 року № 911 [173];

– електронний сертифікат: постанова КМУ від 1 жовтня 2014 р. № 509 [169];

– електронний студентський квиток: постанова КМУ від 18 грудня 2019 р. № 1051 [131].

Окремим інституційним елементом цифрової екосистеми України є Комітет Верховної Ради України з питань цифрової трансформації, утворений 29 серпня 2019 р. у складі парламенту 9-го скликання. До предметної сфери його діяльності належать [168; 240]:

– законодавче забезпечення цифровізації та розбудови цифрового суспільства;

– національні та державні програми інформатизації;

– програми ЄС «Єдиний цифровий ринок» (Digital Single Market, EU4Digital) та інші ініціативи цифрового співробітництва;

– інновації у сфері цифрового підприємництва та розвиток стартап-екосистеми;

– дослідницькі центри у галузі цифрових технологій;

– цифрова промисловість і телекомунікації;

– електронне урядування та державні електронні послуги;

– електронна демократія;

– електронні довірчі послуги та цифрова ідентифікація;

– державні інформаційно-аналітичні системи та електронний документообіг;

– державні інформаційні ресурси, електронні реєстри та бази даних;

– електронна комерція та електронний бізнес;

– віртуальні активи, блокчейн і токенізація;

– розумна інфраструктура міст і громад;

– розвиток відкритих даних;

– радіочастотні ресурси;

– орбітальна економіка;

– законодавче регулювання функціонування та використання мережі Інтернет в Україні;

– кібербезпека та кіберзахист, зокрема у сфері критичної інфраструктури;

– технічний і криптографічний захист інформації;

– розвиток цифрових компетентностей і цифрових прав громадян.

Також в Україні для потреб державних органів Постановою Кабінету Міністрів України «Про затвердження Порядку надання послуг Національного центру резервування державних інформаційних ресурсів» від 3 травня 2022 року № 522 [157] запроваджено Національний центр резервування державних інформаційних ресурсів. Національний центр резервування державних інформаційних ресурсів (далі – Національний центр) – це організована сукупність об'єктів, створених для забезпечення надійності та безперебійної роботи державних інформаційних ресурсів, кіберзахисту, зберігання державних електронних інформаційних ресурсів, резервного копіювання інформації та даних державних електронних інформаційних ресурсів державних органів, військових формувань (крім Збройних Сил України та Головного управління розвідки Міністерства оборони України), утворених законами, підприємствами, установами та організаціями. Обов'язки щодо забезпечення функціонування Національного центру покладено на Державну службу спеціального зв'язку та захисту інформації України [140]. Механізм функціонування Національного центру резервування державних інформаційних ресурсів регулюється Законом України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [170] та Постановами Кабінету Міністрів України «Деякі питання функціонування Національного центру резервування державних інформаційних ресурсів» № 311 від 7 квітня 2023 року [41] та «Про затвердження Порядку надання

послуг Національного центру резервування державних інформаційних ресурсів» від 3 травня 2022 року № 522 [157]. Також Постановою Кабінету Міністрів України «Про затвердження Порядку надання послуг Національного центру резервування державних інформаційних ресурсів» від 3 травня 2022 року № 522 визначено порядок надання послуг Національному центру резервування державних інформаційних ресурсів. Зокрема, надаються наступні послуги [157]:

1. Розміщення обладнання в шафі електронного зв'язку або її частині в загальному залі.

2. Розміщення обладнання в шафі електронного зв'язку в екранованому залі.

3. Розміщення обладнання в шафі електронного зв'язку в окремому екранованому залі.

4. Надання у користування дискового простору для технічних засобів зберігання інформації, що знаходиться в загальному залі.

5. Надання у користування дискового простору для технічних засобів зберігання інформації, що знаходиться в екранованому залі.

6. Надання у користування дискового простору для технічних засобів зберігання інформації, що знаходиться в окремому екранованому залі.

7. Надання обчислювальних ресурсів у загальному залі.

8. Надання у користування обчислювальних ресурсів в екранованому залі.

9. Надання обчислювальних ресурсів в окремому екранованому залі.

10. Надання окремого фізичного сервера в оренду.

11. Надання віртуального сервера в користування.

12. Надання у користування динамічно розподілених дискових ресурсів.

13. Резервне копіювання обчислювальних ресурсів, що використовуються для обробки (збереження) національних електронних інформаційних ресурсів.

14. Резервне копіювання національних електронних інформаційних ресурсів, що використовуються для обробки (збереження) національних електронних інформаційних ресурсів.

15. Надання у користування програмного забезпечення з використанням обчислювальних ресурсів.

16. Розміщення національних електронних інформаційних ресурсів.

17. Адміністрування національних електронних інформаційних ресурсів.

18. Зберігання національних електронних інформаційних ресурсів.

19. Підключення до захищених вузлів доступу до мережі Інтернет систем обробки та збереження національних електронних інформаційних ресурсів.

20. Надання захищених каналів зв’язку для організації доступу до національних електронних інформаційних ресурсів.

21. Надання захищених каналів зв’язку для адміністрування національних електронних інформаційних ресурсів.

22. Надання захищеного мобільного доступу до національних інформаційних ресурсів.

23. Відновлення національних електронних інформаційних ресурсів після катастроф (Пункт 23 із змінами, внесеними Постановою Кабінету Міністрів України «Деякі питання функціонування Національного центру резервування державних інформаційних ресурсів» № 311 від 7 квітня 2023 року).

24. Збереження резервних копій національних електронних інформаційних ресурсів.

25. Збереження архівів даних національних електронних інформаційних ресурсів.

26. Виявлення та захист від кібератак (DDoS-атаки та інші).

27. Розгортання моделювання обчислювальних ресурсів об’єкта кіберзахисту.

28. Захист інформації в системі доменних імен користувачів.

29. Виявлення кіберінцидентів та кібератак на обладнання користувачів.

30. Виявлення та запобігання несанкціонованому доступу до мережі передачі даних.

31. Захист інформаційних ресурсів з використанням технічних можливостей мережевого екрану.

32. Захист електронної пошти від зовнішніх кіберзагроз.

33. Управління доступом до мережі передачі даних за допомогою політик безпеки.

34. Управління обліковими записами привілейованих користувачів.

35. Тестування комп'ютерних систем та мереж на вразливість до кібератак.

36. Забезпечення безпечного, ізольованого віртуального середовища для досліджень безпеки комп'ютерних програм.

37. Захист веб-сайтів від кіберінцидентів та кібератак.

38. Забезпечення віртуальних захищених мереж передачі даних.

Крім того, Державна служба спеціального зв'язку та захисту інформації України, для кіберзахисту державних органів та об'єктів критичної інфраструктури, забезпечує реалізацію Національної телекомунікаційної мережі, яка функціонує згідно з Постановою Кабінету Міністрів України «Деякі питання функціонування Національної електронної комунікаційної мережі» від 16 грудня 2020 р. № 1358. Національна телекомунікаційна мережа призначена для [42]:

– обігу (передачі, прийому, створення, обробки, зберігання) та захисту національних інформаційних ресурсів;

– забезпечення захищених електронних комунікацій;

– надання послуг Національної телекомунікаційної мережі (НТМ) в інтересах державного управління в мирний час, у надзвичайних умовах та особливий період;

– надання користувачам послуг кіберзахисту.

Перелік послуг НТМ визначається Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Переліку послуг Національної електронної комунікаційної мережі» від 17 серпня 2021 року № 502. Зокрема, доступні такі групи послуг [153]:

– транспортні послуги електронного зв'язку НТМ;

– послуги спеціального зв'язку;

– мультимедійні послуги НТН;

– послуги доступу до інформаційних ресурсів;

– послуги кіберзахисту.

Окремо варто виділити систему захищеного доступу державних органів до Інтернету Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, який забезпечує безпечний доступ до Інтернету державним органам [140; 154].

Державний центр кіберзахисту також забезпечує функціонування Групи реагування на комп'ютерні надзвичайні ситуації України CERT-UA33, яка обробляє інформацію, отриману від громадян про кіберінциденти [197]. Основними нормативними документами, що регулюють захист інформації в державних органах України, в якості яких вони надають цифрові послуги, та їх реалізацію, є:

– Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 5 липня 1994 року № 80/94-ВР;

– Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» від 29 березня 2006 р. № 373;

– Постанова КМУ «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19 червня 2019 р. № 518;

– Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI;

– Закон України «Про електронну ідентифікацію та електронні довірчі послуги» від 5 жовтня 2017 року № 2155-VIII;

– Постанова Кабінету Міністрів України «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах» від 16 листопада 2002 р. N 1772;

– Постанова Кабінету Міністрів України «Про затвердження Положення про Реєстр інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління» від 3 серпня 2005 року № 688;

– Постанова Кабінету Міністрів України «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації» від 21 лютого 2025 р. № 205;

– Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Порядку формування й користування інформаційним фондом Реєстру інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління» від 24 квітня 2007 року № 72).

Забезпечення кібербезпеки є необхідним компонентом національної безпеки. Виклики та кіберзагрози національному кіберпростору описані в розділі 3 Стратегії кібербезпеки України «безпечний кіберпростір – запорука успішного розвитку країни» (Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 14 травня 2021 року «Про Стратегію кібербезпеки України») та є запорукою успішного розвитку країни. До них належать [174]:

– активне використання кіберзасобів у міжнародній конкуренції;

– конкурентний характер розвитку інструментів кібербезпеки в умовах швидких прогресивних змін в інформаційно-комунікаційних технологіях,

зокрема хмарних та квантових обчислень, мереж 5G, великих даних, Інтернету речей (IoT), штучного інтелекту (ШІ) тощо;

– мілітаризація кіберпростору та розвиток кіберзброї, що дає змогу приховано здійснювати кібератаки для підтримки бойових дій та розвідувально-підривної діяльності в кіберпросторі;

– вплив пандемії COVID-19 на економічну активність та соціальну поведінку, що спричинило швидку трансформацію та реорганізацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційні комп’ютерні системи;

– впровадження нових технологій, цифрових сервісів та механізмів електронної взаємодії між громадянами та державою, які здійснюються безсистемно з точки зору заходів кібербезпеки та без належної оцінки ризиків.

Провідне місце серед загроз кібербезпеці України посідає гібридна агресія російської федерації у кіберпросторі. Держава-агресор послідовно нарощує потенціал наступальної кіберзброї, застосування якої здатне спричинити незворотні та катастрофічні руйнівні наслідки. Головними об'єктами кібератак з боку російської федерації є інформаційні комп'ютерні системи українських державних органів та елементи критичної інформаційної інфраструктури: їх виведення з ладу, встановлення прихованого контролю над ними, а також здійснення розвідувальної та підривної діяльності є пріоритетними цілями агресора. Окрім цього, кібератаки активно інтегруються до арсеналу спеціальних інформаційних операцій, слугуючи інструментом маніпулятивного впливу на суспільну свідомість, деструктивного втручання у виборчі процеси та дискредитації української державності [104; 112].

Окремим актом Рада національної безпеки і оборони України (РНБО) визначила невідкладні заходи щодо нейтралізації загроз кібербезпеці держави. Держава має процедури щодо [188]:

– виявлення вразливостей та недоліків у конфігурації інформації, електронних комунікацій та інформаційних комп’ютерних систем, в яких обробляються державні інформаційні ресурси;

– виявлення вразливостей та реагування на такі кіберінциденти та кібератаки;

– пошуку та виявлення відкритих вразливостей інформації (автоматизовано);

– електронного зв’язку, інформаційних комп’ютерних систем, мережі електронного зв’язку;

– оцінки стану безпеки державних інформаційних ресурсів в інформації, електронному зв’язку та інформаційних комп’ютерних системах;

– скануванні на наявності вразливостей в державних інформаційних ресурсах, розміщених в Інтернеті;

– огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, а також вимог щодо захисту, встановленого законодавством. Зокрема, для забезпечення функціонування системи виявлення вразливостей та реагування на кіберінциденти та кібератаки, присутні комплекти обладнання підсистеми збору телеметричних даних інформаційних комп’ютерних систем (активні датчики). Комплексні огляди стану кіберзахисту доступні у відповідних періодичних звітах Державної служби спеціального зв’язку та захисту інформації України, зокрема:

– «Звіт про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» (Постанова Кабінету Міністрів України від 11 листопада 2020 р. № 1176);

– «Інформаційно-аналітичні матеріали про стан захисту державних електронних інформаційних ресурсів в інформаційних комп’ютерних системах»;

– «Аналітичний звіт про виконання стратегічного плану кібербезпеки України»;

– «Звіт про виконання Державною службою спеціального зв'язку та захисту інформації України завдань, пов'язаних із забезпеченням кібербезпеки держави»;

– «Аналітичний звіт Державної служби спеціального зв'язку та захисту інформації України за результатами дослідження загроз»;

– «Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України;

– «Звіт про подання та подальшу оцінку щорічного звіту про результати незалежного аудиту діяльності основних суб'єктів національної кібербезпеки»;

– «Попередній аналітичний звіт про моніторинг виконання Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII;

– Аналітичний звіт «Норми законодавства Європейського Союзу, які необхідно впровадити в проєкти законів про кібербезпеку та про об'єкти критичної інфраструктури в Україні» (Комітет з питань цифрової трансформації);

– «Найкращі практики управління кібербезпекою».

Публікації аналітичних та статистичних даних про кібератаки та загрози в кіберпросторі здійснюються урядовою групою реагування, CERT-UA та Національним координаційним центром кібербезпеки РНБО.

Питання кіберзахисту критичної інфраструктури регулюється Законом України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX, Постановою Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19 червня 2019 року № 518, Постановою Кабінету Міністрів України «Деякі питання об'єктів

критичної інфраструктури» від 9 жовтня 2020 р. № 1109, Постановою КМУ «Деякі питання об’єктів критичної інформаційної інфраструктури» від 9 жовтня 2020 року № 943, Наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 15 січня 2021 року № 23 «Про затвердження Методичних рекомендацій щодо категоризації об’єктів критичної інфраструктури», Наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу» від 30 серпня 2023 року № 773, Наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України «Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами» від 29 травня 2023 року № 463.

Сформовано рекомендації щодо підготовки плану захисту об'єктів критичної інфраструктури на підставі проєктної загрози національного рівня «кібератака/кіберінцидент» та відповідного шаблону такого плану. Правовий статус об'єкта критичної інфраструктури набувається після офіційного підтвердження факту включення відомостей про нього до державного реєстру критичної інфраструктури.

Діяльність постачальників хмарних послуг в Україні регулюється Законом України «Про хмарні послуги» від 17 лютого 2022 року № 2075-IX [185]. Цей Закон визначає правовідносини, що виникають при наданні хмарних послуг, та встановлює особливості використання хмарних сервісів органами державної влади, органами місцевого самоврядування, військовими формуваннями, утвореними законами України, державними підприємствами, установами та організаціями суб’єктами владних повноважень та іншими суб’єктами, яким делеговано такі повноваження. Згідно з частиною другою статті 8 Закону, для надання хмарних послуг та/або послуг центру обробки даних публічним користувачам та/або об’єктам критичної інфраструктури, інформація про постачальників хмарних послуг та/або послуг центру обробки

даних має бути включена до переліку. Частиною першою статті 12 Закону встановлюється порядок надання хмарних послуг та/або послуг центру обробки даних, пов’язаних з обробкою державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, на основі принципів взаємодії та збереження конкуренції, та визначає порядок [185]:

– обов’язкового резервного копіювання та зберігання резервних копій у незалежних системах;

– передачі даних від користувача хмарних послуг до постачальника хмарних послуг та/або послуг центру обробки даних для забезпечення надання хмарних послуг, а також від постачальника хмарних послуг до користувача хмарних послуг;

– передачі даних від одного постачальника хмарних послуг та/або послуг центру обробки даних до іншого;

– надання інформації, необхідної для оцінки безпеки мережевих та інформаційних систем постачальників хмарних послуг та/або послуг центру обробки даних, включаючи задокументовані політики безпеки.

Частина друга статті 12 Закону встановлює вимоги до положень, які повинні міститися в процедурі надання хмарних послуг та/або послуг центру обробки даних. Такий порядок повинен містити [185]:

– вимоги до передачі даних у структурованій формі, загальновживаних та машинозчитуваних форматах;

– вимоги до обсягу інформації щодо процесів, технічних вимог, умов та платежів, що застосовуються у разі переходу до іншого постачальника хмарних послуг та/або послуг центру обробки даних або відмови від хмарних послуг, яка має бути надана користувачеві хмарних послуг у зрозумілій та доступній формі для визначення переможця процедури закупівлі (спрощена процедура закупівлі);

– підходи, що сприяють порівнянню хмарних послуг та/або послуг центру обробки даних і хмарної інфраструктури, включаючи, зокрема,

інформацію про управління якістю, управління інформаційною безпекою, управління безперервністю послуг та оцінку впливу на навколишнє середовище.

Стаття 8 Закону України «Про хмарні послуги» від 17 лютого 2022 року № 2075-IX [185] вимагає від постачальника хмарних послуг та/або послуг центру обробки даних виконання кількох вимог. Постачальник хмарних послуг та/або послуг центру обробки даних повинен вживати відповідних, пропорційних технічних та організаційних заходів для управління ризиками, що виникають для безпеки електронної комунікаційної мережі та тих електронних комунікаційних послуг та інформаційних систем, що використовуються для надання хмарних послуг. Такі заходи повинні забезпечувати рівень безпеки електронної комунікаційної мережі, електронних комунікаційних послуг та інформаційних систем, що використовуються для надання хмарних послуг, що відповідає виниклому ризику, та повинні враховувати такі елементи [185]:

– безпека систем та обладнання;

– врегулювання інцидентів;

– управління безперервністю бізнесу;

– моніторинг, аудит та тестування;

– відповідність міжнародним стандартам.

На постачальників хмарних послуг та послуг центрів обробки даних покладається обов'язок невідкладного інформування регулятора послуг зв'язку та CERT-UA про будь-який інцидент, що суттєво порушує або унеможливлює надання відповідних послуг. Таке повідомлення здійснюється у порядку, встановленому регулятором послуг зв'язку.

Постачальник хмарних послуг та/або послуг центру обробки даних повинен [185]:

– надавати державному органу, визначеному для формування та реалізації державної політики у сфері кіберзахисту, інформацію, необхідну для оцінки безпеки мережі електронного зв’язку та послуг електронного

зв’язку та інформаційних систем, включаючи задокументовану політику безпеки;

– усувати будь-які невідповідності вимогам, затвердженим регулятором послуг зв’язку.

Постанова КМУ від «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану» 12 березня 2022 року № 263 [37] передбачає, що в період дії воєнного стану міністерства, інші центральні та місцеві органи виконавчої влади, державні та комунальні підприємства, установи та організації, що належать до сфери їх управління, повинні забезпечити належне функціонування інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, публічних електронних реєстрів як власники (володільці) та/або розпорядники, а також захист будь-якої інформації, що в них обробляється. З цією метою вони можуть вживати таких додаткових заходів [37]:

– розміщувати державні інформаційні ресурси та публічні електронні реєстри на хмарних ресурсах та/або в центрах обробки даних, розташованих за межами України, та реєструвати доменні імена в домені gov.ua для кожного такого розміщення;

– створювати додаткові резервні копії державних інформаційних ресурсів та публічних електронних реєстрів з дотриманням вимог щодо цілісності, конфіденційності та доступності, встановлених для таких ресурсів;

– зупиняти та обмежувати роботу інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, а також публічних електронних реєстрів.

Міністерства, інші центральні та місцеві органи виконавчої влади, державні та комунальні підприємства, установи та організації, що належать до сфери їх управління, можуть використовувати хмарні ресурси та/або центри обробки даних, розташовані за межами державного кордону України, безкоштовно або за плату за користування публічними електронними

реєстрами як власниками (володільцями) та/або розпорядниками, а також за захист будь-якої інформації, що обробляється в них. З цією метою вони можуть вживати таких додаткових заходів [37]:

– розміщувати державні інформаційні ресурси та публічні електронні реєстри на хмарних ресурсах та/або в центрах обробки даних, розташованих за межами України, та реєструвати доменні імена в домені gov.ua для кожного такого розміщення;

– створювати додаткові резервні копії державних інформаційних ресурсів та публічних електронних реєстрів з дотриманням вимог щодо цілісності, конфіденційності та доступності, встановлених для таких ресурсів;

– зупиняти та обмежувати роботу інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, а також публічних електронних реєстрів.

Міністерствам та іншим центральним і місцевим органам виконавчої влади визначено строк у шість місяців із моменту скасування або припинення воєнного стану для завершення реалізації зазначених заходів. Одночасно на них покладається обов'язок невідкладного інформування Апарату Комітету Верховної Ради України з питань цифрової трансформації та Міністерства цифрової трансформації України про факт їх припинення.

На стратегічному рівні координацію з питань кібербезпеки здійснює Національний координаційний центр кібербезпеки (далі – НКЦКБ) РНБО, який є робочим органом РНБО, утвореним рішенням Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 27 січня 2016 року та введеним у дію Указом Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15 березня 2016 року № 96 [176]. НКЦКБ функціонує відповідно до Положення про Національний координаційний центр кібербезпеки, затвердженого Указом Президента України «Про Національний координаційний центр кібербезпеки» від 7 червня 2016 року № 242/2016 [137]. НКЦКБ координує лише діяльність основних суб’єктів

кібербезпеки, а його рішення є обов'язковими для розгляду, але не для виконання всіма державними органами.

НКЦКБ затвердив процедуру взаємодії суб'єктів кібербезпеки під час будь-якого реагування на кіберінциденти/кібератаки. НКЦКБ взаємодіє з CCDCOE НАТО (англ. – the NATO Cooperative Cyber Defence Centre of Excellence) через Технічну угоду, яка включає взаємодію з країнами НАТО та країнами-партнерами, представленими в CCDCOE НАТО [19; 209].

Державна служба спеціального зв'язку та захисту інформації України – це державний орган, призначений для забезпечення функціонування та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового польового зв'язку, активної протидії агресії в кіберпросторі, а також інших завдань, передбачених законодавством [140; 154].

Впровадження об'єктів державної безпеки як складової Національної системи кібербезпеки здійснюється Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, який забезпечує створення та функціонування:

– основних компонентів системи захищеного доступу державних органів до мережі Інтернет;

– системи антивірусного захисту національних інформаційних ресурсів;

– аудиту інформаційної безпеки та стану кіберзахисту інфраструктури критичних інформаційних об'єктів;

– системи виявлення вразливостей та реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту;

– системи взаємодії команд, що реагують на комп'ютерні надзвичайні ситуації, а також у співпраці з іншими суб'єктами кібербезпеки щодо розробки сценаріїв реагування на кіберзагрози, заходів протидії таким загрозам, програм і методів кібернавчання.

Завданнями Урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA є [3; 140]:

– накопичення та аналіз даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

– надання практичної допомоги власникам об’єктів кіберзахисту з питань запобігання, виявлення та ліквідації наслідків кіберінцидентів стосовно цих об’єктів;

– організація та проведення практичних семінарів з питань кіберзахисту для суб’єктів національної системи кібербезпеки та власників об’єктів кіберзахисту;

– підготовка та розміщення на своєму офіційному вебсайті рекомендацій щодо боротьби із сучасними видами кібератак та кіберзагрозами;

– взаємодія з правоохоронними органами, надання їм своєчасної інформації про кібератаки;

– взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти інформаційної безпеки FIRST зі сплатою щорічних членських внесків;

– взаємодія з українськими командами реагування на комп’ютерні надзвичайні ситуації, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які здійснюють діяльність, пов’язану із забезпеченням безпеки кіберпростору;

– обробка інформації, отриманої від громадян, про кіберінциденти щодо об’єктів кіберзахисту;

– сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним законом, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

Також важливою міжнародною взаємодією є участь CERT-UA у Форумі команд реагування на інциденти інформаційної безпеки FIRST та Trusted Introducer (TF-CSIRT) [209; 233].

Обмін інформацією про кіберінциденти здійснюється за Загальними правилами обміну інформацією про кіберінциденти (Протокол TLP), затвердженими на засіданні РНБО. Реагування суб'єктів кібербезпеки на різні типи подій у кіберпросторі регулюється Постановою Кабінету Міністрів України «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» від 4 квітня 2023 року № 299 з урахуванням відповідних методичних рекомендацій, затверджених Наказом Адміністрації Державної служби спеціального зв'язку на захисту інформації України «Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» від 3 липня 2023 року № 570 [40]. Водночас це питання також регулюється Постановою КМУ «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах» від 16 листопада 2002 р. N 1772 [156].

Для управління кризами в кіберпросторі розроблено та введено в експлуатацію сучасну інформаційно-аналітичну систему у складі Головного ситуаційного центру країни «СОТА» у складі Апарату РНБО України. Створено Ситуаційний центр кібербезпеки СБУ, а одним із рішень передбачається створення ситуаційного центру кібербезпеки, зокрема в галузі енергетики. Наразі фахівці Апарату РНБО України разом із зацікавленими міністерствами та відомствами працюють над виконанням рішення Ради національної безпеки і оборони України «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони» від 4 червня 2021 року, введеного в дію Указом Президента України «Про рішення Ради національної безпеки і оборони України від 4 червня 2021 року «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони»» від 18 червня 2021

року № 260/2021 [178], у частині програмного впровадження інформаційно-аналітичної системи «СОТА» в єдину мережу державних ситуаційних центрів.

Війська зв'язку та кібербезпеки Збройних Сил України – це спеціальні сили Збройних Сил України, на які покладено завдання забезпечення функціональності систем зв'язку та інформації на додаток до систем бойового управління та оповіщення, а також їх розширення в мирний час. У цей особливий період, за якого панують умови надзвичайного та воєнного стану, вони повинні вирішувати завдання забезпечення управління військами Збройних Сил України, а також здійснення заходів щодо функціонування національної системи кібербезпеки України [92; 167]. Головне управління зв'язку та кібербезпеки Генерального штабу Збройних Сил України є структурним підрозділом Генерального штабу Збройних Сил України та відповідає за системи зв'язку Збройних Сил України, які призначені для управління системами зв'язку Збройних Сил України, організації їх функціонування, планування заходів щодо їх розширення та масштабування, організації, управління кібербезпекою у Збройних Силах України, захисту інформації в системах зв'язку Збройних Сил України (СЗ Збройних Сил України) та кіберзахисту СЗ Збройних Сил України як у мирний час, так і в будь-який особливий період воєнного стану, планування зв'язку та оборонних кібероперацій Збройних Сил України (участь Збройних Сил України в оборонних кіберопераціях сил оборони) під час стратегічного планування застосування Збройних Сил України, інших складових сил оборони, розвитку системи зв'язку Збройних Сил України, планування забезпечення Збройних Сил України технікою та майном зв'язку. Головне управління зв'язку та кібербезпеки Генерального штабу Збройних Сил України є центральним органом секретного зв'язку Збройних Сил України та головним органом з організації забезпечення польового та поштового зв'язку Збройних Сил України. Головне управління зв'язку та кібербезпеки Генерального штабу Збройних Сил України підпорядковується начальнику Генерального штабу Збройних Сил України. Діяльність Головного управління зв'язку та

кібербезпеки Генерального штабу Збройних Сил України безпосередньо спрямовується, координується та контролюється заступником начальника Генерального штабу Збройних Сил України шляхом розподілу повноважень. Основними завданнями Головного управління зв'язку та кібербезпеки Генерального штабу Збройних Сил України є [167]:

– планування, організація експлуатація та здійснення управління мережею електронного зв'язку Збройних Сил України, організація її розширення та масштабування;

– планування, організація та забезпечення функціонування систем спеціального зв'язку Збройних Сил України, включаючи моніторинг стану організації та забезпечення безпеки спеціального (секретного) зв'язку та криптографічного захисту службової інформації;

– планування, організація та управління інформаційно-комунікаційними системами Збройних Сил України, організація основних та функціональних послуг для керівництва Збройних Сил України, органів військового управління та інших військових організаційних структур Збройних Сил України;

– організація та управління кібербезпекою Збройних Сил України, захист інформації в інформаційно-комунікаційних системах Збройних Сил України та кіберзахист ІКС Збройних Сил України, організація та підготовка оборонних кібероперацій Збройних Сил України, а також участь Збройних Сил України в оборонних кіберопераціях сил оборони;

– планування, організація функціонування та здійснення управління функціонуванням систем польової служби та поштового зв'язку у складі Збройних Сил України;

– планування зв'язку під час стратегічного планування застосування Збройних Сил України та інших складових сил оборони;

– планування забезпечення органів військового управління, військових частин та підрозділів Збройних Сил України технікою та майном (послугами) зв'язку, а також майном польового та поштового зв'язку;

– планування та безпосереднє виконання заходів щодо розвитку системи зв’язку Збройних Сил України.

Головне управління радіоелектронної та кіберборотьби Генерального штабу Збройних Сил України (далі – Головне управління) призначене для [167]:

– організації виконання завдань, пов’язаних з плануванням кібероборони України;

– плануванням та веденням радіоелектронної війни та кібервійни;

– управлінням радіочастотним спектром та розвитком відповідних можливостей.

Основними завданнями Головного управління є:

– планування, організація, підготовка та ведення кібервійни в інтересах стратегічного застосування Сил оборони України та інших складових сил оборони;

– планування та координація дій кібероборони України, органів державної влади та складових сектору безпеки і оборони;

– планування, організація підготовки та ведення радіоелектронної війни в інтересах стратегічного застосування Збройних Сил України та інших складових сил оборони;

– реалізація повноважень Генерального штабу щодо управління у сфері використання радіочастотного спектру спеціальними користувачами Законом України «Про електронні комунікації» від 16 грудня 2020 року № 1089-IX.

Головне управління зв’язку та кібербезпеки Генерального штабу Збройних Сил України також відповідає за [167]:

– організацію кіберзахисту мереж Збройних Сил, організацію та підготовку оборонних кібероперацій Збройних Сил України, а також участь Збройних Сил України в оборонних кіберопераціях сил оборони;

– планування, організацію функціонування та здійснення управління функціонуванням систем польової служби та поштового зв’язку у складі Збройних Сил України;

– планування зв’язку під час стратегічного планування застосування Збройних Сил України та інших складових сил оборони;

– планування забезпечення органів військового управління, військових частин та підрозділів Збройних Сил України технікою та майном (послугами) зв’язку, а також майном польового та поштового зв’язку;

– планування та безпосереднє здійснення заходів щодо розвитку системи зв’язку Збройних Сил України.

20 квітня 2025 року набрав чинності новий Закон України «Про кібербезпеку». Закон запроваджує суттєві інституційні, процедурні та пов’язані з дотриманням вимог зміни до нормативно-правової бази України у сфері кібербезпеки, що може мати наслідки для іноземних постачальників хмарних послуг, IT-рішень та технологій критичної інфраструктури, які співпрацюють органами державної влади та місцевого самоврядування або критично важливими секторами в Україні. Закон також спрямований на узгодження українського законодавства з Директивою NIS 2 (мережева та інформаційна безпека) [19; 209].

Раніше системи державного сектору, що обробляють секретну або службову інформацію, повинні були впроваджувати так звану Комплексну систему захисту інформації (далі – КСЗІ), сертифіковану Державною службою спеціального зв’язку та захисту інформації України [75; 219].

Структура КСЗІ широко вважалася застарілою та неадекватно пристосованою для боротьби з сучасними загрозами та узгодження з найкращими практиками кібербезпеки.

Новий Закон модернізує цей підхід, замінюючи КСЗІ системою «авторизації безпеки». Авторизація безпеки, по суті, є офіційним рішенням, прийнятим державною установою, яке підтверджує, що система працюватиме

відповідно до законодавчих вимог, національних стандартів та нормативних документів у сферах технічного, криптографічного та кіберзахисту.

Згідно з новою структурою, заходи безпеки повинні впроваджуватися та підтримуватися протягом усього життєвого циклу системи на основі визначених профілів безпеки: базового, цільового та секторального. Базовий профіль безпеки визначається Державною службою спеціального зв'язку та захисту інформації України, секторальний профіль встановлюється спільно секторальним регулятором та Державною службою спеціального зв'язку та захисту інформації України, тоді як цільовий профіль розробляється конкретним державним органом після оцінки ризиків системи та на основі базового або секторального профілю безпеки [93; 219].

На відміну від попередньої сертифікації КСІБ Державною службою спеціального зв'язку та захисту інформації України, новий режим дозволяє власнику або адміністратору системи підготувати декларацію про авторизацію безпеки системи.

Це знаменує собою зміщення відповідальності до власників систем та відображає більш децентралізований, ризик-орієнтований підхід.

Як альтернативу авторизації безпеки для систем, що не обробляють державну таємницю, Закон дозволяє сертифікацію відповідності стандартам інформаційної безпеки. Сертифікація має бути видана органом з оцінки відповідності, акредитованим національним органом з акредитації України, або іноземним національним органом з акредитації, визнаним в Україні через членство в міжнародних або регіональних організаціях з акредитації, які мають угоди про взаємне визнання.

Закон забороняє використання програмного забезпечення та мережевого (комунікаційного) обладнання, включеного до загальнодоступного переліку заборонених продуктів, для систем обробки державних інформаційних ресурсів, включаючи державну таємницю та службову інформацію, або систем підтримки критичної інформаційної інфраструктури.

Крім того, технічні та криптографічні засоби захисту, що використовуються в системах державного сектору, повинні пройти оцінку безпеки. Для систем, що потребують авторизації безпеки або сертифікації відповідності, такі засоби повинні бути сертифіковані Державною службою спеціального зв'язку та захисту інформації України (для систем обробки секретних даних) або мати визнаний документ про відповідність від акредитованого органу оцінки (для несекретних систем).

Державна служба спеціального зв'язку та захисту інформації України залишається ключовим регулятором кібербезпеки з розширеними мандатами згідно з новим Законом [165]. Його обов'язки включають розробку політики, встановлення стандартів, контроль та нагляд, аналіз загроз, координацію реагування на інциденти (включаючи CERT-UA – команду реагування на комп'ютерні надзвичайні події), визначення та затвердження базових та секторальних профілів безпеки, ведення репозиторію кіберінцидентів [140; 154].

Національний банк України встановлює вимоги щодо кібербезпеки для фінансових та платіжних систем, що підпадають під його юрисдикцію.

Міністерство оборони та Служба безпеки України відповідають за визначення профілів безпеки для військових та національних систем безпеки.

Структура відповідності вимогам щодо авторизації безпеки та альтернативної сертифікації також застосовується до систем критичної інформаційної інфраструктури, що належать державному сектору.

Крім того, власники та оператори таких систем повинні повідомляти про значні інциденти безпеки, забезпечувати безпечне резервне копіювання державних даних та перевіряти, чи не розташовані жодні компоненти системи на окупованих територіях або в державах-агресорах.

Закон запроваджує нові вимоги до постачальників товарів, робіт чи послуг, що підтримують державні інформаційні системи або критичну інформаційну інфраструктуру.

Зокрема, постачальники повинні впроваджувати заходи безпеки, пропорційні ризику, який становлять їхні товари, роботи чи послуги.

Державна служба спеціального зв'язку та захисту інформації України має завдання визначити критерії критичності таких товарів, робіт та послуг, встановити процедури оцінки ризиків власниками/керівниками відповідних систем, визначити відповідні заходи безпеки та окреслити процес для постачальників, щоб продемонструвати відповідність цим вимогам безпеки [93; 140].

Закон встановлює багаторівневу національну систему реагування на кіберінциденти, атаки та загрози з визначеними ролями для Державної служби спеціального зв'язку та захисту інформації України, CERT-UA та секторальних/регіональних груп реагування. Ця система має покращити координацію та можливості швидкого реагування.

Новий Закон має значні наслідки як для державних установ, так і для зацікавлених сторін приватного сектору, особливо тих, хто пов'язаний з критично важливою інформаційною інфраструктурою.

Хоча це стосується переважно українських організацій, іноземні постачальники продуктів кібербезпеки повинні забезпечити проходження ними необхідної сертифікації, якщо їх буде розгортано в українських мережах державного сектору або критичних інформаційних інфраструктурах, що експлуатуються організаціями державного сектору.

Хоча Закон встановлює загальні рамки, багато його положень потребують подальшої імплементації через підзаконні акти. Очікується, що згідно з новим Законом буде прийнято понад 30 імплементаційних актів. Ці акти надалі формуватимуть практичний ландшафт комплаєнсу в Україні та можуть вимагати коригування стратегій комплаєнсу відповідними зацікавленими сторонами.

Таким чином, організаційно-правовий механізм управління інформаційною безпекою України в умовах гібридних загроз являє собою комплексну багаторівневу систему, що охоплює інституційні, нормативні та

технологічні складові. Ключовими елементами цієї системи є Міністерство цифрової трансформації України як провідний орган цифровізації державного управління, Державна служба спеціального зв'язку та захисту інформації України як головний регулятор у сфері кіберзахисту, Національний координаційний центр кібербезпеки РНБО як стратегічний координатор, а також CERT-UA як оперативний центр реагування на кіберінциденти. Прийняття у 2025 році нового Закону України «Про кібербезпеку» знаменує якісно новий етап у розвитку національної системи кібербезпеки – перехід від застарілої моделі сертифікації до ризик-орієнтованого підходу, що відповідає стандартам Європейського Союзу та вимогам Директиви NIS 2. Водночас ефективність функціонування зазначеного механізму в умовах повномасштабної збройної агресії потребує подальшого вдосконалення міжвідомчої координації, розширення державно-приватного партнерства у сфері кіберзахисту та забезпечення сталого фінансування розвитку цифрової інфраструктури держави.

### 2.2. Оцінювання поточних викликів та суперечностей управління інформаційною безпекою України в умовах гібридних загроз

Нинішній стан системи управління інформаційною безпекою України позначений внутрішньою суперечністю між вагомими здобутками у сфері кіберзахисту та глибинними системними проблемами, загостреними умовами повномасштабного збройного протистояння. Позитивний вимір представлений розбудованою інституційною архітектурою кібербезпеки, прийнятою стратегічною та нормативно-правовою базою, що узгоджується з провідними міжнародними стандартами, а також унікальними практичними компетентностями, здобутими в ході реального протиборства з кібератаками в умовах гібридної війни. Водночас хронічна недостатність фінансування галузі, гострий дефіцит фахівців належної кваліфікації, низький рівень міжвідомчої координації між суб'єктами кібербезпеки та критична залежність

від зарубіжних постачальників кіберрішень суттєво послаблюють захисний потенціал наявних механізмів охорони інформаційного простору держави. Всебічне осмислення цих викликів і суперечностей є необхідною аналітичною передумовою для розроблення виважених і науково обґрунтованих рекомендацій з удосконалення публічного управління у сфері інформаційної безпеки України.

Правовою основою формування системи інформаційної безпеки України слугує Доктрина інформаційної безпеки, затверджена Указом Президента України від 15 березня 2016 року № 96 [177]. Упродовж усього періоду її втілення послідовно здійснювалася розбудова національної системи кібербезпеки. Визначальним кроком у процесі її інституційного оформлення стало ухвалення Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [170], який заклав правові та організаційні підвалини захисту інтересів особи, суспільства і держави в кіберпросторі, окреслив цілі, напрями та принципи державної кібербезпекової політики, розмежував повноваження органів влади, суб'єктів господарювання та громадян у цій галузі, а також визначив засади координації їхньої спільної діяльності. Законом удосконалено нормативне підґрунтя кіберзахисту об'єктів критичної інформаційної інфраструктури, врегульовано порядок їх ідентифікації та встановлено загальні вимоги до їх захисту.

У Державній службі спеціального зв'язку та захисту інформації, Службі безпеки України, Національному банку, Міністерстві інфраструктури, Міністерстві оборони та Збройних Силах України сформовано спеціалізовані центри і підрозділи кібербезпеки та кіберзахисту. Паралельно ведеться розроблення науково-технічних матеріалів, функціонує Національний центр резервування державних інформаційних ресурсів, діє система виявлення вразливостей і реагування на кіберінциденти, а урядова команда реагування на комп'ютерні надзвичайні події CERT-UA забезпечує оперативне усунення кіберзагроз. З метою посилення координації між суб'єктами сектору безпеки та оборони у кіберсфері при РНБО створено Національний координаційний

центр кібербезпеки, рішення якого спрямовані на розв'язання найгостріших проблем галузі.

Активно розширюється міжнародний вимір кібербезпекового співробітництва – із США, Великою Британією, Німеччиною, Нідерландами, Японією та іншими державами, поглиблюється взаємодія з ЄС і НАТО, проводяться спільні навчання з іноземними партнерами. Запроваджено щорічний Місяць кібербезпеки. Указом Президента України від 26 серпня 2021 року № 447/2021 [174] затверджено нову Стратегію кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни», яка розширює коло учасників захисту кіберпростору, залучаючи поряд із профільними державними органами суб'єктів господарювання, громадські об'єднання та пересічних громадян. Провідну координаційну роль у цьому процесі відіграватиме Національний координаційний центр кібербезпеки.

Поряд із цим зазначений орган відповідає за мобілізацію необхідних сил, засобів і ресурсів для забезпечення діяльності національної системи кібербезпеки, а також визначає вимоги до функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури, за винятком об'єктів банківської системи України. Підґрунтям для розбудови системи кібербезпеки держави слугує оперативно-тактичний план, розроблений фахівцями Державної служби спеціального зв'язку та захисту інформації України з урахуванням [90; 92]:

– п'ятирічного досвіду практичного застосування норм і положень чинного законодавства у відповідній сфері;

– накопиченого досвіду формування національної системи кібербезпеки;

– порівняльного аналізу переваг і недоліків моделей кібербезпеки зарубіжних держав;

– практики організації роботи в цій галузі та налагодження взаємодії між суб'єктами кібербезпеки.

Оперативно-тактичний план являє собою комплекс заходів, сил і засобів кіберзахисту, призначених для оперативного реагування на кібератаки та

кіберінциденти кризового характеру, а також для впровадження контрзаходів, що мінімізують вразливість систем зв'язку [93, с. 61]. Відповідне Положення закріплює модель плану, його місію, склад, структуру, механізм функціонування та цільові орієнтири. Вперше на нормативному рівні закріплено визначення сил і засобів кіберзахисту, груп реагування на комп'ютерні надзвичайні події та поняття кібергігієни.

Архітектура оперативно-тактичного плану є багаторівневою і охоплює три взаємопов'язані інфраструктури з відповідними секторами, рівнями та елементами. Верхній щабель займає організаційно-управлінська інфраструктура, що об'єднує суб'єктів кібербезпеки, відповідальних за формування та реалізацію державної політики в цій галузі. Середній щабель утворює технологічна інфраструктура як сукупність сил, засобів кіберзахисту та їх ресурсного забезпечення. Фундаментальний щабель представлений базовою інфраструктурою, що охоплює об'єкти критичної інформаційної інфраструктури та їх критичні активи, суб'єктів господарювання, громадян України та їх об'єднання, а також інших осіб, що провадять відповідну діяльність або надають профільні послуги [91; 92]. Положення про Оперативно-тактичний план визначає, що його впровадження спрямоване на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів та мінімізацію вразливості систем зв’язку. Положення про Оперативно-тактичний план окреслює [40; 152]:

– цілісну, несуперечливу, структуровану систему, об’єднану єдиною ідеєю;

– позиціонування кожного суб’єкта національної системи кібербезпеки в ній;

– характер зв’язків з іншими суб’єктами;

– форми взаємодії між різними суб’єктами одного чи інших рівнів моделі;

– напрямки обміну інформацією;

– основні етапи управління кіберінцидентами;

– основні механізми запобігання, виявлення та ідентифікації;

– реагування на кіберінциденти та кібератаки та відновлення після них. Положення про Оперативно-тактичний план чітко сформулювало екосистему кібербезпеки, в якій усі учасники тісно пов’язані один з одним та доповнюють діяльність одне одного; при цьому характер взаємовідносин переважно має форму партнерства, а не адміністративного командування. Оперативно-тактичний план складається з організаційно-управлінської, технологічної та базової інфраструктури кіберзахисту та впроваджується для забезпечення функціонування національної системи кібербезпеки. Організаційно-управлінська інфраструктура кіберзахисту складається з таких секторів:

– загальнодержавного, що включає основних суб’єктів національної системи кібербезпеки, сили безпеки та оборони, а також Національний координаційний центр кібербезпеки як робочий орган;

– галузевого, що включає центральні органи виконавчої влади, інші державні органи, що забезпечують формування та/або реалізацію державної політики в одній або кількох сферах, або безпосередньо здійснюють заходи щодо забезпечення кібербезпеки за своєю компетенцією, та об’єкти критичної інфраструктури незалежно від форми власності;

– регіонального (місцевого), що включає місцеві органи виконавчої влади, органи місцевого самоврядування, підприємства, установи та організації незалежно від форми власності, що здійснюють діяльність у сфері захисту інформації та кіберзахисту;

– освіти та науки, що включає науково-дослідні установи, заклади вищої освіти у сфері захисту інформації та кібербезпеки, а також ті, що беруть участь у підготовці, підвищенні та перепідготовці професійних кадрів;

– приватного, що включає підприємства недержавної форми власності, організації та установи, що здійснюють захист інформації та кіберзахист (крім об’єктів критичної інфраструктури);

– громадськості, що включає громадські організації, спілки, асоціації, союзи та експертів у сфері кібербезпеки, а також міжнародні та міжурядові організації, що здійснюють свою діяльність у сфері кібербезпеки.

Призначенням базової інфраструктури кіберзахисту є гарантування захисту життєво важливих інтересів особистості, суспільства і держави, а також національних інтересів України в кіберпросторі.

Нарощування потенціалу національної системи кібербезпеки постає нині як першочергове завдання для забезпечення стабільного та захищеного функціонування критичної інформаційної інфраструктури держави в кіберсередовищі. Саме для цього оперативно-тактичний план пропонує відповідне прикладне рішення. Його нормативна сутність полягає у створенні організаційних умов для консолідації зусиль усіх суб'єктів кібербезпеки навколо спільного завдання підвищення кіберстійкості критичної інформаційної інфраструктури. Остання охоплює не лише об'єкти критичної інфраструктури, а й комунікаційно-інформаційні та інші системи, безперебійність і надійність функцій яких є визначальною умовою діяльності органів державної влади, підприємств, установ і організацій усіх форм власності, а також громадських об'єднань [89; 92].

Практичне втілення Стратегії забезпечується на підставі рішення Ради національної безпеки і оборони України «Про План реалізації Стратегії кібербезпеки України» від 30 грудня 2021 року, введеного в дію Указом Президента України від 1 лютого 2022 року № 37/2022. Цим документом на Адміністрацію Державної служби спеціального зв'язку та захисту інформації України покладено обов'язок підготовки та подання уряду проєктів нормативних актів, необхідних для реалізації Плану, а також забезпечення КМУ та Апарату РНБО піврічної звітності про хід його виконання.

У межах реалізації Плану активно виконуються 90 із 94 передбачених завдань. Аналіз стану їх виконання станом на перше півріччя 2023 року засвідчує таку картину [90; 92]:

– 5% завдань перебували на стадії «дуже обмеженого прогресу», що на 5% менше порівняно з 2022 роком;

– 13% перебували на стадії «початкового прогресу», скоротившись на 2% відносно попереднього року;

– 36% знаходилися на стадії «прискорення прогресу», зменшившись на 2% порівняно з 2022 роком;

– 42% досягли стадії «поступового досягнення запланованих результатів», що на 12% перевищує показник 2022 року.

Необхідно зазначити, що кібер-агресія росії проти України актуалізує необхідність розвитку вітчизняного ринку кібербезпеки.

На сучасному етапі ринок кібербепеки України передбачає наявність визначеного переліку кіберрішень – продуктів або послуг, котрі є адаптованими до унікальних вимог організацій з прийняттям до уваги їх ризикових ландшафтів та безпекових стратегій. Зокрема, подібні кіберрішення передбачають [66; 83]:

– безпеку додатків – комплекс методів захисту для забезпечення безпеки програмного забезпечення від загроз зовнішнього походження, а також несанкціонованого доступу до нього;

– хмарну безпеку – комплекс практик захисту в хмарних середовищах публічного, приватного і гібридного типу , орієнтованих на забезпечення безпеки даних, додатків і IT-систем від ризику витоку інформації та кіберзагроз;

– безпеку даних – комплекс заходів, орієнованих на цілісність, конфіденційність, доступність чутливих даних, що передбачає наявність контроль процесів шифрування та доступу для запобігання крадіжкам та випадкам несанкціонованого доступу;

– мережеву безпеку – комплекс процедур і технологій, котрі забезпечують захист мереж від несанкціонованого доступу до даних;

– безпеку кінцевих точок – комплекс заході щодо захисту кінцевих точок, зокрема, мобільних пристроїв, сервері, робочих станцій, від

різнохарактерних атак, із застосуванням сучасних засобів антивірусного захисту та рішень проти загроз нульового дня;

– комплекс додаткових рішень, які орієнтовані на ідентифікацію ризиків та управління ними, що, своєю чергою, дозволяє підтримувати відповідність нормативним вимогам щодо захисту від ризиків доступу.

Порівняльну характеристику кіберінцидентів, зареєстрованих в Україні протягом 2022–2023 рр., показано на рисунку 2.1.

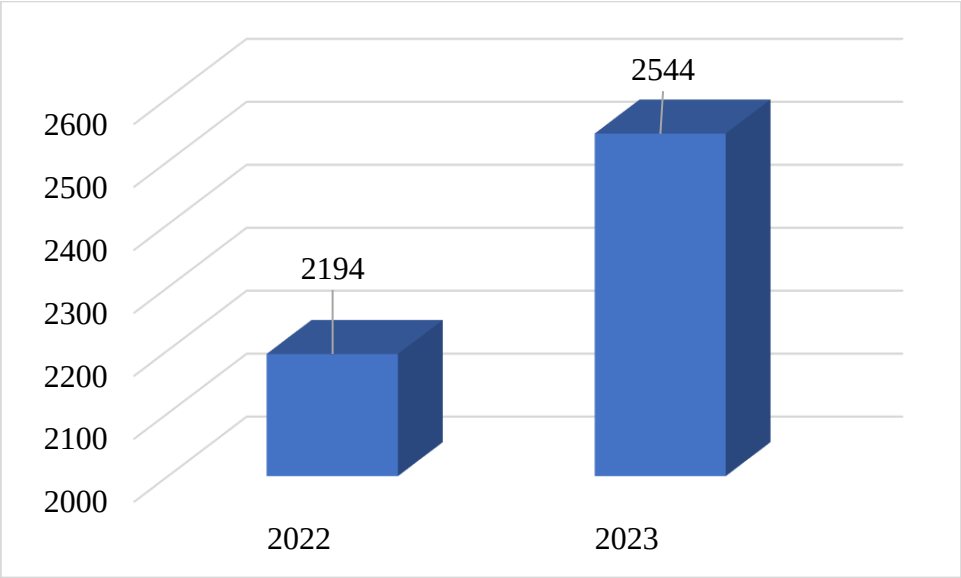


Рис. 2.1. Кількість зареєстрованих кіберінцидентів в Україні

*Джерело: складено на підставі [66; 197]*

З рисунку 2.1 можна побачити, що у 2023 році кількість зареєстрованих кіберінцидентів в Україні збільшилася на 16%. При цьому найбільшим і найактивнішим хакерським угрупуванням росії залишається UAC-0010, яке здійснило 76 кібератак тільки за І півріччя 2022 року та 94 кібератаки – протягом І півріччя 2023 року. При цьому до основних секторів, котрі підлягали кібератакам росії у 2022 році, відносяться ті, котрі показані на рисунку 2.2.

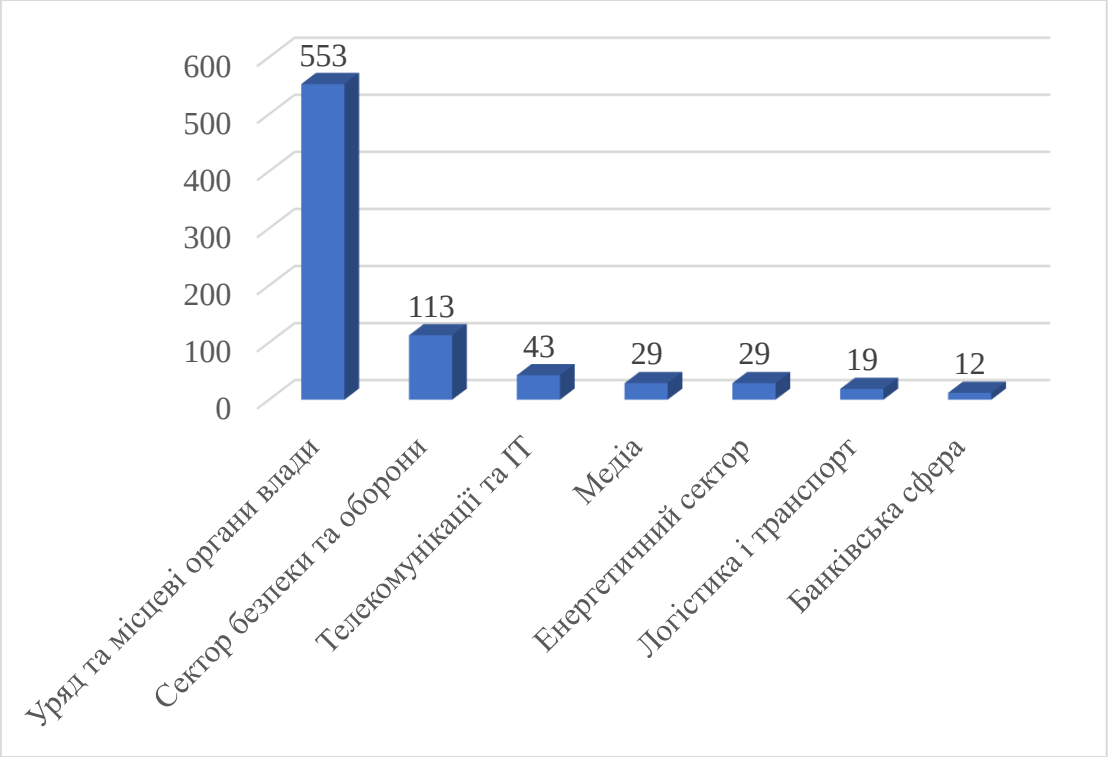


Рис. 2.2. Основні сектори щодо кількості кіберінцидентів

*Джерело: складено на підставі [66; 197]*

З рисунку можна побачити, що перші три позиції в рейтингу основних секторів щодо кількості кіберінцидентів у 2022 році займали:

– уряд та місцеві органи влади (553 випадки);

– сектор безпеки й оборони (113 випадків);

– телекомунікації та ІТ (43 випадки).

У цьому зв'язку слід зазначити, що, незважаючи на те, що частка України на світовому ринку кібербезпеки складає лише 0,07% (або 0,138 млрд. дол. США) (рисунок 2.3), він демонструє активне зростання (рисунок 2.4).

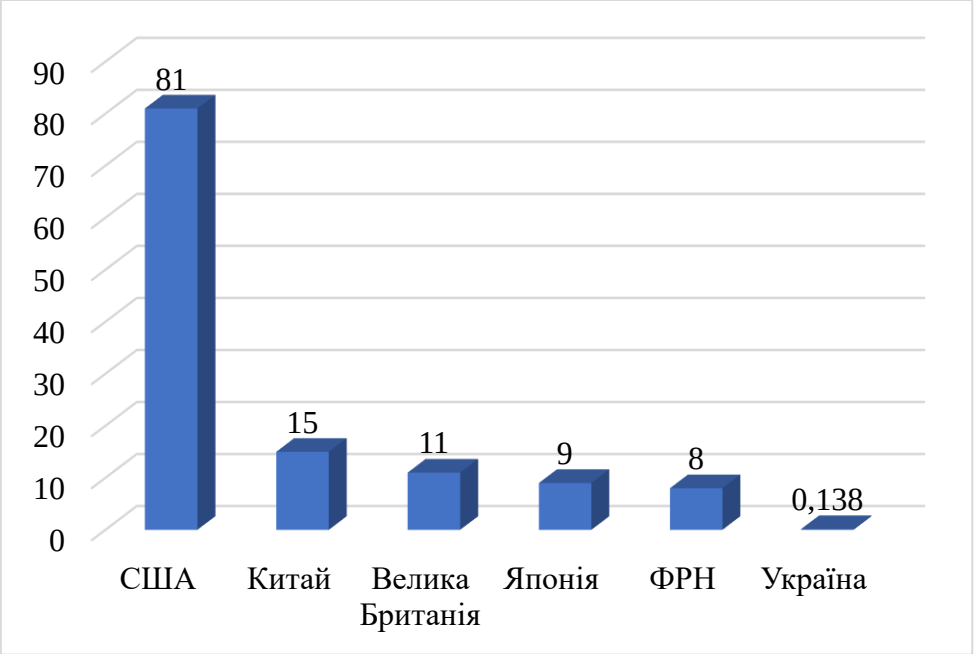


Рис. 2.3. Лідери світового ринку кібербезпеки, млрд. дол. США

*Джерело: складено на підставі [83]*

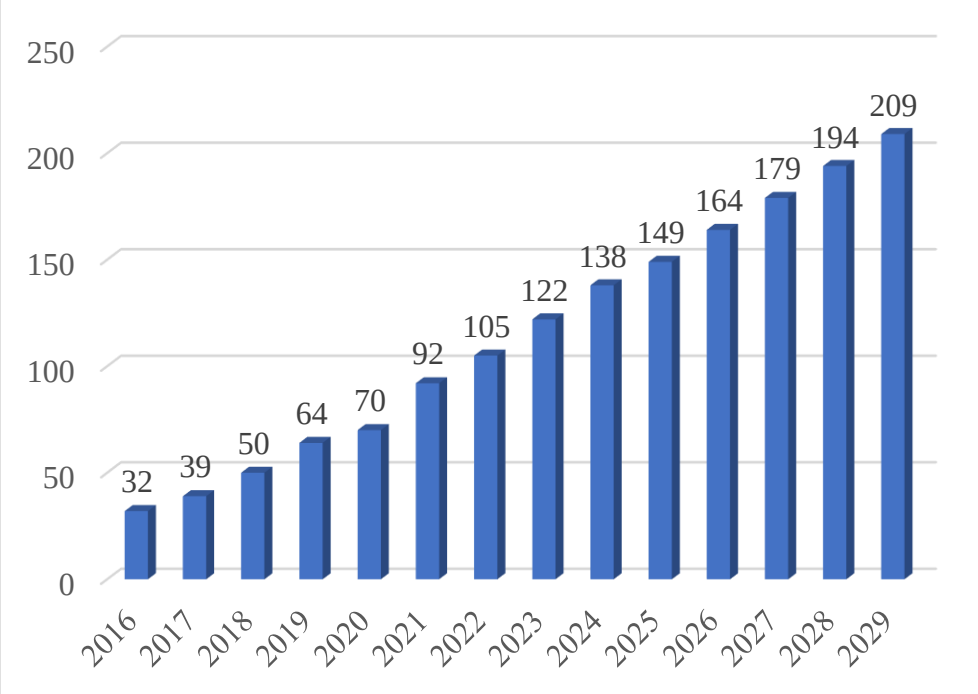


Рис. 2.4. Обсяг українського ринку кібербезпеки протягом 2016–2019 рр. з урахуванням прогнозних даних, млн. дол. США

*Джерело: складено на підставі [83]*

Так, з рисунку 2.4 можна побачити, що протягом 2016–2029 рр., з урахуванням прогнозних даних, вітчизняний ринок кібербезпеки демонструє

стійке зростання. Проте темпи цього зростання є різними (рисунок 2.5). Зокрема, у 2020 році COVID-19 спричинив наявність суттєвих фінансових проблем і бюджетних обмежень щодо інвестицій у сферу кібербезпеки. У наступному 2021 році спостерігалося суттєве підвищення кількості випадків кіберзлочинності у зв'язку з реструктуризацією ділової активності у період карантину. Щодо 2022 року, то в цей період спостерігалося помірне зростанням ринку, пов'язане з релокацією та закриттям компаній.

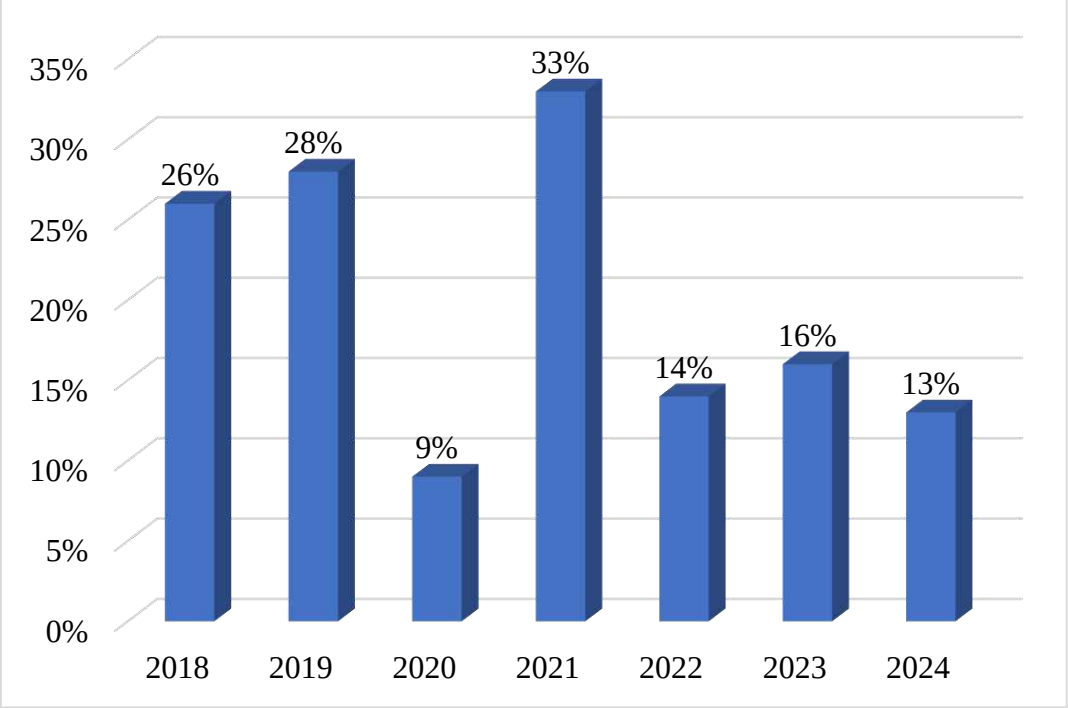


Рис. 2.5. Щорічне зростання українського ринку кібербезпеки

*Джерело: складено на підставі [83]*

Порівняльну характеристику розподілу українського ринку кібербезпеки за секторами у 2024 та 2029 роках, з урахуванням прогнозних даних, наведено на рисунку 2.6.

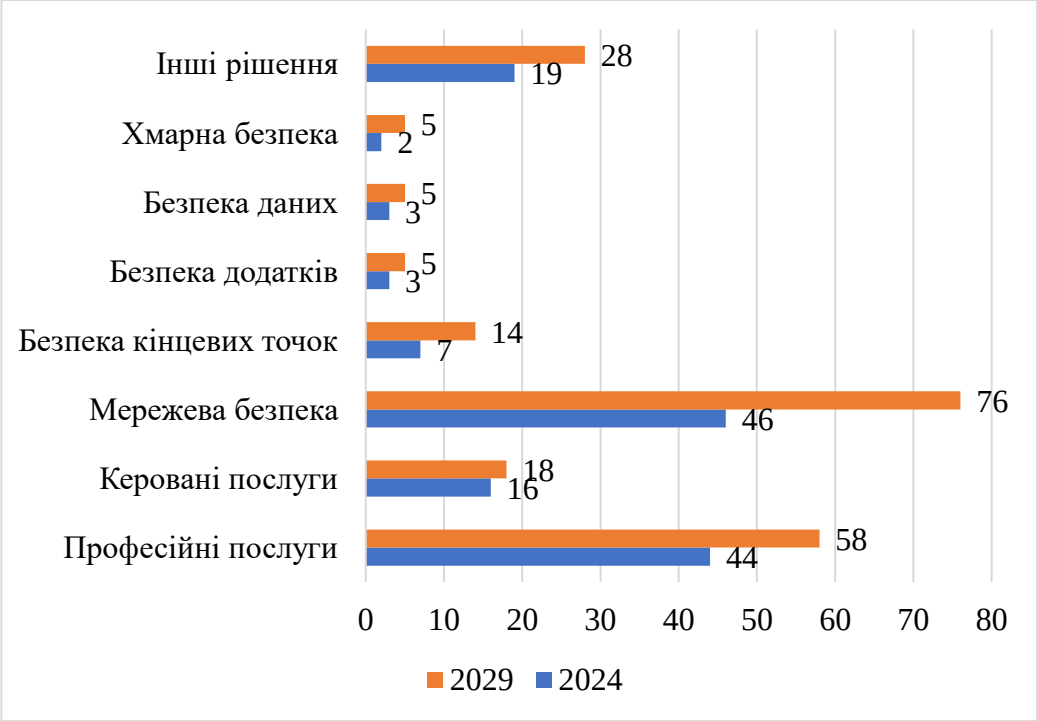


Рис. 2.6. Розмір та зростання українського ринку кібербезпеки за сегментами у 2024 та 2029 роках з урахуванням прогнозних даних, млн. дол. США

*Джерело: складено на підставі [83]*

З рисунку 2.6 можна побачити, що на українському ринку кібербезпеки переважають заходи з мережевої безпеки та професійні послуги. При цьому очікується, що у 2029 році обсяг сегменту з мережевої безпеки збільшиться вдвічі порівняно з 2024 роком. Що стосується сегменту професійних послуг, то його обсяг збільшиться на 31%.

На рисунку 2.7 відображено динаміку зміни відсотку населення, котре користувалося цифровими державними послугами в Україні. Зокрема, можна побачити, що в період з 2020 по 2022 рік цей показник збільшився на 10%.

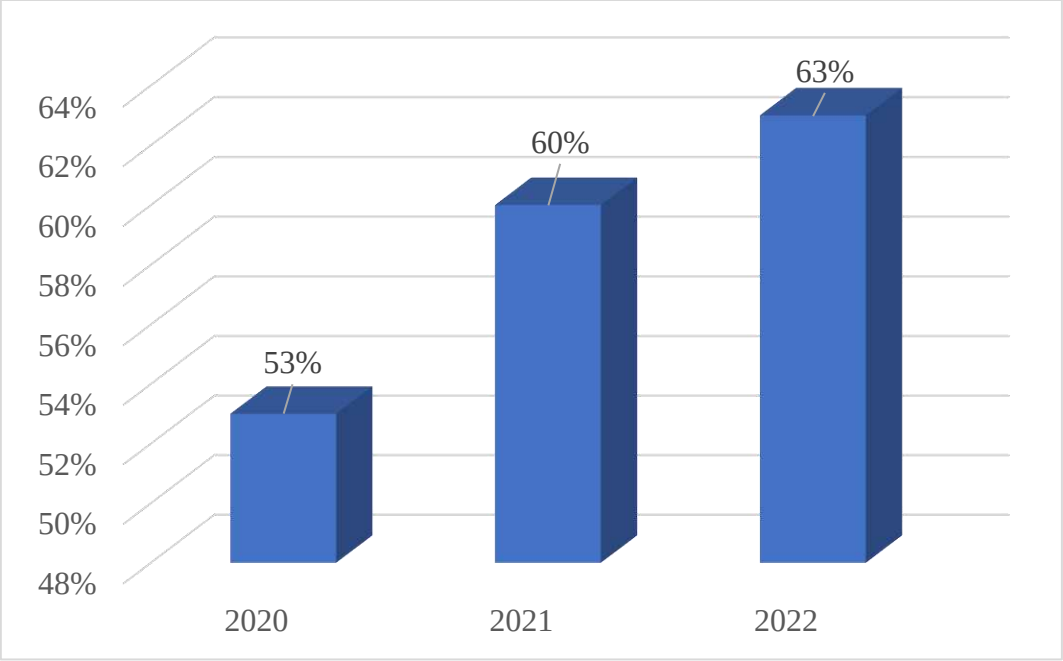


Рис. 2.7. Користування цифровими державними послугами в Україні

*Джерело: складено на підставі [52; 82]*

При цьому збитки громадян України від кіберзлочинності у 2022 році збільшилися вдвічі порівняно з попереднім 2021 роком, що модна побачити на рисунку 2.8.

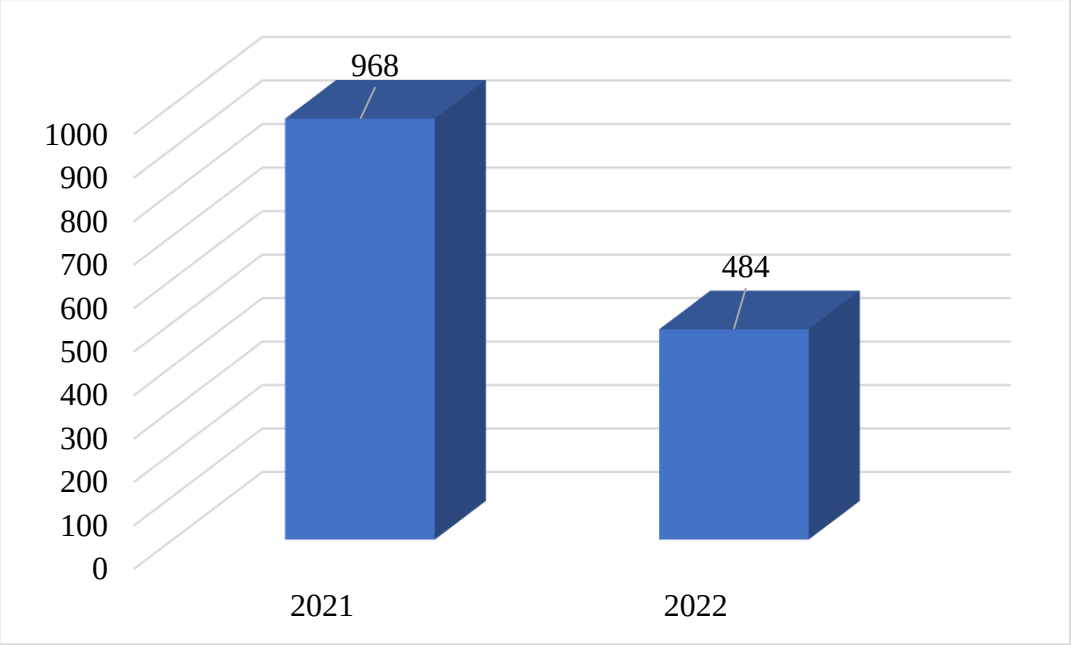


Рис. 2.8. Збитки громадян України від кіберзлочинності, млн. грн.

*Джерело: складено на підставі [66; 197]*

Порівняльну статистику щодо зміни кількості ШІ/ML спеціалістів в Україні в період 2013–2023 рр. показано на рисунку 2.9.

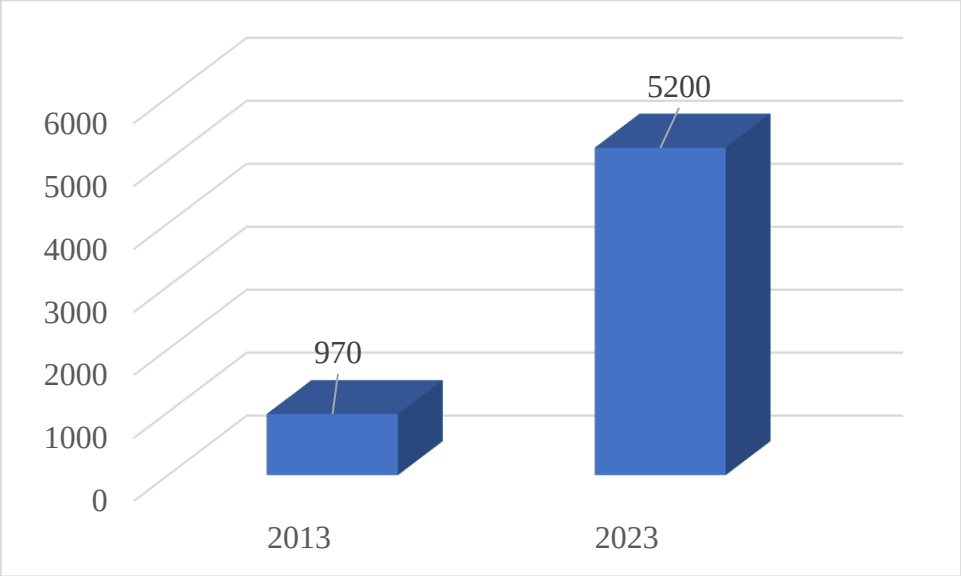


Рис. 2.9. Кількість ШІ/ML спеціалістів в Україні

*Джерело: складено на підставі [9; 227]*

З рисунку 2.9 можна побачити, що кількість ШІ/ML спеціалістів в Україні протягом 10 років збільшилася у 5,4 рази.

Очікується, що протягом наступних 5 років найбільше зростання ринку кібербезпеки забезпечать технології, показані в таблиці 2.1.

Таблиця 2.1

Технології, котрі забезпечуватимуть зростання ринку кібербезпеки протягом наступних 5 років

| Сегмент | Зростання до 2029 року, млн. дол. США | Зростання до 2029 року, % |
|---|---|---|
| Безпека хмарних сервісів | +3,78 | 226 |
| Безпека кінцевих точок | +6,08 | 85,8 |
| Безпека мережі | +29,4 | 63,5 |
| Інше | +14,3 | 58,1 |

*Джерело: складено на підставі [83]*

З таблиці 2.1 можна побачити, що на першому місці серед технологій, котрі забезпечуватимуть зростання ринку кібербезпеки протягом наступних 5 років, знаходиться безпека хмарних сервісів (226%). При цьому за час повномасштабного російського вторгнення обсяг ринку хмарної безпеки України збільшився до 1,7 млн. дол. США (рисунок 2.10). Це пов'язано з тим, що через суттєву ймовірність пошкодження систем і сервісів під час повномасштабного російського вторгнення більшість компаній почала перенесення своїх даних до хмарних сервісів.

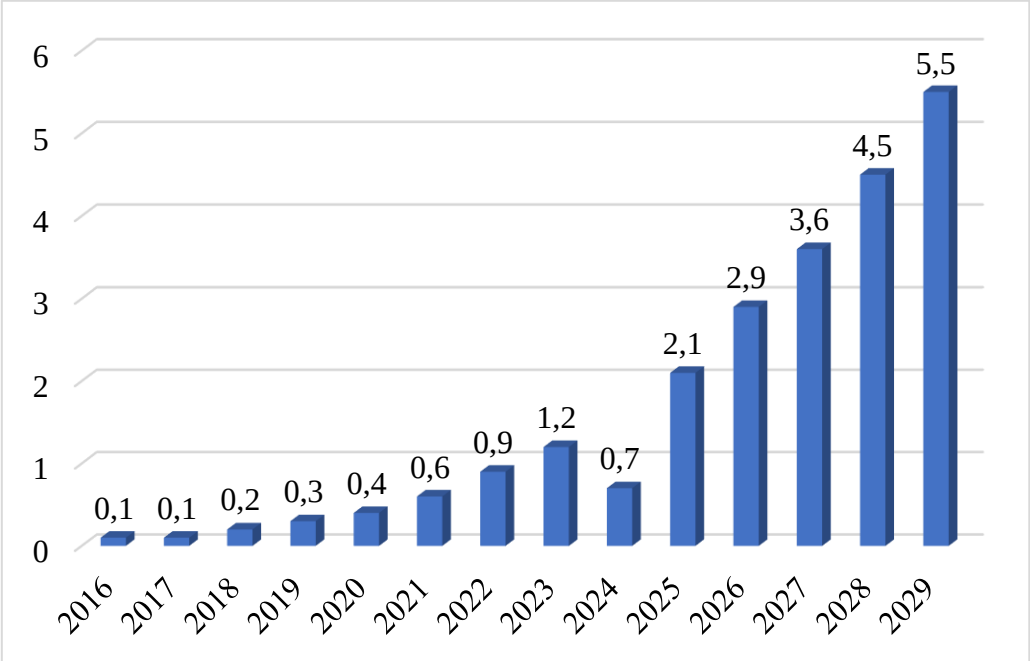


Рис. 2.10. Обсяг ринку хмарної безпеки в Україні протягом 2016 – 2029 років з урахуванням прогнозних даних, млн. дол. США

*Джерело: складено на підставі [83]*

При цьому, за даними експертів, за умов продовження військової агресії, обсяг ринку хмарних технологій України збільшиться до 5,5 млн. дол. США до 2029 року.

Поточний розподіл часток компаній на ринку хмарних сервісів України у 2022 році наведено на рисунку 2.11.

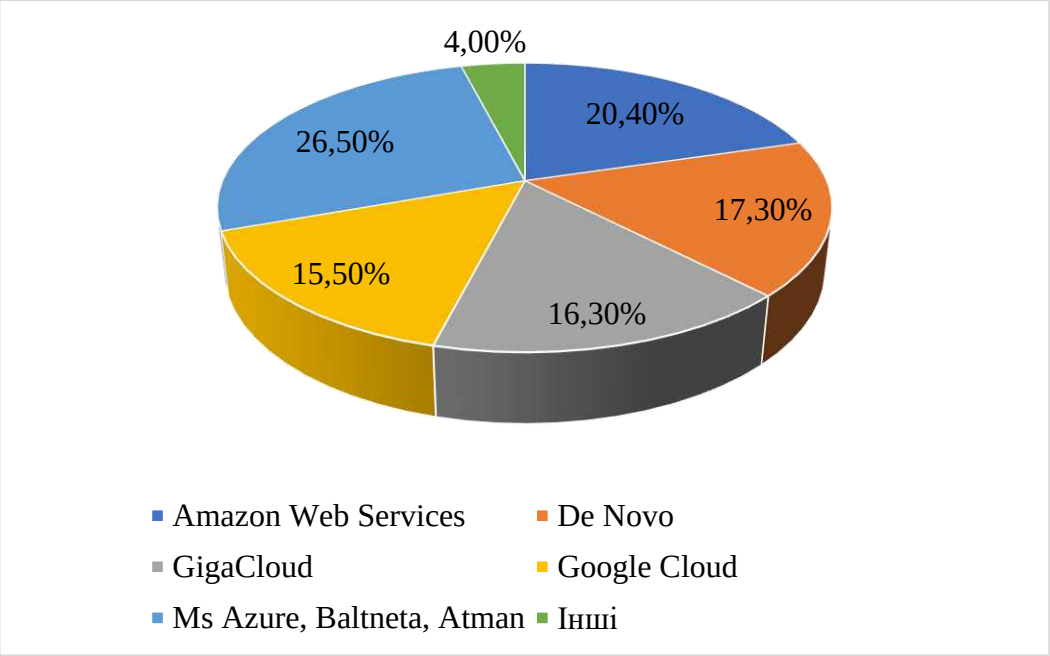


Рис. 2.11. Частка компаній на ринку хмарних сервісів України у 2022 році

*Джерело: складено на підставі [83]*

Слід також відзначити, що в 2029 році очікується зростання ринку мережевої безпеки України майже вдвічі порівняно з 2024 роком (рисунок 2.12).

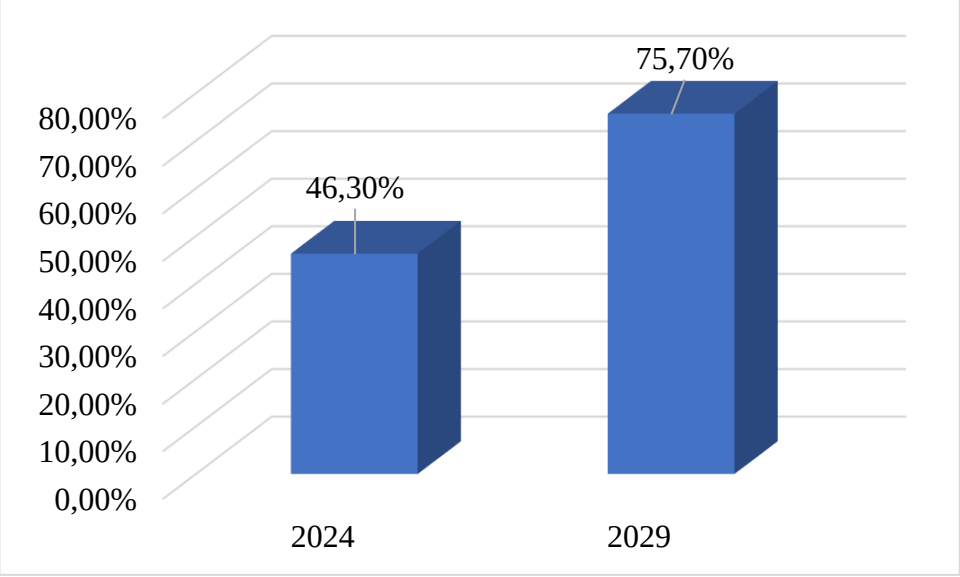


Рис. 2.12. Очікуване зростання ринку мережевої безпеки в Україні, млн. дол. США

*Джерело: складено на підставі [83]*

Щодо ринку безпеки кінцевих точок, то у 2029 році очікується його зростання на 86% порівняно з 2024 роком (рисунок 2.13).

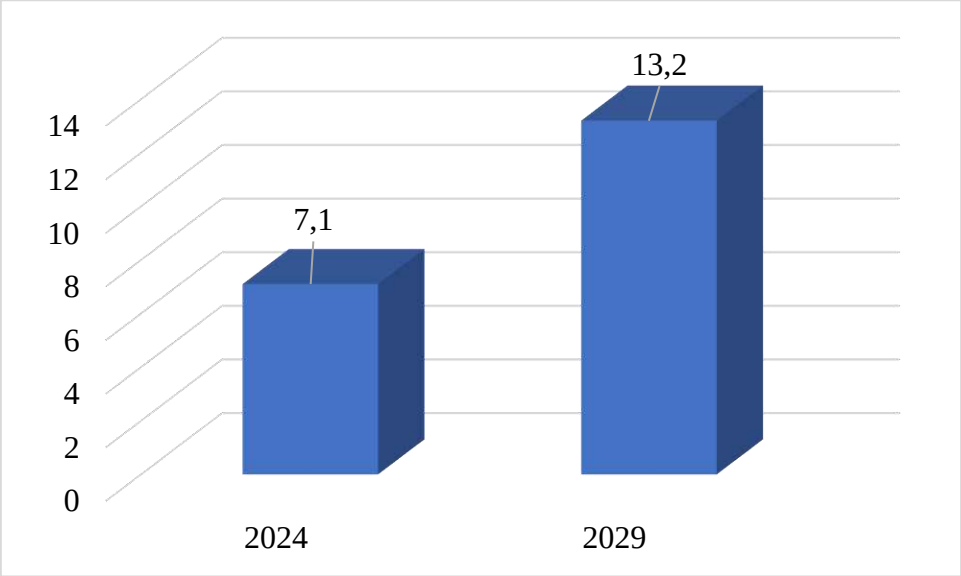


Рис. 2.13. Очікуване зростання ринку безпеки кінцевих точок в Україні, млн. дол. США

*Джерело: складено на підставі [83]*

Цьому сприяють:

– зростання кількості кіберзагроз;

– активізація цифрової трансформації та підвищення рівня залежності від кінцевих пристроїв;

– розширення тенденцій організації віддаленої роботи.

Однією з ключових інновацій на ринку кібербезпеки України є використання штучного інтелекту. Зокрема, розмір світового ринку штучного інтелекту в кібербезпеці систематично збільшуватиметься, і очікується, що в 2032 році він збільшиться у 5 разів порівняно з 2024 роком (рисунок 2.14).

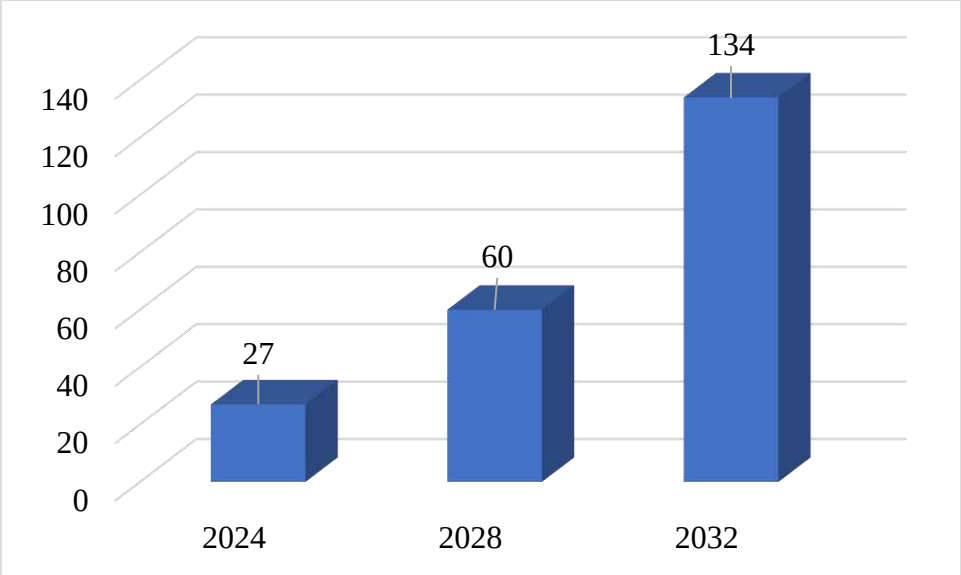


Рис. 2.14. Розмір світового ринку ШІ в кібербезпеці

*Джерело: складено на підставі [265]*

Загальний розподіл витрат на кіберзахист серед компаній в Україні в 2023 році показано на рисунку 2.15.

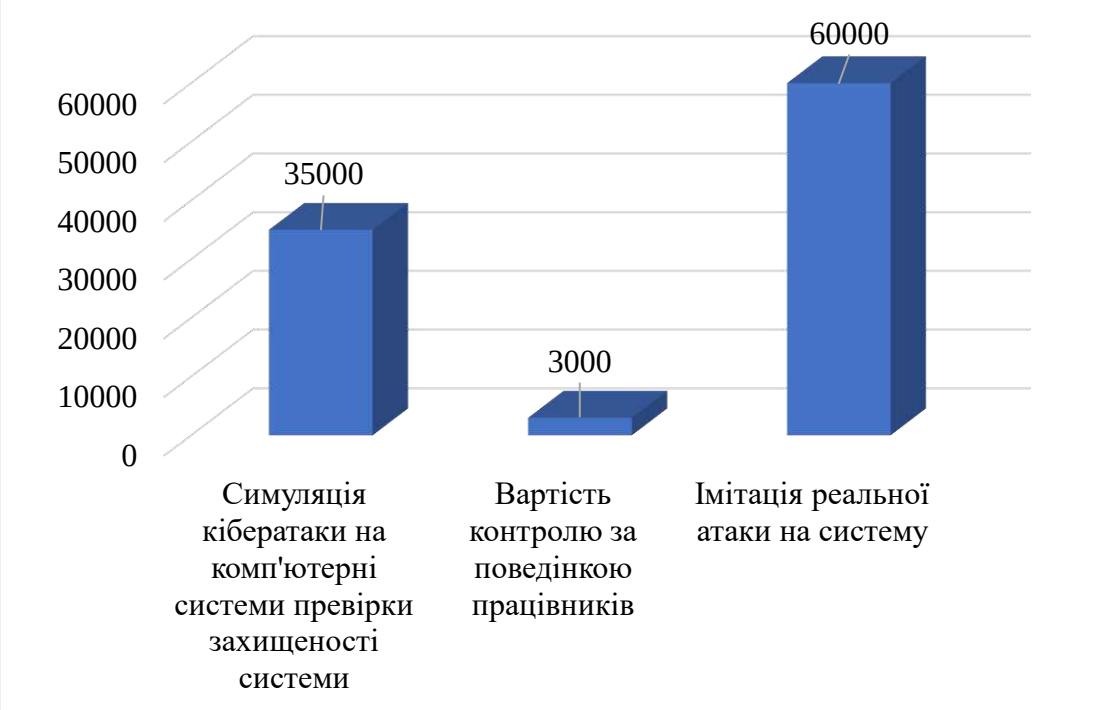


Рис. 2.15. Витрати на кіберзахист компанії в Україні в 2023 році (на прикладі компанії за штатом 200 працівників), дол. США

*Джерело: складено на підставі [83]*

З рисунку 2.15 можна побачити, що найбільший обсяг витрат на кіберзахист стосується імітації реальної атаки на IT-систему (у середньому – 60000 дол. США). У цілому, компанії можуть витрачати на кіберзахист від 10 до 50% власного річного бюджету на кібербезпеку.

Що ж до рівня користування послугами кібербезпеки серед компаній України, то його відображено на рисунку 2.16.

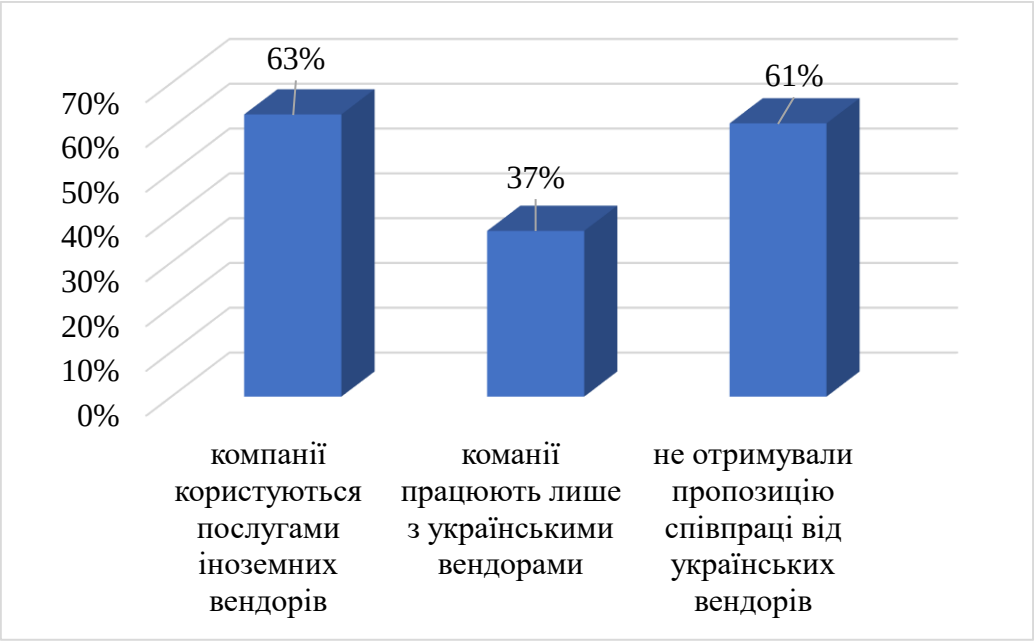


Рис. 2.16. Рівень користування послугами кібербезпеки серед компаній

*Джерело: складено на підставі [83]*

Дані рисунку 2.16 свідчать про те, що переважно вітчизняні компанії користуються послугами іноземних компаній щодо кібербезпеки (63%).

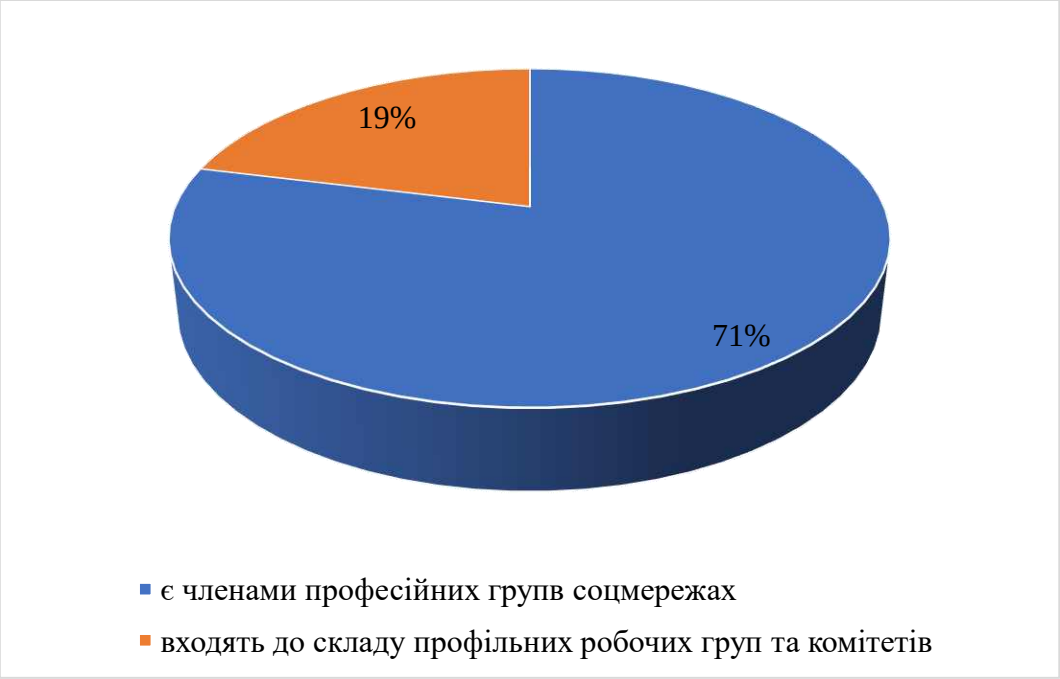


Рис. 2.17. Ступінь участі спеціалістів з кібербезпеки в асоціаціях та клубах

*Джерело: складено на підставі [83]*


Рис. 2.18. Ступінь участі спеціалістів з кібербезпеки в конференціях

*Джерело: складено на підставі [83]*

Варто також зазначити, що абсолютна більшість фахівців із кібербезпеки у вітчизняних компаніях є членами галузевих професійних

асоціацій і клубів та беруть активну участь у профільних конференціях (рисунки 2.17 та 2.18).

Проведений аналіз стану управління інформаційною безпекою України в умовах гібридних загроз виявляє суперечливу динаміку розвитку національної системи кібербезпеки. Незважаючи на відчутний поступ у сфері нормативно-правового регулювання – ухвалення Доктрини інформаційної безпеки, Стратегії кібербезпеки, Закону «Про кібербезпеку» та розроблення Оперативно-тактичного плану – система захисту інформаційного простору держави зіштовхується з комплексом глибинних структурних проблем. Вітчизняний ринок кібербезпеки, попри стале зростання та прогнозоване розширення в усіх ключових сегментах до 2029 року, залишається критично залежним від зарубіжних постачальників: понад 63% українських компаній використовують іноземні рішення у сфері кіберзахисту. Збільшення кількості зареєстрованих кіберінцидентів на 16% у 2023 році, подвоєння фінансових збитків громадян від кіберзлочинності у 2022 році, а також концентрація атак на урядові структури та об'єкти критичної інфраструктури переконливо свідчать про те, що наявна система публічного управління інформаційною безпекою потребує системного перезавантаження – насамперед у частині розвитку вітчизняного ринку кіберрішень, підготовки висококваліфікованих кадрів і зміцнення міжсекторальної координації.

### 2.3. Досвід зарубіжних країн стосовно управління інформаційною безпекою держави в умовах гібридних загроз

Європейський Союз (ЄС) – це унікальне політико-економічне партнерство між 27 європейськими країнами, яке діє через кілька наднаціональних незалежних інституцій та міжурядових механізмів переговорів, котрі обслуговують його держави-члени. Документи, прийняті ЄС, які мають найбільше значення для кібербезпеки, – це або ті, що виражають політичний консенсус, але не є юридично обов’язковими (наприклад,

повідомлення), або різні типи юридично обов'язкових актів, що накладають зобов'язання на держави-члени або конкретні організації.

ЄС працює над питаннями мережевої та інформаційної безпеки й кіберзлочинності вже тривалий час, а в 2013 році опублікував перший комплексний документ, присвячений широкому спектру кіберзагроз – Стратегія кібербезпеки Європейського Союзу [19; 87]. Стратегія окреслює бачення, ролі, обов'язки та необхідні дії для ЄС у сфері кібербезпеки. Важливо, що в документі підкреслюється, що в контексті кібербезпеки централізований нагляд ЄС не є рішенням, і тому національні уряди повинні залишатися основними суб'єктами, що організовують запобігання кіберінцидентам та забезпечують реагування на них на національному рівні. ЄС розглядає кібербезпеку, спираючись на три основні напрямки – мережева та інформаційна безпека, правоохоронні органи та оборона – та визначає перелік національних та європейських суб'єктів, відповідальних за забезпечення кібербезпеки. Дії, пов'язані з кібербезпекою, також були включені до Цифрового порядку денного для ЄС (англ. – Digital agenda for Europe) [240], яка розглядає довіру та безпеку мережі Інтернет як життєво важливі для динамічного цифрового суспільства та для Європейського порядку денного безпеки, який, своєю чергою, визначає кіберзлочинність (разом із тероризмом та організованою злочинністю) як одну з найважливіших нових загроз. Також Рада ЄС ухвалила Рамкову політику ЄС щодо кіберзахисту. Рамкова політика ЄС щодо кіберзахисту розглядається як додатковий документ для підтримки європейських інституцій у їхній роботі, пов'язаний з кіберзахистом, та призначений для забезпечення Стратегії кібербезпеки ЄС необхідними інструментами впровадження [210, с. 130].

У сфері мережевої та інформаційної безпеки основними гравцями ЄС є Європейська комісія, Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (англ. – European Union Agency for Network and Information Security, ENISA), CERT-EU та Європейське державно-приватне партнерство для стійкості [19; 87]. У 2013 році Європейська комісія

запропонувала прийняти Директиву про мережеву та інформаційну безпеку (NIS 2), метою якої є встановлення стандарту для правових заходів та створення стимулів для того, щоб зробити онлайн-середовище ЄС найбезпечнішим у світі. Політика ЄС також підкреслює важливість міжнародної співпраці та взаємодії з приватним сектором [258, с. 134]. Крім того, політика щодо захисту критичної інформаційної інфраструктури має на меті зміцнити безпеку та стійкість життєво важливої ІКТ-інфраструктури шляхом стимулювання та підтримки розвитку високого рівня готовності, безпеки та стійкості як на національному рівні, так і на рівні ЄС [54; 210].

Перш ніж розглядати, що саме конкретне законодавство та політика говорять про кібербезпеку та ІТ-безпеку, важливо розуміти відповідні типи документів, котрі розглядаються в законодавстві ЄС.

Законодавство ЄС може бути п’яти різних типів, які відрізняються за застосуванням, обов’язковим характером та адресатом (стаття 288 Договору про функціонування Європейського Союзу). Хоча держави-члени несуть основну відповідальність за правильне та своєчасне виконання правових актів ЄС, Європейська Комісія бере на себе завдання забезпечення їх дотримання [79; 210].

Регламент – це правовий акт ЄС, який «має загальне застосування, є обов’язковими до виконання в повному обсязі та підлягає безпосередньому застосуванню» у всіх державах-членах ЄС [46, с. 171]. Він не потребує транспозиції на національне законодавство та може бути безпосередньо оскаржений в національних судах держав-членів.

Директива – це правовий акт ЄС, що має загальне застосування та може бути адресовані одній, кільком або всім державам-членам ЄС [46, с. 172]. На відміну від регламентів, директиви є обов’язковими лише «щодо результату, якого необхідно досягти», надаючи державам-членам повноваження та гнучкість «вибирати форму та методи» для досягнення зазначеного результату. Транспонування в національне законодавство необхідне до того, як директиви стануть застосовними в державах-членах, яким вони адресовані.

Рішення – це правовий акт ЄС, який може мати загальне або спеціальне застосування та може мати одного або кількох адресатів (одну або кілька держав-членів ЄС, одну або кілька компаній чи фізичних осіб) [46, с. 174]. Як і регламенти, вони є обов'язковими до виконання в повному обсязі та безпосередньо застосовуються.

Прийняття зазначених трьох типів законодавчих актів здійснюється в межах однієї з двох процедур ЄС, закріплених у статтях 289 та 294 Договору про функціонування Європейського Союзу: звичайної або спеціальної законодавчої процедури. Звичайна процедура є домінуючою формою законотворчості в системі ЄС. У її рамках Європейський парламент і Рада ЄС виступають рівноправними співзаконодавцями та спільно ухвалюють нормативні акти на підставі пропозицій Європейської Комісії – єдиного інституту, наділеного правом законодавчої ініціативи. Спеціальна процедура застосовується лише у випадках, прямо передбачених Договором. Її ключова відмінність від звичайної полягає в тому, що Рада ЄС діє як самостійний законодавець, однак зобов'язана або отримати схвалення Європейського парламенту, або провести з ним консультації щодо відповідної законодавчої пропозиції [79, с. 65].

Окрім правових актів, прийнятих за допомогою звичайної або спеціальної законодавчої процедури, які можна класифікувати як законодавчі акти, Європейська Комісія або, у виняткових випадках, Рада ЄС, може приймати незаконодавчі акти. Делеговані та імплементаційні акти, наприклад, делегований регламент або імплементаційна директива, є найпоширенішими такими актами (ст. 291 та 292 Договору про функціонування Європейського Союзу). Делеговані акти Європейської Комісії доповнюють або змінюють несуттєві частини законодавчих актів. Вони приймаються, наприклад, коли вони передбачені певним правовим актом або коли необхідні коригування законодавчих актів для врахування досягнень у технічній та науковій галузях. Перед прийняттям таких актів Європейська Комісія консультується з експертами з держав-членів ЄС. Імплементаційні акти, прийняті

Європейською Комісією або, у виняткових випадках, Радою ЄС, встановлюють «єдині умови для імплементації» законодавчих актів. Ці акти зазвичай стосуються адміністративних або технічних аспектів і приймаються після консультацій з комітетами, що складаються з технічних експертів з держав-членів ЄС [79; 210].

Окрім регламентів, директив та рішень, правові акти ЄС також містять рекомендації та висновки як юридично необов'язкові види результатів. Рекомендації, з одного боку, дозволяють інституціям ЄС висловлювати свої погляди та пропонувати план дій «без накладання будь-яких юридичних зобов'язань» на адресата. Висновки, з іншого боку, дозволяють інституціям ЄС формулювати заяви «без накладання будь-яких юридичних зобов'язань на предмет висновку» [210, с. 129].

Окрім правових актів, Рада ЄС також може висловлювати свою політичну позицію з питань, що належать до сфери діяльності ЄС, та приймати документи, що не мають юридичної сили, та відображають «політичні зобов'язання або позиції». Наприклад, висновки Ради ЄС можуть бути прийняті після обговорення на засіданні Ради та «містити політичну позицію з конкретного питання». Резолюції Ради ЄС зазвичай окреслюють майбутні ініціативи, передбачені в конкретній сфері політики. Хоча обидва приклади документів не мають юридичної сили, вони можуть закликати Європейську Комісію або інші Європейської бізнес асоціації запропонувати конкретні заходи або вжити подальших заходів [210, с. 131].

Крім того, Європейська Комісія може публікувати інші типи документів, що не мають юридичної сили, зокрема, такі, як повідомлення з певної теми. Іноді Європейська Комісія робить це разом з Комісія та Високий представник ЄС із закордонних справ і безпеки (HR/VP) у формі спільних повідомлень [103, с. 125].

У сфері правоохоронної діяльності основними гравцями ЄС є Європейський центр боротьби з кіберзлочинністю (ЕС3), а також Європол, CEPOL та Євроюст. Окрім уже існуючих інструментів боротьби зі

злочинністю, Директива 2013/40/ЄС про атаки на інформаційні системи та заміну Рамкового рішення Ради 2005/222/ЈНА була прийнята та спрямована на боротьбу з масштабними кібератаками, вимагаючи від держав-членів посилення національного законодавства про кіберзлочинність та запровадження жорсткіших кримінальних санкцій [54; 87].

У сфері оборони основними гравцями ЄС є Європейська служба зовнішніх справ, Військовий штаб Європейського Союзу та Європейське оборонне агентство. Стратегія кібербезпеки ЄС також визначає політику кіберзахисту країн, що розвиваються, та можливості, пов'язані з рамками Спільної політики безпеки та оборони, як одну з її цілей, а також окреслює перелік заходів, передбачених для співпраці Європейського оборонного агентства та держав-членів [19; 210].

Принципово важливим є положення Стратегії кібербезпеки ЄС, яке передбачає, що масштабний кіберінцидент або кібератака особливо серйозного характеру можуть слугувати достатньою підставою для того, щоб держава-член вдалася до механізму Клаузули солідарності ЄС, закріпленого у статті 222 Договору про функціонування Європейського Союзу [254, с. 63].

У разі масштабного кіберінциденту держави-члени Європейського Союзу (ЄС) несуть «головну відповідальність за [...] реагування», разом із їхньою прерогативою щодо питань національної безпеки (ст. 4(2) Договору про Європейський Союз). Водночас, «значне зростання рівня, складності та масштабу кіберзагроз» та «вплив на громадськість, транскордонний характер та ризик поширення кіберзагроз» дозволили зробити міжнародну співпрацю та спільні підходи життєво важливими для реагування на виклики, що виникають, та сприяти стійкій кібербезпеці в усьому ЄС [254, с. 79-80].

На цьому тлі не дивно, що багато чого змінилося з моменту першого ухвалення ЄС Резолюції про спільний підхід та конкретні дії у сфері безпеки мережевої інформації у 2002 році, в якій містився заклик до держав-членів, Європейської комісії та зацікавлених сторін галузі активізувати свої зусилля, спрямовані на підвищення інформаційної безпеки. Наприклад, у 2004 році ЄС

створив ENISA, яке тепер називається Агентством Європейського Союзу з питань мережевої та інформаційної безпеки; у 2013 році Комісія та Високий представник ЄС із закордонних справ і безпеки (HR/VP) опублікували першу Стратегію кібербезпеки Європейського Союзу «Відкритий, надійний і безпечний кіберпростір», а у 2016 році держави-члени ЄС та Європейський парламент ухвалили перше горизонтальне законодавство ЄС щодо кібербезпеки, – перша Директива ЄС 2016/1148 про мережеву та інформаційну безпеку [19; 87; 210].

Пошук за ключовими словами в базі даних документів ЄС EUR-Lex типово відображає еволюцію дій ЄС щодо політики кібербезпеки та IT-безпеки з 1990 року. Тільки за 2023 рік база даних містить 1144 результати для документів, що згадують «кібербезпеку» або «інформаційну (IT) безпеку» [243].

Це помітне збільшення згадок стосується не лише пошуку в документах ЄС загалом. Воно також відображається у збільшенні кількості правових актів ЄС, що стосуються кібербезпеки та/або IT-безпеки, що лежить в основі посиленої регуляторної діяльності ЄС щодо цього питання. Особливо під час роботи Європейської Комісії 2019-2024 років спостерігалося помітне збільшення кількості правових актів ЄС, які прямо згадують кібербезпеку або IT-безпеку [261].

Наведені показники засвідчують послідовне просування ЄС у вирішенні питань кібербезпеки та захисту інформаційних технологій, що перетворює його на дедалі впливовішого гравця в цій сфері та стимулює подальше розширення регуляторної та політичної екосистеми кібербезпеки Союзу.

Не лише ці абстрактні цифри, а й конкретні регуляторні та політичні зміни в різних сферах та секторах політики демонструють підвищену увагу ЄС до кібербезпеки та IT-безпеки:

– перша Директива ЄС 2016/1148 про мережеву та інформаційну безпеку (2023);

– нові правові акти щодо стійкості критично важливих об’єктів (Директива ЄС 2022/2557);

– цифрова операційна стійкість фінансових установ (Директива ЄС 2022/2554);

– кібербезпека інституцій, органів та агентств ЄС (EUIBAs, Регламент ЄС 2023/2841);

– створення Європейської схеми сертифікації кібербезпеки (Регламент ЄС 2019/881);

– можливість контролю експорту інструментів кіберспостереження за певних обставин (Регламент ЄС 2021/821);

– ініціатива щодо Академії навичок з кібербезпеки (2023); або переглянутих імплементаційних керівних принципів Інструментарію кібердипломатії ЄС (2023) – це лише кілька дуже помітних подій, пов’язаних із кібербезпекою на рівні ЄС протягом останніх кількох років.

Як побічний ефект еволюції політики ЄС у сфері кібербезпеки, моніторинг та навігація в екосистемі політики ЄС у сфері кібербезпеки стали дедалі складнішим завданням – як для політиків та осіб, що приймають рішення у державному та приватному секторах, так і для інших зацікавлених сторін, зокрема, таких як громадянське суспільство та наукові кола [54; 210]. Чим більше розвивається галузь політики, тим важливішим стає підтримка всебічного огляду зусиль, що вживаються та застосовуються. Розвиток галузі політики також робить більш необхідним широкі процедури координації між залученими політичними рівнями та організаціями. Отже, огляд політичного ландшафту та ландшафту учасників є фундаментальною передумовою для ефективного впровадження та застосування законодавства та політики, пов’язаних з кібербезпекою, та формування розумної, структурованої та сталої політики кібербезпеки як на рівні ЄС, так і на рівні держав-членів.

Вищезазначене відображає міжгалузевий характер політики кібербезпеки та ІТ-безпеки. Розподіл нормативно-правових актів та політик між цими сферами політики додатково ґрунтується на принципі делегування

повноважень, що означає, що ЄС потребує компетенції – виключної або спільної з державами-членами – для вжиття заходів у певній сфері політики (стаття 5 Договору про функціонування Європейського Союзу). Відповідно, будь-які компетенції, не зазначені в первинному праві ЄС, «залишаються за державами-членами» (стаття 5(2) Договору про функціонування Європейського Союзу) [46, с. 12]. Тобто, будь-який правовий акт ЄС або політика ЄС, що стосуються кібербезпеки, також повинні бути пов’язані з конкретною сферою, в якій ЄС має компетенцію.

Узагальнення досвіду Європейського Союзу у сфері управління інформаційною безпекою в умовах гібридних загроз дозволяє констатувати становлення розгалуженої та динамічно еволюціонуючої регуляторної екосистеми кібербезпеки, в якій юридично обов'язкові нормативні акти органічно поєднуються зі стратегічними документами політичного характеру. Ключовою особливістю підходу ЄС є збалансований розподіл відповідальності між наднаціональним рівнем та державами-членами: Союз визначає мінімальні стандарти та забезпечує координацію, тоді як національні уряди зберігають основну компетенцію у сфері забезпечення кібербезпеки та реагування на інциденти. Прийняття Директиви NIS 2, Закону про кібербезпеку, Закону про кіберстійкість та низки секторальних регуляторних актів у 2019–2024 роках свідчить про якісне прискорення регуляторної активності ЄС у цій сфері. Для України, яка прагне до євроінтеграції та вже імплементує окремі положення законодавства ЄС у сфері кібербезпеки, досвід Союзу є особливо цінним як орієнтир для вдосконалення власної нормативно-правової бази, розбудови інституційної архітектури кіберзахисту та формування культури багаторівневої координації між суб'єктами забезпечення інформаційної безпеки держави.

**Висновки до другого розділу**

1. Виявлено, що серед ключових викликів і кіберзагроз національному кіберпростору України особливої уваги заслуговують такі:

– зростаюче застосування кіберінструментів як засобу міжнародного суперництва;

– загострення конкурентної боротьби за розвиток засобів кібербезпеки в умовах стрімкої технологічної еволюції — хмарних і квантових обчислень, мереж 5G, великих даних, Інтернету речей та штучного інтелекту;

– мілітаризація кіберпростору та нарощування арсеналу кіберзброї, що уможливлює приховане проведення кібератак на підтримку бойових операцій і розвідувально-підривної діяльності;

– прискорена цифрова трансформація суспільних відносин та масштабний перехід до дистанційного режиму взаємодії з широким використанням електронних сервісів, спровоковані пандемією COVID-19;

– безсистемне з погляду кібербезпеки впровадження нових технологій, цифрових сервісів та механізмів електронної взаємодії між громадянами і державою без належного оцінювання супутніх ризиків.

Наголошено, що провідне місце серед загроз кібербезпеці України посідає гібридна агресія російської федерації в кіберпросторі. Держава-агресор послідовно нарощує потенціал наступальної кіберзброї, застосування якої здатне спричинити незворотні та катастрофічні наслідки. Головними об'єктами кібератак з боку російської федерації є інформаційні комп'ютерні системи українських державних органів та елементи критичної інформаційної інфраструктури – їх виведення з ладу, встановлення прихованого контролю, а також здійснення розвідувальної та підривної діяльності є пріоритетними цілями агресора. Окрім того, кібератаки активно інтегруються до арсеналу спеціальних інформаційних операцій як інструмент маніпулятивного впливу на суспільну свідомість, втручання у виборчі процеси та дискредитації української державності.

2. З'ясовано, що в контексті управління інформаційною безпекою в умовах гібридних загроз Україна має сформовані процедури щодо:

– виявлення вразливостей і конфігураційних недоліків в інформаційних, телекомунікаційних та інформаційних комп'ютерних системах, у яких циркулюють державні інформаційні ресурси;

– пошуку відкритих вразливостей та оперативного реагування на кіберінциденти й кібератаки;

– захисту електронних комунікацій, інформаційних комп'ютерних систем і мереж електронного зв'язку;

– оцінювання рівня захищеності державних інформаційних ресурсів в інформаційних, комунікаційних та комп'ютерних системах;

– сканування державних інформаційних ресурсів, розміщених у мережі Інтернет, на наявність вразливостей;

– моніторингу стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів і відповідної інформації, а також перевірки дотримання законодавчо встановлених вимог щодо захисту.

Для забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки розгорнуто комплекти обладнання підсистеми збору телеметричних даних інформаційних комп'ютерних систем на основі активних датчиків.

3. Встановлено, що організаційний механізм кіберзахисту в Україні охоплює шість взаємопов'язаних секторів:

– загальнодержавний, до якого належать ключові суб'єкти національної системи кібербезпеки, сили безпеки та оборони, а також Національний координаційний центр кібербезпеки як координуючий робочий орган;

– галузевий, що об'єднує центральні органи виконавчої влади, інші державні органи, відповідальні за формування та реалізацію державної політики в одній або кількох сферах, чи уповноважені безпосередньо вживати заходів кібербезпеки в межах своєї компетенції, а також об'єкти критичної інфраструктури незалежно від форми власності;

– регіональний (місцевий), представлений місцевими органами виконавчої влади, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності, що провадять діяльність у сферах захисту інформації та кіберзахисту;

– науково-освітній, що включає науково-дослідні установи, заклади вищої освіти у сферах захисту інформації та кібербезпеки, а також ті, що беруть участь у підготовці, перепідготовці та підвищенні кваліфікації фахівців галузі;

– приватний, сформований недержавними підприємствами, організаціями та установами, що здійснюють захист інформації та кіберзахист, за винятком об'єктів критичної інфраструктури;

– громадський, що охоплює громадські організації, спілки, асоціації, союзи та незалежних експертів у сфері кібербезпеки, а також міжнародні та міжурядові організації, що провадять діяльність у цій галузі.

Зазначено, що основними нормативними документами, що регулюють захист інформації в державних органах України, в якості яких вони надають цифрові послуги, та їх реалізацію, є:

– Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 5 липня 1994 року № 80/94-ВР;

– Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» від 29 березня 2006 р. № 373;

– Постанова КМУ «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» від 19 червня 2019 р. № 518;

– Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI;

– Закон України «Про електронну ідентифікацію та електронні довірчі послуги» від 5 жовтня 2017 року № 2155-VIII;

– Постанова Кабінету Міністрів України «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах» від 16 листопада 2002 р. N 1772;

– Постанова Кабінету Міністрів України «Про затвердження Положення про Реєстр інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління» від 3 серпня 2005 року № 688;

– Постанова Кабінету Міністрів України «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації» від 21 лютого 2025 р. № 205;

– Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Порядку формування й користування інформаційним фондом Реєстру інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління» від 24 квітня 2007 року № 72).

4. Зазначено, що на сучасному етапі ринок кібербепеки України передбачає наявність визначеного переліку кіберрішень – продуктів або послуг, котрі є адаптованими до унікальних вимог організацій з прийняттям до уваги їх ризикових ландшафтів та безпекових стратегій. Зокрема, подібні кіберрішення передбачають:

– безпеку додатків – комплекс методів захисту для забезпечення безпеки програмного забезпечення від загроз зовнішнього походження, а також несанкціонованого доступу до нього;

– хмарну безпеку – комплекс практик захисту в хмарних середовищах публічного, приватного і гібридного типу, орієнтованих на забезпечення безпеки даних, додатків і IT-систем від ризику витоку інформації та кіберзагроз;

– безпеку даних – комплекс заходів, орієнованих на цілісність, конфіденційність, доступність чутливих даних, що передбачає наявність контролю процесів шифрування та доступу для запобігання крадіжкам та випадкам несанкціонованого доступу;

– мережеву безпеку – комплекс процедур і технологій, котрі забезпечують захист мереж від несанкціонованого доступу до даних;

– безпеку кінцевих точок – комплекс заходів щодо захисту кінцевих точок, зокрема, мобільних пристроїв, серверів, робочих станцій, від різнохарактерних атак, із застосуванням сучасних засобів антивірусного захисту та рішень проти загроз нульового дня;

– комплекс додаткових рішень, які орієнтовані на ідентифікацію ризиків та управління ними, що, своєю чергою, дозволяє підтримувати відповідність нормативним вимогам щодо захисту від ризиків доступу.

Акцентовано, що зміцнення потенціалу національної системи кібербезпеки є нині пріоритетним стратегічним завданням, від виконання якого залежить захищене та безперебійне функціонування критичної інформаційної інфраструктури держави в кіберпросторі. Інструментом реалізації цього завдання слугує Оперативно-тактичний план, нормативна сутність якого полягає у створенні організаційних умов для консолідації зусиль усіх суб'єктів кібербезпеки навколо підвищення кіберстійкості критичної інформаційної інфраструктури. Остання охоплює не лише об'єкти критичної інфраструктури, а й комунікаційно-інформаційні та інші системи, безперебійна і надійна робота яких є визначальною умовою дієздатності органів державної влади, підприємств, установ та організацій усіх форм власності, а також громадських об'єднань.

5. Визначено, що як побічний ефект еволюції політики ЄС у сфері кібербезпеки, моніторинг та навігація в екосистемі політики ЄС у сфері кібербезпеки стали дедалі складнішим завданням – як для політиків та осіб, що приймають рішення у державному та приватному секторах, так і для інших зацікавлених сторін, зокрема, таких як громадянське суспільство та наукові

кола. Чим більше розвивається галузь політики, тим важливішим стає підтримка всебічного огляду зусиль, що вживаються та застосовуються. Розвиток галузі політики також робить більш необхідним широкі процедури координації між залученими політичними рівнями та організаціями. Отже, огляд політичного ландшафту та ландшафту учасників є фундаментальною передумовою для ефективного впровадження та застосування законодавства та політики, пов'язаних з кібербезпекою, та формування розумної, структурованої та сталої політики кібербезпеки як на рівні ЄС, так і на рівні держав-членів.

Підкреслено, що розподіл нормативно-правових актів та політик між цими сферами політики додатково ґрунтується на принципі делегування повноважень, що означає, що ЄС потребує компетенції – виключної або спільної з державами-членами – для вжиття заходів у певній сфері політики. Відповідно, будь-які компетенції, не зазначені в первинному праві ЄС, «залишаються за державами-членами». Таким чином, будь-який правовий акт ЄС або політика ЄС, що стосуються кібербезпеки, також повинні бути пов'язані з конкретною сферою, в якій ЄС має компетенцію.

# РОЗДІЛ 3
# ШЛЯХИ ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

## 3.1. Стратегічні орієнтири захисту єдиного інформаційного простору України в умовах гібридних загроз

Технологічний злет інформаційної індустрії наприкінці XX – на початку XXI століття став каталізатором формування якісно нового суспільно-технологічного укладу, що отримав назву інформаційного суспільства, або суспільства знань. Визначальною тенденцією цього укладу є невпинне посилення ролі інформації у військовій, політичній, економічній, науковій та інших галузях суспільної життєдіяльності, причому в кожній із них інформація виконує специфічні функції та по-різному детермінує перебіг розвиткових процесів.

Особливої ваги набуває вплив інформації на забезпечення різних видів безпеки – від захисту окремого індивіда чи соціальної групи до безпеки суспільства загалом. Не менш принциповим у сучасному контексті є питання безпеки держави як системного утворення. Саме від її стабільності та динамічного розвитку залежить стан національної безпеки країни, що розуміється як захищеність від руйнування цілісності системи не лише в територіальному чи політичному вимірі, а й у сенсі гарантованого збереження фундаментальних ціннісних засад соціуму.

Існуючі в даний час уявлення про національну безпеку та способи її забезпечення пов’язані з особливостями розстановки сил, що склалися на міжнародній арені, зміною ієрархії ризиків і загроз: конфлікти набувають характеру, пов’язаного з протиріччями між етнічними групами, кланами, ґрунтуються на релігійних і культурних цінностях тощо. Традиційний підхід до визначення національної безпеки радикально розширюється за рахунок включення інших видів безпеки, зокрема, політичної.

Багато ризиків і загроз у сучасному світі породжуються використанням інформації у певних цілях. Види безпеки можуть оцінюватися за характером ризиків, загроз та цілей використання для їх створення, однак поки що всі класифікації такого роду залишаються досить умовними через те, що однозначно віднести конкретні ризики та загрози до певної категорії не завжди можливо.

Фактично інформаційно-політична безпека, як явище, формується перетином інформаційно-комунікативної безпеки, інформаційно-технічної безпеки та інформаційно-психологічної безпеки. При більш докладному розгляді зазначених видів безпеки у цих інтегрованих блоках виділяються:

– безпека психологічного стану окремої людини, групи людей, об’єднаних певними цілями, завданнями, цінностями, місцевих спільнот та більших спільнот;

– безпека експлуатації устаткування, програмних продуктів, мереж та інших технічних пристроїв, що використовується при зборі, накопиченні, аналізі та передачі інформації.

Більш загальні поняття інформаційної та інформаційно-комунікаційної безпеки пов’язані з інформаційним забезпеченням суспільних процесів та комунікативними взаємодіями між ними. Загалом у рамках інформаційно-політичної безпеки виникає великий комплекс проблем, що потребують системних рішень, та розробка та прийняття яких можливі лише на основі глибокого аналізу самого явища.

На думку багатьох фахівців з інформаційної безпеки та військових [8; 104; 138], «кібервійнами» можна вважати «цілеспрямовані дії щодо заподіяння шкоди, перехоплення управління або руйнування критично важливих для функціонування суспільства та держави мереж та об’єктів, виробничої, соціальної, військової та фінансової інфраструктури, а також роботизованих та високоавтоматизованих виробничих, технологічних інновацій. Засобом бойового впливу в кібервійнах можна вважати програмний код, який виводить з ладу, порушує роботу або уможливлює перехоплення процесів управління

різними мережами та матеріальними об’єктами, обладнаними електронними системами управління [8, с. 67].

У мережевому електронному просторі ведуться два види воєн: інформаційні та кібервійни. Окрім Інтернету вони охоплюють закриті військові, державні, корпоративні та приватні мережі. Кожному виду воєн притаманні свої методи, стратегії, інструментарії, можливості запобігання тощо.

Інформаційно-політичну безпеку доцільно визначати, як стан захищеності інформаційно-політичного середовища. Надалі її слід розглядати як комплексну проблему, яка полягає у захисті життєво важливих інтересів громадян, держави та постіндустріального суспільства в цілому в політичній сфері від внутрішніх та зовнішніх інформаційних загроз. Це визначення дозволяє зосередити увагу політичних акторів, зацікавлених у забезпеченні безпеки, на максимально можливому обліку інтересів окремих людей, соціуму в цілому та держави.

Також стосовно інформаційно-політичної безпеки необхідно запровадити поняття допустимого ризику, яким визнається такий збиток, який прийнятний за існуючих суспільних цінностей, а також поняття залишкового ризику, який розуміється як неминучий збиток, пов’язаний із застосуванням захисних заходів.

Під оцінкою ризику, своєю чергою, слід розуміти процес аналізу потенційної небезпеки за допомогою використання інформації для її виявлення та кількісної оцінки, а також засновану на результатах аналізу процедуру перевірки, яка встановлює, чи не перевищено допустимого ризику. На рисунку 3.1 даний процес представлений схематично.

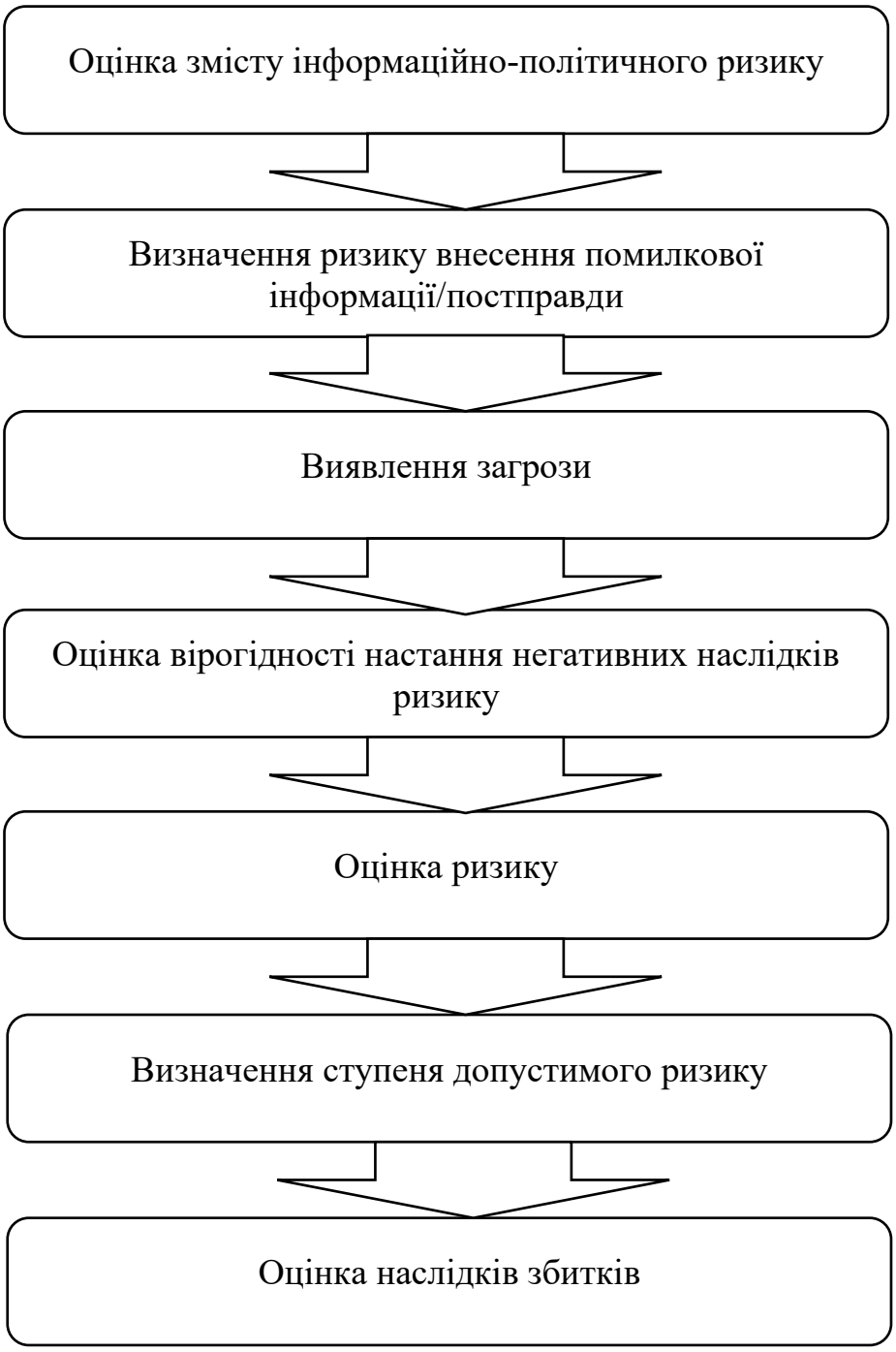


Рис. 3.1. Інтерактивний процес оцінки ступеня захищеності інформаційно-політичного середовища

*Джерело: авторська розробка*

Постправда визначається як інформаційно-політичний деструктивний вплив як на індивідуальну, так і на суспільну свідомість, у процесі якої об’єктивні факти та події цілеспрямовано трансформуються у менш значущі

переживання та переконання, що спотворюють «правду факту» на основі «фейкових новин». Суть явища полягає в тому, що головну роль донесенні інформації грають не факти, а емоції [107; 116].

Інформаційно-політична загроза – це сукупність факторів та умов, що створюють небезпеку порушення інформаційно-політичної безпеки. Для визначення розширеного та уточненого поняття інформаційно-політичної безпеки у продовженні дослідження слід розглядати інформаційно-політичну загрозу як передбачуване заподіяння шкоди інтересам громадян, держави та постіндустріального суспільства в галузі реальної політики на основі використання інформації, що поширюється в політичних структурних елементах суспільства, публічних організаціях та установах, включаючи інтегровані [30; 53].

Політична інформація включає опубліковані дані про рішення та дії органів влади всіх рівнів, думки політиків з різних суспільно значущих проблем, матеріали політичних партій та їх об’єднань, інформацію про передвиборчі кампанії та проведення виборів, а також інші інформаційні джерела політичного характеру [69; 164].

У процесі формування політичних ризиків і загроз на основі використання інформації вона може зазнавати різноманітних модифікацій або зникати в ході різноманітних несанкціонованих дій:

– відомості, що мають певну цінність, можуть бути викрадені. Існує кілька різних варіантів несанкціонованого отримання інформації у злочинних цілях з використанням різних електронних пристроїв та технологій;

– законодавством України передбачено відповідальність за зміну інформації, що також є основою формування загрози, особливо у варіантах політичної інформації, що має велику аудиторію одержувачів;

– неправомірне знищення інформації будь-якими способами, що призводять до її повної чи часткової втрати;

– протидія поширенню інформації, що суперечить вимогам законодавства і генерує додаткові загрози безпеці громадян, а також ризики

для навколишнього природного середовища, що своєю чергою негативно позначається на людині;

– у процесі маніпулювання політичною інформацією, що включає, в тому числі, обмеження обсягу доступної для громадян або організацій інформації, необґрунтоване засекречення або фальсифікацію інформації з протиправними та антиконституційними цілями.

Особливо слід підкреслити, що можливі збитки часто мають критичний характер через те, що маніпулятивні дії з інформацією призводять до знищення найважливіших засад суспільного функціонування та розвитку, зокрема, довіри до органів влади, політиків та громадських організацій. У процес прийняття стратегічних і тактичних рішень включаються додаткові чинники, що збільшують час прийняття рішення та ускладнюють його реалізацію.

Прагнення самих органів влади приховати чи обмежити інформацію про негативні чи трагічні події здатне призвести до соціального вибуху, тим більше що в умовах існування глобального інформаційного простору поширення інформації часто відбувається поза офіційною комунікативною системою та ще більше підриває її дієвість.

Єдиний інформаційний простір [84; 224]:

– з одного боку – важливою обов’язковою ознакою та передумовою успішного формування інформаційного суспільства, необхідною умовою входження у світову інформаційну спільноту;

– з іншого боку – виступає головною умовою збереження інформаційного суверенітету держави та зміцнення державності

Аналізуючи тенденції розвитку єдиного інформаційного простору у глобальному вимірі, варто зазначити, що провідні держави світу – США, Канада, Японія, Німеччина, Франція, Велика Британія та Італія – визнали створення єдиного інформаційного простору одним із стратегічних пріоритетів XXI століття та уклали угоду про співробітництво у розбудові

глобальної інформаційної інфраструктури на основі таких засадничих принципів [103; 250]:

– заохочення динамічної конкуренції на інформаційному ринку;

– активізація залучення приватних інвестицій до розвитку інформаційної інфраструктури;

– запровадження гнучких механізмів регулювання інформаційної сфери;

– гарантування відкритого доступу до мереж та загальнодоступності інформаційних послуг;

– забезпечення рівних можливостей доступу до інформації для всіх верств населення;

– врахування існуючих відмінностей, зокрема культурного та мовного різноманіття;

– утвердження міжнародного співробітництва як необхідної умови розвитку, насамперед щодо менш розвинених країн.

Якщо приміряти цей досвід до України, виходячи тільки з першої рольової функції єдиного інформаційного простору – бути складовою світової інформаційної спільноти, – то відповідь, мабуть, повинна бути безумовно позитивною. Так, на міжнародній конференції Світової організації торгівлі (далі – СОТ), що пройшла в лютому 1997 року, було прийнято Угоду 69 країн про лібералізацію ринку зв'язку, де в якості основного пропонується принцип конкуренції – можливості вільного вибору базової інфраструктури зв'язку та інформатизації для постачальників послуг, що вимагає скасування обмежень на використання інфраструктур електрозв'язку [246].

З прикладу реалізації першого запропонованого принципу – розвиток конкуренції та максимальна відкритість – серед потенційних загроз (небезпек) збереження єдиного інформаційного простору можна виділити дві основні: зовнішню та внутрішню.

Зокрема, щодо зовнішньої загрози слід зазначити наступне.

На сьогоднішній день у світі сформувалися три основні відносно ізольовані регіональні центри спеціалізації з виробництва інформаційних

продуктів і високотехнологічних компонентів: Північноамериканське співтовариство, що включає в себе США і Канаду (лідирують у виробництві нових програмних продуктів для широкого використання та розробках нових зразків комп'ютерної техніки), Західна Європа а Китай (має виробничі потужності і порівняно дешеву робочу силу, являє собою масового постачальника елементів комп'ютерної продукції). Україна у цьому міжнародному поділі праці, на жаль, грає поки що, переважно, роль споживача.

За оцінками Світового банку, на розвиток інформаційних технологій у наступні п'ять років потрібно щорічно витрачати 60 млрд. дол. США, що вимагатиме припливу нових інвестицій у галузь [271]. Привабливість даного сектора ринку створює умови для різкої конкурентної боротьби. Ця боротьба має низку особливостей:

– по-перше, серед умов, які забезпечують привабливість ринку для інвесторів, висувається їхня відкритість. Характерно, що найгарячішими прихильниками цієї тези стали США. Протягом 80-90-х років XX ст. на американські корпорації припало 40% світових інвестицій у комп'ютеризацію; вони витрачали на інформаційні технології з розрахунку на душу населення вдвічі більше, ніж європейські компанії, і у вісім разів більше, ніж у середньому усі країни світу [250, с. 44]. На сьогоднішній день кількість комп'ютерів у розрахунку на одну зайняту особу в США у шість разів вища, ніж у Західній Європі чи Японії. Тому, прагнучи закріпити та комерційно використовувати свою перевагу на ключових ринках сучасних послуг та технологій, США ініціювали підписання низки міжнародних угод, що передбачають радикальне скорочення або зниження різних обмежень у галузі міжнародної торгівлі інформаційними продуктами та телекомунікаційними послугами. Ще наприкінці 1996 р. на першій міністерській конференції Світової організації торгівлі (СОТ) у Сінгапурі 14 держав підписали декларацію про торгівлю товарами інформаційних технологій. Мета документа – забезпечити до 2000 р. повну ліквідацію митних тарифів та інших

зборів на такі товари, як комп'ютерна техніка, телекомунікаційне устаткування, напівпровідники, програмне забезпечення тощо. Як умова набуття чинності цієї угоди було приєднання до неї країн, що контролюють понад 90% світового ринку інформаційних технологій;

– по-друге, намітилася ще з початку 80-х років тенденція до винесення ліній з виробництва комп'ютерних компонентів та електроніки за межі національної території США, насамперед у країни Південно-Східної Азії. Такий процес відбувається у Європі та Японії, тобто у найбільш розвинених в інформаційному плані країнах. На даний час в силу низки причин цей процес набув практично незворотної форми. Серед них – низька вартість робочої сили в країнах Південно-Східної Азії; загальна тенденція в розвинених країнах до звільнення власної території від різноманітних масових виробництв за збереження центрів розробки, подібних до «силіконових долин». Прийнята «Стратегія сталого розвитку США» з її особливим акцентом на екологізацію та зміну структури ринку праці всередині США також є внутрішнім фактором, що ускладнює зміну існуючого становища, незважаючи на те, що воно ставить у небезпечну залежність від масових виробників навіть такого лідера інформаційних технологій, як США;

– по-третє, в останні роки зросла небезпека загального спаду обсягів виробництва на ринку високих технологій. Вже в даний час він спостерігається в Азії, Східній Європі та Латинській Америці. Найбільш показовими виявилися зміни на ринку мікросхем оперативної комп'ютерної пам'яті – найстійкіших і найдорожчих компонентів комп'ютерного виробництва. Протягом 1993-1995 років цей сегмент ринку інформаційних технологій переживав загальне піднесення, що супроводжувалося отриманням рекордних прибутків. Основні корейські виробники цієї продукції Samsung Electronics, LG Semicon, Hyndai Electronics у 1995 році отримали понад 5 млрд. дол. США, їх чистий прибуток був більше сукупного доходу всіх інших корейських фірм. Кризові тенденції почали виявлятися ще на початку 1996 р., коли було відзначено падіння цін на ці компоненти. Спочатку падіння цін

торкнулося лише японських та корейських компаній, зайнятих їх випуском. Проте вже на початку 1997 р. східно-азіатські, насамперед тайванські, малазійські та китайські фірми розпочали активне просування на ринку спеціалізованих мікросхем пам'яті, що безпосередньо торкнулося інтересів найбільших американських компаній. Якщо в 1995 р. ринкова вартість 1мБ оперативної пам'яті становила 30 дол. США, на початку 1998 р. – 3 дол. США, а на початку 1999 р. вона становила лише 2 дол. США [257]. Аналогічне демпінгове падіння цін відзначено на ринку виробництва флеш-пам'яті, сигнальних процесорів стільникових телефонів, модемів та іншого комунікаційного обладнання, жорстких дисків та ін.

Отже, можна дійти висновку відносно того, що інтенсивний розвиток інформаційних технологій є важливим викликом часу сучасної епохи. Очевидно, що країни, які намагатимуться не брати до уваги цей фактор, ризикують не лише уповільнити темпи свого соціально-економічного розвитку, а й можуть поставити під удар інтереси своєї національної безпеки в цілому

У рекомендаціях Європейської комісії щодо побудови інформаційного суспільства представлені в узагальненому вигляді такі основні завдання інформаційної політики розвинених країн [244]:

– розвиток інформаційно-телекомунікаційної інфраструктури;

– забезпечення широкого вільного доступу до інформаційних ресурсів;

– забезпечення громадян та суспільства значимою та затребуваною інформацією;

– підготовка людини до життя та роботи в інформаційному суспільстві.

Комплекс заходів, спрямованих на протидію використанню інформації у терористичних цілях включає також необхідність протидії використанню інформаційного простору, і, зокрема, мережі Інтернет.

На сьогоднішній день у законодавстві більшості держав міститься заборона надання засобами масової інформації своїх ресурсів терористичним організаціям, через що терористи активно реалізують свою пропагандистську

діяльність за допомогою використання мережі Інтернет, яка у зв’язку з анонімністю, а також недоліком належного правового регулювання, є сприятливою для розповсюдження несприятливої інформації.

Як справедливо зазначають дослідники, мережу Інтернет нині використовують практично всі відомі терористичні організації, у тому числі для публікації обґрунтування застосування насильства, пропаганди тероризму, вербування у свої лави нових прихильників, фінансування такої діяльності [138; 139].

У той же час вчені в галузі інформаційного права також наголошують на тому, що представники терористичних організацій у питаннях проведення психологічної та пропагандистської роботи в інформаційному просторі по всьому світу діють професійно.

Усі вищеперелічені факти свідчать про те, що з кожним днем загроза поширення деструктивних ідей на масову свідомість у вигляді застосування інформаційно-комп’ютерних технологій лише зростає. Масштабується й використання інформаційно-комп’ютерних технологій для здійснення вербування та залучення до терористичної діяльності нових прихильників. У відповідь на це світове співтовариство має прагнути консенсусу в питаннях необхідності протидії використанню мережі Інтернет для розповсюдження потенційно загрозливої інформації. Усе це вказує на очевидну необхідність формування ефективної системи протидії цій загрозі.

Найбільш ефективними заходами у сфері протидії загрозі діяльності терористичних організацій є вдосконалення нормативної правової бази, а також активізація роз’яснювальної та інформаційно-роз’яснювальної роботи у молодіжному середовищі

Про необхідність врегулювання публічних свобод, які спотворюються терористичною пропагандою, через поширення радикальних ідей та інформації за допомогою Інтернету, а також створення нових правових норм, згадують у своїх роботах численні вчені.

Тероризм, що базується на пропаганді екстремізму в мережі Інтернет, як одну з ключових загроз для держави та суспільства виділяють також науковці у галузі інформаційного права. Активне розповсюдження терористичної та екстремістської ідеології через мережу Інтернет обумовлено, зокрема, відсутністю універсального правового фундаменту як на міжнародному, так і на внутрішньодержавному рівнях.

Проте, одного лише вдосконалення законодавства про боротьбу з тероризмом недостатньо, і набагато важливішою є розробка механізмів запобігання такого роду злочиній діяльності.

Деякі вчені також наголошують на тому, що формуванню ефективної системи протидії тероризму сприятимуть три основні складові, до яких слід відносити інформаційну та роз'яснювальну роботу органів державної влади та місцевого самоврядування, профілактичні заходи щодо терористичної діяльності у молодіжному середовищі, а також удосконалення законодавчої основи протидії тероризму [138; 139; 221].

Погоджуючись із вищезгаданою позицією, слід зазначити, що формування системи протидії тероризму в інформаційному просторі має здійснюватися комплексно і включати в себе в сукупності такі складові, як:

– вдосконалення правового регулювання, а також правових механізмів протидії (пропаганди тероризму, вербування, фінансування злочинної діяльності з використанням інформаційно-комп'ютерних технологій);

– здійснення інформаційно-просвітницької діяльності та формування культури інформаційної безпеки у молодіжному середовищі;

– забезпечення антитерористичної профілактики.

Вихідним кроком у цьому напрямі є вироблення організаційно-правового рішення щодо розбудови впорядкованої системи протидії, яка залучала б ресурси не лише органів державної влади та місцевого самоврядування, а й громадських організацій, зокрема для здійснення моніторингу мережі Інтернет з метою виявлення терористичного контенту.

Отже, нейтралізація загроз протиправного використання інформаційного простору, включаючи терористичні прояви, потребує функціонування комплексної та безперебійно діючої системи протидії як її неодмінної організаційної основи.

Наприклад, доцільним є створення державної системи реагування на інформаційно-психологічні загрози, у складі яких слід виділити так звані контентні загрози, пов’язані, в тому числі з пропагандою тероризму.

У цьому контексті першочергового значення набуває з'ясування змісту поняття «механізм правового регулювання». Правове регулювання традиційно розглядається як одна з форм впливу права на суспільні відносини, що здійснюється за допомогою специфічного юридичного інструментарію: норм права, правовідносин та актів реалізації права. При цьому категорія «механізм правового регулювання» вживається переважно для характеристики динаміки та функціонування права як живого соціального явища [31; 73].

Сьогодні одним з ефективних механізмів впливу на суспільні відносини, а також протидії використанню інформаційно-комп’ютерних технологій в терористичних цілях є блокування інформації в мережі Інтернет, що містить обґрунтування та (або) виправдання здійснення терористичної діяльності.

Також слід навести аргументи фахівців ІТ-компаній, які розглядають питання блокування протиправного контенту безпосередньо з точки зору правозастосування. На їхню думку, з метою забезпечення успішної роботи з блокування протиправного контенту, система має поєднувати у собі кілька основних складових, у тому числі [76; 111; 115]:

– єдиний реєстр ресурсів, які містять протиправну інформацію;

– систему аналітики інформації на наявність протиправного контенту;

– програму з використанням DPI (англ. – dots per inch) та контентної фільтрації.

Звертаючись до тлумачення понять «концепція» та «стратегія», і, навіть, їх співвідношення, можна дійти висновку, що основна відмінність залежить від ступеня конкретизації заходів, які містяться в подібних документах. Якщо

«концепція» – це лише система поглядів, що передбачає відбиток основної ідеї щодо розвитку будь-якої сфери, то стратегія – це вже документ, пов'язаний із плануванням конкретних заходів щодо реалізації наміченого курсу.

Водночас теоретики зазначають, що таку логіку не завжди можна простежити у затверджених на сьогоднішній день державних документах, які називаються у тому числі стратегіями, концепціями чи доктринами, де концепція, наприклад, може містити більш детальні положення та структуру, ніж стратегія [33; 72].

У цьому зв'язку необхідною є розробка нормативно-правового акту, присвяченого питанням використання інформаційно-комп'ютерних технологій у терористичних цілях, що продиктовано її відображенням як однієї з нових загроз національній безпеці.

У зв'язку з тим, що саме стратегія є актом, який містить довгострокові завдання суспільного розвитку поряд із законодавчим регулюванням, представляється, що такого роду акт має бути прийнятий у сфері протидії тероризму з використанням інформаційно-комп'ютерних технологій.

За результатами порівняльного аналізу нормативно-правових актів з питань безпеки можна зробити висновок про те, що питання протидії використанню інформаційно-комп'ютерних технологій у терористичних цілях сьогодні не мають уніфікованого характеру в єдиному інформаційному просторі, а питання відображення такої загрози містяться в різних стратегічних документах.

Для побудови комплексного правового фундаменту доцільною є розробка нормативно-правового акту щодо протидії інформаційному тероризму. Необхідність відображення такого роду загрози у стратегічному документі обумовлена безперервним процесом виникнення нових викликів та загроз, особливо в умовах зміни світопорядку та веденням росією гібридної (інформаційної) війни проти України.

У зв’язку з цим, дослідження дозволило сформулювати низку пропозицій щодо змісту зазначеного проєкту документа стратегічного планування.

Так, у даному проєкті доцільно визначити цілі, завдання та принципи, пріоритети, вектори розвитку та механізми протидії, засновані на системі організаційно-правових заходів у цій галузі, включаючи волонтерську діяльність кібердружин.

Окремої уваги потребує питання нормативного закріплення в зазначеному проєкті цілісної системи термінів і понять у сфері протидії тероризму, зокрема чіткого визначення таких категорій, як «протидія», «інформаційний тероризм» та суміжних понять.

Розробка та прийняття документа стратегічного планування в даній сфері дозволить визначити цілі, завдання, принципи та найбільш ефективні механізми протидії кожному з зазначених типів загрози. Розробка подібних нормативно-правових актів має супроводжуватися застосуванням ризикоорієнтованого підходу. Відповідно до такого підходу, рівень регулювання (включаючи деталізацію сфери) нормативно-правових актів, що розробляються, повинен відповідати рівню наявних у сфері ризиків, які в умовах нового цифрового середовища стрімко розширюються. Але водночас слід наголосити, що будь-яка технологія має і негативні аспекти, у зв’язку з чим необхідно передбачити можливості подолання небажаних наслідків впровадження технологій.

Наприклад, з урахуванням ступеня ризиків та загроз, які походять сьогодні від технологій, слід порушити питання щодо необхідності розроблення спеціального нормативного-правового акта, основу якого, в свою чергу, складе базовий документ у сфері штучного інтелекту. Проте вчені наголошують і на дискусійності поставленого питання.

Очевидно, що використання технологій з протиправною метою, включаючи терористичну, сьогодні стало реальним викликом для сучасного світу. Це виклик для права та правової системи, оскільки в умовах стрімкого

їх розвитку необхідні науково обґрунтовані міждисциплінарні підходи до питань правового забезпечення інформаційної безпеки.

Таким чином, обґрунтованою є позиція щодо розвитку в Україні національної системи політико-правових документів, пов'язаних із протидією використанню інформаційно-комп'ютерних технологій з метою здійснення терористичної діяльності. Таким документом могла б стати Стратегія протидії тероризму, з урахуванням зростання нових викликів та загроз у ІКТ-середовищі, включаючи технології штучного інтелекту та робототехніку.

У дослідженнях, пов'язаних із створенням глобальної системи контртерористичної діяльності в якості одного з найскладніших питань виділяється необхідність встановлення системи контролю за дотриманням конвенційних норм [54; 103].

Також наголошується на тому, що діючі предметні конвенції по боротьбі з терористичною діяльністю в різних сферах не містять спеціальних механізмів відповідальності за недотримання конвенційних норм, що породжує загрозу недотримання взятих на себе тією чи іншою державою обов'язків [54; 124].

Водночас противники створення нового механізму контролю вказують на наявність у системі ООН низки підрозділів, до компетенції яких належать функції протидії тероризму [103; 124].

Справді, наразі в ООН діє Контртерористичне управління ООН, засноване 15 червня 2017 року Генеральною Асамблеєю ООН 71/291, серед основних повноважень якого виділено [267]:

– підвищення рівня координації дій структур, які беруть участь у Глобальному договорі ООН з контртерористичної діяльності;

– підвищення ефективності надання ООН допомоги для зміцнення контртерористичного потенціалу держав;

– інформаційно-просвітницька робота ООН у контексті контртерористичної діяльності.

Контртерористичне управління ООН будує свою антитерористичну діяльність на засадах широкої багатосторонньої взаємодії, залучаючи до співпраці держави-члени, структурні підрозділи системи ООН, інститути громадянського суспільства, міжнародні та регіональні організації, наукову спільноту та інших зацікавлених партнерів.

Однак, як показує аналіз функціоналу цього Управління, жодних спеціальних повноважень щодо вироблення світових стандартів у сфері протидії використанню інформаційно-комп'ютерних технологій у терористичних цілях, а також щодо здійснення оцінки відповідності національних систем, немає.

Позицію щодо доцільності створення окремого спеціалізованого міжнародного органу з контртерористичної діяльності деякі вчені аргументують тим, що в даний час структури ООН не в змозі повноцінно забезпечити реалізацію заходів протидії, які дійсно відповідають сучасним викликам і загрозам у сфері, що підлягає дослідженню. При цьому вони наголошують на тому, що чинні структури ООН нерідко мають програми з дублюючими положеннями, а їх компетенції є дуже заплутаними, що не сприяє формуванню стрункої системи протидії та викликає певні складнощі у міжнародних комунікаціях [54; 103; 233].

На противагу складній системі взаємодії, яка існує на сьогодні в ООН, науковою спільнотою висувається пропозиція про створення концептуально нового договірного органу, який стане ефективною альтернативою чинному механізму та включить до свого складу максимальну кількість напрямків протидії світовому тероризму. До повноважень такого органу також доцільно віднести питання протидії інформаційному тероризму.

Разом з тим геополітична обстановка, що стрімко ускладнюється, а також тиск, який чиниться на ООН та інші глобальні міжнародні майданчики, призначені для узгодження інтересів різних держав, спричинив суттєві труднощі, а найчастіше, – і неможливість вироблення колективних рішень у

таких міжнародних форматах, що також зумовлюють необхідність пошуку альтернативних майданчиків взаємодії.

Вчені відзначають, що для відновлення провідного становища, підвищення значущості та обов'язковості міжнародних інститутів необхідне реформування правозахисних органів ООН, а також пошуки нових способів забезпечення сталого миру та безпеки за допомогою досягнення компромісів та взаємних поступок сторін, що знаходяться у стані протистояння [103; 124; 233].

Усвідомлюючи кризу глобальної системи, що чинить негативний вплив на міжнародне право, а також розвиваючи думку про необхідність заснування універсальної міжнародної організації, одним із прийнятних варіантів у поточних політичних умовах є створення міжурядової організації на регіональному рівні, у контексті розвитку відносин по побудові системи протидії використанню терористами інформаційно-комп'ютерних технологій.

Відповідно, слід дотримуватися позиції щодо необхідності активного розвитку взаємодії у міжнародних регіональних і двосторонніх форматах та доцільності розробки основ відповідного міжнародного законодавства у сфері забезпечення протидії використанню інформаційно-комп'ютерних технологій у терористичних цілях.

У той же час на підставі проведеного аналізу як механізму, що сприяє подальшій імплементації таких міжнародних норм у національні правові системи держав-учасниць міждержавних об'єднань, пропонується дослідити можливість створення спеціалізованого міжнародного регіонального органу (наприклад, міжурядової організації). У зв'язку з цим доцільно проаналізувати повноваження та порядок функціонування міжнародних органів у сфері протидії тероризму, що діють в даний час, аналогічних запропонованому.

З огляду на зазначене, детального аналізу потребує глобальна система протидії легалізації доходів злочинного походження та фінансуванню терористичної діяльності.

Слід підкреслити, що фінансування тероризму найчастіше здійснюється у тому числі за допомогою можливостей інформаційно-комп'ютерних технологій, включаючи мережу «Інтернет», криптовалюту.

Заслуговує на увагу також позиція щодо того, що здійснення фінансування тероризму можливе за допомогою легального використання інформаційно-комп'ютерних технологій, внаслідок чого терористичні загрози можна назвати інтегративними із загрозами в інформаційній сфері, які в сукупності можна розглядати як об'єкт протидії міжнародних та національних систем забезпечення інформаційної безпеки».

Наприклад, мережа Інтернет сьогодні активно використовується терористами з метою збору коштів за допомогою прохання про пожертвування, використання платіжних інструментів, електронної комерції та ін.

Висновок про необхідність дослідження підходів до формування механізмів протидії загрозам використання інформаційно-комп'ютерних технологій в терористичних цілях, і, зокрема, з метою фінансування тероризму, через призму співвідношення існуючих інструментів протидії загрозам як в інформаційній сфері, так і у фінансовій сфері, підтверджується багатьма тезами.

При цьому істотною загрозою є можливість терористичних організацій отримувати кошти від осіб, які не обізнані про справжні цілі збору грошових коштів, та вважають, що спрямовують кошти на благі цілі. Так, низка терористичних організацій створюють підставні організації, які маскуються під благодійні для збору коштів нібито на гуманітарні потреби електронним каналом.

Ще у 2011 році з'явилися повідомлення про те, що близько 90% терористичної діяльності в Інтернеті здійснюється за допомогою інструментів соціальних мереж, у зв'язку з чим одним із основних занепокоєнь експертної спільноти стали можливі наслідки використання терористами подібних сервісів, відкритість і доступність яких використовується ними як ефективний

засіб залучення потенційних прихильників, спосіб комунікації, пропаганди, підбурювань і навіть планування терористичних актів [269].

На підставі вищевикладеного можна зробити висновок про необхідність дослідження підходів до формування механізмів протидії загрозам використання інформаційно-комп'ютерних технологій у терористичних цілях, включаючи порядок імплементації міжнародних норм, зближення національних законодавства через призму співвідношення існуючих інструментів протидії загрозам як в інформаційній, так і у фінансовій сфері.

Провідною міжнародною міжурядовою структурою глобального масштабу у сфері протидії легалізації злочинних доходів і фінансуванню тероризму є група FATF — Міжнародна організація з боротьби з відмиванням грошей.

За даними офіційного вебсайту організації, FATF здійснює безперервний моніторинг нових загроз фінансовій системі, регулярно актуалізує свої оцінки та вносить уточнення до Рекомендацій, забезпечуючи державам доступ до сучасного інструментарію переслідування злочинців [245]. Концептуальним фундаментом Рекомендацій FATF є ризикоорієнтований підхід, який зобов'язує держави самостійно ідентифікувати притаманні їм ризики відмивання грошей і фінансування тероризму з метою оптимального розподілу ресурсів у сегментах із найвищим рівнем загроз.

З метою надання підтримки державам при впровадженні своїх Рекомендацій, FATF також готує керівництва (роз'яснення) та документи про передову практику з цілої низки питань, які регулярно переглядаються з урахуванням досвіду, накопиченого державними органами та приватним сектором. Цей процес може включати проведення роз'яснювальної роботи із заінтересованими сторонами або консультацій з громадськістю.

Зважаючи на те, що держави мають різні правові та адміністративні структури, а також різні фінансові системи, Рекомендації FATF, що встановлюють міжнародні стандарти, підлягають адаптації до конкретних

умов кожної держави. Дані стандарти визначають комплекс заходів, необхідних для виконання державами з метою вироблення державної політики у сфері протидії відмиванню доходів, отриманих злочинним шляхом, та фінансування тероризму, включаючи визначення ризиків, повноважень та відповідальності органів влади, а також вироблення превентивних заходів протидії та інше.

Відповідно, особливий науковий інтерес являє вироблений FATF механізм перевірки дотримання державами встановлених стандартів за допомогою проведення експертами з різних держав виїзних оцінок національних систем протидії відмиванню доходів, отриманих злочинним шляхом, та фінансування тероризму. Звіти, підготовлені групою експертів за підсумками проведення перевірок, використовуються для виправлення державами наявних недоліків та вжиття необхідних заходів щодо їх усунення.

Водночас в інформаційній сфері також спостерігається тенденція до формування норм м’якого права.

Деякі автори справедливо зазначають, що назріла необхідність переосмислення традиційних підходів до формування системи правового регулювання в галузі забезпечення інформаційної безпеки, і, як чинники, що впливають на трансформацію права, виділяють зміну парадигм у міжнародному правовому регулюванні інформаційної безпеки, включаючи створення права різних міждержавних об’єднань, підвищення ролі міжнародних принципів правового забезпечення інформаційної безпеки, а також розвиток загроз у зазначеній сфері [56; 73].

Також слід зазначити, що великі виклики зумовили необхідність пошуку більш універсальних, складноорганізованих механізмів побудови системи правового регулювання, які враховували б особливості механізмів трансформації права, а також необхідність більш тісного розвитку правових, технічних, моральних та корпоративних норм. Це, безумовно, є характерним для правового регулювання системи міжнародної інформаційної безпеки.

У зв’язку з цим необхідно звернутися до історичного аспекту і відзначити, що динаміка розвитку суспільства ще в минулому столітті зумовила появу ширшого спектру правил, ніж правові норми. Таке явище має назву «м’яке право».

Дослідники зазначають, що термін «м’яке право» вперше використав голова Європейського суду з прав людини; після цього зазначене поняття стало активно застосовуватися [54; 73; 113].

Дедалі помітнішою тенденцією в діяльності міжнародних організацій стає звернення до інструментів «м'якого права» як засобу гнучкого, оперативного та результативного регулювання міжнародних відносин.

Деякі дослідники зазначають, що основна причина появи такого явища, як м’яке право, полягала в тому, що норми, які не є юридично обов’язковими, стали відігравати все більшу роль у житті суспільства [73; 113].

Процедура укладання міжнародних договорів регламентована національними актами держав і займає, як правило, значний час, що не сприяє ефективній взаємодії держав за умов прискореного розвитку певного виду суспільних відносин, включаючи інформаційну сферу.

Відповідно, сьогодні термін «м’яке право» включає такі види міжнародних документів як: резолюції, комюніке різних міжнародних організацій, стандарти, керівництва та рекомендації щодо дотримання загальновизнаних принципів та фундаментальних прав, декларації, кодекси найкращої практики тощо.

На сьогоднішній день інформаційне право також не обійшлося без використання інструментів «м’якого права», скоріше навпаки. Про це свідчить щорічне ухвалення резолюцій Генеральної Асамблеї ООН про «Досягнення в сфері інформатизації та телекомунікацій у контексті міжнародної безпеки», положення яких формально не мають юридично обов’язкової сили для держав.

Прикладом є розроблені Групою урядових експертів ООН правила відповідальної поведінки, які не мають обов’язкової сили, і «відбивають очікування міжнародного співтовариства, визначають стандарти

відповідальної поведінки та дозволяють міжнародній спільноті давати оцінку діям та намірам держав».

Разом із тим норми, які мають обов’язкову силу, неспроможні замінювати собою міжнародні правові норми. Слід розглядати такі норми як ті, що узгоджуються з цілями і принципами ООН.

Однак єдине розуміння механізму їх узгодження в даний час відсутнє, у зв’язку з чим одним з найбільш важливих завдань міжнародного співробітництва є підготовка пропозицій щодо створення умов, котрі сприяють використанню одночасно двох способів регулювання міжнародних відносин: нормативно-правового та способу використання норм відповідальної поведінки, що, у свою чергу, надасть ефективне сприяння підтримці міжнародного миру.

За відсутності юридично обов'язкового нормативного масиву у сфері міжнародної інформаційної безпеки особливої актуальності набувають альтернативні регуляторні механізми – політичні документи та інструменти «м'якого права». Дослідники наголошують, що добровільне застосування міжнародною спільнотою необов'язкових норм в інформаційній сфері сприяє зниженню рівня загроз міжнародній інформаційній безпеці та може слугувати відправною точкою для подальшого формування юридично обов'язкової міжнародно-правової бази.

Пропозиції щодо можливості ширшого застосування інструментів м’якого права в питаннях регулювання глобального інформаційного суспільства, а також безпосередньо в галузі забезпечення міжнародної інформаційної безпеки є предметом наукових обговорень [73; 113].

Становлення концепції глобального інформаційного суспільства та спроби її нормативного оформлення загострили питання ефективності саме інструментів м'якого міжнародно-правового регулювання цієї сфери правовідносин. Причина полягає в технічній орієнтованості переважної більшості нормативних актів у галузі інформаційного суспільства, належне розуміння яких потребує глибоких знань інфраструктурних і технологічних

характеристик відповідних систем. Це відкриває можливість для делегування державами повноважень із розроблення стандартів і правил поведінки профільним технічним спільнотам.

Інші дослідники, вважають, що для зміцнення колективної відповідальності держав у галузі глобальної кібербезпеки та стримування кібертероризму необхідно розвивати міжнародні механізми, призначені для держав, котрі не мають законодавства щодо протидії кіберзлочинам [54; 92].

Застосування необов’язкових норм, що регулюють відносини на основі м’якого права, також передбачає підготовку та прийняття деяких доповнень, які уточнюють терміни, що використовуються в необов’язкових нормах, що пропонують методи та способи вирішення проблем.

Відсутність уніфікованої термінологічної бази унеможливлює вироблення єдиного підходу до забезпечення міжнародної інформаційної безпеки та національної безпеки в контексті протидії загрозам у сфері інформаційно-комп'ютерних технологій.

Розбудова та практичне застосування інституту м'якого права на міжнародному рівні є дієвим інструментом реагування на загрози, що стрімко еволюціонують у галузі міжнародної інформаційної безпеки, та протидії використанню інформаційно-комп'ютерних технологій терористичними угрупованнями. Це зумовлено насамперед недостатньою оперативністю традиційних законотворчих механізмів у вирішенні відповідних питань.

Широке впровадження норм м'якого права відкриває можливість для швидкого реагування на виклики і загрози, що виникають у системі міжнародної інформаційної безпеки, та може слугувати ефективним доповненням до уніфікованого законодавства. Такий підхід дозволить державам досягати консенсусу з дискусійних питань і налагоджувати результативну взаємодію попри розбіжності в національних правових системах, що в кінцевому підсумку сприятиме формуванню цілісної архітектури міжнародної інформаційної безпеки.

Підсумовуючи, до ключових висновків належить необхідність імплементації конвенційних норм у національні правові системи держав-учасниць та заснування міжнародного міжурядового органу. До кола повноважень такої організації доцільно включити розроблення рекомендацій, що фактично виконуватимуть роль міжнародних стандартів в інформаційній сфері, а також здійснення контролю за їх дотриманням шляхом проведення регулярного взаємного інформаційного моніторингу держав з метою взаємного оцінювання стану їхніх національних систем.

Нагальним завданням є також вироблення механізму звітування про виконання міжнародних стандартів за аналогією із системою взаємних оцінок відповідності національних законодавств у галузі протидії легалізації злочинних доходів і фінансуванню тероризму.

Так, практика роботи міжурядової організації та її взаємодії з державами-учасницями, що склалася у фінансовій сфері, є успішною, а створення аналогічної моделі взаємодії з питань забезпечення інформаційної безпеки є необхідною з урахуванням того, що кількість загроз у даній сфері тільки зростає, а отже, і зростає потреба у підвищенні швидкості та якості реагування на такі загрози.

Саме в рамках діяльності такої міжнародної міжурядової організації глобального характеру повинні також утримуватися повноваження щодо вироблення універсальних стандартів в інформаційній сфері, де одним із ключових напрямків має стати розробка стандартів у сфері протидії використанню інформаційно-комп’ютерних технологій у терористичних цілях.

Зважаючи на те, що регіональний формат міжнародного співробітництва є пріоритетним для України в нинішніх геополітичних умовах, варто зазначити, що міжнародні організації відіграють особливу роль і в системі протидії легалізації злочинних доходів та фінансуванню тероризму.

Транскордонний характер протиправних діянь у цих сферах, так само як і злочинів в інформаційній площині, зумовлює стійку тенденцію до

виникнення та інституційного зміцнення наднаціональних контрольних органів.

Показовим прикладом є ухвалення Радою Європейського Союзу в травні 2024 року оновленого нормативного пакету у сфері протидії відмиванню злочинних доходів і фінансуванню тероризму, яким передбачено створення Європейського управління з протидії відмиванню доходів та фінансуванню тероризму як координуючого наднаціонального органу, що здійснює нагляд за діяльністю підрозділів фінансової розвідки держав-учасниць.

Узагальнення результатів аналізу антивідмивної системи дозволяє констатувати, що саме її всеосяжний характер є підставою для кваліфікації її як дієвого інструменту нейтралізації загроз у сфері легалізації злочинних доходів і фінансування тероризму. Безперервна еволюція та модернізація цієї діяльності суттєво звужує можливості злочинців, зокрема терористичних організацій, що намагаються використати фінансову систему у власних цілях.

Подібний алгоритм може бути застосовний і при формуванні глобальної системи забезпечення інформаційної безпеки, де невід’ємною складовою є напрямок формування системи протидії використанню інформаційно-комп’ютерних технологій у терористичних цілях.

## 3.2. Модернізація механізмів управління інформаційною безпекою держави

Комплексний механізм протидії інформаційним загрозам різного типу є цілісною системою, елементами якої є заходи різного характеру, здатні протидіяти заподіянню шкоди або нівелюванню цієї шкоди шляхом використання механізмів політичного, організаційного, економічного, правового, соціально-психологічного впливу. Він включає:

– цільові орієнтири та детально розроблені завдання у рамках їх досягнення;

– множинні суб’єкти застосування;

– загрози;

– принципи, які дозволяють досягати ефективності застосування;

– основні прийоми та послідовність їх застосування (рисунок 3.2).

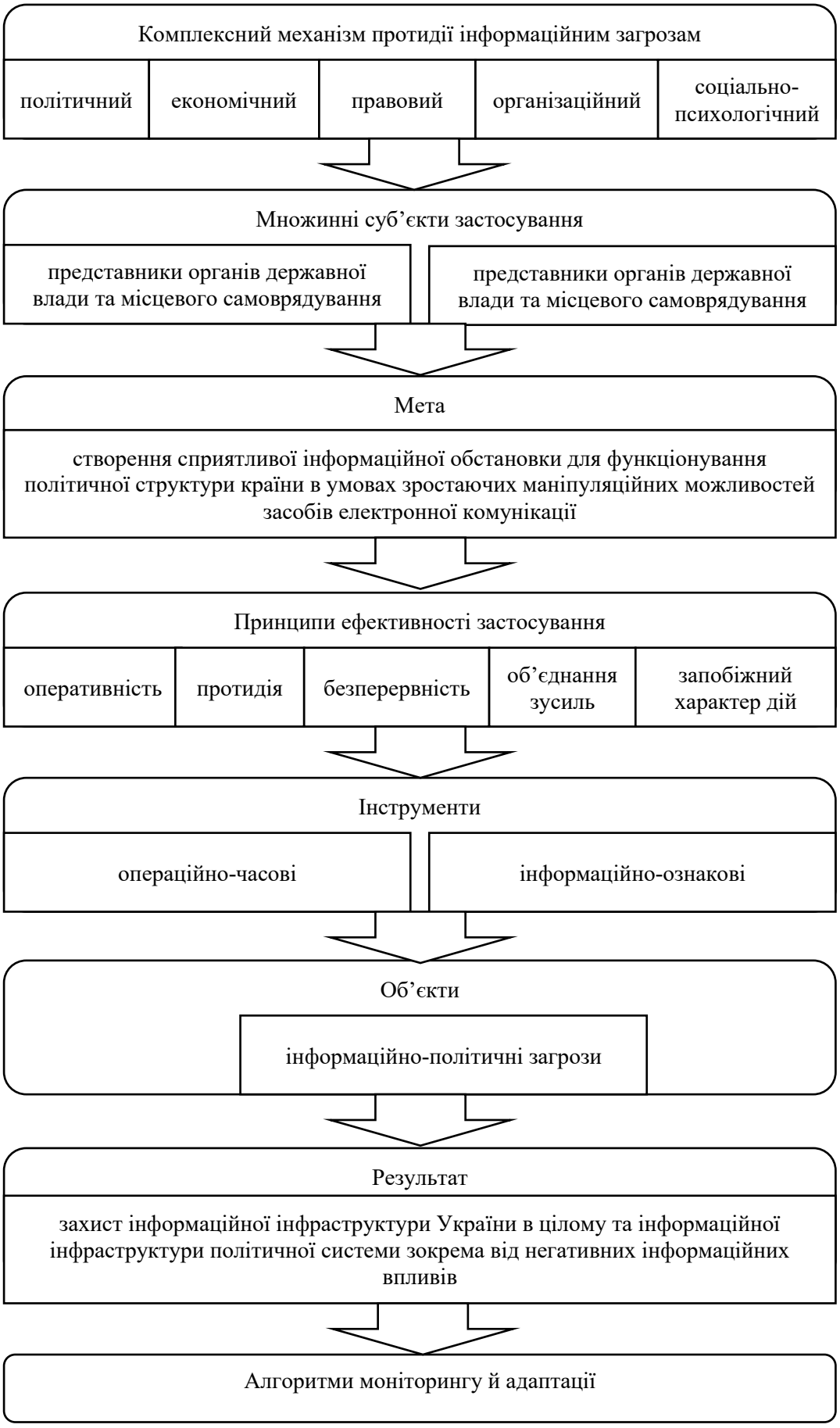


Рис. 3.2. Комплексний механізм протидії інформаційним загрозам

*Джерело: авторська розробка*

Крім того, в сам механізм мають бути вбудовані алгоритми його моніторингу та адаптації, щодо нових змінних, які можуть додаватися до процесу його функціонування. Результати застосування механізму не можуть бути отримані без відповідної ресурсної бази.

Основні елементи механізму протидії інформаційно-політичним загрозам в Інтернеті відповідають наступному критерію: основною метою протидії інформаційно-політичним загрозам є створення сприятливої інформаційної обстановки для функціонування політичної структури країни в умовах зростаючих маніпуляційних можливостей інтернету та інших засобів електронної комунікації шляхом формування спеціальної системи захисту.

Виходячи з поставленої мети, до основних стратегічних завдань протидії інформаційно-політичним загрозам слід віднести:

– прогнозування, виявлення та оцінка джерел і характеру інформаційно-політичних загроз, основних суб’єктів інформаційно-політичного впливу, інформаційно-критичних елементів політичної системи та політичної важливості кожного з них;

– збір інформації про використовувані та перспективні інформаційні технології органів інформаційної протидії стосовно політичної сфери діяльності об’єкта впливу;

– захист елементів політичної системи, і навіть суспільної свідомості на всіх рівнях (починаючи з індивідуального і до загальнонаціонального) від впливів інформаційного характеру, вкладених у поширення ворожої для України політичної інформації;

– захист інформаційної інфраструктури України в цілому та інформаційної інфраструктури політичної системи зокрема від негативних інформаційних впливів;

– створення та розробка стратегії проведення контрінформаційних операцій в інформаційно-політичній сфері у різних умовах внутрішньополітичної та зовнішньополітичної обстановки;

– формування нормативно-правового підґрунтя інформаційно-політичної безпеки, здійснення спеціальних операцій в інформаційній та інформаційно-політичній сферах, а також застосування засобів інформаційної зброї та методів ведення інформаційної війни.

Вирішення цих завдань на початковому етапі передбачає формування переліку суб'єктів інформаційно-політичних загроз з урахуванням того, що політична діяльність представляє сукупність свідомих, цілеспрямованих, вольових дій соціальних суб'єктів щодо реалізації своїх політичних інтересів. До суб'єктів інформаційно-політичних загроз слід віднести представників держави та інших політичних акторів різної природи, включаючи членів громадянського суспільства. Всі ці суб'єкти здатні ефективно вирішувати свої завдання, ведучи активну діяльність в інформаційному просторі. Багато сучасних політиків все частіше звертають увагу на свою присутність у різних соціальних мережах та інтернет-ресурсах: Instagram, YouTube та блогах. 68% глав держав та урядів зі 193 країн-членів ООН мають свої власні акаунти у соціальних мережах [26; 86].

Об'єктами аналізованого механізму протидії є інформаційно-політичні загрози.

До основних принципів ефективного функціонування механізму протидії інформаційно-політичним загрозам слід зарахувати:

– принцип оперативності застосування заходів технології інформаційно-політичного впливу, що полягає у добуванні інформаційних ознак цих заходів у строки, допустимі для вжиття ефективних заходів протидії. В основі принципу оперативності лежить передбачення можливості застосування різноманітних технологій інформаційно-політичного маніпулювання;

– принцип запобіжного характеру дій, сутність якого полягає у запобіганні (та обґрунтуванні) подальшого застосування конкретної технології інформаційно-політичного маніпулювання. Попередження про можливі наслідки та своєчасне вжиття заходів щодо відкритого викриття маніпуляційних дій;

– принцип активності протидії, який полягає у наполегливому прагненні виявити в інформаційному просторі (у тому числі в інтернеті) маніпуляційну інформацію шляхом прояву розумної ініціативи, сміливості та рішучості дій, що ґрунтуються на правильному розумінні інформаційно-політичних загроз та реальних умов інформаційно-політичної обстановки;

– принцип безперервності протидії інформаційно-політичним загрозам, що полягає у постійному виявленні інформації, призначеної для маніпуляцій. Сучасні інтернет технології дозволяють в автоматичному режимі виявляти ознаки такої інформації. Для цього мають бути розроблені дескриптори, що відображають сутність поточних та перспективних політичних процесів, а також можливі варіанти модифікації політичної інформації, що циркулює в інформаційно-критичних елементах політичної структури;

– принцип об’єднання зусиль державних органів інформаційного протиборства, систем внутрішньої безпеки елементів політичної структури та безпосередніх учасників політичного процесу – передбачає їх узгоджені дії на основі чіткого розмежування їхньої компетенції.

Основний сферою інформаційно-політичних загроз є інформаційне забезпечення дій політичної системи як цілісної системи, що включає множинних державних та недержавних акторів, роль яких у стабільному розвитку країни є основною. Цей процес значно ускладнюється через те, що Інтернет має необмежені можливості у сфері політичної інформації. Причому ці можливості мають індивідуалізований характер. Контент, призначений для дезінформації або формування хибних уявлень, може бути трансльований протягом максимально короткого часу практично кожній людині. Контроль над контентом, що розповсюджується у мережі, здійснюється недостатньо ефективно. Крім того, посилення цього контролю набуває суперечності зі свободою інформації.

У мережі досить часто проходять різні заходи політичного характеру, які досить сильно впливають на громадську думку.

Загальний алгоритм протидії інформаційно-політичним загрозам в Інтернеті може бути наведений наступною послідовністю дій.

На першому етапі мають бути розроблені операційно-часові та інформаційно-ознакові моделі інформаційно-політичних дій. Найважливішим елементом цих моделей є термінологічний словник з інформатики, що свідчать про модифікацію (у широкому розумінні – маніпуляції, підміни, розкрадання тощо) інформації.

На наступному етапі в кожному інформаційному контенті, що з'являється в Інтернеті і стосується якогось напряму політичної діяльності, виявляються фрагменти інформації, що характеризують сутність політичних процесів. Далі ці ознаки порівнюються з ознаками, що присутні в словнику. При виявленні інформаційних ознак, що відповідають фактам маніпулювання, робиться висновок про проведення заходу інформаційно-політичного впливу та формується прогноз про використання будь-якої маніпуляційної технології. Це дозволяє, по-перше, вжити заходів протидії інформаційно-політичному впливу на проміжних етапах реалізації технологій, та, по-друге, отримати уявлення про варіанти подальших дій маніпуляторів. Це дозволить зорієнтувати співробітників на цілеспрямований пошук інформаційних ознак, що свідчать про реалізацію технології інформаційного маніпулювання у прогнозованому напрямку, а також виробити спільну стратегію протидії відповідній інформаційно-політичній загрозі.

Як основні джерела інформації при моніторингу інформаційного простору можуть бути використані електронні ЗМІ, пошукові інформаційні масиви текстів, інформація з Інтернет-сайтів та поштових серверів, корпоративні бази даних та електронні архіви документів, а також інформація на матеріальних носіях, результати масового опитування згідно з певними критеріями та інші джерела неструктурованої інформації.

Основними засобами моніторингу інформаційного простору є спеціалізовані інформаційно-аналітичні системи.

Застосування будь-якої технології інформаційно-політичного впливу на політичну структуру країни породжує певні ризики для інформаційно-політичної та загалом національної безпеки країни. При ідентифікації такої технології необхідно проаналізувати причини, джерела та фактори ризику, розкрити специфіку поглядів на ведення інформаційної війни з боку зацікавлених осіб, оцінити рівень інформаційно-політичної загрози та ефективність різних методів протидії їй.

Для реалізації механізму протидії інформаційно-політичним загрозам необхідні певні ресурси, заходи та інструменти протидії, особливо правові, спрямовані на зниження негативних явищ і причин, що їх породжують. Необхідність удосконалення правового забезпечення механізму протидії інформаційно-політичним загрозам нині є постійним предметом політичних дискусій. Питання свободи слова, безпосередньо пов’язане з поширенням інформації в Інтернеті, не має однозначної відповіді.

До основних проблем у правовій сфері, що створюють додаткові можливості щодо використання маніпуляційного потенціалу інформації, слід віднести наступні.

1. Проблему недостатньо чіткої та неповної термінології.

2. Розмитість кордонів юрисдикції України щодо відносин, пов’язаних з використанням мережі Інтернет, недостатньо чітке визначення яких ускладнює розслідування кіберзлочинів, скоєних за кордоном та спрямованих проти України.

3. Невизначеність обов’язків та нечіткий розподіл відповідальності між учасниками відносин, у яких використовується мережа Інтернет. Особливо це стосується знущань та образ у соціальних мережах, чорного піару, негативних/образливих висловлювань на адресу конкретної особи, наклепу, самозванства тощо.

4. Притягнення до юридичної відповідальності за створення та розміщення в мережі Інтернет підроблених вебсайтів, порталів, інформаційних систем або їх складових, що імітують ресурси органів

державної влади, місцевого самоврядування, комерційних і некомерційних організацій з метою введення користувачів в оману – так звані «фішингові» атаки – ускладнюється відсутністю однозначного нормативного визначення правового статусу та допустимих форм електронних доказів;

5. Недостатньо захищені персональні дані, що дозволяють незаконне розповсюдження їх у мережі Інтернет.

Таким чином, розглянуті особливості механізму протидії інформаційно-політичним ризикам та загрозам передбачають вирішення низки нових проблем технічного, організаційного та правового характеру:

– розробка апаратно-програмних засобів, що забезпечують оперативний моніторинг значних обсягів інформації, що циркулює в Інтернет-просторі;

– формування спеціальних інформаційних контурів у діючих інформаційних системах елементів політичної структури, націлених на виявлення інформаційно-політичних загроз;

– вдосконалення інформаційного законодавства України.

Розглянувши механізм протидії інформаційно-політичним загрозам, необхідно включити все вищезазначене до контексту кібербезпеки. Цей вид безпеки є у сучасному світі всеосяжною умовою безпечної, стійкої та ефективної взаємодії із застосуванням будь-якого електронного пристрою, підключеного до мережі. Від цієї умови залежить ефективність економіки, управління, взаємодії між численними учасниками всіх процесів, починаючи з окремих людей аж до урядів та держав.

При цьому найслабшим місцем у загальній системі кібербезпеки є «людський фактор». Це змушує всіх, хто керує процесом, постійно вдосконалювати криптографічні, технічні та інші засоби безпеки. Проте більшість рішень, здатних поліпшити ситуацію, має нетехнічний характер.

Хакерські атаки, які у більшості випадків є продуктом діяльності окремої людини, багатьма державами визнаються нині більш небезпечними, ніж прямі терористичні атаки. Хибна або спотворена інформація, розміщена в мережі, може створювати сильний ефект. Процес поширення такої інформації

часто протікає в режимі ланцюгової реакції та діє за алгоритмом «зіпсованого телефону». Все це разом розриває існуючі інформаційні зв’язки та породжує додаткову нестабільність, страхи не перед реальними подіями, а перед їх інформаційним відображенням.

У побут входить нове поняття «хективізм» (від поєднання англ. haker + activism). Воно визначається як використання хакерських методів для організації протестних акцій та розміщення у мережі політичних заяв, найчастіше екстремістського характеру. Політичні активісти, кіберзаколотники та шкідники роблять атаки практично щодня. З ними дуже важко боротися через те, що ці атаки непередбачувані та раптові. Особливо чутливі до подібних впливів організації, чия діяльність носить характер секретності, та які мають інформацію, що становить державну таємницю [104; 139].

Удосконалення механізмів забезпечення інформаційно-політичної безпеки, так само, як і постійна розробка нових заходів захисту бізнес-даних та персональних даних громадян, потребує розуміння значущості цих механізмів для кожної людини, а не лише для організацій, установ, органів влади та інших політичних акторів. Захист інформаційних мереж та комунікативних механізмів від різних негативних впливів може відігравати вирішальну роль у збереженні стабільності соціуму з одного боку, та його поступального розвитку – з іншого.

Дослідження правового забезпечення протидії загрозам використання інформаційно-комп'ютерних технологій у терористичних цілях як однієї з ключових загроз інформаційній безпеці потребує передусім звернення до термінологічного апарату, зокрема до поняття «інформаційний тероризм», а також з'ясування його співвідношення з категорією «кібертероризм», що набули широкого наукового обігу в сучасній дослідницькій літературі.

Попри значний масив вітчизняних і зарубіжних наукових праць, присвячених феномену інформаційного тероризму та кібертероризму,

загальновизнані та універсальні визначення цих понять у чинних міжнародно-правових актах досі відсутні.

При цьому дослідники відзначають, що в даний час відомі різні види тероризму, серед яких інформаційний тероризм займає особливе місце через використання з його метою досягнень науки і техніки, інформаційно-комунікаційних технологій та інформаційного простору, що дозволяє терористам долати низку обмежень, пов’язаних з територіальними кордонами держав, та в геометричної прогресії збільшує аудиторію, на яку вони можуть впливати [138; 139].

Вироблення спільних міжнародних механізмів протидії терористичним проявам та створення єдиного універсального нормативного документа ускладнюються неоднаковою політичною оцінкою цього явища різними державами, неоднозначним ставленням окремих з них до актів тероризму як до кримінально карних діянь, а також розбіжністю підходів до тлумачення таких категорій, як «інформаційна безпека», «кібертероризм» та «інформаційний тероризм».

Дослідження феномена інформаційного тероризму потребує осмислення крізь призму інформаційного права з двох причин. По-перше, всі правові категорії, що утворюють його зміст, об'єднуються навколо базового поняття інформаційного права, а саме поняття інформації. По-друге, використання інформаційно-комп'ютерних технологій у терористичних цілях належить до найсерйозніших загроз сучасності.

На противагу використанню терміну «інформаційний тероризм» низка держав (наприклад, Іспанія, Індія та ін.) у своїх відповідях на запити Секретаріату ООН з проблематики міжнародної інформаційної безпеки використовують поняття «кібертероризм», а деякі з них (зокрема, Україна) у рамках перспективних напрямів своєї політики ставили завдання щодо закріплення даного терміну (Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [170]).

Враховуючи, що зазначені терміни використовуються у різних трактуваннях, особливий інтерес представляє дослідження наукових підходів до співвідношення понять «інформаційний тероризм» та «кібертероризм.

Зокрема, частина дослідників пропонує тлумачити інформаційний тероризм як сукупність дій, орієнтованих на порушення функціонування інформаційних систем і мереж зв'язку, що створюють загрозу людському життю, заподіяння значної майнової шкоди або інших суспільно небезпечних наслідків, за умови що такі дії вчиняються з метою впливу на прийняття політичних рішень органами влади [113; 115].

Інша група дослідників розкриває співвідношення понять «кібертероризм» та «інформаційний тероризм» через категорію кіберзлочинності [73; 92]. При цьому інформаційний тероризм кваліфікується як явище, орієнтоване на інформаційно-психологічне середовище особистості, суспільства та держави, що застосовує інформаційну зброю для досягнення політично значущих цілей [104; 138 Поняття «використання інформації в терористичних цілях» пропонується виокремити як самостійну категорію, що охоплює пропаганду тероризму, вербувальну та навчальну діяльність [54; 113].

Розгляд використання інформації в терористичних цілях як самостійної категорії дозволяє виокремити три основні напрями пропагандистської діяльності в мережі Інтернет: вербування, радикалізацію та підбурювання до протиправних дій.

У контексті вербування мережа Інтернет слугує платформою для налагодження цілеспрямованих контактів із особами, найбільш сприйнятливими до пропагандистського впливу.

Радикалізація – це ідеологічна обробка з метою здійснення завербованими особами дій протиправного характеру.

Інформаційний тероризм піддається також інтерпретації як різновид терористичної діяльності, що характеризується застосуванням різноманітних методів деструктивного впливу на інформаційну інфраструктуру держави або

її складові, а також навмисним використанням цієї інфраструктури для створення умов, здатних спричинити тяжкі наслідки для держави та суспільства.

Спираючись на наведені наукові позиції, а також аналіз положень досліджених міжнародних актів та інших документів, можна обґрунтувати висновок про те, що категорія «кібертероризм» є вужчою за обсягом стосовно поняття інформаційного тероризму. Вважається, що цей термін вперше з'явився у 1980 році, задовго до того, як Інтернет набув свого нинішнього вигляду. У 1997 році під кібертероризмом було запропоновано розуміти навмисну, політично вмотивовану атаку на інформацію, комп'ютерні системи, програми та бази даних, що спричиняє насильство щодо невійськових цілей, груп цивільного населення або таємних агентів. Наведене формулювання засвідчує, що кібертероризм пов'язується передусім із цілеспрямованими атаками на комп'ютерні мережі.

Однак деякі автори наголошують на багатофункціональному характері кібертехнологій, у зв’язку з чим поняття «кібертероризм» має безліч визначень. Так, поширення пропаганди та радикалізації людей в Інтернеті за допомогою соціальних мереж також підпадають під визначення кібертероризму [86; 269].

Слід зазначити, що в даний час можна виділити два основні підходи до визначення поняття «кібертероризм».

Згідно з першим підходом, кібертероризм можна визначити, ґрунтуючись на ознаках навмисної атаки або загрози її вчинення щодо інформації, мережі та комп’ютера

Зокрема, кібертероризм розглядається як протиправна атака або загроза атаки на комп'ютери, мережі чи інформацію, що в них зберігається, вчинена з метою примушення органів влади до сприяння досягненню певних політичних або соціальних цілей [113, с. 41].

Узагальнюючи наведені підходи, кібертероризм доцільно кваліфікувати як умисний деструктивний вплив на інформацію, що перебуває під правовим

захистом та зосереджена в сегментах критичної інформаційної інфраструктури держави і приватного сектору, який здійснюється шляхом протиправного використання інформаційних систем із політичною метою. Наслідками такого впливу є реальна небезпека загибелі людей, заподіяння значної майнової шкоди або настання інших суспільно небезпечних наслідків.

Прихильники другого підходу наголошують на цільовому характері діянь злочинця. У зв'язку з цим як головна ознака кібертероризму виділяється мета – залякування уряду, населення для примусу вчинити необхідні політичні чи соціальні дії. У цьому зв'язку кібертероризм можна розголядати як «терористичну атаку проти комп'ютерів та мережевих інфраструктур (або як атаку, здійснену за допомогою комп'ютерів), метою якої є дестабілізація роботи критично важливих сфер та здійснення терористичних цілей» [92, с. 11]. У вузькому значенні слова кібертероризм, таким чином, можна визначити виключно як використання мережевих інфраструктур для атак на важливі сфери життєдіяльності. Основною метою атак терористів є залякування органів державної влади та місцевого самоврядування для примусу до виконання необхідних терористами дій.

Таким чином, є обґрунтованим висновок про можливість використання терміна «кібертероризм» для визначення будь-якого акту тероризму, що використовує комп'ютерні технології або мережеву інфраструктуру.

Кібертероризм піддається визначенню як сукупність протиправних діянь у кіберпросторі, що охоплюють посягання на життя людей, погрози розправою, деструктивні дії щодо матеріальних об'єктів, навмисне спотворення об'єктивної інформації та інші дії, спрямовані на нагнітання страху і соціальної напруженості з метою здобуття певних переваг.

Альтернативне тлумачення кваліфікує кібертероризм як умисну діяльність із поширення ідеології насильства та практики тиску на органи державної влади, місцевого самоврядування або міжнародні організації шляхом залякування населення чи застосування інших форм протиправного

насильства з використанням комп'ютерів і комп'ютерних мереж, тобто як систему злочинів у сфері комп'ютерної інформації.

Ще одна наукова позиція тлумачить кібертероризм як ідеологічно та політично вмотивовану злочинну діяльність, що здійснюється в кіберпросторі засобами цифрових технологій та спрямована проти інформації, комп'ютерних систем, програм і баз даних, а також об'єктів критичної інформаційної інфраструктури. Така діяльність створює загрозу життю чи здоров'ю людей або настанню інших тяжких наслідків, слугуючи інструментом залякування населення й органів влади, реалізації злочинних намірів та провокації збройних конфліктів. При цьому дослідники зазначають, що терористичні кібератаки можуть бути спрямовані як проти об'єктів віртуального середовища, так і реальної дійсності.

Поряд із наведеними підходами пропонується ширше формулювання: кібертероризм охоплює протиправне діяння або сукупність таких діянь, що здійснюються із застосуванням комп'ютерних технологій, інформаційних систем та телекомунікаційних мереж, порушують нормальне функціонування комп'ютерної інфраструктури, спричиняють значну майнову шкоду або інші тяжкі наслідки та спрямовані на дестабілізацію діяльності органів влади чи міжнародних організацій або вплив на прийняття ними рішень, включаючи погрозу вчинення зазначених дій із тією самою метою.

На окрему увагу заслуговує позиція, що в кібертероризмі можна виділити дві самостійні групи діянь та у цьому зв’язку розуміти кібертероризмом як навмисне злочинне посягання на інформаційний ресурс або використання цього ресурсу, що лякає населення і створює небезпеку загибелі людини. При цьому в першій групі злочинних діянь об’єктами атак є інформаційні мережі та комп’ютери, а до другої слід відносити злочини, пов’язані з розповсюдженням у мережі «Інтернет» інформації, що чинить жахливий вплив та має ознаки терористичного акту [113; 138].

Важливим також є розмежування в теоретичних дослідженнях понять «кібертероризм» та «кібертеракт».

Зокрема, можна зазначити, що кібертероризму властива різноманітніша структура терористичної поведінки в кіберпросторі, ніж тільки здійснення атак. Таким чином, поняття «кібертероризм» є ширшим і включає в себе також терористичні злочини, що скоюються з використанням Інтернету і пов'язані з вербуванням, фінансуванням, навчанням, популяризацією терористичної ідеї, рекрутуванням до лав терористичних організацій тощо.

Дослідження різноманіття використовуваних у наукових колах дефініцій понять «кібертероризм» показує, що найчастіше дослідники приписують явищу кібертероризму ознаки, характерні для ширшого трактування явища – інформаційного тероризму, що включає в себе, крім технічної складової, психологію вербування, навчання, фінансування, підбурювання).

Крім того, деякі вчені ототожнюють поняття «кібертероризм» та «кібертеракт», що також є неправильним.

Розглядаючи феномен використання інформаційно-комп'ютерних технологій з терористичною метою як загрозу міжнародній інформаційній безпеці, а також при визначенні термінологічного апарату, слід керуватися ширшими формулюваннями і не обмежуватися використанням термінів з приставкою «кібер».

Це, в першу чергу, пов'язано з тим, що тероризм в інформаційному просторі включає не лише технічну складову (комп'ютерні атаки), а також гуманітарну: психологічний вплив, пропаганду, фінансування, рекрутування за допомогою використання інформаційно-комп'ютерних технологій.

З проведеного аналізу можна дійти висновку у тому, що у міжнародних актах найчастіше законодавець використовує термін «інформаційний тероризм» з метою відображення дефініції поняття використання інформаційно-комп'ютерних технологій у терористичних цілях.

Особливий науковий інтерес представляє розгляд питань щодо правових та пов'язаних з ними організаційних механізмів протидії

застосуванню ІКТ терористами, які сьогодні не тільки актуальні, а й необхідні для вдосконалення системи політико-правових документів у цій галузі.

Формування системного підходу до вироблення превентивних заходів реагування на нові виклики та загрози в інформаційній сфері, що особливо загострилися в умовах повномасштабного російського вторгнення, потребує принципово нових науково обґрунтованих концептуальних рішень. Це завдання стосується не лише захисту критичної інформаційної інфраструктури України, а й убезпечення інших інформаційних систем, зокрема цифрових платформ, що виступають провідними рушіями економічного зростання.

З огляду на зазначене, інструменти правового забезпечення системи протидії деструктивним інформаційним впливам потребують суттєвого перегляду та оновлення.

Комплексне дослідження й оцінювання організаційно-правових механізмів протидії використанню інформаційно-комунікаційних технологій у терористичних цілях щодо комп'ютерної та інформаційної інфраструктури, включаючи критичну, передбачає з'ясування ключових етапів становлення системи безпеки в цій сфері та аналіз відповідної нормативно-правової бази.

Поряд із базовими інструментами протидії зазначеним явищам, що охоплюють розроблення всеосяжної стратегії кібербезпеки організації з визначенням конкретних процедур реагування на кожен тип інцидентів інформаційної безпеки та відповідне навчання персоналу, особливої уваги потребує вдосконалення системи правового забезпечення.

Практика засвідчує, що кібертерористичні атаки спрямовані передусім на порушення функціонування інформаційних систем, пов'язаних з управлінням реальними фізичними процесами в різних сферах життєдіяльності особистості, суспільства і держави, що безпосередньо становить загрозу національній безпеці.

Фахівці в галузі інформаційних технологій виокремлюють різноманітні типи атак на інформаційну інфраструктуру, у зв'язку з чим у дослідженні пропонується звернутися до однієї з найбільш поширених класифікацій, що

активно застосовується хакерами в умовах наростаючої кризи світового порядку.

Так, APT-атаки (англ. – Advanced Persistent Threat) – це цілеспрямовані ретельно сплановані і добре організовані кібератаки, що становлять найбільшу небезпеку для комерційних організацій і державних органів, та включають кілька етапів, у тому числі:

– підготовку (виявлення мети атаки, збирання інформації про інформаційні системи, програмне забезпечення, розробка стратегії);

– впровадження (обхід засобів захисту, експлуатація вразливостей, інвентаризація мереж);

– поширення (у тому числі пошук необхідної інформації);

– досягнення цілей (розкрадання інформації, зміна даних), а також знищення слідів присутності. Як відзначають фахівці в галузі інформаційних технологій, такого роду атаки можуть бути скоєні не тільки на конкретний об’єкт, а й на цілу галузь, а зловмисники можуть залишатися непоміченими протягом періоду атаки, протягом якого мають доступ до всієї інформації, котра міститься в інформаційних системах, що атакуються.

Дослідники серед найнебезпечніших видів атак виділяють використання шкідливого програмного забезпечення (далі – ПЗ). ПЗ – це комп’ютерна програма або переносний код, до основних видів яких фахівці в галузі інформаційних технологій відносять, так званих мережевих черв’яків, класичні комп’ютерні віруси, троянські та інші шкідливі програми, призначені для реалізації прихованого нецільового використання ресурсів комп’ютерної системи або іншого негативного впливу, що перешкоджає штатному функціонуванню інформаційної системи [228; 238].

DoS-атаки (англ. – distributed denial-of-service) – розподілені атаки типу «відмова від обслуговування, за принципом здійснення бомбардування порожніми запитами сервера сотнями або тисячами географічно розподілених хостів, після чого відбувається перевантаження сервера та неможливість своєчасної обробки легітимних запитів.

Фішинг – вид інтернет-шахрайства, в ході якого користувач переходить на заявлений інтернет-сайт і фактично перенаправляється на підставний сайт, метою якого є отримання таких конфіденційних даних користувача, як логін та пароль [111; 115].

Спуфінг являє собою різновид кібератаки, за якої зловмисник маскується під надійне джерело з метою отримання несанкціонованого доступу до потрібних даних або інформації. Очевидно, що всі згадані вище типи комп'ютерних атак можуть застосовуватися у тому числі з терористичною метою. При цьому загострення геополітичної ситуації після початку повномасштабного російського вторгнення зумовило суттєве зростання кількості кібератак на об'єкти критичної інфраструктури України [66; 197].

Комплексна протидія використанню інформаційно-комп'ютерних технологій у терористичних цілях охоплює також заходи щодо унеможливлення протиправного використання інформаційного простору загалом і мережі Інтернет зокрема.

На сьогоднішній день у законодавстві більшості держав міститься заборона надання засобами масової інформації своїх ресурсів терористичним організаціям, через що терористи активно реалізують свою пропагандистську діяльність за допомогою використання мережі «Інтернет», яка у зв’язку з анонімністю, а також недоліком належного правового регулювання є сприятливою для регулювання.

Як справедливо зазначають дослідники, мережу «Інтернет» нині використовують практично всі відомі терористичні організації, у тому числі для публікації обґрунтування застосування насильства, пропаганди тероризму, вербування у свої лави нових прихильників, фінансування такої діяльності тощо [138; 139].

Як справедливо зазначається вченими в галузі правових і політичних наук, усі вищеперелічені факти свідчать про те, що з кожним днем загроза поширення впливу деструктивних ідей на масову свідомість у вигляді

застосування ІКТ лише зростає [54; 113]. Масштабується використання ІКТ для здійснення вербування та залучення до терористичної діяльності нових прихильників. У відповідь на це світове співтовариство має прагнути консенсусу в питаннях необхідності протидії використанню в терристичних цілях мережі «Інтернет». Усе це вказує на очевидну необхідність формування ефективної системи протидії цій загрозі.

При цьому спочатку необхідне організаційно-правове рішення щодо створення впорядкованої системи протидії, із залученням не лише ресурсів органів публічної влади, а й громадських організацій, включаючи можливості так званих кібердружин, у тому числі з метою здійснення моніторингу мережі «Інтернет» щодо виявлення терористичної інформації.

Позасудове блокування терористичного контенту в мережі Інтернет набуло сьогодні статусу одного з найбільш дієвих інструментів регулювання суспільних відносин і протидії використанню інформаційно-комунікаційних технологій у терористичних цілях. Йдеться насамперед про обмеження доступу до інформації, що обґрунтовує або виправдовує здійснення терористичної діяльності.

На підтвердження цієї позиції слід навести аргументи фахівців IT-компаній, які розглядають питання блокування протиправного контенту безпосередньо з правозастосування. На їхню думку, з метою забезпечення успішної роботи з блокування протиправного контенту, система має поєднувати у собі кілька основних складових, у тому числі [76; 111; 115]:

– єдиний реєстр ресурсів, які містять протиправну інформацію;

– систему аналітики інформації на наявність протиправного контенту;

– програму з використанням DPI та контентної фільтрації.

Результати проведеного аналізу переконливо засвідчують, що оновлення механізмів державного управління інформаційною безпекою в умовах гібридних загроз є багатовимірним завданням, що інтегрує технічні, організаційні та правові складові в єдину взаємозалежну систему. Розроблений комплексний механізм протидії інформаційно-політичним

загрозам, що ґрунтується на засадах оперативності, запобіжності, активності та безперервності, закладає концептуальний фундамент для розбудови ефективної системи захисту інформаційного простору держави. Практичне впровадження цього механізму наштовхується на комплекс системних перешкод: термінологічну невизначеність у сферах інформаційного тероризму та кібертероризму, розмитість юрисдикційних меж, недостатній рівень захисту персональних даних і прогалини в правовому регулюванні інтернет-середовища. Особливої гостроти набуває проблема чіткого розмежування категорій «інформаційний тероризм» та «кібертероризм», адже точність термінологічного апарату безпосередньо визначає якість як національного законодавства, так і міжнародної взаємодії у протидії протиправному застосуванню інформаційно-комп'ютерних технологій. Сукупність зазначених викликів підтверджує необхідність системного вдосконалення правового забезпечення інформаційної безпеки України із залученням як кращих міжнародних практик, так і унікального досвіду, здобутого в умовах повномасштабної збройної агресії.

### 3.3. Моделювання ризиків для інформаційно-критичних елементів політичної інфраструктури для  в умовах гібридних загроз

Один із головних принципів впливу на будь-яку структуру – це принцип поразки. Його мета – нанесення максимальної шкоди при мінімальних витратах. Він передбачає деструкцію суб’єкту та його структури за рахунок виведення з ладу системоутворюючих елементів. Частіше за все принцип структурної поразки містить фізичний вплив на ключові елементи.

Цінність інформації та її сила впливу на в інформаційному суспільстві суттєво збільшується. Внаслідок цього організаційно-соціальна структури схильні до структурного маніпуляційного впливу. До такого типу структур слід зарахувати політичну систему країни.

У найзагальнішому вигляді до складу політичної системи входять [72; 112]:

– інституційна підсистема, що включає державу, партії, громадські об’єднання, засоби масової інформації (ЗМІ), церкву;

– нормативна підсистема, що включає політичні, правові і моральні норми, звичаї, традиції, символи;

– комунікативна підсистема, що включає форми взаємодії влади, суспільства, індивіда (зустрічі, виступи, прес-конференції, ЗМІ тощо);

– культурно-ідеологічна підсистема, що включає систему цінностей, ментальність (характер і спосіб мислення), ідеологія, релігія;

– функціональна підсистема, що включає засоби та способи реалізації влади (примус, переконання, авторитет, заохочення, насильство тощо).

Наведені елементи політичної системи мають різні організаційні, технічні, інформаційні й інші зв’язки, утворюючи відповідну структуру системи. У зв’язку з істотним зростанням значущості інформаційних процесів приділяють значну увагу забезпеченню ефективності функціонування інформаційних структур. При цьому як критичні елементи інформаційної інфраструктури зазвичай розглядають інформаційні системи та інформаційно-телекомунікаційні мережі всіх базових елементів систем управління в промисловості, соціальній сфері, а також органах публічної влади [89; 92]. У зв’язку з цим в політичній структурі важливе значення має інформаційно-психологічний вплив на окремі особистості (насамперед, політично та соціально значущі), громадські та соціальні групи, на все населення загалом.

Інформаційно-критично важливим елементом політичної структури вважається акт маніпуляційного інформаційного впливу, щодо якого порушено (чи припинено) функціонування інформаційної складової. Він є елементом інформаційної складової політичної структури. Це може призвести до втрати керованості в масштабах країни або окремої частини її території, а також до важких дисфункцій в інфраструктурі та економіці на тривалий період.

Інформаційно-критично важливими елементами політичної структури України слід уважати [89; 91]:

– політичних, державних, громадських діячів, які впливають на розвиток політичної системи;

– правлячу політичну й економічну еліту;

– суспільно-політичні організації (об’єднання), що працюють у найважливіших сферах життя соціуму та забезпечують такий важливий та складний параметр якості життя як духовний розвиток людини, самореалізацію особистості, передачу знань та ціннісних орієнтацій соціуму, національної та місцевій спільноті, новим поколінням;

– соціально-демографічні групи;

– державні інформаційні ресурси та доступ до них відповідно до чинного законодавства з метою забезпечення всіх учасників інформаційної взаємодії достовірною та актуальною інформацією.

Значність інформаційно-критичних елементів у конкретному варіанті політичної структури може визначатися двома наступними основними способами.

1. Шляхом проведення експертного опитування. Метод експертних оцінок є добре апробованим методом для прогнозування поведінки складних об’єктів та процесів, до яких належить політична діяльність. Особливістю застосування методу експертних оцінок у розглянутому випадку є необхідність формування експертної групи, до якої повинні входити експерти, які займають об’єктивну, незалежну позицію щодо подій, що відбуваються в країні.

Складність вирішення цього завдання полягає:

– по-перше, у тому, що більшість фахівців не завжди мають єдину думку, але займають чітко означену позицію з питань політичної організації країни, що в результаті не дозволяє отримати консолідовану оцінку процесу, що розглядається, або навпаки – забезпечує домінування одних поглядів над іншими;

– по-друге, ці експерти самі можуть бути об’єктами інформаційно-політичних маніпуляцій і можуть під їх впливом дійти неоднозначних висновків та вчинків;

– по-третє, реалізація методу потребує значних часових витрат, що в умовах високої динаміки інформаційно-політичної обстановки не завжди відповідає вимогам оперативності.

2. Шляхом проведення багатовимірного аналізу. Цей метод враховує формальний вплив зв’язків між елементами будь-якої, зокрема, політичної структури.

До його переваг можна віднести:

– по-перше, наявність арсеналу знань, що дозволяють точно визначити ключові елементи будь-якої структури;

– по-друге, вирішення цього завдання легко автоматизувати.

Отже, щодо інформаційно-критичних елементів політичної структури доцільно використовувати метод, який частково усуває окремі недоліки кожного методу.

Наявність впливу на інформаційно-критичні елементи політичної системи України через Інтернет підтверджується наступними ознаками.

По-перше, зростанням інформаційних контентів, спрямованих на конкретні інформаційно-критичні елементи політичної структури, аналізу їхнього змісту та інтенсивності.

По-друге, зміною поведінки елементів політичної системи після реалізації виявлених інформаційно-політичних загроз.

По-третє, зростанням інформаційних контентів, спрямованих на тісно пов’язані з конкретними інформаційно-критичними елементами політичної структури особами (об’єктами, процесами), аналізу їхнього змісту та інтенсивності.

По-четверте, посиленням інтенсивності появи в інтернет-просторі позитивних оцінок у діяльності окремих інформаційно-критичних елементів політичної системи з боку політичних конкурентів.

Таким чином, до інформаційно-критичних елементів політичної системи відносяться як одухотворені, так і неживі об’єкти. Кожен із цих елементів є першочерговим об’єктом масованого маніпуляційного інформаційного впливу, чому багато в чому сприяють потенційні можливості інтернету. Наявність такого впливу на інформаційно-критичні елементи політичної системи підтверджується зростанням цільових інформаційних контентів як негативістського, так і компліментарного характеру. А також зміною характеру прийнятих рішень особами, котрі зазнали інформаційно-політичного впливу, після безпосереднього контакту з суб’єктом впливу або порушенням режиму функціонування інформаційних систем.

Інформаційно-політичні ризики та загрози є процесами, що розвиваються, на основі використання методів політичної маніпуляції. Їхня мета: створення в об’єктів маніпуляції необхідних поглядів на соціально-політичний розвиток країни.

Основу моделювання таких процесів становить теорія сценаріїв. На її основі створюються логічно пов’язані (гіпотетичні) послідовності подій. Ця теорія дає можливість визначати конкретні варіанти розвитку інформаційно-політичних ризиків та загроз. Також існує можливість давати якісну чи кількісну оцінку можливих альтернативних варіантів їх реалізації.

До основних видів подібних сценаріїв слід відносити наступні: вербальні сценарії, фрейм-сценарії, віяла варіантів (рішень, концепцій), інформаційно-ознакові моделі.

Як вихідні дані для побудови сценаріїв можна використовувати:

– наявність проблемної ситуації (економічної, політичної чи іншої), що включає всі необхідні дані для прийняття рішень про загальний характер сценарію (оптимістичний, збереження статус-кво або песимістичний), а також для детальної розробки його окремих етапів та елементів;

– конкретний і поетапний план дій для якомога швидшого вирішення проблемної ситуації.

Зазначені вихідні дані широко застосовуються для виявлення стандартних сценаріїв розвитку ризиків і загроз. Однак у відомих методах сценарного моделювання слабо враховується вплив стану інформаційного середовища на процес формування та розвитку цих загроз загалом, а також не розглядається залежність стану акторів від інформаційного впливу. Крім того, типові моделі вимагають їхньої адаптації до конкретної суспільно-політичної обстановки, особливостей політичних поглядів різних верств населення, соціальних груп, державних, політичних та громадських діячів, у тому числі їх індивідуальних властивостей.

Разом із тим у відомих підходах є низка методологічних прийомів, комплексне застосування яких дозволяє на їх основі побудувати нову загальну технологію сценарного моделювання інформаційно-політичного впливу (маніпулювання), що враховує інформаційний фактор у процесі формування та розвитку загрози. Ця технологія є взаємопов’язаною реалізацією наступних модельних блоків: «структура інформаційно-політичної загрози», «політична структура», «визначення інформаційно-критичних елементів політичної структури», «операційно-тимчасова модель інформаційно-політичного впливу», «оцінка поточного стану інформаційно-політичного впливу» (рисунок 3.3).

Зокрема, модельний блок «структура інформаційно-політичної загрози» є сукупністю інформаційних ознак, та виявляються в інформаційному просторі, що характеризують об’єктивно сформовану сукупність несприятливих умов і факторів.

Модельний блок «політична структура» визначає важливі елементи політичної структури країни, вказує на їх взаємозв’язки та зв’язки із довкіллям. При моделюванні політичної структури основну увагу слід приділяти аналізу залежності стану будь-якого елемента політичної структури від різних видів інформації.


Рис. 3.3. Загальна технологія сценарного моделювання інформаційно-політичного впливу (маніпулювання)

*Джерело: авторська розробка*

Модельний блок «визначення інформаційно-критичних елементів політичної структури» є важливим механізмом визначення елементів її нормативної, комунікативної, інституційної, функціональної, культурно-ідеологічної підсистем. Маніпуляційний вплив порушує функціонування інформаційних складових, викликає важкі збої в управлінні та інфраструктурі,

а також економіці країни та регіонах. Першочерговий інформаційно-політичний вплив здійснюється саме на ці елементи.

Модельний блок «операційно-тимчасова модель інформаційно-політичного впливу» встановлює сукупності інформаційних ознак, що склалися, а також зв'язки між ними на конкретний момент часу. Ця процедура характеризує будь-який маніпуляційний вплив в Інтернет-просторі.

Модельний блок «оцінка поточного стану інформаційно-політичного впливу» є механізмом визначення суми інформаційних ознак окремих заходів щодо застосування методів інформаційно-політичного впливу.

Далі слід представити елементи, що характеризують структуру потенційної інформаційно-політичної загрози, що виникає в інформаційному просторі:

– сукупність несприятливих факторів та умов;

– суб'єктивні наміри;

– об'єктивні можливості здійснення суб'єктивних намірів;

– умови, що формуються без участі суб'єкта;

– умови, що формуються суб'єктом.

– наявність існуючих засобів та сил;

Так, якщо технологія інформаційно-політичного впливу спрямована на значну високопосадову особу, то вона повинна враховувати:

– специфіку її характеру та способу життя;

– можливість впливу на цю особу в процесі її контактів з високопоставленими представниками держав-конкурентів на офіційних заходах та в ході приватних зустрічей;

– ступінь участі цієї особи в інформаційному просторі в цілому та в інтернет-просторі, зокрема, на офіційному та особистому рівні;

– ступінь довіри до посадової особи під час виконання нею своїх обов'язків;

– рівень взаємовідносин посадової особи з системною та несистемною опозицією та її подання в інформаційному просторі;

– наявність близького оточення, здатного приймати управлінські рішення;

– наявність у країні подій негативного характеру;

– техногенні катастрофи, що відбулися;

– недостатнє нормативне забезпечення діяльності посадових осіб у сфері національної безпеки.

Крім того, повинні бути розглянуті зв'язки цієї посадової особи з іншими інформаційно-критичними елементами політичної структури та виявлено потенційний ступінь впливу цих елементів на посадову особу, що розглядається.

Наявність цих властивостей дозволяє виділити основні взаємозалежні напрями інформаційно-політичного впливу при формуванні та реалізації загрози «нав'язування неприйнятних стандартів у розвитку демократичного суспільства» в частині зміни його керівництва:

– інформаційно-політична атака на саму посадову особу;

– інформаційно-політична атака на її близьке оточення (родичі, друзі, соратники);

– інформаційно-політична операція щодо тісно пов'язаних із посадовцем інформаційно-критичних елементів політичної структури;

– інформаційно-політична операція щодо населення.

У процесі реалізації інформаційно-політичних технологій в інтернет-просторі використовують як відкриті види інформаційно-політичної маніпуляції, так і методи прихованих маніпуляцій з метою спонукання до різноманітних дій. У цьому зв'язку слід виділити три групи інформаційних ознак:

– інформаційні ознаки відкритого інформаційного впливу на всі елементи політичної структури в усіх розглянутих напрямах. Ці ознаки можуть бути визначені шляхом сутнісного аналізу інформаційних контентів, що з'являються у відкритій частині інтернету;

– інформаційні ознаки, що відображають результати прихованої інформаційно-політичної дії. Ці ознаки можуть бути визначені двома способами:

а) по-перше, шляхом аналізу прихованої частини інтернету («глибока зона» – це тисячі сторінок інтернету, які приховані від індексації пошукових систем, а потрапити на них можна лише з зашифрованих інтернет-з'єднань);

б) по-друге, за результатами діяльності посадової особи після її планових офіційних чи приватних контактів з представниками;

– інформаційні ознаки, що відповідають загальним результатам інформаційно-політичної дії. Ці ознаки можуть бути вироблені шляхом аналізу поточного стану суспільно-політичної обстановки в країні та її висвітлення в Інтернеті.

Реалізація інформаційно-політичної загрози «нав'язування неприйнятних стандартів розвитку демократичного суспільства» в інтернет-просторі також супроводжується певними інформаційними ознаками.

Розподіл усіх інформаційних ознак на три групи призводить до особливостей побудови та використання інформаційно-політичних впливів, до основних з яких належать:

– синхронізація частини елементів моделі з тимчасовим графіком діяльності посадової особи. Саме під час проведення важливих політичних заходів: по-перше, створюються найбільш сприятливі можливості для інформаційно-політичного впливу на посадову особу; по-друге, спостерігається особлива активність інформаційної війни;

– використання переліку прогнозованих інформаційних ознак, які можуть виникнути в результаті прихованого інформаційно-політичного впливу на посадову особу з урахуванням, по-перше, потенційних можливостей маніпуляційних технологій в цілому, та в інтернет-просторі зокрема, по-друге, ділових, морально-психологічних та інших особистісних характеристик самої посадової особи. Фіксування потенційних інформаційних ознак після

проведення заходів може вимагати серйозного коригування інформаційно-психологічного впливу;

– виділення фрагментів, пов’язаних із заходами загального інформаційно-політичного впливу на всі елементи політичної структури та кількох фрагментів, пов’язаних із заходами прихованого інформаційно-політичного впливу щодо посадової особи та оточуючих її осіб;

– облік кореляції відкритих та прихованих видів інформаційно-психологічного впливу: інтенсифікація відкритих інформаційно- політичних впливів дає можливість прогнозувати аналогічний процес щодо певних політиків чи посадових осіб.

Пропонований метод сценарного моделювання інформаційно-політичних загроз дає можливість:

– побудувати моделі інформаційно-політичного впливу, реалізовані на основі методів інформаційно-політичного маніпулювання в інтернет-просторі з урахуванням його інформаційно-ресурсного потенціалу;

– визначити основні напрямки інформаційно-політичного впливу (інформаційно-критичні елементи політичної системи).

Таким чином, розроблена в межах підрозділу загальна технологія сценарного моделювання інформаційно-політичного впливу є авторським внеском у вирішення актуального наукового завдання — формування аналітичного інструментарію для виявлення, оцінювання та протидії інформаційним загрозам в умовах гібридної війни. Запропонований підхід, що інтегрує п'ять взаємопов'язаних модельних блоків — від структури інформаційно-політичної загрози до оцінки поточного стану інформаційного впливу, — дозволяє системно аналізувати маніпуляційні процеси в інтернет-просторі з урахуванням специфіки інформаційно-критичних елементів політичної структури України. Принципово важливим є те, що запропонована технологія охоплює як відкриті, так і приховані форми інформаційно-політичного впливу, а також враховує індивідуальні характеристики об'єктів маніпуляції — від окремих посадових осіб до широких соціально-

демографічних груп. Практична цінність розробленої моделі полягає у можливості її використання суб'єктами забезпечення інформаційної безпеки для своєчасного виявлення ознак інформаційно-політичних загроз, прогнозування подальших дій маніпуляторів та формування адекватних стратегій протидії, що є особливо значущим в умовах триваючої російської інформаційної агресії проти України.

**Висновки до третього розділу**

1. Зазначено, що формування системи протидії тероризму в інформаційному просторі має здійснюватися комплексно і включати в себе в сукупності наступні складові:

– вдосконалення правового регулювання, а також правових механізмів протидії (пропаганди тероризму, вербування, фінансування злочинної діяльності з використанням інформаційно-комп’ютерних технологій);

– здійснення інформаційно-просвітницької діяльності та формування культури інформаційної безпеки у молодіжному середовищі;

– забезпечення антитерористичної профілактики.

Зазначено, що при цьому спочатку необхідне організаційно-правове рішення щодо створення впорядкованої системи протидії, із залученням не лише ресурсів органів державної влади та місцевого самоврядування, а й громадських організацій, у тому числі з метою здійснення моніторингу мережі Інтернет щодо виявлення терористичної інформації.

2. Визначено стратегічні пріоритети протидії інформаційно-політичним загрозам:

– випереджувальне прогнозування, своєчасне виявлення та комплексне оцінювання джерел і природи інформаційно-політичних загроз, провідних суб'єктів інформаційно-політичного впливу, інформаційно-критичних елементів політичної системи та ступеня їхньої політичної значущості;

– накопичення відомостей про застосовувані та перспективні інформаційні технології органів інформаційного протиборства щодо політичної сфери діяльності об'єкта впливу;

– убезпечення елементів політичної системи та суспільної свідомості на всіх рівнях, від індивідуального до загальнонаціонального, від інформаційних впливів, спрямованих на поширення ворожої щодо України політичної інформації;

– протидія негативним інформаційним впливам на інформаційну інфраструктуру України загалом та інформаційну інфраструктуру політичної системи зокрема;

– формування та реалізація стратегії проведення контрінформаційних операцій в інформаційно-політичній сфері за різних умов внутрішньо- та зовнішньополітичної кон'юнктури;

– формування нормативно-правового підґрунтя інформаційно-політичної безпеки, здійснення спеціальних операцій в інформаційній та інформаційно-політичній сферах, а також застосування засобів інформаційної зброї та методів ведення інформаційної війни.

3. Запропоновано комплексний механізм протидії інформаційно-політичним ризикам і загрозам різного типу, котрий складається з політичного, організаційного економічного, правового, соціально-психологічного компонентів, та який передбачає застосування різнохарактерних заходів, здатних протидіяти заподіянню шкоди або нівелюванню цієї шкоди. Зазначений комплексний механізм включає:

– цільові орієнтири та детально розроблені завдання у рамках їх досягнення;

– множинні суб’єкти застосування;

– загрози;

– принципи, які дозволяють досягати ефективності застосування;

– основні прийоми та послідовність їх застосування.

Підкреслено, що в комплексний механізм протидії інформаційно-політичним ризикам і загрозам мають бути вбудовані алгоритми його моніторингу та адаптації, щодо нових змінних, які можуть додаватися до процесу його функціонування.

Запропонований комплексний механізм протидії інформаційно-політичним ризикам передбачає вирішення низки нових проблем технічного, організаційного та правового характеру:

– розробка апаратно-програмних засобів, що забезпечують оперативний моніторинг значних обсягів інформації, що циркулює в Інтернет-просторі;

– формування спеціальних інформаційних контурів у діючих інформаційних системах елементів політичної структури, націлених на виявлення інформаційно-політичних загроз;

– вдосконалення інформаційного законодавства України.

4. Показано, що наявність впливу на інформаційно-критичні елементи політичної системи України через Інтернет підтверджується наступними ознаками.

По-перше, зростанням інформаційних контентів, спрямованих на конкретні інформаційно-критичні елементи політичної структури.

По-друге, зміною поведінки елементів політичної системи після реалізації виявлених інформаційно-політичних загроз.

По-третє, зростанням інформаційних контентів, спрямованих на тісно пов’язані з конкретними інформаційно-критичними елементами політичної структури особами (об’єктами, процесами).

По-четверте, посиленням інтенсивності появи в інтернет-просторі позитивних оцінок у діяльності окремих інформаційно-критичних елементів політичної системи з боку політичних конкурентів.

5. Запропоновано нову загальну технологію сценарного моделювання інформаційно-політичного впливу (маніпулювання), що враховує інформаційний фактор у процесі формування та розвитку загрози. Ця технологія є взаємопов’язаною реалізацією наступних модельних блоків:

«структура інформаційно-політичної загрози», «політична структура», «визначення інформаційно-критичних елементів політичної структури», «операційно-тимчасова модель інформаційно-політичного впливу», «оцінка поточного стану інформаційно-політичного впливу».

Зокрема, модельний блок «структура інформаційно-політичної загрози» є сукупністю інформаційних ознак, та виявляються в інформаційному просторі, що характеризують об’єктивно сформовану сукупність несприятливих умов і факторів.

Модельний блок «політична структура» визначає важливі елементи політичної структури країни, вказує на їх взаємозв’язки та зв’язки із довкіллям. При моделюванні політичної структури основну увагу слід приділяти аналізу залежності стану будь-якого елемента політичної структури від різних видів інформації.

Модельний блок «визначення інформаційно-критичних елементів політичної структури» є важливим механізмом визначення елементів її нормативної, комунікативної, інституційної, функціональної, культурно-ідеологічної підсистем. Маніпуляційний вплив порушує функціонування інформаційних складових, викликає важкі збої в управлінні та інфраструктурі, а також економіці країни та регіонах. Першочерговий інформаційно-політичний вплив здійснюється саме на ці елементи.

Модельний блок «операційно-тимчасова модель інформаційно-політичного впливу» встановлює сукупності інформаційних ознак, що склалися, а також зв’язки між ними на конкретний момент часу. Ця процедура характеризує будь-який маніпуляційний вплив в інтернет-просторі.

Модельний блок «оцінка поточного стану інформаційно-політичного впливу» є механізмом визначення суми інформаційних ознак окремих заходів щодо застосування методів інформаційно-політичного впливу.

Пропонований метод сценарного моделювання інформаційно-політичних загроз дає можливість:

– побудувати моделі інформаційно-політичного впливу, реалізовані на основі методів інформаційно-політичного маніпулювання в Інтернет-просторі з урахуванням його інформаційно-ресурсного потенціалу;

– визначити основні напрямки інформаційно-політичного впливу (інформаційно-критичні елементи політичної системи).

# ВИСНОВКИ

У дисертаційній роботі здійснено теоретичне узагальнення та запропоновано вирішення актуального для науки публічного управління та адміністрування науково-прикладного завдання, яке полягає в обґрунтуванні теоретичних засад і розробленні практичних рекомендацій щодо вдосконалення процесів управління інформаційною безпекою держави в умовах гібридних загроз. Це дозволило сформулювати низку висновків, які мають теоретичне і практичне значення, та виносяться на захист.

1. З’ясовано сутність інформаційної безпеки як об’єкту публічного управління. Визначено, що інформаційна безпека держави – це стан інформаційної сфери, котрий характеризується стійкістю, та спрямований на сприяння гармонізації процесів розвитку сучасного інформаційного суспільства через забезпечення своєї цілісності та захисту об'єктів у випадку присутності несприятливих впливів внутрішнього та зовнішнього походження на основі усвідомлення суб'єктами соціуму власних цінностей, життєво важливих інтересів та цілей розвитку.

Визначено, що ключовий зміст дефініції «інформаційна безпека» полягає у:

– забезпеченні безпеки даних;

– захисті суб'єктів, котрі є складовими інформаційної взаємодії, від деструктивного впливу;

– задоволенні потреби соціальних суб'єктів в інформації у вигляді підтримки інформаційного середовища у безпечному стані.

2. Охарактеризовано сучасний стан організаційно-правового механізму управління інформаційною безпекою України.

Відмічено, що організаційно-правовий механізм управління інформаційною безпекою України складається з загальнодержавного, галузевого, регіонального (місцевого), приватного та громадського секторів.

Підкреслено, що вдосконалення організаційно-правового механізму публічного управління інформаційною безпекою України здійснюється на основі оперативно-тактичного плану, котрий розроблено фахівцями Державної служби спеціального зв’язку та захисту інформації України на основі:

– п'ятирічної практики застосування норм та положень чинного законодавства;

– досвіду побудови національної системи кібербезпеки;

– аналізу сильних та слабких сторін моделей кібербезпеки інших країн;

– практики організації роботи в цій сфері та взаємодії з іншими суб'єктами кібербезпеки.

3. Оцінено поточні виклики та суперечності публічного управління інформаційною безпекою в Україні в умовах гібридних загроз.

Показано, що серед викликів та загроз для національного кіберпростору України слід акцентувати увагу на наступних:

– активне застосування кіберзасобів у конкурентних процесах на міжнародному рівні за наявності активізації прогресивних змін інформаційно-комунікаційних технологій;

– процеси мілітаризації кіберпростору та розповсюдження кіберзброї в умовах повномасштабного російського вторгнення;

– реорганізація та трансформація суспільних відносин на рівні дистанційного режиму з масштабним застосуванням інформаційно-комп’ютерних систем й електронних сервісів через вплив пандемії COVID-19 на соціально-економічну активність;

– безсистемне впровадження нових механізмів, технологій та цифрових сервісів стосовно взаємодії держави з громадськістю з низьким рівнем ризикоорієнтованості.

Підкреслено, що ключовою загрозою кібербезпеці України є кібератаки російської федерації, спрямовані на об'єкти критичної інформаційної інфраструктури й інформаційні комп’ютерні системи органів державної влади

та місцевого самоврядування з метою забезпечення маніпулятивного впливу, проведення розвідувальної й розвідувально-підривної діяльності та отримання прихованого доступу й контролю з метою дискредитації української державності.

4. Проаналізовано досвід зарубіжних країн стосовно управління інформаційною безпекою держави. Визначено, що як побічний ефект еволюції політики ЄС у сфері інформаційної безпеки, моніторинг та навігація в екосистемі політики ЄС у сфері кібербезпеки стали дедалі складнішим завданням – як для політиків та осіб, що приймають рішення у державному та приватному секторах, так і для інших зацікавлених сторін, зокрема, таких, як громадянське суспільство та наукові кола. Це є фундаментальною передумовою для ефективного впровадження та застосування законодавства та політики, пов'язаних з інформаційною безпекою, та формування розумної, структурованої й сталої політики інформаційної безпеки як на рівні ЄС, так і на рівні держав-членів.

Підкреслено, що розподіл нормативно-правових актів, що регулюють питання інформаційної безпеки, ґрунтується на принципі делегування повноважень, що означає, що ЄС потребує компетенції – виключної або спільної з державами-членами – для вжиття необхідних заходів для захисту інформаційного простору. Таким чином, будь-який правовий акт ЄС або політика ЄС, що стосуються інформаційної безпеки, також повинні бути пов'язані з конкретною сферою, в якій ЄС має компетенцію.

5. Обґрунтовано стратегічні орієнтири захисту єдиного інформаційного простору України в умовах гібридних загроз:

– прогнозування, ідентифікація й оцінка характеру і джерел інформаційно-політичних загроз, основних суб'єктів інформаційно-політичного впливу, інформаційно-критичних елементів політичної системи та політичної важливості кожного з них;

– збір інформації про використовувані та перспективні інформаційні технології органів інформаційної протидії стосовно політичної сфери діяльності об'єкта впливу;

– захист елементів політичної системи та суспільної свідомості на всіх рівнях (починаючи з індивідуального і до загальнонаціонального) від впливів інформаційного характеру, вкладених у поширення ворожої для України політичної інформації;

– захист інформаційної інфраструктури України в цілому та інформаційної інфраструктури політичної системи зокрема від негативних інформаційних впливів;

– створення та розробка стратегії проведення контрінформаційних операцій в інформаційно-політичній сфері у різних умовах внутрішньополітичної та зовнішньополітичної обстановки;

- розробка нормативно-правової бази інформаційно-політичної безпеки, реалізація спеціальних операцій в інформаційній, зокрема, інформаційно-політичній сферах, використання інформаційної зброї та методів й інструментів інформаційної війни.

6. Виокремлено шляхи модернізації механізмів управління інформаційною безпекою держави.

Запропоновано комплексний механізм протидії інформаційно-політичним ризикам і загрозам різного типу, котрий складається з політичного, організаційного економічного, правового та соціально-психологічного компонентів, та який передбачає застосування різнохарактерних заходів, здатних протидіяти заподіянню шкоди від розповсюдження негативної інформації або нівелюванню цієї шкоди. Зазначений комплексний механізм включає:

– цільові орієнтири та детально розроблені завдання у рамках їх досягнення;

– множинні суб'єкти застосування;

– загрози;

– принципи, які дозволяють досягати ефективності застосування;

– основні прийоми та послідовність їх застосування.

Підкреслено, що в комплексний механізм протидії інформаційно-політичним ризикам і загрозам мають бути вбудовані алгоритми його моніторингу та адаптації, щодо нових змінних, які можуть додаватися до процесу його функціонування.

Показано, що запропонований комплексний механізм протидії інформаційно-політичним ризикам передбачає вирішення низки нових проблем технічного, організаційного та правового характеру:

– розробка апаратно-програмних засобів, котрі забезпечують оперативний моніторинг значних обсягів інформації, що циркулює в Інтернет-просторі;

– формування спеціальних інформаційних контурів у діючих інформаційних системах елементів політичної структури, націлених на виявлення інформаційно-політичних загроз;

– вдосконалення інформаційного законодавства України.

7. Здійснено моделювання ризиків для інформаційно-критичних елементів політичної інфраструктури для  в умовах гібридних загроз.

Запропоновано нову загальну технологію сценарного моделювання інформаційно-політичного впливу (маніпулювання), що враховує інформаційний чинник у процесі формування та розвитку загрози. Ця технологія є взаємопов'язаною реалізацією наступних модельних блоків: «структура інформаційно-політичної загрози», «політична структура», «визначення інформаційно-критичних елементів політичної структури», «операційно-тимчасова модель інформаційно-політичного впливу», «оцінка поточного стану інформаційно-політичного впливу».

Зокрема, модельний блок «структура інформаційно-політичної загрози» є сукупністю інформаційних ознак, котрі виявляються в інформаційному просторі, та характеризують об'єктивно сформовану сукупність несприятливих умов і факторів.

Модельний блок «політична структура» визначає важливі елементи політичної структури країни, вказує на їх взаємозв'язки та зв'язки із довкіллям. При моделюванні політичної структури основну увагу слід приділяти аналізу залежності стану будь-якого елемента її елемента від різних видів інформації.

Модельний блок «визначення інформаційно-критичних елементів політичної структури» є важливим механізмом визначення елементів її нормативної, комунікативної, інституційної, функціональної та культурно-ідеологічної підсистем. Маніпуляційний вплив порушує функціонування інформаційних складових, викликає важкі збої в управлінні та інфраструктурі, а також економіці країни та регіонах. Першочерговий інформаційно-політичний вплив здійснюється саме на ці елементи.

Модельний блок «операційно-тимчасова модель інформаційно-політичного впливу» встановлює сукупності інформаційних ознак, що склалися, а також зв'язки між ними на конкретний момент часу. Ця процедура характеризує будь-який маніпуляційний вплив в Інтернет-просторі.

Модельний блок «оцінка поточного стану інформаційно-політичного впливу» є механізмом визначення суми інформаційних ознак окремих заходів щодо застосування методів інформаційно-політичного впливу.

Пропонований метод сценарного моделювання інформаційно-політичних загроз дає можливість:

– побудувати моделі інформаційно-політичного впливу, реалізовані на основі методів інформаційно-політичного маніпулювання в Інтернет-просторі з урахуванням його інформаційно-ресурсного потенціалу;

– визначити основні напрямки інформаційно-політичного впливу (інформаційно-критичні елементи політичної системи).

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авер'янова Н.М. Гібридна війна: російсько-українське протистояння. *Молодий вчений*, 2017. №3 (43). С. 30-34.

2. Арістотель. Про душу / пер. з давньогрец. Київ : Основи, 1999. 232 с.

3. Арсенович Л. А. Організація професійної підготовки фахівців із кібербезпеки основними суб'єктами національної системи кібербезпеки: практичний аспект. *Ефективність державного управління : зб. наук. пр.* 2020. Вип. 1 (62). С. 91–105. URL: https://doi.org/10.33990/2070-4011.62.2020.205817

4. Бабіч О. Особливості маніпуляції масовою свідомістю в друкованих ЗМІ під час висвітлення воєнних подій. *Вісник Київського національного університету імені Тараса Шевченка: військово-спеціальні науки*. 2007. Вип. 14 – 15, С. 89–93

5. Баранов О.І. Основи інформаційної безпеки: навч. посіб. Київ : НАВС, 2021. 248 с.

6. Берназюк О.О. Роль та місце цифрових технологій у сфері публічного управління. *Підприємництво, господарство і право*. 2017. № 10(260). С. 166–170.

7. Бехтер А.А. Загрози інформаційної безпеки та захист інформації як складова економічної безпеки сільськогосподарських підприємств. *Агросвіт*. 2020. № 12. С. 66–70.

8. Бєлай С.В., Корнієнко Д.М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою держави. Київ : Національна академія Служби безпеки України, 2018. 408 с.

9. Бєлова М.В., Бєлов Д.М. Імплементація штучного інтелекту в досудове розслідування кримінальних справ: міжнародний досвід. *Аналітично-порівняльне правознавство*. 2023. № 2. С. 448–454.

10. Биркович Т.І., Биркович В.І., Кабанець О.С. Механізми публічного управління у сфері цифрових трансформацій. *Державне управління:*

*удосконалення та розвиток.* 2019 № 9. URL:http://www.dy.nayka.com.ua/?op=1&z=1488

11. Біленчук П.Д. Правові засади інформаційної безпеки України. Харків. 2018. 289 с.

12. Біленчук П.Д., Борисова Л.В., Неклонський І.М., Собина В.О. Правові засади інформаційної безпеки України : монографія. Харків, 2018. 289 с.

13. Валіулліна З.В. Інформаційна безпека корпоративної економіки в умовах глобалізаційних процесів. *Вісник Дніпропетровського університету*. 2016. Вип. 6. С. 34–43.

14. Велігура А. В. Дослідження шляхів розробки комплексів інформаційної безпеки. *Вісник Східноукраїнського національного університету імені В. Даля*. 2009. № 6(136). Ч. 1 С. 154–161.

15. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики. Київ : НІСД, 2016. 528 с.

16. Войтко О., Кацалап В., Рахімов В. Аналіз особливостей маніпуляції як інструменту психологічного впливу на свідомість. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2019. № 2(35). С. 121–126.

17. Войціховський А.В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В.Н. Каразіна. Серія «ПРАВО»*. 2020. № 29. С. 281–288.

18. Воропаєва Т.С. Національна ідентичність громадян України у контексті інформаційної безпеки. *Людинознавчі студії: Збірник наукових праць.* Дрогобич. 2009. Т. 20. С. 16-35.

19. Гавриляк В. Б. Стратегія кібербезпеки ЄС (2021) на цифрове десятиліття: перспективи для України. *Вісник Національної академії державного управління при Президентові України. Сер. «Державне управління»*. 2021. № 1 (100). С. 46–52.

20. Гладиш С. В. Формування вимог щодо безпеки державних інформаційних ресурсів в телекомунікаційній мережі загального

користування. *Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні»*, вип. 1 (14), 2007. С. 33-40

21. Гнатенко В. Інформаційно-економічна безпека як фактор стабільного розвитку держави. *Публічне урядування*. 2020. № 5 (25). С. 63–74.

22. Горбулін В. П. Стратегічне планування : вирішення проблем національної безпеки : монографія. Київ : НІСД, 2010. 288 с.

23. Горбулін В. П., Додонов О.Г.,Ланде Д. В Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія Київ: Інтертехнологія, 2009. 164 с.

24. Гордієнко С. Особливості функціонування системи управління інформаційною безпекою. *Інформаційна безпека людини, суспільства, держави*. 2025. № 1 (38). С. 72–82.

25. Гринь О. О. Вплив соціальних мереж на забезпечення національної безпеки держави. *Юридичний науковий електронний журнал*. 2023. № 7. С. 254– 256.

26. Гуз А. М. Історія захисту інформації в Україні та провідних країнах світу : навч. посіб. Київ : КНТ, 2011. 260 с.

27. Гурковський В. І. Безпека як об’єкт правовідносин в умовах глобального інформаційного суспільства. Правова інформатика. 2010. № 2(26). С. 72−77.

28. Данильян О. Г., Дзьобань О. П. Філософія : підручник. 3-тє вид., переробл. Харків : Право, 2020. 432 с.

29. Данільян О. Г., Дзьобань О.П., Панов М.І Національна безпека України: сутність, структура та напрями реалізації. Харків : Фоліо, 2010. 296 с.

30. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об’єктам інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави.* 2015. № 2 (18). с. 16−22.

31. Державна політика: аналіз та механізм її впровадження в Україні : навч. посіб. / кол. авт. ; за заг. ред. В. А. Ребкала, В. В. Тертички. – Київ : УАДУ, 2000. – 232 с.

32. Державне управління : навч. посіб. / А. Ф. Мельник, О. Ю. Оболенський, А. Ю. Васіна ; за заг. ред. А. Ф. Мельник. Київ : Знання, 2009. 582 с.

33. Державне управління : словник-довідник / заг. ред. В. М. Князєв, В. Д. Бакуменко. Київ : Видавництво УАДУ, 2002. 228 с.

34. Державне управління в Україні : навч. посіб. / за заг. ред. В. Б. Авер'янова. Київ : Юрінком Інтер, 1998. 432 с.

35. Державне управління в Україні: наукові, правові, кадрові та організаційні засади : навч. посіб. / за заг. ред. Н. Р. Нижника, В. М. Олуйка. – Львів : Вид-во Національного університету «Львівська політехніка», 2002. 352 с.

36. Деякі питання діяльності підрозділів з питань цифрового розвитку, цифрових трансформацій і цифровізації центральних та місцевих органів виконавчої влади та заступників керівників центральних органів виконавчої влади, обласних, Київської та Севастопольської міських державних адміністрацій з питань цифрового розвитку, цифрових трансформацій і цифровізації : постанова Кабінету Міністрів України від 03.03.2020 № 194. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/194-2020-%D0%BF#Text.

37. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану : постанова Кабінету Міністрів України від 12.03.2022 № 263. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text.

38. Деякі питання об'єктів критичної інформаційної інфраструктури : постанова Кабінету Міністрів України від 09.10.2020 № 943. *Верховна Рада України. Законодавство України.* URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text.

39. Деякі питання об'єктів критичної інфраструктури : постанова Кабінету Міністрів України від 09.10.2020 № 1109. Верховна Рада України.

Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

40. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : постанова Кабінету Міністрів України від 04.04.2023 № 299. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text.

41. Деякі питання функціонування Національного центру резервування державних інформаційних ресурсів : постанова Кабінету Міністрів України від 07.04.2023 № 311. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/311-2023-%D0%BF#Text.

42. Деякі питання функціонування Національної електронної комунікаційної мережі : постанова Кабінету Міністрів України від 16.12.2020 № 1358. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/1358-2020-%D0%BF#Text.

43. Джигирей І. М., Квітка О. О., Запорожець Ю. А. Технології розроблення програмного забезпечення. Інформаційні системи і комплекси: навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2020. 123 с.

44. Дітковська М. Ю. Впровадження новітніх інформаційних технологій в органах державної влади та місцевого самоврядування. *Теорія та практика державного управління.* 2008. № 3. С. 147-151.

45. Довгань О. Д. Сучасні інформаційні структури як компоненти інформаційної безпеки. *Інформація і право.* 2015. № 2(14). С. 111−120.

46. Договір про функціонування Європейського Союзу : консолідована версія станом на 26.10.2012. Офіційний вісник Європейського Союзу. 2012. С. 326. URL: https://eur-lex.europa.eu/legal-content/UK/TXT/?uri=CELEX%3A12012E%2FTXT

47. Домбровська С. М. Механізми забезпечення інформаційної безпеки як складової державної безпеки України. *Теорія та практика державного управління*. 2015. Вип. 1 (48). с. 2−4.

48. Домбровська С. М., Коленко В. В. Державна політика з забезпечення безпеки інформаційного середовища. *Вісник Національного університету цивільного захисту України. Сер. «Державне управління» : зб. наук. пр.* Харків : НУЦЗУ, 2021. Вип. 1 (14). С. 3–10. URL: http://repositsc.nuczu.edu.ua/handle/123456789/13256.

49. Дубас О. П. Інформаційний розвиток сучасної України у світовому контексті : монографія. Київ : Генеза, 2011. 208 с.

50. Жарков Я. М. Інформаційна безпека особистості, суспільства, держави : підручник. Київ: Видавничо-поліграфічний цента «Київський університет», 2008. 256 с.

51. Желновач Є. Інформаційне суспільство в умовах війни: українські реалії та правові аспекти. *Юридичний вісник*. 2023. № 4. С. 184-191.

52. Жиляєв І. Б., Семенченко О. І Сучасна державна політика розвитку цифрових навичок публічних службовців та громадян України. *Теорія та практика державного управління*. 2020 №1(68) С. 198-209.

53. Захаренко К. В. Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі. *Гуманітарний вісник ЗДІА*. 2018. Вип. 72. С. 44−52.

54. Захаренко К. Міжнародний досвід інформаційної безпеки. *Сучасне суспільство: політичні науки, соціологічні науки, культурологічні науки*. 2019. № 1. С. 95–109.

55. Золотар О. О. Досвід правового забезпечення інформаційної безпеки в країнах Східного партнерства ЄС (Молдова, Грузія). *Lex Portus*. 2017. № 3. С. 70-80.

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

57. Іванюк О.В., Довженко В.А., Кравець І.В. Перспективи впровадження інформаційних технологій у вітчизняній системі публічного управління. Електронний журнал «Державне управління: удосконалення та розвиток». 2018. № 4. URL: http://www.dy.nayka.com.ua/pdf/4_2018/37.pdf

58. Інформаційна безпека (соціально-правові аспекти) : підручник В. Остроухов та ін. Київ : КНТ, 2010.776 с.

59. Інформаційна безпека України : глосарій / за загальною редакцією доктора юридичних наук, професора Р. А. Калюжного. Київ: Текст, 2011. 180 с.

60. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок та ін. Київ: ДУТ, 2015. 288 с.

61. Інформаційні загрози та комунікативна інфраструктура в державному секторі : монографія / Домбровська С.М., Помаза-Пономаренко А.Л., Крюков О.І., Порока С.Г. Харків : НУЦЗУ, 2024. 244 с.

62. Інформаційно-комунікативна діяльність органів публічної влади : монографія / Куйбіда В.С. Київ : ЦП «Компринт», 2018. 364 с.

63. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека: навчальний посібник. Ч. 2. Харків : Вид. ХНЕУ, 2018. 196 с.

64. Карпенко О.В., С. О. Шайхет С.О. Застосування поняття «безпека» в галузі державного управління: етимологія та сучасне тлумачення. *Науковий вісник Академії муніципального управління*., 2016. Вип. 3. С. 26-35. – (Серія «Управління»). URL: http://academy.gov.ua/infpol/pages/dop/2/files/9f7f3c6b-004c-4403-848e-1410645127d4.pdf

65. Качинський А. Б. Індикатори національної безпеки: визначення та застосування їх граничних значень : монографія. Київ : НІСД, 2013.101 с.

66. Кількість зареєстрованих кіберінцидентів минулого року зросла на 62,5% – Держспецзв'язку. *Армія інформ*. URL: https://armyinform.com.ua/2024/01/12/kilkist-zareyestrovanyh-kiberinczydentiv-mynulogo-roku-zrosla-na-625-derzhspeczzvyazku.

67. Ковалів М. В., Красницький І. В., Пєтков С. В., Єсімов С. С., Корецька В. В., Явний О. І. Правові засади електронної ідентифікації в Україні. *Міжнародний науковий журнал «Інтернаука». Серія: Юридичні науки*. 2024. № 4. С. 21−27.

68. Колодій І. Поняття та зміст інформації: соціальні та правові аспекти. *Підприємство, господарство і право.* 2007. № 1. С.83−86.

69. Конах В. К. Нормативно-правові засади державної політики України у сфері інформаційно-психологічної безпеки. *Стратегічні приоритети.* 2012. № 3 (24). С. 152−157.

70. Конвенція про захист прав людини і основоположних свобод : від 04.11.1950. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.

71. Кононенко В. П., Здоровко С. С., Корольова А. Є. Інформаційна безпека як стан. Науковий вісник Ужгородського Національного Університету. Серія право. 2023. Випуск 76: частина 2. С. 244−250.

72. Концептуальні засади взаємодії політики й управління : навч. посіб. / Е. А. Афонін та ін. Київ: НАДУ, 2010. 299 с.

73. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України : монографія. Одеса : Юридична література, 2007. 471 с.

74. Корнейко О. Застосування та визначення терміна «інформаційна безпека» в національному законодавстві. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Науково-технічний збірник. 2009. Вип. 2(19). С. 9−13.

75. Котляров В. Система забезпечення інформаційної безпеки України. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2024. № 2(74). С. 45-49.

76. Котух Є. В. Формування систем кібербезпеки в органах публічної влади. *Державне управління: удосконалення та розвиток.* № 3 (2020). URL: http://www.dy.nayka.com.ua/?op=1&z=1596

77. Кохановська О. В. Правове регулювання у сфері інформаційних відносин : монографія . Київ: Націон. акад. внутр. справ України, 2010. 212 с.

78. Кравченко М. С, Кєтриш О. С. Управління інформаційними ресурсами як інструмент управляння соціальними та економічними процесами в Україні. URL: http://ves.pstu.edu/article/viewFile/105569/100702

79. Красноступ Г. М. Становлення національного законодавства про інформацію: врахування найкращих європейських практик. Інформація і право. 2023. № 2 (45). С. 64–72.

80. Криштанович М. Ф. Реалізація механізмів публічного управління у сфері цивільного захисту України щодо національної безпеки. *Вісник Національного університету цивільного захисту України.* Серія. Державне управління. 2017. Вип. 1 (6).С. 341–347.

81. Крюков О. І. Інформаційне забезпечення публічної влади як чинник національної безпеки держави в умовах глобалізації. *Вісник Національного університету цивільного захисту* : зб. наук. праць. Серія: Державне управління. Харків, 2016. № 1 (4). С. 142–149.

82. Куйбіда В. С., Карпенко О. В., Наместнік В. В. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. *Вісник Національної академії державного управління при Президентові України. Сер. «Державне управління»*. 2018. № 1. С. 5-11.

83. Куліков Є. Огляд українського ринку кібербезпеки. *КО. IT для бізнесу*. URL: https://ko.com.ua/oglyad_ukrayinskogo_rinku_kiberbezpeki_149176.

84. Курас І. Інтеграція інформаційних ресурсів – стратегічний напрям забезпечення інформаційних потреб суспільства. *Бібліотечний вісник*. 2009. №1. С. 2−6.

85. Курбан О. В. PR-аспекти інформаційної безпеки організаційних структур. *Вісник книжкової палати.* 2014. №5. С. 48– 51.

86. Курбан О.В. Соціальні мережеві комунікаційні технології в структурі сучасних інформаційних потоків. *Україна в системі глобального інформаційного обміну: теоретико-методологічні аспекти дослідження і підготовки фахівців. Матеріали ІІ Всеукраїнської наукової конференції*. Львів: Лігі-Прес, 2013. С.137–143.

87. Куренда Л.Д. Окремі аспекти забезпечення інформаційної безпеки Європейського Союзу. *Правова інформатика*. 2011. № 3–4.

URL: http://ippi.org.ua/kurenda-ld-okremi-aspekti-zabezpechennya-informatsiinoi-bezpeki-%D1%94vropeiskogo-soyuzu

88. Курило А.Г. Місце інформаційної безпеки в системі національної безпеки. *Вісник Національного університету цивільного захисту України*. Серія: Державне управління. 2022. № 1 (14). URL:http://repositsc.nuczu.edu.ua/bitstream/123456789/13266/1/Kurilo.pdf

89. Кушніков В. В. Державна політика у сфері забезпечення інформаційної безпеки в умовах гібридних загроз. *Інвестиції: практика та досвід*. 2026. № 3. С. 416–420.

90. Кушніков В. В. Методи вибору стратегічних напрямів розвитку державної політики України у сфері забезпечення інформаційної безпеки. *Державне управління: удосконалення та розвиток*. 2025. № 7. URL: https://nayka.com.ua/index.php/dy/article/view/6979/7087.

91. Кушніков В. В. Механізми публічного управління у сфері інформаційної безпеки: роль та специфіка формування. *Інвестиції: практика та досвід*. 2025. № 15. С. 311–314.

92. Кушніков В. В., Дєгтяр А. О. Забезпечення інформаційної безпеки держави в умовах гібридних загроз як глобальна проблема. *Державне управління: удосконалення та розвиток*. 2025. № 11. С. 9–20. URL: https://nayka.com.ua/index.php/dy/article/view/8019/8150.

93. Кушніков В. В., Курило А. Г., Механізми розвитку інформаційних технологій в контексті модернізації політики інформаційної безпеки. Вісн. Нац. ун-ту цивільного захисту України. Серія: Державне управління. 2025. Вип. 2(23). С. 59–63.

94. Кушніков В. Інформаційна безпека суспільства і держави. *Управління розвитком соціально-економічних систем: матеріали X Міжнародної науково-практичної конференції* (м. Харків, 05-06 березня 2026 року). Харків: Державний біотехнологічний університет, 2026. С. 223–225.

95. Кушніков В.В. Ефективне публічне управління у сфері інформаційної безпеки як запорука забезпечення громадського здоров'я. *Громадське здоров'я в Україні: проблеми та способи їх вирішення «Томілінські читання» : матеріали VIII науково-практичної конференції з міжнародною участю, Харків, 30 жовтня 2025 р.* / Ред. кол.: О. А. Наконечна, К. Г. Помогайбо, В. Г. Нестеренко та ін. Харків, 2025. С. 193–194.

96. Кушніков В.В. Проблеми та перспективи публічного управління щодо забезпечення інформаційної безпеки під час повномасштабного російського вторгнення та у повоєнний період. *Війна в історичній та індивідуальній пам'яті* : *колективна монографія за матеріалами VIII Міжнародної науково-практичної конференції, присвяченої 81-й річниці Визволення України від гітлерівських загарбників, 11-й річниці Великої Національної війни (гібридної), розв'язаної рашизмом XXI століття проти Незалежності України, державного суверенітету та територіальної цілісності 1 березня 2014р. (м. Кривий Ріг, 28 жовтня 2025 року).* Кривий Ріг, 2025, С. 759–761.

97. Кушніков В.В. Специфіка дотримання інформаційної етики в межах державної політики інформаційної безпеки. *ІТ-простір сьогодення: тенденції, інновації та перспективи розвитку : збірник тез доповідей ІІ Міжнародної науково-практичної студентської конференції (м. Харків, 15 жовтня 2025 р.)*. Харків : Харківський національний університет імені В. Н. Каразіна, 2025. С. 79–80.

98. Кушніков В.В. Формування державної політики у сфері інформаційної безпеки: теоретико-методологічний аспект. *Інформаційні технології і автоматизація – 2025 : матеріали XVIII міжнародної науково-практичної конференції (м. Одеса, 30–31 жовтня 2025 року)*. Одеса: Видавництво ОНТУ, 2025. С. 293–295.

99. Кушніков В.В. Цифровізація у воєнній сфері як об'єкт публічного управління. *Виклики і можливості для агробізнесу: наука, практика та цифрове майбутнє : збірник матеріалів Міжнародної науково-практичної*

*конференції (м. Одеса, 4 листопада 2025 року)*. Одеса: ІКОСГ НААН, 2025. С. 24–26.

100. Ленков С. В. Захист національних інформаційних ресурсів в аспекті інформаційної безпеки України / С. В. Ленков // Вісн. Східноукр. нац. ун-ту ім. В. Даля. – 2009. Т. 1. № 5. С. 21−28.

101. Ліпкан В. А. Національна безпека України : навч. посіб. / В. А. Ліпкан. Київ : КНТ, 2009. 574 с.

102. Луценко С. М. Особливості інформаційного забезпечення в державно-управлінській діяльності. *Держава та регіони : зб. наук. праць*. Запоріжжя: Класичний приватний університет, 2010. № 2. С. 41–45.

103. Макаренко Є. А. Європейська інформаційна політика : монографія. Київ : Наша культура і наука, 2010. 368 с.

104. Макєєв С.А. Інформаційна безпека держави в умовах гібридної війни. Київ : Ліра-К, 2020. 186 с.

105. Маклюен М. Галактика Гутенберга. Становлення людини друкованої книги / пер. з англ. Київ : Лабораторія, 2024. 392 с.

106. Малик Я. Національна безпека : навч. посіб. / Я. Малик, О. Береза, М. Криштанович ; Львів. регіон. ін-т держ. упр. Нац. акад. держ. упр. при Президентові України. Львів : ЛРІДУ НАДУ, 2010. 280 с.

107. Маруненко О. Зовнішні і внутрішні інформаційні війни у медійному просторі України Освіта регіону. *Політологія, психологія, комунікації. Український науковий журнал.* 2011. № 4. с. 92.

108. Марущак А. І. Інформаційне право: регулювання інформаційної діяльності : навч. посібник. Київ : Видавничий дім «Скіф», КНТ, 2010. 344 с.

109. Милосердна І.М. Інформаційна безпека як елемент національної безпеки: теоретичний вимір та особливості впровадження. *Науковий журнал «Політикус»*. 2024. № 4. С. 179–185.

110. Момот А. Аналіз основних напрямків забезпечення інформаційної безпеки. *Актуальні проблеми міжнародних відносин*. Вип. 659 (Ч.1). №1. 2008 С. 265−278.

111. Мохор В. В., Цуркан В. В., Дорогий Я. Ю., Штифурак Ю. М. Структури архітектури систем управління інформаційною безпекою. *Informatics & Mathematical Methods in Simulation*. 2019. № 9(4). С. 209–221.

112. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: національна доповідь / ред. кол. С. Пирожков, О. Майборода, Н. Хамітов, Є. Головаха, С. Дембіцький, В. Смолій, О. Скрипнюк, С. Київ : Стоєцький Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України, 2022. 552 с.

113. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ: «Гельветика», 2017. 168 с.

114. Ніколаєць Ю. Державна інформаційна політика України в умовах повномасштабного воєнного вторгнення російської федерації: суспільно-мобілізаційний потенціал і ефективність. Political Studies. 2024. № 1 (7). С. 42–67.

115. Носок С.О., Фаль О.М., Ткач В.М. Управління інформаційною безпекою. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.

116. Ожеван М. А. Основні напрями зовнішніх інформаційно-маніпулятивних впливів на суспільні трансформації в Україні: засоби протидії. *Стратегічні пріоритети*. 2011. № 3. С. 118–126.

117. Олійник О. В. Державна політика інформаційної безпеки України. *Юридичний вісник*. 2012. №4(25). С.65−69.

118. Основи інформаційного права України : навч. посіб / В. С. Цимбалюк та ін. Київ . Знання, 2010. 274 с.

119. Основи інформаційної безпеки / за ред. проф. В. О. Хорошка. – Київ : ДУІКТ, 2008. 186 с.

120. Пальчинська М. Соціокультурні детермінанти інформаційного суспільства: соціально-філософський аспект. *Науково-теоретичний альманах Грані*. 2022. Том 25. № 6. С. 98–104.

121. Панфілова Ю. М., Коба В. В. Трансформація зовнішньої політики держави: роль інформаційної безпеки у сучасному світі. *Сучасний науковий журнал*. 2024. № 5(3). С. 97–104.

122. Панченко О. А. Проблеми правового забезпечення державного управління інформаційною безпекою. *Державне управління: удосконалення та розвиток*. 2019. № 11. URL: http://www.dy.nayka.com.ua/?op=1&z=1561.

123. Панченко О.А. Інформаційна безпека в контексті викликів і загроз національній безпеці. *Державне управління та місцеве самоврядування*. 2020. Вип. 2(45). С. 57–63.

124. Парахонський Б.О. Зовнішня політика України в умовах кризи міжнародного безпекового середовища: аналіт. доп. Київ : НІСД, 2015. 100 с.

125. Пархоменко В. Д. Наукові і організаційні проблеми управління інформаційними ресурсами. *Науково-технічна інформація.* 2007. № 3. С. 31−36.

126. Петров С. Г. Правові основи взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України. *Інформація і право.* № 4(31)/2019. С. 107-112. URL: http://ippi.org.ua/sites/default/files/15_11.pdf

127. Пилипчук В. Г. Еволюція наукових поглядів стосовно поняття «державна безпека». *Стратегічна панорама.* 2006. № 2. С.17−21.

128. Пирожков С. І. Національна та регіональна безпека: погляд України. *Нова безпека*. 2003. №2. С. 9–16.

129. Питання Єдиного державного вебпорталу електронних послуг та Реєстру адміністративних послуг : постанова Кабінету Міністрів України від 04.12.2019 № 1137. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/1137-2019-%D0%BF#Text.

130. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України від 08.02.2021 № 92. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/92-2021-%D0%BF#Text.

131. Питання застосування електронних студентських (учнівських) квитків : постанова Кабінету Міністрів України від 18.12.2019 № 1051.

Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/1051-2019-%D0%BF#Text.

132. Питання Міністерства цифрової трансформації : постанова Кабінету Міністрів України від 18.09.2019 № 856. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text.

133. Платоненко А. В. Сучасні загрози інформаційної безпеки для державних та приватних установ України. *Сучасний захист інформації*. 2015. №4. С. 86−90.

134. Подорожна Т. С. Забезпечення інформаційної безпеки України в умовах сучасних викликів та загроз з боку рф. *Аналітично-порівняльне правознавство*. 2023. № 12. С. 491−497.

135. Покровська А. Національна стійкість як основа забезпечення національної безпеки держави. *Стратегічне позиціонування України в сучасному міжнародному просторі: матеріали міжнародної науково-теоретичної конференції*. Київ, 2018. С. 37.

136. Політанський В. С. Інформаційне суспільство в Україні: від зародження до сьогодення. *Науковий вісник Ужгородського національного університету*. 2017. Вип. 42. С. 16−22.

137. Положення про Національний координаційний центр кібербезпеки : указ Президента України від 07.06.2016 № 242/2016. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text.

138. Почепцов Г. Сучасні інформаційні війни. К. : Вид. дім “Києво-Могилянська академія”, 2015. 497 с.

139. Прибутько П.С., Лук’янець І.Б. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. Київ: Вид. А. В. Паливода, 2007. 252 с.

140. Про Державну службу спеціального зв’язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV. *Відомості Верховної Ради*

*України*. 2006. № 30. Ст. 258. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

141. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. *Відомості Верховної Ради України*. 1994. № 16. Ст. 93. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

142. Про деякі питання цифрової трансформації : розпорядження Кабінету Міністрів України від 02.08.2024 № 735-р. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/735-2024-%D1%80#Text.

143. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

144. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. *Відомості Верховної Ради України*. 2003. № 36. Ст. 275. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

145. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. Відомості Верховної Ради України. 2021. № 21. Ст. 163. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

146. Про електронну ідентифікацію та електронні довірчі послуги. Закон України від 05.10.2017 № 2155-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст. 400. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

147. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19.06.2019 № 518. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

148. Про затвердження Концепції формування системи національних електронних інформаційних ресурсів : розпорядження Кабінету Міністрів України від 05.05.2003 № 259-р. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/259-2003-%D1%80#Text.

149. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29.05.2023 № 463. URL: https://zakon.rada.gov.ua/laws/show/z0949-23#Text.

150. Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 № 23. URL: https://zakon.rada.gov.ua/laws/show/z0226-21#Text.

151. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30.08.2023 № 773. URL: https://zakon.rada.gov.ua/laws/show/z1637-23#Text

152. Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 03.07.2023 № 570. URL: https://zakon.rada.gov.ua/laws/show/z1196-23#Text.

153. Про затвердження Переліку послуг Національної електронної комунікаційної мережі : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 17.08.2021 № 502. URL: https://zakon.rada.gov.ua/laws/show/z1008-21#Text.

154. Про затвердження Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України : постанова Кабінету Міністрів від 03.09.2014 № 411. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF#Text.

155. Про затвердження Положення про інтегровану систему електронної ідентифікації : постанова Кабінету Міністрів України від

03.11.2023 № 1150. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/1150-2023-%D0%BF#Text.

156. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах : постанова Кабінету Міністрів України від 16.11.2002 № 1772. *Верховна Рада України. Законодавство України*.URL: https://zakon.rada.gov.ua/laws/show/1772-2002-%D0%BF#Text.

157. Про затвердження Порядку надання послуг Національного центру резервування державних інформаційних ресурсів : постанова Кабінету Міністрів України від 03.05.2022 № 522. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/522-2022-%D0%BF#Text.

158. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом : постанова Кабінету Міністрів України від 11.11.2020 № 1176. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text.

159. Про затвердження Порядку формування та перевірки е-паспорта і е-паспорта для виїзду за кордон, їх електронних копій : постанова Кабінету Міністрів України від 18.08.2021 № 911. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/911-2021-%D0%BF#Text

160. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29.03.2006 № 373. *Верховна Рада України. Законодавство України*.URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.

161. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.94 № 80/94-ВР. *Відомості Верховної Ради*

*України*. 1994. № 31. Ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

162. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

163. Про звернення громадян : Закон України від 02.10.1996 № 393/96-ВР. Відомості Верховної Ради України. 1996. № 47. Ст. 256. URL: https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#Text.

164. Про інформацію : Закон України від 02.10.1992 № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

165. Про кібербезпеку : Закон України від 20.02.2025 № 4336-IX. Відомості Верховної Ради України. 2025. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text.

166. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. Відомості Верховної Ради України. 2022. № 9. Ст. 57. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

167. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради*. 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

168. Про Національну програму інформатизації. Закон України від 01.12.2022 № 2807-IX. *Відомості Верховної Ради*. 2023. № 51. Ст. 127. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text.

169. Про облік внутрішньо переміщених осіб : постанова Кабінету Міністрів України від 01.10.2014 № 509. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/509-2014-%D0%BF#Text.

170. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

171. Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади: постанова Кабінету Міністрів України від 04.01.2002 № 3. *Верховна Рада України. Законодавство України*.URL: https://zakon.rada.gov.ua/laws/show/3-2002-%D0%BF#Text.

172. Про продовження строку реалізації Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та плану заходів щодо її реалізації : розпорядження Кабінету Міністрів України від 13.05.2025 № 464-р. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/464-2025-%D1%80#Text.

173. Про реалізацію експериментального проекту щодо застосування відображення в електронному вигляді інформації, що міститься у свідоцтві про народження, та інформації про зареєстроване місце проживання, що є у володінні та розпорядженні Державної міграційної служби : постанова Кабінету Міністрів України від 23.09.2020 № 1154. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/1154-2020-%D0%BF#Text.

174. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : указ Президента України від 26.08.2021 № 447/2021. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

175. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : указ Президента України від 28.12.2021 № 685/2021. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

176. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : указ Президента України від 15.03.2016 № 96/2016. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text.

177. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : указ Президента України від 25.02.2017 № 47/2017. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/go/47/2017.

178. Про рішення Ради національної безпеки і оборони України від 4 червня 2021 року «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони» : указ Президента України від 18.06.2021 № 260/2021. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/260/2021#Text.

179. Про стратегію національної безпеки України. Указ Президента України від 14.09.2020 № 392/2020. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/392/2020#n5.

180. Про стратегію реформування державного управління на 2022-2025 роки України : розпорядження Кабінету Міністрів України від 21.07.2021 № 831-р. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/831-2021-%D1%80#n9.

181. Про стратегію цифрової трансформації соціальної сфери : розпорядження Кабінету Міністрів України від 28.10.2020 № 1353-р. *Верховна Рада України. Законодавство України*.URL: https://zakon.rada.gov.ua/laws/show/1353-2020-%D1%80#Text.

182. Про схвалення Концепції розвитку електронного урядування в Україні : розпорядження Кабінету Міністрів України від 20.09.2017 № 649-р. *Верховна Рада України. Законодавство України.* URL: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text.

183. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2030 року та затвердження плану заходів щодо її реалізації : розпорядження Кабінету Міністрів України; від 17.11.2021 № 1467-р.

*Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80#Text.

184. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15.07.2013 р. № 386 р. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text.

185. Про хмарні послуги : Закон України від 17.02.2022 № 2075-IX. Відомості Верховної Ради України. 2022. № 27. Ст. 187. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text.

186. Проданюк Р. І. Інформаційна безпека в соціологічному контексті: до постановки проблеми. *Грані: науково-теоретичний альманах*. 2018. Т. 21. № 4. С. 84−90.

187. Прокоф'єва Д. М. Інформаційна війна та інформаційна злочинність. *Вісник Запорізького юридичного інституту*. 2000. №1. С. 288−307.

188. Рада національної безпеки і оборони України (офіційний сайт). URL: https://www.rnbo.gov.ua.

189. Размєтаєва Ю. С. Приватність в інформаційному суспільстві: проблеми правового розуміння та регулювання. *Науковий вісник Ужгородського національного університету. (Серія: Право)*. 2016. Вип. 37. Т. 1. С. 43−46.

190. Ржевська Н. Сучасна інформаційна політика: досвід США для України. *Political Studies*. 2024. № 1 (7). С. 68−85.

191. Савченко О.С. Проблеми запровадження цифровізації у систему публічного управління. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування*. 2022. № 3, С. 102–108.

192. Семенченко А. І. Інформаційно-комунікаційні технології в публічному управлінні місцевими фінансами: стан та перспективи розвитку. *Інвестиції: практика та досвід*. 2020. № 13–14.

193. Семченко-Ковальчук О.Б. Використання блокчейну в публічному управлінні: трансформація технологічних можливостей. *Науковий журнал «ECONOMIC SYNERGY»*. 2023. Вип. 2 (8). URL: https://doi. org/10.53920/ES-2023-2-5

194. Сенченко О. П. Стратегія побудови та розвитку інформаційного суспільства. Перспективи. 2008. № 2. С. 8−19. (Серія : філософія, історія, соціологія, політологія).

195. Сердюк І.А. Підходи публічного управління до інформаційної безпеки особистості. *Публічне урядування*. 2022. № 3 (31). С. 53–59.

196. Сидоренко Н. Сучасні тенденції розвитку публічного управління. *Аспекти публічного управління*. 2022. Том 10. № 3. С. 59−63.

197. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Q3. Звіт про роботу. Оперативний центр реагування на кіберінциденти державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. URL: https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1ba/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1ba.pdf.

198. Сідак В. С, Артемов В.Ю. Забезпечення інформаційної безпеки в країнах НАТО та ЄС : навч. посіб. Київ. КНТ, 2010. 160 с.

199. Сілкова Г. Інформаційно-аналітичні дослідження в структурі інформаційних ресурсів. Вісн. Кн. палати. 2005. № 2. С. 14−18.

200. Соснін О. Передумови формування в Україні інформаційного права. Право України. 2005. № 11. С.99-103.

201. Соціально-правові основи інформаційної безпеки: навч. посіб. / В. М. Петрик та ін. – Київ: Росава, 2007. 496 с.

202. Степанов В. Державна інформаційна політика: проблеми та перспективи : монографія. Харків: С.А.М., 2011. 548 с.

203. Степанова О. М., Дегтярьова Л. М. Інформаційна безпека в умовах розвитку інформаційної системи підприємства. *Інформаційна безпека*. 2009. № 1. Сс. 59−63.

204. Терещенко В. В. Особливості державної інформаційної політики в умовах війни. *Юридичний науковий електронний журнал*. 2023. № 2. 391−395.

205. Тихомиров О. О. Діяльнісний підхід у дослідженнях забезпечення інформаційної безпеки: мета, засоби і методи, принципи, результати. *Information Security of the Person, Society and State*. 2012. № 3(10). С. 11−17.

206. Ткаченко В. В. Загрози інформаційній безпеці України як проблематика національної безпеки. *Юридичний науковий електронний журнал*. 2022. № 10. С. 496-498.

207. Торічний В. О. Інформаційне забезпечення безпеки держави в умовах інформаційного суспільства: державно-управлінський аспект: Монографія. Харків : НУЦЗУ, 2020. 274 с.

208. Тоффлер Е. Третя хвиля / пер. з англ. Київ : Основи, 2000. 784 с.

209. Троян С.С. Інформаційно-безпекова політика Європейського Союзу. *Зовнішні справи*. 2019. № 2-3. С. 28-32.

210. Форос Г. В., Жогов В. С. Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. *Правова держава*. 2019. № 33. С. 128–134.

211. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об’єктів інформаційної діяльності. *Сучасний захист інформації*. 2016. № 4. С. 65−70.

212. Цифрова трансформація публічного управління : кол. моногр. / О. В. Карпенко та ін. Київ : НАДУ, 2020. 256 с.

213. Чмир Я. Сучасні проблеми інформаційної безпеки України та перспективні напрями їх вирішення. Наукові праці Міжрегіональної Академії управління персоналом. *Політичні науки*. 2022. № 2(62). С. 149–154.

214. Шаповал Р. В. Вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України. *Наше право*. 2014. № 6. С. 5−9.

215. Шевчук М.О. До питання ґенези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського Національного Університету. Серія право*. 2023. Випуск 78: частина 2. С. 134−139.

216. Шемчук В.В. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Порівняльно-аналітичне право*. 2019. № 2. С. 188–191.

217. Шемшученко Ю. С. Інформаційне законодавство України : науково-практичний коментар. Київ : Юридична думка, 2011. 232 с.

218. Шемшученко Ю. С. Правове забезпечення інформаційної діяльності в Україні. Київ : Юридична думка, 2011. 384 с.

219. Шиманський О.В. Національна система кібербезпеки України: правові та організаційні аспекти. Інформація і право. 2021. № 1. С. 23–31.

220. Шинкар Т. Організаційні та правові засади обмеження права на інформацію в інтересах національної безпеки: монографія. Львів: Львівський державний університет внутрішніх справ, 2023. 392 с.

221. Шопіна І. М. Поняття інформаційної безпеки: концептуальні підходи до визначення. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького*. 2022. № 13. С. 133–140.

222. Шпига П. С. SMART-підхід до визначення завдань цифровізації робочих місць публічних службовців. *Вісник НАДУ. Серія «Державне управління».* 2020. № 4 (99). С. 77–83. URL: http://academy.gov.ua/infpol/pages/dop/2/files/7bb89df3-d121-4aaf-a6de-4792502589d1.pdf

223. Юдін О. К. Інформаційна безпека держави : навч. посіб. Харків : Консул, 2011. 576 с.

224. Ярема О. Г. Зміст інформаційного суверенітету у контексті державного суверенітету. *Юридичний науковий електронний журнал*. 2022. № 3. С. 191–194.

225. Ярема О. Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. Науковий вісник Львівського державного університету внутрішніх справ. 2016. № 2. С. 244−252. (Серія: «Право»).

226. Яременко О. І. Політико-правові засади цифровізації системи публічного управління: європейський досвід. *Побудова інформаційного суспільства: ресурси і технології* : матеріали XVIII Міжнар. наук.-практ. конф., Київ, 19-20 верес. 2019 р. / МОН України, УкрІНТЕІ [та ін.]. Київ : УкрІНТЕІ, 2019. 260 с.

227. Яровой Т.С. Можливості та ризики використання штучного інтелекту в публічному управлінні. *Науковий журнал «ECONOMIC SYNERGY»*. 2023. Випуск 2 (8). URL: https://es.istu.edu.ua/EconomicSynergy/article/view/113/84

228. Abomhara M., Koien G. Cyber Security and the Internet Of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security. 2015. Vol. 4. P. 65–88.

229. Angell I. 'Winners and Losers in the Information Age', LSE Magazine, 7 (1),1995 P 10–12.

230. Arnstein S. A ladder of citizen participation in the USA. *Journal of the Royal Town Planning Institute*, vol. 57, no. 4, P. 176–182.

231. Ashby W. R. An Introduction to Cybernetics. London : Chapman & Hall, 1956. 295 p.

232. Baker J. Process, Practice and Principle: Teaching National Security Law and the Knowledge that Matters Most. *The Georgetown Journal of Legal Ethics*. 2014. Vol. 27. P. 163-189.

233. Batko I., Pavlenko D. International experience in the formation and development of the information security institute as an integral component of the modern state. *Analytical and Comparative Jurisprudence*. 2023. P. 397–401.

234. Bell D. The Coming of Post-Industrial Society: A Venture in Social Forecasting. New York : Basic Books, 1973. 507 p.

235. Bilynska M. The Formation of the Paradigm of National Resilience in the State Administration of Ukraine. *International Scientific Journal «Progress*. 2018. №.1-2. P. 41-45.

236. Brillouin L. Science and Information Theory. New York : Academic Press, 1956. 320 p.

237. Brody R. The problem of information naïveté. Journal of the American Society for Information Science and Technology. 2008. Vol. 59(7). P. 1124–1135. URL: https://doi.org/10.1002/asi.20849

238. Buczak A.L., Guven E.A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials. 2016. Vol. 18(2). P. 1153–1176.

239. Castells M. The Information Age, Volume I: The Rise of the Network Society Blackwell, Oxford, 1996. URL: https://deterritorialinvestigations.wordpress.com/wp-content/uploads/2015/03/manuel_castells_the_rise_of_the_network_societybookfi-org.pdf

240. Digital agenda for Europe. URL: https://eige.europa.eu/resources/digital_agenda_en.pdf

241. Dizard Wilson J. Old media, mass communications in the information age. New York: Longman, 1994. P. 215.

242. EIIA, EUSIDIC, EIRENE. Code of practice for information brokers. Information Services and Use. 1994. Vol. 14(2). P. 207–213. URL: https://doi.org/10.3233/ISU-1994-14207

243. EUR-Lex. Access to European Union law. URL: https://eur-lex.europa.eu

244. European Commission. 2030 Digital Compass: the European Way for the Digital Decade. COM(2021) 118 final. Brussels : European Commission, 2021. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0118

245. Financial Action Task Force (FATF). Official website. URL: https://www.fatf-gafi.org

246. Fourth Protocol to the General Agreement on Trade in Services (Basic Telecommunications Agreement) : WTO document S/L/20. World Trade Organization, 15 February 1997. URL: https://www.wto.org/english/news_e/pres97_e/pr67_e.htm

247. Goban-Klas'омT. Media i komunikowanie masowe: Teorie i analizy prasy, radia, telewizji i Internetu. Warszawa; Kraków: Wydawnictwo Naukowe PWN SA, 1999. C. 52–79.

248. Habermas J. The Structural Transformation of the Public Sphere. Cambridge : MIT Press, 1989. 301 p.

249. Hayashi Y. Johoka shakai: hado na shakai kara sofuto na shakai e [The Information Society: From «Hard» to «Soft» Society]. Tokyo : Kodansha, 1969. 261 p.

250. Hundley R. O. The Global Course of the Information Revolution: Political, Economic and Social Conséquences / R. O. Hundley. RAND, 2000. P. 109.

251. ISO/EC 27002:2022. Information security, cyber security and privacy protection. Information security controls Requirements. URL: https://www.iso.org/ru/standard/75652.html.

252. ISO/IEC 27001:2022. Information security, cyber security and privacy protection. Information security management systems. Requirements. URL: https://www.iso.org/ru/standard/27001.

253. ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:en.

254. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels : European Commission, 2013. JOIN(2013) 1 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001

255. Kurilo A.The place and role of forming information security in the system of public policy. *Public administration and state security aspects*. Series:

Vol.1/2022.
URL:http://repositsc.nuczu.edu.ua/bitstream/123456789/15387/3/Kurilo.pdf

256. M. Carr. Public-private partnerships in national cyber-security strategies. URL: https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf.

257. McCallum J. C. Memory Prices 1957+. URL: https://jcmit.net/memoryprice.htm

258. McQuail D. Media Performance. Mass Communication and the Public Interest. London ; Newbury Park ; New Delhi : SAGE Publications, 1993. – 350 p.

259. Mijwil M., Aljanabi M., Ali A. ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information. Modern Journal of Computer Science. 2023. DOI: 10.58496/ MJCS/2023/004.

260. Moles A. Information Theory and Esthetic Perception. Urbana : University of Illinois Press, 1966. 217 p.

261. Navigating the EU Cybersecurity Policy Ecosystem. Interface EU. 2024. URL: https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem

262. Pomaza-Ponomarenko A., Hren M., Durman O., Bondarchuk N., Vorobets V. Management mechanisms in the context of digitalization of all spheres of society. Revista San Gregorio. SPECIAL EDITION-2020. Núm. 42. URL: http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/issue/view/RSAN42/showToc.

263. Shannon C. E. A Mathematical Theory of Communication. Bell System Technical Journal. 1948. Vol. 27. P. 379–423. URL: https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

264. Taherdoost H. Cybersecurity vs. Information Security. *Procedia Computer Science*. 2022. Vol. 215.P. 483–487.

265. The EU Data Protection Reform and Big Data: Factsheet». URL: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41523

266. Thomson, K.L., Von Solms, R., Louw, L. 2006. “Cultivating an organizational information security culture”. *Computer Fraud & Security*. vol. 10, p. 7-11.

267. United Nations General Assembly. Resolution 71/291 «Establishment of the United Nations Office of Counter-Terrorism» : adopted by the General Assembly on 15 June 2017. UN Document A/RES/71/291. URL: https://undocs.org/A/RES/71/291

268. Vroom C., von Solms R. Towards information security behavioral compliance. *Computers & Security*. 2003. № 23 (1). P. 191–198.

269. Weimann G. Terrorism in Cyberspace: The Next Generation. Washington : Woodrow Wilson Center Press, 2015. 312 p.

270. William D. Eggers, Joel Bellman, The journey to government’s digital transformation, 2015. URL: https://www2.deloitte.com/content/dam/insights/us/articles/digital-transformation-in-government/DUP_1081_Journey-to-govt-digital-future_MASTER.pdf.

271. World Bank. Digital Development. URL: https://www.worldbank.org/en/topic/digital

# ДОДАТКИ

**Додаток А**

**Довідка про впровадження результатів дисертаційного дослідження**

Вих. №26/15 від 21.04.2026

**ДОВІДКА**

**про використання результатів дисертаційного дослідження**

**Кушнікова Вадима Вадимовича**

**«УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ»**

Результати дисертаційного дослідження Кушнікова В.В. знайшли відображення у практичній діяльності в контексті вдосконалення державної системи реагування на інформаційно-психологічні контентні загрози, яка забезпечує інформаційну та роз'ясновальну роботу органів державної влади та місцевого самоврядування щодо культури інформаційної безпеки та поєднує в собі єдиний реєстр ресурсів, котрі містять протиправну інформацію; систему аналітики інформації на наявність протиправного контенту; програму з використанням контентної фільтрації, та яка уможливлює блокування протиправного контенту. Зокрема, завдяки пропозиціям автора підвищено результативність функціонування державної системи реагування на інформаційно-психологічні контентні загрози.

На особливу увагу заслуговують пропозиції автора щодо моделювання ризиків для інформаційно-критичних елементів політичної інфраструктури в умовах гібридних загроз.

У цілому, дисертаційне дослідження Кушнікова В.В. містить важливі результати стосовно обґрунтування теоретичних засад і розроблення практичних рекомендацій щодо вдосконалення процесів управління інформаційною безпекою держави в умовах гібридних загроз.

Кандидат наук з державного управління, доцент,
директор ОКЗ «ХОМЦТ» Валентина ХОЛОДОК

**Додаток Б**

**Довідка про впровадження результатів дисертаційного дослідження**

МІНІСТЕРСТВО ЕКОНОМІКИ, ДОВКІЛЛЯ ТА СІЛЬСЬКОГО ГОСПОДАРСТВА УКРАЇНИ
НАЦІОНАЛЬНЕ АГЕНТСТВО З АКРЕДИТАЦІЇ УКРАЇНИ

MINISTRY OF ECONOMY, ENVIRONMENT AND AGRICULTURE OF UKRAINE
NATIONAL ACCREDITATION AGENCY OF UKRAINE

Вих. №20-06К
Від 20.05.2026

**ДОВІДКА**

**про використання результатів дисертаційного дослідження**

**Кушнікова Вадима Вадимовича**

**«УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ»**

Практична значущість дисертаційного дослідження Кушнікова В.В. полягає у розробці та впровадженні теоретичного підходу до модернізації державної політики у сфері інформаційної безпеки через виокремлення в ній нормативно-правової, організаційної, технологічної та кадрової складових.

Вищезазначене уможливлює своєчасне виявлення інформаційних загроз безпеці особистості, суспільства і держави та протидію ним, а також реалізацію стратегічних інтересів держави у складному конкурентному інформаційному просторі сьогодення на основі загальновизнаних принципів та норм міжнародного права щодо забезпечення інформаційної безпеки.

Так, у рамках державної політики у сфері інформаційної безпеки існує можливість впровадження наступних кроків: розробити узгоджену концепцію правового забезпечення інформаційної безпеки; запровадити практику популяризації та пропаганди основних принципів інформаційної безпеки, прав та обов'язків в інформаційній сфері; створити науково-методологічну базу в галузі інформаційної безпеки.

У цілому, дисертаційне дослідження Кушнікова В.В. має суттєву практичну значущість та дозволяє вдосконалити процеси управління інформаційною безпекою держави в умовах гібридних загроз.

В.о.директора Юрій ЯРОЩУК

EUROPEAN ACCREDITATION

ІААУ є підписантом Багатосторонньої Угоди про взаємодію з Європейською кооперацією з акредитації (EA) та Global Accreditation Corporation Incorporated

**Додаток В**

**Довідка про впровадження результатів дисертаційного дослідження**

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Директорат європейської та євроатлантичної інтеграції**

пр. Берестейський, 10 м. Київ, 01135, тел.(044) 481 32 08, e-mail: euroDG@mon.gov.ua

**ДОВІДКА**
**про впровадження результатів дисертаційного дослідження**
**Кушнікова Вадима Вадимовича**
**«УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ» за спеціальністю 281 «Публічне управління та адміністрування»**

Результати дисертаційної роботи В.В. Кушнікова на тему "Управління інформаційною безпекою держави в умовах гібридних загроз" були апробовані в роботі директорату європейської та євроатлантичної інтеграції Міністерства освіти і науки України впродовж 2024-2025 років.

Зокрема, окремі результати дослідження щодо підходів до формування державної політики у сфері інформаційної безпеки використані для підготовки інформаційно-аналітичних документів в рамках переговорів про вступ України до Європейського Союзу, зокрема за переговорними розділами 10 «Цифрова трансформація та медіа» та 31 «Зовнішня політика, безпека та оборона». Крім того, з огляду на важливість своєчасного виявлення інформаційних загроз безпеці особистості, суспільства і держави та протидію ним у всіх сферах державної політики, в тому числі освіті, науці та інноваціях, окремі результати дослідження були використані при підготовці позиції Української Сторони за переговорними розділами 25 «Наука та дослідження» та 26 «Освіта та культура», зокрема в частині медіаграмотності та критичного мислення, інтеграції компонентів цифрової безпеки в освітні програми, розвитку міжнародної наукової співпраці щодо вивчення дезінформації, інформаційних впливів та суспільної стійкості.

**Генеральний директор** **Олександра ГУСАК**

**МОН** № 2/43-26 від 22.05.2026

Підписав: Гусак Олександра Юріївна
Сертифікат: 04AF21283640SD9904000000C0192B006385F100
Дійсний: з 07.05.2026 22:23:04 по 07.05.2026 22:23:04