Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин

КВАЛІФІКАЦІЙНА

РОБОТА МАГІСТРА

на тему: **«СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІЗРАЇЛЮ: ДОСВІД ДЛЯ УКРАЇНИ»**

Виконав:
студент 2-го курсу, групи УМІБ-61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»

Гончаренко Владислав Сергійович
(прізвище, ім'я, по батькові)

Керівник:
к.п.н., доц. Пересипкіна Ірина Валентинівна
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

Рецензент:
к.п.н., доц. Калюжна Юлія Іванівна
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

ХАРКІВ – 2025 р.

Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин
Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Освітньо-професійна програма «Міжнародна інформаційна безпека»
Рівень вищої освіти: другий (магістерський)

ЗАТВЕРДЖУЮ
завідувачка кафедри

_____ _____ **Наталія ВІННИКОВА**
«_2_» червня 2025 року
(зі змінами від 10.09.2025; 06.10.2025)

ЗАВДАННЯ
на кваліфікаційну роботу магістра

Гончаренко Владислав Сергійович

Тема роботи «Система інформаційної безпеки Ізраїлю: досвід для України»

1. керівник роботи к.п.н., доц. Пересипкіна Ірина Валентинівна
затверджені наказом по університету від «02» червня 2025 року № 4001-5/1324 зі змінами від «10» вересня 2025 року № 4001-5/3049, зі змінами від «6» жовтня 2025 року № 4001-5/3656.
2. Строк подання здобувачем вищої освіти роботи 21 листопада 2025 р.

3. Перелік питань, які потрібно розробити:
– Еволюція поняття «інформаційної безпеки» у сучасних міжнародних відносинах;
– Система забезпечення інформаційної безпеки на міжнародному рівні;
– Теоретичні підходи до формування національних систем інформаційної безпеки;
– Інституційна складова системи інформаційної безпеки Ізраїлю;
– Нормативно-правова складова системи інформаційної безпеки Ізраїлю: від військової доктрини до кібернетичної стратегії;
– Практичні кейси функціонування системи інформаційної безпеки Ізраїлю;
– Стан та проблеми національної системи інформаційної безпеки України;
– Порівняльний аналіз моделей Ізраїлю та України у сфері інформаційної безпеки;
– Напрямки імплементації ізраїльського досвіду в Україні: стратегічні, правові та організаційні рекомендації.

4. План роботи

№ з/п	Назви етапів роботи	Строк виконання етапів
1	Вибір здобувачем теми КРМ і подання заяви на кафедру; затвердження теми та призначення наукового керівника; складання та затвердження індивідуального завдання на виконання КРМ	19.05.2025-30.06.2025
2	Підготовка вступу і розділу 1 КРМ	01.09.2025-30.09.2025
3	Підготовка розділу 2 КРМ	01.10.2025-15.10.2025
4	Підготовка розділу 3 КРМ	16.10.2025-31.10.2025
5	Підготовка висновків і переліку використаних джерел	03.11.2025-14.11.2025
6	Подання студентом завершеної КРМ науковому керівнику для перевірки та оформлення відгуку, перевірка КРМ на відсутність запозичень	17.11.2025-21.11.2025
7	Попередній розгляд КРМ на комісії від кафедри	24.11.2025-28.11.2025
8	Прийняття кафедрою рішення про допуск роботи до захисту в ЕК, оформлення та зовнішнє рецензування	01.12.2025-05.12.2025
9	Захист КРМ в ЕК і присвоєння випускникам кваліфікації	08.12.2025-24.12.2025

5. Дата видачі завдання: 2 червня 2025 року (зі змінами від 10.09.2025; 06.10.2025).

Здобувач вищої освіти _____ Владислав ГОНЧАРЕНКО
(підпис) (ім'я, прізвище)

Керівник роботи _____ Ірина ПЕРЕСИПКІНА
(підпис) (ім'я, прізвище)

ЗМІСТ

ВСТУП

Актуальність теми обумовлена різким зростанням масштабів, інтенсивності й технологічної складності сучасних гібридних загроз, що безпосередньо впливають як на стійкість державних інститутів, так і на національну безпеку в широкому розумінні. Зокрема, Ізраїль посідає провідні позиції у сфері кібероборони, стратегічних комунікацій та протидії інформаційно-психологічним операціям, адже впродовж десятиліть перебуває у зоні постійної конфліктності та вимушений адаптовувати свої інструменти до швидкоплинної динаміки загроз. Саме тому його досвід, без перебільшення, виступає унікальною лабораторією формування ефективної моделі інформаційної безпеки, де поєднуються інновації, висока технологічність і глибока інтеграція оборонного сектору з цивільним. Крім того, важливо врахувати, що українська держава, подібно до Ізраїлю, переживає масштабну воєнну агресію, в якій інформаційний вимір відіграє ключову роль. Тому, по-перше, ізраїльська багато-рівнева структура реагування на кібератаки та інформаційні впливи дає змогу побачити, яким чином варто поєднувати військові, урядові та приватні ініціативи для створення стійкого інформаційного середовища. По-друге, практики оперативної взаємодії між державою та бізнесом, що стали основою ізраїльської кіберекосистеми, демонструють ефективність публічно-приватного партнерства у посиленні кіберзахисту критичної інфраструктури. До того ж, ізраїльський акцент на розвитку людського капіталу, включно зі спеціалізованою підготовкою молоді та широким залученням експертних спільнот, може бути надзвичайно корисним у контексті потреб України формувати кадровий резерв для кібероборони.

Ступінь вивченості теми. Окремі аспекти правового регулювання інформаційної сфери та кібербезпеки в Ізраїлі ґрунтовно аналізує Бєлєвцева В. В.[3], яка розкриває особливості ізраїльської моделі правового забезпечення інформаційної безпеки. Безпосередньо приклад застосування ізраїльського досвіду до українських реалій простежується в роботах Дзеньківа В.[9] та

Живила Є. О., Докіля В. М.[11], де акцент робиться на інституційних механізмах кіберзахисту й можливостях їх адаптації. У ширшому контексті національної безпеки Ізраїлю важливими є напрацювання Войтовського К.[6] та Якубовича М.[29], які інтерпретують ізраїльську модель оборони як орієнтир для реформ українського сектору безпеки. Зарубіжні дослідники Голдман Е. О.[8], Арвац А.[32], Фреліх С., Коен М., Сібоні Г.[46], Табанські Л.[74], Шарма Р. К.[70], Станку А.-І., Павел Т.[72] детально аналізують становлення Ізраїлю як «кібердержави», його стратегічні підходи, організаційну архітектуру та регуляторне середовище. Окремий напрям становлять праці Спайєра Дж., Кагана Б.[71], Трудолюбова М.[26], Шапіро Д.Б., Ракова Д.[27], де безпекова модель Ізраїлю розглядається саме крізь призму її релевантності для України в умовах війни та гібридних загроз. Водночас комплексних досліджень, що поєднують правові, інституційні, технологічні та політичні компоненти ізраїльської системи інформаційної безпеки з цілісним аналізом можливостей її імплементації в українську практику, поки що бракує, що й зумовлює наукову новизну обраної теми.

Мета дослідження – визначити особливості організації та функціонування системи інформаційної безпеки Ізраїлю, а також можливостей адаптації ізраїльського досвіду для удосконалення національної системи інформаційної безпеки України.

Завдання дослідження:

– розглянути еволюцію поняття «інформаційної безпеки» у сучасних міжнародних відносинах та основні підходи до формування міжнародної системи її забезпечення;

– визначити теоретичні засади та ключові моделі розбудови національних систем інформаційної безпеки;

– розкрити інституційну та нормативно-правову складові системи інформаційної безпеки Ізраїлю;

– виявити практичні кейси функціонування системи інформаційної безпеки Ізраїлю, зокрема механізми нормативно-правового регулювання, міжвідомчої координації та державно-приватного партнерства;

– встановити специфіку моделей Ізраїлю та України у сфері інформаційної безпеки, визначити сучасний стан і ключові проблеми української системи та виявити напрями імплементації ізраїльського досвіду.

Об'єкт дослідження – система забезпечення інформаційної безпеки держави.

Предмет дослідження – система функціонування інформаційної безпеки Ізраїлю та виявлення досвіду її діяльності щодо імплементації в Україні.

Теоретико-методологічна база дослідження спирається на комплексний підхід, що дає змогу всебічно охопити багатовимірність інформаційної безпеки як складного політико-стратегічного явища. Насамперед, у роботі використано положення теорії національної безпеки, яка дозволяє зрозуміти інформаційну сферу як один із ключових компонентів державної безпекової архітектури, що забезпечує захист життєво важливих інтересів суспільства і держави. Важливе значення має і системний підхід, завдяки якому система інформаційної безпеки Ізраїлю розглядається як цілісна структура, що поєднує правові механізми, інституційні ресурси, технологічні інструменти та стратегічні пріоритети. Крім того, використано інституціоналістський підхід, що дозволяє проаналізувати діяльність ключових установ кібербезпеки Ізраїлю у контексті вироблення політики захисту державного інформаційного простору. Методологічно дослідження ґрунтується на поєднанні загальнонаукових і спеціальних методів. Так, аналіз і синтез дають змогу узагальнити концептуальні підходи до розуміння інформаційної безпеки та виокремити структурні елементи ізраїльської моделі. Порівняльний метод використано для виявлення відмінностей та подібностей між українською й ізраїльською практиками у сфері кіберзахисту, протидії дезінформації та забезпечення стійкості суспільства. Історичний

метод дозволяє простежити еволюцію формування ізраїльської системи інформаційної безпеки, адже вона розвивалася в умовах постійних загроз і стала однією з найбільш ефективних.

Інформаційна база дослідження охоплює комплекс офіційних документів, аналітичних матеріалів, міжнародних звітів, профільних законодавчих актів, а також наукових публікацій, що дають змогу всебічно проаналізувати специфіку ізраїльської моделі забезпечення кібер- та інформаційної безпеки. Передусім використовуються нормативно-правові акти Держави Ізраїль, зокрема урядові постанови щодо створення та діяльності National Cyber Directorate, закони про захист критичної інфраструктури, положення про обмін інформацією в умовах надзвичайних ситуацій, а також стратегічні доктрини, що визначають засади інформаційної протидії та попередження гібридних загроз. Крім того, у роботі застосовуються офіційні звіти Національного кіберуправління Ізраїлю, щорічні огляди кіберінцидентів, аналітичні доповіді Israel Defense Forces та Міністерства комунікацій, які дозволяють відстежити динаміку загроз і реакцію державних інституцій. Значну роль у формуванні інформаційної бази відіграють матеріали міжнародних організацій, зокрема НАТО, OECD та ITU, що містять оцінки ефективності ізраїльської кіберполітики та порівняльні дані щодо рівня цифрової стійкості держав. Водночас, для ґрунтовного наукового аналізу використовуються праці вітчизняних та зарубіжних дослідників, присвячені еволюції ізраїльської системи безпеки, трансформації підходів до кібероборони, ролі оборонно-технологічного сектору та приватних компаній, включно зі стартап-індустрією, у зміцненні інформаційної стійкості. Особливу увагу приділено публікаціям, що досліджують взаємодію між військовими структурами й цивільними інституціями, адже саме цей компонент вирізняє Ізраїль серед інших держав.

Практичне значення отриманих результатів полягає в тому, що вони дають змогу органам влади України, по-перше, сформувати більш цілісну та проактивну модель реагування на гібридні загрози, використовуючи

ізраїльський досвід інтеграції військових, технологічних і цивільних інструментів захисту. По-друге, запропоновані висновки дозволяють удосконалити систему кібероборони шляхом розширення партнерства держави з приватним сектором, що, як показує приклад Ізраїлю, істотно підвищує стійкість критичної інфраструктури. Крім того, результати можуть бути застосовані для розроблення сучасних протоколів кризового менеджменту та комунікацій, що, відповідно, забезпечить швидшу й ефективнішу координацію між усіма суб'єктами національної безпеки. Запропоновані у кваліфікаційній роботі магістра теоретичні положення та висновки можуть бути використані у навчальному процесі Харківського національного університету імені В.Н. Каразіна та інших вищих навчальних закладів при розробці та викладанні дисциплін, за програмами підготовки магістрів міжнародних відносин, суспільних комунікацій та регіональних студій.

Апробація дослідження була здійснена у вигляді публікації тез наукової доповіді для участі у Всеукраїнському науково-практичному круглому столі «Стратегічні напрями зовнішньої політики та дипломатії країн світу» (м. Харків, 21 листопада 2025 р.), на тему: «Features of Israel's information security system».

Структура роботи. Кваліфікаційна робота магістра складається зі вступу, трьох розділів, висновків, списку використаних джерел, що налічує 80 найменувань. Загальний обсяг роботи становить 87 сторінок, з яких основного тексту – 77 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

1.1. Еволюція поняття «інформаційної безпеки» у сучасних міжнародних відносинах

Еволюція поняття «інформаційної безпеки» у сучасних міжнародних відносинах демонструє складний і багатовимірний процес трансформації, що відбувається під впливом глобалізації, цифровізації та радикальної зміни природи міжнародних загроз. Упродовж останніх десятиліть інформація перетворилася з допоміжного елемента зовнішньої політики на ключовий стратегічний ресурс держав, що забезпечує як національну безпеку, так і міжнародну стабільність. Водночас, якщо наприкінці XX століття інформаційна безпека розглядалася переважно через призму технічного захисту інформаційних систем, то вже у 2020-х роках вона охоплює політичний, когнітивний, соціальний, правовий і навіть психологічний виміри. Саме тому, аналізуючи її еволюцію, слід звернути увагу на зміну її сутнісного змісту, інституційного забезпечення та міжнародного контексту. На початку інформаційної епохи ключовим завданням держав було забезпечення безпеки інфраструктур зв’язку та обміну даними. Кіберзагрози трактувалися переважно як технічні інциденти: віруси, несанкціонований доступ, збої в мережах. Однак з поширенням цифрових технологій та збільшенням кількості акторів, які можуть впливати на глобальний інформаційний простір, перед державами постали нові виклики. Примітно, що після 2014 року, а особливо після 2022 року, міжнародні організації, ЄС, НАТО, ООН, почали розглядати інформаційну безпеку не тільки як технологічну проблему, але й як елемент політичного протиборства, інформаційних операцій та інструмент гібридної війни [35]. Зокрема, Європейський Союз у Стратегії кібербезпеки 2020 року прямо вказує, що інформаційні атаки стали засобом впливу на демократичні процеси, економічну стабільність і національну безпеку держав-членів.

У цьому контексті інформаційна безпека почала розумітися як здатність держави, суспільства та міжнародних інституцій забезпечувати захист від деструктивних інформаційних впливів, гарантувати достовірність інформаційних потоків, захищати критичну інфраструктуру, підтримувати цифровий суверенітет і водночас забезпечувати свободу слова та відкритість комунікацій. Показово, що ця еволюція супроводжувалася зростанням ролі недержавних акторів: транснаціональних корпорацій (Meta, Google, Microsoft), хактивістських груп (Anonymous Sudan, Killnet), приватних кіберкомпаній, які здатні змінювати баланс сил у міжнародному інформаційному просторі. Сучасні приклади 2023-2024 років демонструють, що атаки на державні ресурси Польщі, Литви, України, Німеччини та Ізраїлю мають не лише технічний, але й політичний характер, адже часто координуються з інформаційними кампаніями, спрямованими на підрив довіри до урядів або на створення соціальної напруги [49].

Еволюція поняття інформаційної безпеки також нерозривно пов’язана з розвитком концепції гібридних загроз. Держави-агресори, зокрема Росія, дедалі частіше застосовують інформаційні операції для маніпуляції суспільною думкою, втручання у вибори, дискредитації міжнародних організацій та легітимних урядів. Наприклад, у США втручання у президентські вибори 2016 та 2020 років стало каталізатором перегляду підходів до інформаційної безпеки. У 2023 році Конгрес США ухвалив низку документів, спрямованих на посилення боротьби з дезінформацією та захист цифрової демократії, зокрема через посилення регулювання соціальних мереж. У 2024 році Єврокомісія запустила ініціативу з протидії іноземним інформаційним втручанням (FIMI), що стала відповіддю на зростання активності прокремлівських мереж у Європі напередодні виборів до Європарламенту. Важливим етапом у трансформації поняття інформаційної безпеки стало усвідомлення необхідності захисту не лише технічної, але й когнітивної сфери. Сучасні інформаційні впливи спрямовані на зміну переконань, підрив суспільної довіри та маніпуляцію колективною поведінкою

[14]. Інакше кажучи, мішенню стає людська свідомість. Саме тому такі держави, як Ізраїль, Франція, Естонія, Велика Британія, а також Україна в умовах війни почали активно розвивати системи стратегічних комунікацій, медіаграмотності та інформаційної стійкості. Естонія у 2022 році оновила свою Концепцію національної безпеки, визначивши інформаційну стійкість одним із базових елементів державної оборони. Україна, своєю чергою, у 2023 році ухвалила Стратегію інформаційної безпеки, що включає компоненти протидії дезінформації, кіберзагрозам і психологічним операціям [23].

Разом із цим, еволюція поняття інформаційної безпеки пов’язана з формуванням глобальної цифрової інфраструктури. Поява штучного інтелекту, розвиток технологій deepfake, автоматизація інформаційних кампаній докорінно змінюють природу інформаційних загроз. Нині країни змушені реагувати на ризики, які ще кілька років тому не вважалися критичними. Наприклад, у 2023 році Генеральна Асамблея ООН обговорювала питання регулювання штучного інтелекту у сфері безпеки, підкреслюючи, що неконтрольоване поширення генеративних технологій може спричинити масове виробництво фейків і масштабні когнітивні атаки на міжнародні інститути [44]. Одним із показових прикладів стала поява фейкових відео з використанням голосів політичних лідерів під час виборчих кампаній у Словаччині та Аргентині у 2023 році. Водночас, незважаючи на ускладнення інформаційних процесів, держави прагнуть сформувати спільні правила гри в міжнародному інформаційному просторі. Стратегічні документи ЄС 2020-2025 років, «Керівні принципи НАТО з кібероборони», рекомендації ООН щодо відповідальної поведінки держав у кіберпросторі свідчать про прагнення виробити консенсус щодо базових норм інформаційної безпеки [35]. Проте формування таких норм залишається складним процесом, адже різні держави інтерпретують інформаційний простір по-різному. Наприклад, демократичні країни наголошують на балансі між свободою слова та захистом від дезінформації, тоді як авторитарні режими використовують концепт інформаційної безпеки для обмеження прав людини, цензури та контролю над

суспільством. Китай у 2023 році вкотре посилив контроль над цифровими платформами, обґрунтовуючи це потребами «цифрового суверенітету», тоді як ЄС зосереджується на забезпеченні прозорості алгоритмів та підзвітності платформ перед суспільством.

Крім того, у сучасній міжнародній системі інформаційна безпека стала ключовим інструментом геополітичної конкуренції. США та Китай ведуть змагання за домінування у сфері штучного інтелекту, квантових технологій, 5G-мереж, супутникових систем, що відображається в їх інформаційних стратегіях [80]. Так, у 2023 році США ухвалили «National Cybersecurity Strategy Implementation Plan», де підкреслюється потреба у зміцненні співпраці з союзниками для протидії кіберзагрозам з боку КНР. Китай, зі свого боку, розвиває проєкт «Цифровий Шовковий шлях», що передбачає будівство телекомунікаційної інфраструктури у країнах Африки, Азії й Латинської Америки, фактично формуючи залежність від своїх технологій і стандартів цифрового контролю.

Наступним важливим елементом еволюції поняття стає розширення його концептуальних меж. Інформаційна безпека нині включає також сфери енергетичної, економічної та військової безпеки. Наприклад, атаки на трубопроводи, логістичні системи або електромережі мають інформаційно-кібернетичну природу, як це продемонстрував інцидент з Colonial Pipeline у США у 2021 році. У 2024 році кілька країн ЄС зазнали кібератак на системи управління залізницею, що викликало широке обговорення необхідності інтеграції інформаційної безпеки у стратегії транспортної та енергетичної безпеки [1]. Сучасний етап еволюції поняття «інформаційної безпеки» характеризується його синтезом із концепцією інформаційної стійкості. Якщо раніше пріоритетом був захист систем, то тепер держава має забезпечити здатність суспільства протистояти кризам, швидко відновлювати інформаційну інфраструктуру та нейтралізувати психологічні наслідки інформаційних атак. Україна, яка після 2022 року стала полігоном для випробування новітніх інформаційних технологій війни, демонструє приклад

переходу до моделі стійкості [10]. Створення Центру протидії дезінформації, розвиток кіберкомандування ЗСУ, партнерство з ЄС і США у сфері кіберзахисту, широке залучення громадянського суспільства до інформаційної оборони, усе це відображає новий підхід, який інтегрує технічні, когнітивні та політичні складові.

Суттєвою ознакою сучасного етапу еволюції інформаційної безпеки є зближення її з концепцією стратегічних комунікацій, які вже давно перестали бути виключно інструментом державної дипломатії. У 2023–2024 роках натівські країни, зокрема Велика Британія, Канада та Литва, наголошують, що стратегічні комунікації – це не лише реактивна діяльність щодо спростування дезінформації, але й проактивне формування наративів, спрямованих на посилення демократичних цінностей та об’єднання суспільства [35]. У цьому контексті поняття інформаційної безпеки набуває гуманітарного виміру, адже стосується захисту людської гідності, свободи висловлювань і права суспільства на доступ до достовірної інформації. Показовим є приклад Фінляндії, яка ще у 2016 році запровадила комплексну програму медіаграмотності у школах, а у 2023 році розширила її на всі рівні освіти, ефективно довівши, що освічене суспільство є запорукою інформаційної стійкості. Більш того, еволюція поняття інформаційної безпеки стає очевидною у світлі нових економічних реалій. Нині діяльність корпорацій, які володіють критичними інформаційними інфраструктурами, впливає на державні політики не менше, ніж дипломатичні рішення. У 2024 році глобальна дискусія про відповідальність технологічних компаній за поширення дезінформації спонукала ЄС до активного застосування положень Digital Services Act, що передбачає штрафи для платформ, які не забезпечують прозорість алгоритмів або дозволяють масштабні маніпулятивні кампанії [1]. Це означає, що інформаційна безпека перестає бути винятково державною справою, вона перетворюється на спільну відповідальність держави, бізнесу та громадянського суспільства.

Ще одним важливим аспектом є мілітаризація інформаційного простору, яка стала особливо помітною після початку повномасштабної агресії Росії проти України у 2022 році. Інформаційні операції супроводжують військові кампанії, впливають на моральний стан населення, визначають міжнародну підтримку та формують політичні рішення [10]. У результаті інформаційна безпека дедалі більше інтегрується у традиційні стратегії оборони. Наприклад, у 2023 році НАТО ухвалило рішення підвищити рівень готовності кіберсил, а Стратегічне командування альянсу визначило інформаційні операції як ключовий компонент колективної оборони [35]. Україна у цьому контексті стала унікальним прикладом держави, яка вибудовує інформаційну безпеку на тлі безпрецедентних зовнішніх викликів, активно поєднуючи державні, корпоративні та громадські ресурси, що дозволяє ефективно чинити опір інформаційним атакам великої інтенсивності [4]. Неможливо оминути й той факт, що сучасна інформаційна безпека пов’язана з глобальними нормотворчими процесами. У 2023-2024 роках ООН, Ради Європи та ОБСЄ активізували дискусії про міжнародні стандарти у сфері кіберпростору та інформаційної поведінки держав. Проте узгодження таких стандартів стикається з фундаментальними розбіжностями між демократичними та авторитарними моделями. Наприклад, Європейський Союз наполягає на пріоритетності прав людини та верховенства права, тоді як Росія та Китай пропонують моделі «суверенного інтернету», які передбачають жорсткий контроль за інформаційними потоками [66]. Ця суперечність вказує на те, що еволюція поняття інформаційної безпеки є не лише технічним, але й світоглядним, ціннісним процесом.

Важливою тенденцією останніх років є формування нової парадигми «інформаційної довіри». У світі, де інформаційні атаки, дезінформаційні кампанії та глибокі фейки стають звичним явищем, критичну роль відіграє спроможність суспільства відрізняти факти від маніпуляцій. Саме тому у 2024 році низка країн, зокрема Австралія та Нідерланди, започаткували програми з розробки систем автоматичної перевірки достовірності цифрового контенту

[17]. У глобальному вимірі інформаційна безпека поступово перетворюється на визначальний чинник формування міжнародного порядку. Вона впливає на зовнішню політику, торговельні відносини, регіональну безпеку, діяльність міжнародних організацій. Еволюція цього поняття демонструє, що інформаційний простір є водночас ресурсом розвитку, полем конфлікту та платформою співпраці [80]. Саме через це держави вимушені інтегрувати питання інформаційної безпеки у стратегії національного розвитку, освіти, оборони, цифрової трансформації й дипломатії.

У підсумку, трансформація поняття інформаційної безпеки відображає ширші зміни у міжнародних відносинах, де інформація стала не просто ресурсом, а стратегічним простором взаємодії держав, недержавних акторів і глобальних корпорацій. Варто зауважити, що, попри намагання міжнародної спільноти створити універсальні механізми регулювання, інформаційний простір залишається фрагментованим, а підходи різних держав, нерідко суперечливими. Це формує нову архітектуру міжнародної безпеки, у якій центральне місце посідає саме здатність держави адаптуватися до швидкозмінних технологічних умов, розвивати стійкість суспільства та вибудовувати ефективні партнерства зі стратегічними союзниками.

1.2. Система забезпечення інформаційної безпеки на міжнародному рівні

Система забезпечення інформаційної безпеки на міжнародному рівні формується як багатовимірний, багаторівневий та динамічний комплекс інституцій, норм, практик і технологічних рішень, що спрямовані на захист глобального інформаційного простору від зростаючих загроз. Вона охоплює як міждержавні механізми, так і інструменти транснаціональних організацій, приватних корпорацій та широкого спектру недержавних акторів, які сьогодні відіграють не менш значущу роль у підтриманні стійкості глобальних цифрових систем. У сучасних умовах, коли інформаційні операції, кібератаки, дезінформаційні кампанії, втручання у виборчі процеси та порушення

конфіденційності стали інструментами геополітичної конкуренції — міжнародна система інформаційної безпеки перетворюється з периферійного напряму міжнародних відносин на один із ключових елементів глобальної безпеки. Саме тому, розглядаючи її структуру, необхідно враховувати як еволюцію міжнародно-правових засад, так і розвиток інституційних форматів та практик міждержавної взаємодії. Передусім фундамент міжнародної системи інформаційної безпеки становить діяльність Організації Об'єднаних Націй, яка з кінця 1990-х років поступово виробляє політичні та правові підходи до поведінки держав у кіберпросторі. Важливо підкреслити, що, з одного боку, ООН не має універсального обов'язкового договору, що регулює інформаційну безпеку в комплексі. Але, з іншого боку, саме вона забезпечує вироблення принципів, які визнаються глобальною спільнотою. Наприклад, у 2021 році Група урядових експертів ООН підтвердила, що норми міжнародного гуманітарного права та Статут ООН у повному обсязі застосовуються до кібероперацій [10]. Це рішення стало одним із ключових кроків до формування міжнародного режиму кіберповедінки, адже воно підкреслює, що навіть у цифровому середовищі держави зобов'язані утримуватися від використання сили, втручання у внутрішні справи та порушення суверенітету.

Разом із тим у структурі міжнародного забезпечення інформаційної безпеки ключову роль відіграють регіональні організації. Насамперед це НАТО, яке визнало кіберпростір окремим операційним доменом ще у 2016 році, створивши підґрунтя для інтегрованої політики кіберзахисту [35]. Зокрема, у 2023-2024 роках Альянс активно модернізував свою Стратегію кібероборони, посиливши вимоги до держав-членів щодо кіберстійкості критичної інфраструктури. Важливо також зазначити, що успішні спільні операції НАТО щодо стримування російських кібератак на енергетичні та військові об'єкти країн Балтії у 2022–2023 роках стали доказом ефективності колективної моделі. Європейський Союз, своєю чергою, формує систему інформаційної безпеки, що поєднує нормативно-правові механізми,

інституційні структури та технологічні рішення. Зокрема, ухвалення Директиви NIS2 у 2022 році встановило нові стандарти кіберзахисту для операторів критично важливих послуг та цифрової інфраструктури [1]. Починаючи з 2024 року країни-члени ЄС впроваджують усі її вимоги, розширюючи перелік об’єктів, що підлягають обов’язковому захисту, і суттєво підвищуючи санкції за недотримання норм.

Окремим елементом міжнародної системи інформаційної безпеки є ОБСЄ, яка розробила механізми довіри і безпеки у кіберсфері, включно з обміном інформацією, локалізацією інцидентів та каналами екстреної комунікації між державами. Не менш значущу роль у забезпеченні глобальної інформаційної стійкості відіграє приватний сектор. Компанії Microsoft, Google, Meta, IBM та інші володіють інфраструктурою, яка становить основу цифрової екосистеми світу, а отже, несуть відповідальність за її захист. У 2022–2024 роках Microsoft зафіксувала понад 4 тисячі масштабних кібератак, спрямованих на державні установи у США, Україні, країнах ЄС та Японії, що стали частиною більш широких геополітичних операцій [2]. Поряд із цим, важливо відзначити роль Будапештської конвенції Ради Європи про кіберзлочинність, яка залишається єдиним міжнародно-правовим інструментом у сфері кримінального переслідування кіберзлочинів. У 2022 році було ухвалено Другий додатковий протокол, який розширює можливості транскордонного доступу до електронних доказів. Крім міжурядових механізмів у сучасній системі інформаційної безпеки важливе місце посідають багатосторонні ініціативи державних та приватних акторів. Наприклад, у 2024 році G7 ухвалила спільну декларацію щодо розвитку «відповідального штучного інтелекту», яка передбачає моніторинг маніпулятивних практик, пов’язаних із використанням генеративних моделей у виборчих процесах.

Водночас міжнародна система інформаційної безпеки залишається фрагментованою. Причиною цього є не лише різні політичні інтереси держав, але й відсутність універсального підходу до визначення інформаційної безпеки як явища. Так, країни Заходу наголошують на пріоритеті прав людини, свободи

слова та відкритості інтернету, тоді як Китай і Росія просувають концепт «цифрового суверенітету», що передбачає контроль держави над інформаційним потоком [80]. Попри це, система міжнародного забезпечення інформаційної безпеки поступово розширюється та адаптується до нових викликів. Так, війна Росії проти України, що супроводжується масштабними кібератаками, дезінформаційними кампаніями та спробами впливу на державні процеси, стала важливим каталізатором координації міждержавних механізмів кіберзахисту [10].

Крім того, розвиток міжнародної системи забезпечення інформаційної безпеки нерозривно пов’язаний із трансформацією глобальних технологічних ланцюгів та ускладненням взаємозалежності між державами [38]. Важливо наголосити, що сьогодні жодна країна не здатна повністю ізолювати свою цифрову інфраструктуру, оскільки виробництво, обслуговування та програмування більшості технологічних продуктів є результатом транскордонної співпраці. Наприклад, виробництво мікрочипів, на яких працюють сучасні системи штучного інтелекту та засоби кіберзахисту, здійснюється на підприємствах у США, Південній Кореї, Тайвані, Нідерландах і Японії. Це означає, що порушення глобальних ланцюгів постачання, наприклад, у разі конфлікту навколо Тайваню — може завдати серйозного удару по системі міжнародної інформаційної безпеки. Відповідно, зростає роль таких форматів, як Quad (США–Японія–Індія–Австралія) або Індо-Тихоокеанська економічна структура (IPEF), у межах яких формується координаційна політика у сфері технологічної безпеки.

Суттєвим елементом міжнародної системи інформаційної безпеки є також співпраця у сфері протидії дезінформації. У 2022–2025 роках світ спостерігав активізацію російських і китайських інформаційних кампаній, спрямованих на підрив демократій Заходу, зокрема перед виборами у США (2024), Європейський парламент (2024) та низці європейських країн, серед яких Франція, Польща та Німеччина [17]. У відповідь Європейський Союз створив Європейську обсерваторію цифрових медіа (EDMO), яка об’єднує

дослідницькі центри, медіаорганізації та технологічних аналітиків для моніторингу і викриття маніпулятивного контенту. Крім того, ЄС посилив Кодекс практик щодо дезінформації, який з 2023 року став частиною регуляторної екосистеми, що охоплює також і Закон про цифрові послуги (DSA). Завдяки цьому великі цифрові платформи, такі як X, Meta чи TikTok, отримали чіткі юридичні зобов'язання щодо прозорості алгоритмів, маркування політичної реклами та оперативного реагування на виявлення маніпулятивних кампаній. Окремою складовою є глобальна співпраця у сфері штучного інтелекту, який дедалі більше впливає на інформаційну сферу та безпекову політику. Саме тому у 2023 році Великобританія організувала перший у світі глобальний Саміт із безпеки штучного інтелекту в Блетчлі-парку, результатом якого стала «Блетчлійська декларація» – документ, підписаний понад 30 державами, включно зі США, ЄС, Австралією, Японією та Канадою. У 2024 році аналогічні саміти відбулися у Південній Кореї та Франції, де було погоджено створення міжнародної мережі центрів з оцінки ризиків ШІ [44].

Проте важливо зазначити, що міжнародна система інформаційної безпеки не може бути ефективною без забезпечення кіберстійкості найбільш уразливих держав, які часто стають об'єктами кібератак через брак ресурсів та кваліфікації. Так, країни Глобального Півдня стикаються з масштабними проблемами інституційної слабкості, відсутності цифрової інфраструктури та обмеженими можливостями реагувати на складні інформаційні інциденти. У відповідь ООН, Світовий банк та Міжнародний союз електрозв'язку активно впроваджують програми технічної допомоги, спрямовані на розвиток національних центрів реагування на кіберінциденти (CERT), цифрову просвіту та підтримку урядових структур [48]. Необхідно також підкреслити, що міжнародна система інформаційної безпеки поступово розширює співпрацю з громадянським суспільством, академічною спільнотою та медіаорганізаціями. Показово, що навіть у питаннях кібербезпеки дедалі більше уваги приділяється людському фактору, адже статистика за 2023–2024 роки свідчить, що понад 70

% інцидентів спричинені фішинговими атаками, які використовують психологічні методи впливу [49].

Водночас міжнародна система стикається з новими викликами, що ускладнюють вироблення універсальних норм. Серед них: розвиток квантових технологій, які потенційно можуть зробити традиційні методи шифрування застарілими. Уже сьогодні Китай активно інвестує у квантові комунікації та будівництво квантового інтернету, що, за оцінками фахівців, може радикально змінити баланс сил у сфері кіберзахисту [80]. Таким чином, міжнародна система забезпечення інформаційної безпеки є не статичною структурою, а складним і безперервно змінюваним механізмом, який реагує на розвиток технологій, геополітичні виклики та зміни в глобальній архітектурі безпеки [66]. Сучасні приклади, від протидії дезінформації під час виборів у Європі та США до формування глобальних стандартів безпеки штучного інтелекту, демонструють, що інформаційна безпека стала ключовим виміром міжнародної політики.

1.3. Теоретичні підходи до формування національних систем інформаційної безпеки

Національні системи інформаційної безпеки у сучасних міжнародних відносинах формуються на перетині низки теоретичних підходів, які, з одного боку, відображають еволюцію уявлень про інформацію як стратегічний ресурс, а з іншого, демонструють розширення спектра загроз у цифрову епоху. Саме через це концептуальне осмислення інформаційної безпеки потребує врахування міждисциплінарних знань, що включають політологію, міжнародні відносини, кібернетику, комунікативні студії та управління ризиками. Відтак, поступове переорієнтування держав на превентивні моделі захисту інформаційного простору зумовлює необхідність аналізу ключових теоретичних підходів, які пояснюють принципи, структури та механізми функціонування національних систем інформаційної безпеки [20]. Передусім слід зазначити, що реалізм як одна з базових парадигм міжнародних відносин

пропонує бачення інформаційної безпеки крізь призму конкуренції держав за владу та ресурси. Інформація у цьому контексті трактується як інструмент примусу, маніпуляції або стримування, а тому розбудова національної системи інформаційної безпеки орієнтована на захист суверенітету та забезпечення балансу сил. У межах цього підходу держава виступає головним актором, що володіє монополією на застосування інструментів інформаційного впливу та контролю. Як свідчить сучасна практика, зокрема протистояння між США та Китаєм у галузі штучного інтелекту, космічних технологій і цифрових комунікацій, інформаційна перевага дедалі частіше стає критичним фактором у визначенні геополітичного домінування [38]. Крім того, інформаційно-когнітивні операції, які активно використовує Росія у війні проти України, підтверджують, що держави застосовують інформаційні інструменти для дестабілізації безпекового середовища противника, руйнування суспільної довіри та підриву політичної єдності [10]. Тому реалізм формує підґрунтя для державоцентричної моделі інформаційної безпеки, орієнтованої на створення потужного інституційного апарату та розвинених механізмів стратегічних комунікацій.

У контексті ліберального підходу інформаційна безпека осмислюється значно ширше: не як виключна сфера контролю держави, а як результат взаємодії багатьох акторів: міжнародних організацій, недержавних інституцій, приватних компаній, громадянського суспільства та технологічних корпорацій. Лібералізм наголошує на важливості кооперації, спільного управління та вироблення універсальних правил поведінки у цифровому просторі. Так, Європейський Союз, базуючись саме на ліберальній логіці, формує загальноєвропейську архітектуру кібербезпеки: Директива NIS2 (2022), Європейський акт про кіберстійкість (2023), а також створення Європейського центру компетенцій з кібербезпеки у Румунії демонструють, що сучасні інформаційні загрози долаються не лише національними ресурсами, а й через мережеві форми партнерства [1]. У цьому контексті національна система інформаційної безпеки трактується як частина ширшого міжнародного

режиму, який регулює цифрові потоки, стандарти безпеки та механізми реагування на інциденти. Ліберальний підхід також наголошує на прозорості, інклюзивності та необхідності залучення приватного сектору, що є особливо важливим за умов, коли критична інфраструктура у більшості країн світу перебуває у руках недержавних суб'єктів.

Трансформаційні процеси цифрової доби зумовили звернення до конструктивізму як теоретичної основи для формування національних систем інформаційної безпеки. Конструктивісти наголошують, що загрози та ризики у сфері інформаційної безпеки не існують об'єктивно — вони є соціально сконструйованими та залежать від того, як суспільство, політики, експерти чи міжнародні інституції інтерпретують інформаційні процеси. Показовим є приклад країн Балтії, де загроза російської дезінформації була усвідомлена задовго до її глобалізації, що дозволило Естонії, Латвії та Литві створити ефективні механізми медіаграмотності, національного мовного захисту та стратегічних комунікацій [17]. Водночас значного поширення у сучасних дослідженнях набув інституціональний підхід, що розглядає інформаційну безпеку як системний процес, який забезпечується через формування організаційних структур, нормативно-правових засад та процедур управління ризиками. У національних системах інформаційної безпеки ключову роль відіграють спеціалізовані агентства, ради, центри реагування на кіберінциденти (CERT), наглядові органи та аналітичні структури. Наприклад, у Франції функціонує ANSSI, одна з найавторитетніших у Європі агенцій з кіберзахисту, яка визначає стандарти, проводить сертифікацію обладнання та координує взаємодію між державою та бізнесом. У США важливим елементом виступає CISA, створена у 2018 році, яка стала центром міжвідомчої координації у галузі кібербезпеки [1].

Певною мірою національні системи інформаційної безпеки також формуються під впливом мережевого підходу, який виходить з того, що сучасний світ являє собою складну конфігурацію взаємозалежних мереж — цифрових, політичних, економічних, соціальних. Прикладом цього є

діяльність НАТО Cooperative Cyber Defence Centre of Excellence, який з 2022 року координує кіберзахист у країнах-членах і проводить міжнародні навчання Locked Shields – наймасштабніші у світі кіберзмагання, що дозволяють тестувати мережеву стійкість критичної інфраструктури [35]. Не менш важливим для формування національних систем інформаційної безпеки є ризикологічний підхід, який фокусується на прогнозуванні, попередженні та мінімізації потенційних загроз. Ризикологічний підхід активно використовується у країнах ЄС для розроблення національних стратегій кіберстійкості, які містять комплекс заходів для захисту критичної інфраструктури. Наприклад, Німеччина у 2023 році представила нову стратегію кібербезпеки, у якій детально описано модель оцінки ризиків, систему зонування кіберпростору та підходи до запобігання масштабним кібератакам [1].

Суттєвий вплив на сучасні теоретичні підходи має концепція цифрового суверенітету, яка набуває дедалі більшого значення у країнах ЄС, Індії, Японії та Південної Кореї. Яскравим прикладом у цьому контексті є регулювання Big Tech у Європейському Союзі, зокрема ухвалення Digital Markets Act та Digital Services Act, що спрямовані на посилення національного та наднаціонального контролю над цифровими платформами [1]. В той же час, системний підхід, який розглядає інформаційну безпеку як цілісну динамічну систему, дозволяє аналізувати взаємозв’язки між її елементами, виявляти слабкі місця та вбудовувати механізми адаптивного управління. Показовим прикладом застосування системного підходу є модель Zero Trust, яку активно впроваджують США, Велика Британія та Австралія [77].

Не слід оминати і поведінковий підхід, який акцентує на людському факторі як ключовому елементі національної інформаційної безпеки. Саме люди є найвразливішою ланкою у системах кіберзахисту, що підтверджують численні глобальні інциденти останніх років: витоки інформації внаслідок фішингових атак на державні установи США у 2023 році чи компрометація даних громадян Сінгапуру через соціотехнічні методи впливу [14]. Нарешті,

важливе місце у концептуалізації інформаційної безпеки посідає критичний підхід, який аналізує її через призму влади, дискурсів та структурних нерівностей. Питання етичного регулювання штучного інтелекту, які активно обговорюються після ухвалення AI Act у ЄС у 2024 році, є прикладом застосування критичного підходу у сучасних політичних дискусіях [66].

Важливо підкреслити, що розвиток теоретичних підходів до формування національних систем інформаційної безпеки не є статичним процесом, адже він постійно адаптується до швидкоплинної логіки цифрової трансформації та ескалації міжнародних загроз. Зокрема, у постпандемічний період зросла увага до концепцій інформаційної стійкості, які доповнили традиційні парадигми безпеки [25]. Інформаційна стійкість передбачає не лише здатність держави протидіяти атакам чи втручанню, а й можливість швидкого відновлення функціонування систем, підтримання довіри громадян та збереження демократичних інститутів у кризових умовах. У цьому контексті зростає значення холістичного підходу, що поєднує технологічні, психологічні та організаційні компоненти інформаційної безпеки. Одним із ключових елементів цього підходу стає розвиток стратегічних комунікацій та державної політики у сфері протидії дезінформації. Сучасні приклади, зокрема діяльність Центру протидії дезінформації при РНБО України (створеного у 2021 році), свідчать про необхідність інституційного закріплення механізмів стратегічного інформування, які допомагають формувати єдиний наратив держави, підвищувати рівень суспільної стійкості та ефективно реагувати на інформаційні атаки [23]. Аналогічні підходи застосовуються у Литві та Швеції, де створені спеціальні центри психологічної оборони, що координують дії органів влади, ЗМІ та громадянського суспільства у період кризових ситуацій. Ці приклади демонструють, що сучасні теоретичні моделі інформаційної безпеки виходять за межі технічного захисту і дедалі більше охоплюють гуманітарний вимір, формуючи комплексну архітектуру безпеки.

Разом із тим у глобальному дискурсі інформаційної безпеки посилюється роль технологічно-орієнтованих підходів, зокрема тих, що

ґрунтуються на використанні штучного інтелекту та алгоритмічних систем у процесах кіберзахисту. Моделі машинного навчання нині використовуються для прогнозування атак, аналізу аномалій у мережевому трафіку та автоматичного виявлення шкідливих програм. Наприклад, у 2024 році Агентство з кібербезпеки ЄС (ENISA) представило рекомендації щодо інтеграції AI-based systems у критичну інфраструктуру з метою підвищення ефективності захисту [1]. Ці новітні інструменти водночас вимагають переосмислення теоретичних підходів, адже створюють нові ризики, від залежності від алгоритмів до етичних дилем використання автономних систем. Таким чином, формування національної системи інформаційної безпеки поступово зміщується у бік кібернетичної парадагми, що аналізує інформаційний простір як складну систему взаємодії людини й машинних технологій.

Ще одним перспективним теоретичним напрямом є підхід, заснований на моделі багаторівневого врядування. Він визнає, що сучасні інформаційні загрози не можуть бути подолані виключно на рівні центральної влади, оскільки вони проникають у локальні спільноти, корпоративні структури, міжнародні організації та транскордонні цифрові мережі [18]. Багаторівневе врядування пропонує побудову національної системи інформаційної безпеки як узгодженої вертикально-горизонтальної мережі взаємодії між державою, регіональними органами, місцевими громадами, приватним сектором та громадянським суспільством. Усе частіше саме місцеві інституції відіграють важливу роль у забезпеченні інформаційної стійкості: наприклад, муніципальні центри цифрової безпеки у Нідерландах або локальні програми кіберосвіти у Канаді, які інтегрують дітей та молодь у процеси формування цифрової культури. Це вказує на те, що національна система інформаційної безпеки має бути не лише ієрархічною, а й мережевою та інклюзивною.

У межах глобалізаційних процесів зростає роль також і геоекономічного підходу, який трактує інформаційну безпеку як складову економічного розвитку держави та її конкурентних переваг на світовому ринку. У цій логіці

дані розглядаються як «нова нафта», а цифрова інфраструктура, як стратегічний актив, що визначає здатність країни брати участь у глобальних ланцюгах створення вартості. Сучасні приклади демонструють посилення конкуренції за контроль над дата-центрами, хмарними технологіями та ринками кіберпослуг. Так, інвестиційні стратегії Південної Кореї, Сінгапуру та ОАЕ показують, що формування ефективної національної системи інфо рмаційної безпеки стає чинником залучення міжнародних інвестицій, розвитком цифрової економіки та зміцненням глобальних позицій держави [11]. Окремої уваги потребує гуманітарний підхід, що фокусується на людині як центральному елементі інформаційної системи держави. У цій теоретичній моделі безпека не може обмежуватися технічними характеристиками: вона передбачає захист прав людини, свободи слова, приватності, а також забезпечення доступу до достовірної інформації. Саме гуманітарний вимір став ключовим у дискусіях навколо регулювання штучного інтелекту, захисту персональних даних та боротьби з медіаманіпуляціями. Прикладом є впровадження у 2024 році Європейського акту про штучний інтелект, який вводить жорсткі обмеження на використання AI для масового стеження та оцінювання поведінки громадян [1].

Узагальнюючи, можна стверджувати, що сучасні теоретичні моделі формування національних систем інформаційної безпеки пропонують різноспрямовані, але взаємодоповнювальні інструменти, які дозволяють державам створювати комплексні, гнучкі та стійкі механізми захисту. У перспективі важливою тенденцією буде подальша інтеграція національних систем у міжнародні мережі безпеки, розвиток алгоритмічних методів прогнозування та адаптація правових моделей до викликів штучного інтелекту й транснаціональних інформаційних потоків. Саме така еволюція забезпечує можливість формувати системи, здатні підтримувати стабільність, розвиток і безпеку у світі, де інформація набуває дедалі більшої стратегічної ваги.

Висновки до розділу 1

У висновку зазначимо, що еволюція поняття «інформаційної безпеки» у сучасних міжнародних відносинах демонструє його поступовий перехід від вузького технократичного розуміння до комплексної категорії, яка охоплює політичні, правові, інституційні та соціокультурні виміри. Спершу інформаційна безпека асоціювалася переважно із захистом інфраструктури та технічних систем, проте з розвитком цифровізації її трактування значно розширилося. Вона почала включати питання кіберзагроз, інформаційного впливу, медіаманіпуляцій, стратегічних комунікацій, а також забезпечення стійкості суспільства до дезінформації. Причому важливо наголосити, що, на відміну від минулих десятиліть, інформаційна безпека нині сприймається як ключовий елемент національної та міжнародної безпеки, що прямо впливає на політичну стабільність, зовнішню політику та міжнародну взаємодію держав.

Водночас система забезпечення інформаційної безпеки на міжнародному рівні продовжує формуватися під впливом глобалізаційних процесів і технологічних змін. З одного боку, міжнародні організації, такі як ООН, НАТО, ОБСЄ, ЄС, напрацьовують нормативні підходи, створюють інституційні механізми координації та виробляють стандарти реагування на кіберінциденти. З іншого боку, держави демонструють різні моделі поведінки, що ускладнює формування універсальних правил гри. Проте, як показує аналіз, саме міжнародні формати співпраці дозволяють забезпечити більш ефективну взаємодію у сфері обміну інформацією, раннього попередження та розвитку спільних механізмів протидії загрозам.

Не менш важливим є дослідження теоретичних підходів до формування національних систем інформаційної безпеки, адже вони окреслюють рамки стратегічного бачення держав щодо захисту інформаційного простору. Функціоналістський, інституціональний, мережевий, системний та соціоконструктивістський підходи підкреслюють, відповідно, роль інституцій, нормативних структур, взаємодії акторів та суспільного сприйняття загроз. Усі вони, зрештою, дозволяють зрозуміти, що національні системи інформаційної

безпеки мають будуватися на принципах комплексності, адаптивності, міжвідомчої координації та активної взаємодії держави з приватним сектором і громадянським суспільством. Саме поєднання цих підходів забезпечує здатність держав ефективно реагувати на інформаційні загрози в умовах сучасної глобальної турбулентності.

РОЗДІЛ 2. СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІЗРАЇЛЮ

2.1. Інституційна складова системи інформаційної безпеки Ізраїлю

Інституційна складова системи інформаційної безпеки Ізраїлю формувалася протягом кількох десятиліть і є результатом унікального поєднання геополітичних умов, високої технологічної спроможності держави та системної державної політики, зорієнтованої на випередження загроз у цифровому середовищі. Насамперед слід зазначити, що Ізраїль, розташований у середовищі постійних воєнно-політичних викликів, вимушений був раніше за багато інших держав створити комплексну модель інформаційної безпеки, яка включає координацію діяльності військових, розвідки, спеціалізованих урядових агентств, приватного сектору та дослідницьких установ [8]. Саме ця багаторівнева структура стала основою для сучасної національної системи інформаційної безпеки, що вирізняється динамічністю, високим ступенем інтегрованості та чітким розподілом функцій між інституціями. При цьому ключовим принципом є забезпечення постійної комунікації між органами влади та приватними компаніями, які у цифрову епоху володіють значною часткою критичної інфраструктури [32]. Одним із центральних компонентів інституційної системи є Національне кібернетичне управління Ізраїлю, яке з 2018 року функціонує як інтегрована структура, Israel National Cyber Directorate (INCD) [1]. Воно об’єднало два раніше окремі органи: Національне управління кібернетичної безпеки та Національне управління кібернетичної ініціативи. Через таке об’єднання вдалося посилити стратегічне планування, підвищити ефективність реагування та уникнути дублювання функцій [9]. INCD координує загальнодержавну політику у сфері інформаційної та кібербезпеки, розробляє регуляторні акти, здійснює моніторинг загроз, а також відповідає за обмін інформацією про інциденти між державними і недержавними структурами. Більше того, значна увага приділяється взаємодії з критичною інфраструктурою: у 2023-2024 роках INCD впровадило оновлену систему оцінювання кіберризиків для енергетики, водопостачання та

медичного сектору, що дозволило підвищити стійкість ключових об’єктів до кібератак і дезінформаційних кампаній [49].

Разом із тим важливе місце у системі посідають розвідувальні органи. Передусім варто згадати військову розвідку АМАН (Directorate of Military Intelligence), підрозділи якої відповідають не лише за перехоплення й аналіз даних, а й за проведення оперативних кібероперацій. Особливу роль відіграє підрозділ 8200 – один із найбільш технологічно розвинених у світі [46]. Він виконує функції спеціалізованого центру сигнальної розвідки, займається збором та аналізом цифрової інформації, забезпечує прогнозування загроз і розробку інструментів для кіберзахисту та кібернападу. З огляду на це багато сучасних технологічних рішень у сфері захисту інформаційних систем Ізраїлю беруть початок саме в інноваціях цієї структури, а її випускники нерідко стають засновниками провідних компаній у сфері кібербезпеки, зокрема Check Point, SentinelOne, Wiz, Cybereason та інших [32].

Поряд із військовою розвідкою надзвичайно вагому роль відіграє служба загальної безпеки Шабак (Shin Bet). Вона відповідає за контррозвідувальну діяльність, боротьбу з тероризмом усередині країни та захист державних інститутів від інформаційних та кіберзагроз [74]. Шабак має спеціалізовані підрозділи для моніторингу соціальних мереж, аналізу інформаційних потоків та виявлення екстремістських мережевих активностей. Після збройного загострення конфлікту на Близькому Сході у 2023 році служба суттєво розширила можливості аналізу великих даних для оперативного виявлення загроз, пов’язаних із радикалізацією у цифровому середовищі. Слід підкреслити, що інституційна система Ізраїлю не обмежується військовими чи безпековими структурами. Зокрема, значну роль відіграє Міністерство комунікацій, яке встановлює регуляторні норми щодо діяльності телекомунікаційних операторів та інформаційних платформ [40]. Воно визначає вимоги до захисту даних, управління ризиками, реагування на інциденти та обміну інформацією з органами безпеки. У 2022–2024 роках міністерство активізувало роботу над регулюванням платформ соціальних

мереж, у тому числі щодо боротьби з онлайн-радикалізацією, мови ненависті та розповсюдження дезінформації.

Не менш важливою є діяльність Міністерства оборони, яке відповідає не лише за воєнні аспекти безпеки, а й за розвиток технологічної інфраструктури, що забезпечує стійкість держави у кіберпросторі. Наприклад, саме під егідою Міністерства оборони реалізуються програми досліджень та інновацій у сфері штучного інтелекту, спрямовані на модернізацію системи кіберзахисту [44]. Окремим, але дуже впливовим елементом інституційної системи виступає Національний центр CERT-IL – організація, що координує реагування на кіберінциденти, здійснює аналітичний супровід та консультує приватний сектор [78]. Після хвилі атак на ізраїльські медичні установи у 2023 році, CERT-IL запустив спеціальну платформу для оперативного обміну інформацією між лікарнями, страховими компаніями та держорганами [13].

Важливою складовою є також безпекова співпраця держави з приватним секто ром. Ізраїль відомий як один зі світових центрів cybersecurity-індустрії, що налічує понад 500 компаній та десятки стартапів, які працюють у сфері інформаційної безпеки [41]. Держава активно сприяє їхньому розвитку, зокрема через податкові стимули, інвестиції в інноваційні кластери та підтримку науково-дослідних проєктів. Науково-дослідні інституції також посідають важливе місце у системі. Університети, такі як Тель-Авівський, Техніон, Єврейський університет у Єрусалимі, мають спеціалізовані лабораторії та дослідницькі центри у сфері cybersecurity [39]. Важливо підкреслити, що інституційна система інформаційної безпеки Ізраїлю діє на основі принципу багаторівневої взаємодії, що охоплює стратегічний, оперативний та тактичний рівні [59]. Такий підхід дозволяє швидко адаптуватися до нових викликів, що особливо важливо з огляду на зростання кількості атак з боку Ірану та пов’язаних з ним хакерських угруповань.

Водночас важливо наголосити, що інституційна система Ізраїлю базується на гнучкому правовому та стратегічному підґрунті, що постійно оновлюється відповідно до нових технологічних тенденцій. Так, уряд Ізраїлю

регулярно ухвалює національні програми та дорожні карти, спрямовані на удосконалення кіберзахисту. Програма «CyberNet», запущена у 2022 році, створила національну платформу для об'єднання всіх державних органів, що працюють у сфері інформаційної безпеки [30]. У межах цієї ініціативи з'явилася можливість в автоматичному режимі обмінюватися сигнатурами шкідливого програмного забезпечення, інформацією про вектори атак і рекомендаціями щодо їхнього нейтралізування [65].

Крім того, держава приділяє значну увагу підготовці людського капіталу. Це важливо, оскільки ефективність інституційного механізму у сфері інформаційної безпеки залежить від рівня кваліфікації спеціалістів. Серед ключових інструментів слід назвати програму Talpiot – одну з найпотужніших освітньо-військових ініціатив світу, яка готує спеціалістів із високими компетенціями у сфері кіберзахисту, математичного аналізу та інформаційних технологій [46, с. 112–119]. Багато випускників цієї програми стають частиною підрозділів 8200, інших військових структур або приватних компаній, що забезпечує безперервний обіг знань та інновацій між державою і бізнесом [8]. У 2023–2024 роках Talpiot була модернізована: введено курси з квантових обчислень, штучного інтелекту та протидії широкомасштабним інформаційним кампаніям, що відповідає глобальним тенденціям цифрової трансформації [49]. Система інформаційної безпеки Ізраїлю також має інституційні механізми співпраці на міжнародному рівні. Зокрема, INCD бере участь у роботі Глобального форуму з кібереконономічної безпеки, співпрацює з ЄС у рамках програм Horizon Europe та обмінюється аналітичними даними з відповідними структурами США, Канади, Великої Британії та Австралії [53]. Після серії складних атак у 2023 році, пов'язаних із кіберактивністю груп, що працюють на Іран, Ізраїль розширив співпрацю з Агентством кібербезпеки і безпеки інфраструктури США (CISA) та з британським National Cyber Security Centre [49]. У результаті було створено спільні протоколи обміну інформацією, які дозволили скоротити час від виявлення до нейтралізації складних інфраструктурних атак у середньому на 40 % [49].

Важливим аспектом інституційної складової є створення механізмів суспільної комунікації та взаємодії з населенням. Ізраїльські органи влади активно популяризують культуру інформаційної безпеки серед громадян через національні онлайн-платформи, соціальні кампанії та програми у школах. Наприклад, у 2024 році INCD запровадило проєкт «Cyber for Youth», спрямований на підвищення цифрової грамотності молоді та вміння протистояти маніпуляціям у соціальних мережах [49]. Сукупність інституційних механізмів в Ізраїлі охоплює також розвинену нормативно-технічну інфраструктуру. Держава встановлює стандарти у сфері кіберзахисту, обов’язкові до виконання для операторів критичної інфраструктури. У 2023 році були ухвалені оновлені Cyber Defense Regulations, які деталізували вимоги до управління ризиками, створення систем журналювання кіберінцидентів, проведення регулярних аудитів та тестів на проникнення [1, с. 15–17]. Важливо підкреслити, що виконання цих вимог є обов’язковим, а їх порушення тягне за собою серйозні санкції [40].

Однією з визначальних рис інституційної складової Ізраїлю є її інтегрованість із концепцією «національної стійкості». Кібератаки, інформаційні операції, психологічний вплив, спроби маніпуляції громадською думкою – усі ці виклики розглядаються як елементи комплексної гібридної загрози, що потребує відповідної інституційної відповіді. У цьому контексті важливу роль відіграє Міністерство стратегічних справ, яке координує політику протидії дезінформації, антиізраїльським кампаніям у міжнародних медіа та пропаганді, що поширюється недержавними та державними акторами [50]. Наприклад, кампанії 2023 року, спрямовані на дискредитацію ізраїльських військових дій у Газі, супроводжувалися масштабними інформаційними маніпуляціями у соцмережах. Реакція міністерства полягала у створенні оперативної групи з аналізу наративів, яка співпрацювала з Meta, X та YouTube для блокування акаунтів, пов'язаних з іноземними спецслужбами та екстремістськими організаціями [49].

У ширшому вимірі інституційна система Ізраїлю – це не просто набір відомств, а комплексний механізм, де кожен інститут виконує свою частину спільного завдання. Важливо, що взаємодія між структурними елементами не є формальною; навпаки, вона базується на регулярному обміні даними, спільному плануванні та взаємному контролі. Наприклад, INCD і підрозділ 8200 мають спільні аналітичні групи, що дозволяє оперативно оцінювати технічні параметри нових загроз [46, с. 201–208]. Також слід наголосити, що інституційна складова інформаційної безпеки Ізраїлю постійно модернізується. У 2024 році уряд розпочав реформу кіберрегулювання, яка передбачає створення більш глибокої інтеграції між секторами економіки та державними структурами. У рамках проєкту «Cyber Resilience 2030» планується впровадити чотирирівневу систему оцінювання стійкості організацій, що дозволить виявляти слабкі ланки ще до того, як вони стануть об'єктом атак [56]. Заплановано також розвиток системи раннього попередження на основі штучного інтелекту, що аналізує десятки інформаційних каналів і дозволяє в реальному часі прогнозувати потенційні загрози [65].

Узагальнюючи, інституційна складова системи інформаційної безпеки Ізраїлю є багатошаровим, технологічно насиченим і надзвичайно ефективним механізмом, що поєднує державне управління, розвідувальні структури, приватні технологічні компанії та наукові установи. Її сила полягає у гнучкості, стратегічній далекоглядності та здатності швидко адаптуватися до нових форм гібридних загроз. Завдяки цьому Ізраїль залишається одним із глобальних лідерів у сфері захисту інформаційного простору й демонструє приклад того, як інституційна координація та технологічний розвиток можуть створити надзвичайно стійку систему безпеки в умовах постійної трансформації міжнародного середовища.

2.2. Нормативно-правова складова системи інформаційної безпеки Ізраїлю: від військової доктрини до кібернетичної стратегії

Нормативно-правова складова системи інформаційної безпеки Ізраїлю формувалася під впливом складного безпекового середовища, у якому держава перебуває з моменту свого заснування, а тому вона поєднує жорсткі військово-стратегічні підходи з гнучкими інструментами цифрового врядування. Упродовж десятиліть Ізраїль розвивав концепцію безпеки, яка, з одного боку, спирається на превентивні дії та стримування, а з іншого – на побудову технологічно насиченої інфраструктури для захисту критичних систем. Саме тому еволюція нормативно-правових засад інформаційної безпеки цієї держави відображає не лише реакцію на зовнішні загрози, але й стратегічне бачення майбутнього, у якому кіберпростір стає ключовим полем боротьби [8].

Якщо розглядати витоки ізраїльської моделі, то слід зазначити, що її фундамент було закладено у військовій доктрині, що тривалий час визначала структуру сектору безпеки. Доктрина передбачала широке застосування розвідувальних можливостей, оперативну координацію між армією, спецслужбами та урядовими структурами, а також пріоритет раннього виявлення загроз [6]. Наприклад, діяльність Управління військової розвідки АМАН тривалий час залишалася ключовою в забезпеченні стійкості держави перед атаками на інформаційні мережі. Водночас, ще у 1990-х роках Ізраїль почав формувати перші нормативні положення щодо захисту урядових комунікацій та стійкості інфраструктури, що стало фактичним прообразом подальшої кібернетичної стратегії [74]. Поступово, у міру того як інформаційні технології почали інтегруватися у всі сфери життя, Ізраїль усвідомив необхідність створення цілісної правової архітектури, яка б регулювала не лише діяльність силових структур, але й взаємодію держави з приватним сектором та громадянами. У 2002 році було ухвалено один з перших значущих документів – Закон про захист приватних даних, який започаткував правове регулювання цифрового середовища [40]. Хоча цей акт потребував подальшої модернізації, він став наріжним каменем формування правової культури

захисту інформації. Також у цей період активно розвивалася нормативна база щодо критичної інфраструктури, адже ізраїльські технологічні компанії та енергетичні об’єкти дедалі частіше ставали цілями атак з боку недержавних акторів.

Особливо важливим етапом став 2011 рік, коли уряд ухвалив рішення створити Національне управління з питань кібербезпеки (INCB) – інституцію, яка отримала не лише координаційні, а й стратегічні повноваження [1]. Ця реформа була відповіддю на масштабне зростання кіберінцидентів. Наприклад, атаки групи Anonymous на урядові ресурси Ізраїлю у 2012–2013 роках наочно продемонстрували вразливість відкритих мереж та потребу в системній реакції. Формулювання мандату INCB супроводжувалося підготовкою нормативних актів щодо кіберзахисту критичної інфраструктури, впровадженням обов’язкових стандартів безпеки для операторів життєво важливих об’єктів та створенням механізмів обміну інформацією про інциденти. У подальші роки нормативно-правова база зазнала суттєвого оновлення. Так, у 2015 році Ізраїль ухвалив комплексний підхід до кіберуправління, створивши дві ключові інституції – Національне кібернетичне бюро (INCB) та Національне управління кібербезпеки (INCD). Ці два органи мали різні функції: перше займалося розробкою державної політики, друге – практичним забезпеченням захисту державних і цивільних систем. Згодом вони були об’єднані в єдину Національну дирекцію з кібербезпеки (Israel National Cyber Directorate, INCD), що стало важливим кроком у напрямі оптимізації та уніфікації кіберполітики [72].

Одним із ключових нормативно-стратегічних документів став «Національний кібернетичний план Ізраїлю», який окреслив методологію захисту держави в цифровому просторі [69]. У цьому документі підкреслювалися принципи багаторівневого підходу, відповідальність приватного сектору у сфері впровадження стандартів безпеки, а також значення інновацій для національної стратегії. Не менш важливим стало затвердження вимоги до підприємств критичної інфраструктури регулярно

проводити оцінку ризиків, дотримуватися протоколів реагування на інциденти та забезпечувати постійний контакт з INCD. Ці норми набули особливої актуальності після кібератак на систему водопостачання країни у 2020 році, коли було здійснено спробу втрутитися в роботу насосних станцій [31]. Інцидент підкреслив необхідність оновлення законодавства, яке мало б посилити обов'язки операторів інфраструктури та передбачити суворіший контроль. У межах реформ 2020-2023 років Ізраїль активізував роботу над новим проектом Закону про кібербезпеку, який має на меті узгодити фрагментовані норми та створити юридично чітку систему розподілу відповідальності. Розробники наголошують, що сучасні загрози вимагають нового підходу: сьогодні атаки здійснюють не лише держави, але й організовані кримінальні угруповання, хакерські активісти та терористичні групи, які використовують штучний інтелект, deepfake-технології та методи інформаційно-психологічного впливу [44].

Цікаво, що ізраїльська правова система активно інтегрує положення щодо державного-приватного партнерства. З огляду на те, що значна частина технологічних рішень створюється саме приватними компаніями, законодавство стимулює передачу інновацій до державного сектору, зокрема в рамках програм підтримки стартапів та спільних платформ кіберзахисту [46]. Такий підхід демонструє, що нормативно-правові акти Ізраїлю орієнтовані не лише на реагування, але й на превентивний розвиток екосистеми кіберстійкості.

Окремої уваги заслуговує нормативно-правова регламентація діяльності спецслужб у сфері інформаційної безпеки. Наприклад, Моссад, ШАБАК і АМАН мають законодавчо визначені мандати, які передбачають право збирати інформацію, здійснювати аналіз кіберзагроз та запобігати атакам, що спрямовані на підрив національної безпеки. Закон про діяльність ШАБАК 2002 року визначив юридичні рамки роботи служби внутрішньої безпеки, зокрема механізми контролю за її діяльністю [40]. Протягом останніх років ізраїльські законодавці дедалі частіше звертаються до проблематики штучного інтелекту

та його використання у сфері інформаційної безпеки. У 2023 році було розпочато підготовку рекомендацій щодо регулювання AI, які мають на меті запровадити етичні стандарти, забезпечити прозорість алгоритмів та запобігти зловживанням у сфері національної безпеки [44]. Ізраїль усвідомлює, що штучний інтелект може використовуватися не лише як засіб оборони, але й як інструмент ведення інформаційних операцій, зокрема для автоматизованого створення пропагандистського контенту чи впливу на суспільну думку.

Особливо важливим елементом нормативної архітектури є міжнародно-правові зобов'язання Ізраїлю. Хоча держава не є членом багатьох європейських структур, вона активно співпрацює з НАТО, США, ЄС та низкою азійських партнерів у сфері обміну інформацією, боротьби з кіберзлочинністю та розроблення стандартів кіберзахисту [53]. Наприклад, у 2022 році Ізраїль приєднався до Глобального форуму з кіберекономічної безпеки, що дозволило інтегрувати національну нормативну базу у міжнародні механізми співробітництва. Більш того, ізраїльська нормативно-правова модель характеризується інституційною гнучкістю. Наприклад, після хвилі атак на медичний сектор у 2021 році, коли кілька лікарень було тимчасово паралізовано внаслідок шифрувальних вірусів, уряд швидко оновив вимоги до захисту персональних медичних даних [13]. Було запроваджено обов'язкові стандарти шифрування та створено додаткові механізми аудиту. Така динаміка нормативних змін демонструє адаптивність ізраїльської системи, що суттєво вирізняє її від моделей інших країн, де законодавчі процеси часто тривають роками [72]. Ізраїль також активно працює над формуванням правового механізму протидії інформаційно-психологічним операціям. У 2020–2024 роках парламент обговорював законодавчі ініціативи щодо регулювання соціальних мереж, спрямовані на боротьбу з дезінформацією, онлайн-радикалізацією та координацією терористичної діяльності [3, с. 165]. Такі ініціативи часто критикуються міжнародними правозахисними організаціями за ризики обмеження свободи слова, однак ізраїльська влада підкреслює їхню необхідність у контексті унікальних загроз, з якими стикається держава.

Зрештою, спроби створення правових механізмів контролю за інформаційними потоками є прямим відображенням еволюції від традиційної військової доктрини до комплексної кібернетичної стратегії [46].

Важливо, що нормативно-правове підґрунтя інформаційної безпеки Ізраїлю має не лише оборонний, але й структурний характер, адже воно сприяє розвитку кіберіндустрії, наукових досліджень та інновацій. Програми, що регулюють співпрацю між державними органами та університетами, дозволяють залучати молодих фахівців до роботи над національними проектами. Наприклад, у межах програм Talpiot та CyberGym студенти та військовослужбовці навчаються моделювати кіберінциденти й розробляти відповідні сценарії реагування [11, с. 130–132]. Наявність таких програм також має нормативне підґрунтя, оскільки вони реалізуються відповідно до державних стратегічних документів. Крім того, нормативно-правові підходи Ізраїлю до забезпечення інформаційної безпеки відзначаються високим рівнем інтегрованості між секторами, що, власне, і зумовлює їхню ефективність. Наприклад, регулювання діяльності компаній телекомунікаційного сектору здійснюється не лише Міністерством комунікацій, але й INCD, що дозволяє одночасно контролювати технічні параметри мереж та їхній захист від кіберзагроз [72]. Таке багатосуб’єктне управління формує мережеву модель нормативного контролю, у якій різні інституції відповідають за окремі сегменти, але працюють в одному стратегічному векторі. Додатково, саме завдяки нормативному закріпленню вимоги до обов’язкового повідомлення про інциденти Ізраїлю вдалося створити одну з найефективніших систем кібермоніторингу у світі [40].

Важливо, що нормативна база країни включає також положення щодо захисту демократичних процесів від зовнішнього втручання. Після низки атак на інформаційну інфраструктуру політичних партій та спроби кібервпливу на вибори 2019 року, уряд Ізраїлю розробив спеціальні нормативні механізми захисту електорального процесу [9, с. 80]. Було ухвалено нові регуляції, які визначають порядок аудиту інформаційних систем партій, правила зберігання

та обробки виборчих даних, а також вимоги до провайдерів соціальних мереж щодо виявлення координованих маніпуляцій. Ізраїльська нормативно-правова система приділяє особливу увагу захисту критичної інфраструктури на тлі загострення регіональних конфліктів, що підтверджується становленням спеціальних регуляторів у сфері енергетики, водопостачання, транспорту та охорони здоров'я. Наприклад, після спроби проникнення у системи водопостачання у 2020 році уряд ухвалив вимогу щодо створення секторних центрів операційної безпеки, які повинні виконувати постійний моніторинг усіх процесів та взаємодіяти з національною кібердирекцією [31]. Схожі норми були введені й для медичного сектору після серії атак на лікарні в 2021 році [13].

Нормативно-правовий розвиток Ізраїлю у сфері інформаційної безпеки демонструє поступовий перехід від фрагментарних норм до комплексної правової екосистеми, у якій законодавчі акти, підзаконні регуляції та стратегічні документи створюють єдине середовище. Зокрема, із запуском Національної програми кіберосвіти сучасні норми були орієнтовані також на формування культури безпечної поведінки у цифровому середовищі серед населення [36]. Такий підхід має фундаментальне значення, оскільки людський фактор залишається одним із найуразливіших елементів у системах інформаційної безпеки. Водночас слід зазначити, що нормативна система не позбавлена викликів. Наприклад, суспільні дискусії розгортаються навколо вимог щодо доступу спецслужб до персональних даних громадян. Хоча Ізраїль прагне дотримуватися демократичних стандартів, постійні загрози тероризму змушують державу використовувати більш жорсткі інструменти контролю [3, с. 167-168]. У результаті законодавство постійно адаптується, намагаючись враховувати обидві потреби. Наприклад, у 2022 році було внесено зміни до регулювання діяльності ШАБАК, згідно з якими будь-які операції зі збору цифрових даних підлягають розширеному парламентському контролю.

Останні роки також характеризуються розвитком нормативів, що регулюють взаємодію держави із зовнішніми партнерами у сферах обміну

інформацією, боротьби з кіберзлочинністю та стандартизації кіберзахисту. Наприклад, у межах співпраці з Європейським Союзом Ізраїль бере участь у проєктах із гармонізації стандартів реагування на кіберінциденти [54]. Крім того, участь у програмах НАТО з кібероборони сприяє вдосконаленню нормативної бази щодо кіберзахисту оборонного сектору [35].

Зазначимо, що нормативно-правова складова системи інформаційної безпеки Ізраїлю постійно розвивається під впливом зовнішніх і внутрішніх факторів. Вона включає не лише військову доктрину як історичний фундамент, але й сучасні стратегії кіберзахисту, правові механізми регулювання приватного сектору, міжнародні зобов'язання, а також політики у сфері регулювання нових технологій. Сукупність цих елементів формує комплексну правову інфраструктуру, здатну забезпечити ефективний захист держави в умовах зростання гібридних загроз та ескалації кіберконфліктів. Ізраїльська модель доводить, що успішне забезпечення інформаційної безпеки неможливе без постійного оновлення нормативних актів, їхньої адаптації до нових реалій та створення умов для взаємодії держави, бізнесу й суспільства [46]. Завдяки цьому Ізраїль продовжує залишатися одним із глобальних лідерів у сфері інформаційної та кібернетичної безпеки, а його нормативно-правовий досвід стає важливим орієнтиром для країн, які прагнуть зміцнити власні моделі стійкості в цифрову епоху.

2.3. Практичні кейси функціонування системи інформаційної безпеки Ізраїлю

Практичні кейси функціонування системи інформаційної безпеки Ізраїлю демонструють унікальну адаптивність, інноваційність та комплексність, що перетворили цю державу на одного з глобальних лідерів у сфері кіберзахисту. Насамперед слід наголосити, що ізраїльська модель поєднує технологічні рішення, інституційну взаємодію, нормативно-правові механізми та стратегічну культуру, сформовану багаторічними безпековими загрозами. Усе це дозволило створити середовище, у якому інформаційна

безпека є не лише сектором державної політики, а й ключовою складовою національної стратегії виживання та розвитку. Власне, практичні кейси відображають можливість гнучкого реагування на виклики, що швидко змінюються, а також свідчать про високу ефективність ізраїльського підходу до управління ризиками. Зокрема, досвід Ізраїлю включає успішну протидію кібератакам на критичну інфраструктуру, впровадження технологій штучного інтелекту для раннього виявлення загроз, створення цифрових платформ для кризового реагування та розвиток широкої мережі державно-приватного партнерства [32].

Першим вагомим практичним кейсом є діяльність Національного кібердиректорату Ізраїлю (INCD), який у 2020-2024 роках продемонстрував інноваційний підхід до реагування на атаки, спрямовані проти об’єктів енергетичної, медичної та транспортної інфраструктури [30]. Так, у 2020 році Ізраїль успішно відбив серію спроб зовнішнього втручання в систему водопостачання, коли хакери намагалися змінити параметри роботи насосних станцій [31]. Цей випадок став поворотним моментом, оскільки продемонстрував не тільки технічну витонченість атаки, а й надзвичайну важливість скоординованої реагувальної моделі. INCD, діючи спільно з місцевими муніципалітетами, приватними операторами та підрозділами безпеки, запровадив багаторівневі протоколи аналізу події, що дозволило виявити джерело атаки, мінімізувати наслідки та посилити системи контролю. Цей кейс показує, наскільки важливою є інтеграція кібербезпеки з управлінням критичними інфраструктурними процесами та наскільки ефективно Ізраїль реалізує принцип превентивності [1].

Іншим прикладом є діяльність урядового CERT-IL, який функціонує як головний центр оперативного реагування на кібератаки [78]. CERT-IL постійно взаємодіє з державними установами, приватними компаніями та громадськістю, забезпечуючи цілодобовий моніторинг кіберінцидентів. Зокрема, у 2022–2023 роках CERT-IL координував масштабні операції із захисту медичних закладів, що стали мішенню хакерів під час пандемії

COVID-19. Одним з найгучніших інцидентів стала атака на ізраїльську лікарню «Хіллел Яффе» у 2021 році, коли зловмисники вимагали викуп за розблокування даних пацієнтів [13]. CERT-IL не тільки локалізував кібератаку, а й забезпечив відновлення роботи медичного закладу без сплати викупу.

Окремо варто розглянути практичні кейси у сфері військово-інформаційної безпеки, адже Ізраїль має складне геополітичне середовище та постійно стикається з кіберзагрозами з боку недержавних акторів, зокрема угруповань «Хамас» та «Хізбулла». Прикладом може слугувати операція «Залізні мечі» у 2023 році, під час якої Ізраїль застосував інтегровану платформу на основі штучного інтелекту для аналізу потоків інформації та виявлення ворожих інформаційних операцій [49]. Завдяки використанню алгоритмів машинного навчання ізраїльські сили оборони (IDF) змогли виявити спроби маніпулювання інформаційним простором шляхом створення фальшивих акаунтів у соціальних мережах, спрямованих на поширення паніки та дезінформації серед населення. У практиці Ізраїлю важливе місце займає модель державно-приватного партнерства, яка забезпечує стійкість інформаційного середовища [41]. Насамперед це проявляється у співпраці між урядом та хайтек-сектором, де діють такі компанії, як Check Point, CyberArk, NSO Group, XM Cyber та інші. Наприклад, Check Point активно співпрацює з INCD у тестуванні нових методів запобігання фішинговим атакам, що має особливе значення з огляду на зростання кількості соціотехнічних атак у 2021–2024 роках.

Цікавою та показовою є також практика функціонування кіберпарку Be’er Sheva CyberSpark, який став глобальним центром з розвитку інновацій у сфері кібербезпеки [46]. У цьому технологічному хабі співпрацюють університети (зокрема Бен-Гуріонський університет), приватні корпорації, військові структури та державні відомства. CyberSpark є прикладом того, як Ізраїль реалізує принцип «інновації як фактор національної безпеки» [32]. Суттєвим є й досвід Ізраїлю у захисті виборчих процесів. У 2019, 2021 та 2022 роках країна посилювала інформаційні та кіберзахисні заходи під час

проведення парламентських виборів [30]. INCD запровадив спеціальні протоколи моніторингу цифрових платформ, що дозволило виявляти спроби зовнішнього втручання у політичні процеси.

У 2022-2024 роках Ізраїль також активно розвивав практику міжнародного співробітництва у сфері інформаційної безпеки, що є окремим важливим напрямом його політики [53]. Одним із показових прикладів стало партнерство з США та ВеликоюБританією у рамках об'єднаних кібернавчань, спрямованих на відпрацювання сценаріїв реагування на масштабні атаки на фінансовий сектор. Одним із найцікавіших та найінноваційніших кейсів є проєкт «Cyber Dome», розроблений Ізраїлем у 2022 році за аналогією з «Iron Dome» – системою протиракетної оборони [56]. «Cyber Dome» інтегрує штучний інтелект, машинне навчання та великі масиви даних з метою забезпечення раннього виявлення кіберзагроз і автоматизованої нейтралізації атак на рівні національних мереж [65]. Слід згадати й про боротьбу з фінансовими кіберзлочинами, яка стала одним із головних напрямів діяльності ізраїльських структур у 2021-2024 роках [49]. Відомі випадки, коли ізраїльські спецслужби виявляли міжнародні мережі з відмивання коштів за допомогою криптовалюти.

До практичних кейсів можна віднести також розвиток системи кіберосвіти, адже підготовка кадрів є фундаментальною передумовою інформаційної безпеки. Ізраїль давно застосовує модель ранньої професійної ідентифікації талантів, створюючи спеціалізовані програми для старшокласників, військових та студентів. Програма «Magshimim» стала однією з найвідоміших ініціатив, яка дозволяє майбутнім фахівцям опановувати складні технічні навички ще до вступу до університету [36]. Це дає змогу державі підтримувати високий рівень професійної спроможності у сфері кібербезпеки, а також забезпечувати кадровий резерв для військових підрозділів, державних інституцій та приватного сектору [46]. Важливим практичним кейсом, який варто розглянути детальніше, є моделювання та відпрацювання сценаріїв кібервійн, що щороку проводяться під егідою INCD

та військових структур. У 2023 році Ізраїль здійснув одну з найбільших у своїй історії кібернавчальних операцій, у якій брали участь понад 120 організацій різних секторів: від енергетики до медіа та фінансів [49]. Сценарії навчань включали симуляцію масованих атак на телекомунікаційні системи, спроби виведення з ладу логістичних мереж, а також операції з маніпулювання громадською думкою через «вкидання» фальшивих матеріалів у соцмережах. Навчання продемонстрували, що критичні сектори країни не тільки здатні працювати в умовах інформаційних криз, а й володіють інструментами швидкої локалізації загроз. Саме регулярність таких перевірок і постійне вдосконалення алгоритмів реагування забезпечують стійкість держави перед обличчям невизначених ризиків.

Ще один практичний кейс стосується ролі військової розвідки Unit 8200, яка вважається одним із найпотужніших підрозділів у сфері кіберрозвідки у світі [46]. Практичний досвід цієї структури охоплює не лише перехоплення інформації та аналіз ворожих кібероперацій, а й активну участь у створенні технологічних стартапів після завершення служби їхніми випускниками. Завдяки цьому Unit 8200 виконує подвійну функцію – забезпечення національної безпеки та розвиток інноваційного середовища, що працює на економічну та інформаційну стійкість держави. Багато сучасних технологій, які сьогодні використовуються в ізраїльському та світовому кіберсекторі, мають витоки саме у практичних розробках цього підрозділу [32]. Це створює унікальну ситуацію, коли військова система стає своєрідним генератором цивільних інновацій, що кардинально підвищують рівень інформаційної безпеки не тільки в оборонній сфері, а й у приватному секторі. Практичні кейси Ізраїлю також демонструють важливість стратегічної комунікації як інструменту підтримання інформаційного суверенітету. У 2023–2024 роках уряд активно протидіяв хвилям дезінформації, пов’язаним із ескалаціями конфліктів на кордонах і внутрішньополітичними процесами. Зокрема, під час загострення ситуації в Газі у 2023 році Ізраїль зафіксував масові спроби поширення фальшивих відео в соціальних мережах, створених за допомогою

технологій дипфейків [49]. Для протидії цим кампаніям уряд розгорнув систему перевірки інформації, що включала співпрацю зі світовими технологічними компаніями і незалежними фактчекінговими організаціями.

Окремо варто підкреслити значення правового регулювання у формуванні практичної платформи кіберзахисту. Запроваджені в Ізраїлі у 2021-2024 роках законодавчі реформи у сфері захисту даних, кіберінцидентів та відповідальності операторів критичної інфраструктури забезпечили високий рівень прозорості та правової визначеності [1]. Власне, одним із практичних результатів цих реформ стало створення обов'язкової системи звітності про кіберінциденти, завдяки якій INCD отримує можливість оперативно аналізувати загальнодержавний рівень загроз [40]. На практиці це дозволяє моделювати тенденції, визначати нові типи атак та оновлювати стратегії безпеки у режимі реального часу. У свою чергу, прозора та чітка правова база викликає довіру з боку приватного сектору, що є необхідною умовою ефективного державно-приватного партнерства.

Не менш важливим практичним кейсом є досвід Ізраїлю у забезпеченні безпеки цифрових сервісів державного управління. Оскільки країна активно розвиває е-урядування та надає громадянам широкий спектр цифрових послуг, від онлайн-оподаткування до медичних записів, питання надійності та конфіденційності цих сервісів є критично важливим. У 2022–2023 роках Ізраїль провів мо дернізацію державних цифрових платформ, інтегрувавши до них системи багатофакторної автентифікації, автоматизованого виявлення аномалій та «цифрових сейфів» для персональних даних [30]. Цікавим є також практичний кейс забезпечення безпеки транспортної інфраструктури, яка в умовах високого технологічного розвитку країни є вразливою до потенційних кібервтручань. Зокрема, у 2023 році Ізраїль протестував систему захисту залізничної інфраструктури від цілеспрямованих атак, які могли б спричинити затримки руху, аварії або збої у системах навігації [49]. Ще один важливий аспект практичного досвіду – це активна участь Ізраїлю у міжнародних розслідуваннях кіберзлочинів, що мають транскордонний характер. У 2022–

2024 роках країна взяла участь у кількох операціях Європолу й Інтерполу, спрямованих на нейтралізацію глобальних мереж викрадачів даних і фішингових груп [53].

Загалом наведені практичні кейси підтверджують, що система інформаційної безпеки Ізраїлю є не лише високотехнологічною, але й глибоко інтегрованою у державне управління, військову сферу, приватний сектор і міжнародні механізми. Вона ґрунтується на проактивності, гнучкості та інноваційному мисленні. І саме ці риси дозволяють Ізраїлю ефективно реагувати на новітні загрози, адаптуватися до глобальних трансформацій та відігравати значну роль у формуванні міжнародних стандартів кіберстійкості.

Висновки до розділу 2

Слід підкреслити, що інституційна та нормативно-правова складові системи інформаційної безпеки Ізраїлю формують цілісну, багаторівневу та внутрішньо узгоджену модель, яка забезпечує високу ефективність державної політики у сфері протидії сучасним інформаційним загрозам. Інституційний вимір, у свою чергу, репрезентований комплексом спеціалізованих органів, серед яких ключову роль відіграють Національне кібернетичне управління, розвідувальні структури та військові формування, що діють у тісній координації та, що важливо, демонструють здатність до гнучкого реагування на нові виклики. Саме ця міжвідомча взаємодія, доповнена ефективними механізмами державно-приватного партнерства, дозволяє вибудувати систему раннього попередження й оперативного реагування, яка охоплює як державний сектор, так і критичну інфраструктуру.

У нормативно-правовій площині Ізраїль поступово еволюціонував від переважно військової доктрини до розгалуженої кібернетичної стратегії, що інтегрує норми, процедури та стандарти інформаційної безпеки в широку систему національної безпеки. Причому слід зазначити, що сучасні ізраїльські політики та стратегії, включаючи Cybersecurity Strategy та низку підзаконних актів, забезпечують не лише реагування на загрози, а й превентивний,

аналітичний і освітній виміри. Завдяки цьому формуються сталий правовий фундамент, чіткі межі відповідальності й узгоджені правила взаємодії держави з бізнесом та суспільством.

Практичні кейси функціонування ізраїльської системи, від нейтралізації кібератак на об’єкти критичної інфраструктури до швидкого відновлення систем управління під час масштабних деструктивних операцій, демонструють її високу адаптивність. Більше того, вони підтверджують здатність держави впроваджувати інноваційні технології, зокрема штучний інтелект, автоматизований моніторинг і аналітичні платформи для оцінки ризиків. У підсумку можна зробити висновок, що ізраїльська модель інформаційної безпеки є однією з найуспішніших у світі, адже поєднує інституційну узгодженість, нормативно-правову чіткість та ефективні практичні механізми реалізації, які разом забезпечують її стійкість перед широким спектром сучасних загроз.

РОЗДІЛ 3. ВИКОРИСТАННЯ ІЗРАЇЛЬСЬКОГО ДОСВІДУ У ФОРМУВАННІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

3.1. Стан та проблеми національної системи інформаційної безпеки України

Нинішній стан національної системи інформаційної безпеки України слід розглядати крізь призму комплексних трансформацій, що відбуваються як у внутрішньополітичному, так і в міжнародному середовищі, адже саме взаємодія цих чинників визначає характер ризиків, загроз та можливостей у сфері захисту інформаційного простору держави. Україна, вступивши у фазу повномасштабної війни проти Російської Федерації у 2022 році, де-факто стала епіцентром глобальної боротьби за інформаційну стійкість, а тому її досвід формування сучасної системи інформаційної безпеки набуває особливої значущості. Водночас, попри численні позитивні зрушення, ця система все ще перебуває у стані інституційної, технологічної та нормативної еволюції, що, власне, і створює широке поле для аналізу її сильних і слабких сторін [25]. З одного боку, саме війна стимулювала державу до активнішого впровадження інструментів кіберзахисту, цифрової модернізації, розбудови системи стратегічних комунікацій, а також посилення ролі державних інституцій у координації дій у цифровому середовищі. З іншого боку, під впливом надзвичайних обставин загострилися й хронічні проблеми, пов’язані з дисбалансом між швидкістю технологічного розвитку та здатністю держави своєчасно адаптувати нормативно-правову й інституційну базу до цих змін.

Насамперед варто зазначити, що сучасна національна система інформаційної безпеки України функцінує в умовах безпрецедентного рівня зовнішніх гібридних впливів. Російська Федерація активно використовує комплекс засобів інформаційно-психологічного тиску, який включає дезінформацію, інформаційні операції, кібератаки, маніпулювання громадською думкою через соціальні мережі, втручання у виборчі процеси, а також підривну діяльність, спрямовану на руйнування довіри до державних

інститутів [12]. Показовим у цьому контексті є збільшення кількості масштабних кібератак на державні органи України у 2022-2024 роках, включно з атаками на ресурси Державної служби спеціального зв'язку та захисту інформації, Міністерства оборони, енергетичної інфраструктури та низки систем органів виконавчої влади. Наприклад, кібератака «WhisperGate» у січні 2022 року, що передувала повномасштабному вторгненню, стала одним із найяскравіших ранніх сигналів щодо агресивного наміру РФ паралізувати державні комунікації, знищити інформацію та дестабілізувати суспільство в передвоєнний період [10]. Крім того, протягом 2023–2024 років було зафіксовано масштабні атаки на системи операторів критичної інфраструктури, зокрема на енергетичних підприємств, серед яких однією з найрезонансніших була атака на «Укренерго» у грудні 2023 року, яка супроводжувалася паралельними дезінформаційними кампаніями в соціальних мережах щодо нібито неспроможності держави забезпечити енергетичну безпеку.

Характеризуючи стан системи інформаційної безпеки України, не можна оминути увагою той факт, що країна значною мірою орієнтується на європейські стандарти цифрового врядування та інформаційного захисту. Впровадження нових інституційних механізмів, серед яких важливе місце посідає створення Центру стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики, стало серйозним кроком уперед [15]. Цей Центр координує державні інформаційні кампанії, протидіє дезінформаційним операціям, аналізує інформаційні загрози та співпрацює з міжнародними партнерами, що дозволяє Україні бути частиною глобальних мереж протидії інформаційним впливам. Крім того, інтеграція України в європейський кіберпростір, зокрема участь у програмах кіберстійкості ЄС, співпраця з НАТО у сфері кіберзахисту, а також приєднання до Європейської програми кібернетичної безпеки (2023) створюють нові можливості для модернізації системи національного захисту [1]. Водночас, незважаючи на розширення кола інституційних механізмів, у державі все ще бракує системної

координації між різними органами, що ускладнює реагування на складні багатовекторні загрози [25]. Варто підкреслити, що нормативно-правове забезпечення інформаційної безпеки України потребує суттєвого оновлення. Хоча Закон України «Про основні засади забезпечення кібербезпеки» (2017) та Закон «Про інформацію» створюють певний правовий фундамент, однак вони не завжди відповідають сучасним викликам, пов’язаним із розвитком штучного інтелекту, алгоритмічних платформ, біометричних систем, технологій діпфейків та високотехнологічних інформаційно-психологічних операцій [7]. До прикладу, актуальні дискусії 2023–2025 років щодо регулювання штучного інтелекту в Україні свідчать про відставання темпів нормативної адаптації, адже Європейський Союз уже в 2024 році ухвалив AI Act – перший у світі комплексний акт зі встановлення правил використання ШІ [1]. Українська правова база наразі не містить достатньо детальних норм щодо використання алгоритмічних систем у медіа, політичних комунікаціях чи електронному урядуванні, що створює прогалини у сфері захисту персональних даних та інформаційної приватності.

Крім нормативного аспекту, одним із найбільш проблемних елементів національної системи інформаційної безпеки залишається стан медіапростору. Українські медіа, хоча й значною мірою демократизовані та плюралістичні, все ж характеризуються високим рівнем економічної залежності від політичних і бізнесових груп [17]. Це створює умови для маніпулювання громадською думкою, політизації інформаційних потоків, поширення недостовірної інформації та фрагментації суспільного дискурсу. Додатково, соціальні мережі, які стали ключовими платформами для поширення інформації, формують нову архітектуру ризиків, пов’язаних зі швидкістю циркуляції дезінформаційних наративів. Наприклад, у 2024 році було зафіксовано масштабну дезінформаційну кампанію, спрямовану на дискредитацію оборонної допомоги Україні з боку партнерів, яка поширювалася через TikTok, Telegram та X (Twitter) [5].

У структурі проблем, які визначають слабкі місця національної системи інформаційної безпеки, важливо виокремити питання кадрової спроможності державних інституцій. Брак висококваліфікованих фахівців у сфері кібербезпеки, стратегічних комунікацій, OSINT-аналізу, кризового інформаційного менеджменту та цифрової криміналістики є одним із критичних чинників, що впливає на ефективність системи загалом [22]. Попит на фахівців у цих сферах у 2022-2025 роках значно перевищує пропозицію, що зумовлено як стрімким зростанням обсягів інформаційних загроз, так і активним переходом приватного сектору на конкурентні моделі цифрового захисту. Важливо також згадати про проблеми технічної модернізації критичної інформаційної інфраструктури. Значна частина державних інформаційних систем, особливо на місцевому рівні, досі функціонує на застарілих програмних комплексах, що підвищує вразливість до сучасних кібератак [19]. Надії на швидку модернізацію покладаються на проєкт «Цифрова держава 2030», який передбачає повний перехід державних органів на оновлені стандарти кіберзахисту та мережевої безпеки, однак реалізація цього плану потребує значних інвестицій та комплексної координації з європейськими партнерами.

Окремого аналізу потребує стан стратегічних комунікацій держави. Після початку повномасштабної війни Україна значно посилила свої позиції у сфері міжнародних інформаційних кампаній, проте всередині країни стратегічні комунікації все ще стикаються з проблемами фрагментації меседжів, нестачею системної методології та обмеженим доступом до високоточних аналітичних інструментів [15]. Нарешті, говорячи про проблеми національної системи інформаційної безпеки, важливо звернути увагу на недостатній рівень інтеграції державних інститутів з громадянським суспільством та приватним сектором. Хоча у 2022-2025 роках спостерігається тенденція до посилення державно-приватного партнерства у сфері кіберзахисту, проте вона все ще не має системного характеру [25]. Створення у 2023 році Координаційного центру з кіберстійкості при Раді національної

безпеки і оборони стало важливим кроком на шляху інтеграції різних секторів, однак процес залучення бізнесу та експертного середовища лише набирає обертів.

У продовження аналізу важливо наголосити, що ефективність національної системи інформаційної безпеки значною мірою залежить від здатності держави адаптуватися до швидкоплинних технологічних реалій, адже інформаційні загрози стають дедалі складнішими, багатовимірнішими та менш передбачуваними [15]. Наприклад, активне поширення штучного інтелекту та генеративних технологій, які здатні створювати переконливі фейкові аудіо й відео, суттєво ускладнює процес верифікації інформації та ставить під загрозу інформаційну стійкість як державних інституцій, так і суспільства. У 2024 році було зафіксовано декілька випадків використання діпфейків із голосами українських військових командирів, що мали на меті деморалізацію суспільства та дискредитацію командних структур. Хоча державні органи оперативно відреагували на ці інциденти, вони продемонстрували необхідність оновлення технічних засобів виявлення маніпулятивного контенту та активізації співпраці з міжнародними платформами, що спеціалізуються на верифікації цифрових матеріалів [5]. Крім того, не менш важливим залишається питання інформаційного суверенітету України, який передбачає здатність держави самостійно контролювати розвиток власної цифрової екосистеми та протидіяти зовнішньому впливу на неї [25]. У цьому контексті слід звернути увагу на той факт, що значна частина інформаційної інфраструктури, включно з хмарними сервісами, телекомунікаційним обладнанням та платформами обробки даних, належить міжнародним компаніям. З одного боку, це відкриває Україні доступ до високотехнологічних рішень, однак з іншого, формує залежність, яка може стати критичною в умовах загострення міжнародних конфліктів. Саме тому важливим стратегічним напрямом є розвиток власних технологічних платформ, підвищення суверенності цифрових даних та створення умов для національного виробництва програмного забезпечення. У 2023–2024 роках

були реалізовані перші етапи проєкту національної хмарної платформи, яка має забезпечити збереження критично важливих державних даних виключно на серверах, що перебувають під контролем українських структур. Утім, цей процес ще далекий від завершення, що створює додаткові ризики для довгострокової інформаційної стійкості.

Поряд із цим проблемним аспектом залишається нерівномірний розвиток інформаційної безпеки у різних секторах державного управління. Хоча центральні органи влади мають відносно високий рівень цифрової захищеності, місцеві органи самоврядування, комунальні підприємства та регіональні структури залишаються надзвичайно вразливими [22]. Це підтверджують регулярні інциденти із витоками персональних даних, які протягом 2023-2024 років траплялися як у великих містах, так і в малих громадах. Наприклад, у 2024 році було зафіксовано витік даних із системи електронного документообігу однієї з міських рад центральної України, що призвело до поширення персональної інформації працівників і внутрішніх документів. Подібні інциденти засвідчують, що державна політика інформаційної безпеки потребує комплексної децентралізації, з рівномірним розподілом ресурсів, навчанням персоналу та технічним оновленням на місцях. Не менш важливою проблемою є недостатній рівень кіберкультури громадян. Попри активні кампанії з медіаграмотності та протидії дезінформації, значна частина населення все ще демонструє вразливість до маніпуляцій, фішингових атак, псевдоновин та пропагандистських наративів. Дослідження соціологічної групи «Рейтинг» 2024 року показало, що близько 32% громадян схильні довіряти неперевіреним джерелам інформації, тоді як майже половина опитаних не може впевнено визначити, чи є інформаційний матеріал частиною маніпулятивної операції [14]. Такий рівень інформаційної вразливості створює широке поле для інформаційних атак ворога та потребує посилення державних і громадських просвітницьких ініціатив.

Окреслюючи проблеми, варто підкреслити й обмеженість фінансування сектору інформаційної безпеки. Попри збільшення бюджетних видатків , вони

все ще не відповідають масштабу загроз, із якими стикається держава [28]. Частина важливих проєктів, зокрема модернізація кіберінфраструктури судової системи, цифрова трансформація освіти та впровадження захищених каналів комунікації для місцевих органів влади, фінансується за рахунок міжнародної допомоги, що, з одного боку, є позитивом, але з іншого – створює залежність від зовнішніх джерел.

Важливою проблемою також є недостатня адаптивність державної системи реагування на кризові інформаційні ситуації. Хоча українські інституції продемонстрували здатність оперативно реагувати на ключові інформаційні інциденти, проте механізм кризового менеджменту ще не набув системного характеру [7]. Часто спостерігається ситуація, коли державні відомства реагують на інформаційні кризи несинхронно, що призводить до дублювання інформації, появи суперечливих меседжів та втрати оперативного контролю над інформаційним простором. У 2023 році під час інформаційного інциденту, пов’язаного з фейковим повідомленням про нібито «ви хід України з переговорів із ЄС», різні державні структури надали коментарі з затримкою та без належної координації, що дозволило дезінформації певний час домінувати в соціальних мережах. Окремою проблемою є недостатня інтеграція України у глобальні системи обміну інформацією про кіберзагрози. Хоча Україна активно співпрацює з ЄС, НАТО, США та іншими партнерами, проте в окремих сегментах вона все ще залишається на периферії міжнародних інформаційних мереж [1]. Показовим є те, що багато українських інституцій не мають повного доступу до міжнародних баз даних щодо індикаторів компрометації, що використовуються у провідних країнах для виявлення кібератак.

Водночас, попри складність ситуації, Україна демонструє значний прогрес у напрямі цифрової стійкості, розбудови кіберзахисних механізмів, посилення стратегічних комунікацій та взаємодії з міжнародними партнерами. З огляду на це, подальший розвиток системи інформаційної безпеки має ґрунтуватися на комплексному підході, що поєднує модернізацію нормативно-

правової бази, технологічне оновлення інфраструктури, удосконалення міжвідомчої координації та посилення взаємодії держави з суспільством і бізнесом. Лише за умови стратегічної узгодженості та довгострокового планування можливо забезпечити стійкість національного інформаційного простору в умовах сучасних глобальних викликів.

3.2. Порівняльний аналіз моделей Ізраїлю та України у сфері інформаційної безпеки

Порівняльний аналіз моделей Ізраїлю та України у сфері інформаційної безпеки показує, що обидві держави розвивають свої системи під потужним впливом воєнних загроз, хоча вихідні умови, історичний контекст і рівень інституційної зрілості суттєво різняться. Ізраїль формував модель інформаційної безпеки в умовах постійної збройної конфронтації з моменту створення держави, що, власне, зумовило раннє переорієнтування на кібер- та інформаційний вимір безпеки як ключовий. Україна ж, попри наявність окремих елементів інформаційної політики ще до 2014 року, по-справжньому інтенсивно почала розбудову системи інформаційної безпеки лише після початку російської агресії, а особливо – після повномасштабного вторгнення 2022 року [4]. Саме тому, порівнюючи ці моделі, важливо враховувати не лише формальну наявність стратегій чи інституцій, а й глибину їхньої інтегрованості в загальну систему національної безпеки, ефективність реагування на сучасні гібридні загрози, а також рівень взаємодії держави з приватним сектором і суспільством.

Передусім привертає увагу інституційна архітектура. В Ізраїлі ключову роль у сфері кібер- та інформаційної безпеки відіграє Ізраїльське національне кіберуправління (Israel National Cyber Directorate, INCD), яке функціонує при Офісі прем’єр-міністра і поєднує стратегічні, координаційні й оперативні функції, зокрема щодо захисту критичної інфраструктури, реагування на кіберінциденти та розвитку кіберекосистеми загалом [1]. Паралельно значну роль відіграють спеціальні служби – військова розвідка (зокрема легендарний

підрозділ 8200) та Служба загальної безпеки (Шабак), що активно працюють у сфері кібероперацій і контррозвідки [46]. В Україні, натомість, головним координатором у сфері кібербезпеки та частково інформаційної безпеки виступає Рада національної безпеки і оборони України, яка через систему рішень і доктрин задає стратегічний курс, тоді як безпосереднє технічне та організаційне забезпечення покладене на Державну службу спеціального зв'язку та захисту інформації України (Держспецзв'язок), Службу безпеки України, Міністерство оборони, Міністерство цифрової трансформації та низку інших органів [15]. Таким чином, ізраїльська модель тяжіє до більш концентрованої вертикалі управління кібер- та інформаційною безпекою, тоді як українська система має більш фрагментований і поліцентричний характер з широкою міжвідомчою координацією [9] (Таблиця 3.1.).

Таблиця 3.1.

Порівняльний аналіз моделей Ізраїлю та України у сфері інформаційної безпеки

Критерій	Ізраїль	Україна
Модель управління	Централізована модель з домінуванням Національного кібердиректорату (INCD).	Змішана модель: повноваження розподілені між РНБО, Держспецзв'язком, СБУ, Міністерством цифрової трансформації.
Нормативно-правова база	Комплексний, детально структурований законодавчий масив кібербезпеки, постійні оновлення.	Фрагментована нормативна база, посилена після 2014 та 2022 рр., триває процес гармонізації з ЄС і НАТО.
Міжвідомча координація	Високий рівень координації через єдиний центральний орган; чіткі протоколи.	Координація ускладнена через розпорошеність повноважень;

		створюються нові механізми взаємодії.
Державно-приватне партнерство	Розвинута система співпраці з технологічним сектором (особливо стартапами); інкубатори, Sandboxes.	Партнерства розвиваються, проте менш інституціоналізовані; значний потенціал IT-сектору.
Освітньо-наукова база	Сильна військово-технічна школа; кіберпідготовка інтегрована у військову службу.	Потужний IT-ринок, але нерівномірний рівень спеціалізованої підготовки; поступове реформування.
Операційні інструменти реагування	Швидка реакція, проактивний моніторинг, обов'язкове інформування про інциденти.	Реакція покращується, але залишається переважно реактивною; не всі сектори зобов'язані повідомляти про інциденти.
Пріоритети	Превентивність, інновації, захист критичної інфраструктури, розвиток кіберіндустрії.	Захист критичної інфраструктури, протидія кібертероризму та гібридним атакам РФ, інтеграція з євроатлантичними структурами.

З погляду нормативно-правових засад обидві держави закріплюють інформаційну безпеку як компонент національної безпеки, проте підходи до структурування документів і ступінь їхньої деталізації відрізняються. В Ізраїлі, з огляду на специфіку безпекового середовища, великі масиви регулювання стосуються саме кібербезпеки, захисту критичної інфраструктури, протидії терористичним організаціям та ворожим державам в інформаційному просторі [3]. У низці документів робиться акцент на превентивних кібероперація х, що

виходять за межі суто оборонної парадигми. Україна, своєю чергою, у Стратегії кібербезпеки України 2021 року чітко фіксує пріоритети захисту від російської агресії в кіберпросторі, протидії дезінформації та зміцнення стійкості суспільства до інформаційних впливів, а в Стратегії національної безпеки та Доктрині інформаційної безпеки визначає інформаційну безпеку як окремий вимір загальної безпеки держави [23]. Тут варто підкреслити, що українська модель значною мірою орієнтується на стандарти ЄС і НАТО, інтегруючи до національного поля такі поняття, як «стійкість» (resilience), «глобальний цифровий ринок», «правове регулювання цифрових платформ» [16].

Ще одна важлива площина порівняння – стратегічні пріоритети та баланс між оборонною й наступальною складовими інформаційної та кібербезпеки. Ізраїль, виходячи з доктрини превентивної оборони, активно розвиває наступальні кіберспроможності, про що побічно свідчать гучні кейси, які пов’язують із ізраїльськими структурами, як-от кібероперації проти ядерної програми Ірану (зокрема атака із застосуванням вірусу Stuxnet, що часто вважається результатом співпраці США та Ізраїлю) [46]. Хоча офіційно ці дії не завжди визнаються, вони демонструють загальну логіку: інформаційний та кіберпростір використовується не лише для захисту, а й як потужний інструмент стримування та впливу на стратегічного противника. Україна ж, навпаки, набагато більше зосереджена на обороні, передусім на відбитті масованих російських кібератак на енергетичну, транспортну, урядову інфраструктуру, на протидії інформаційно-психологічним операціям, що мають на меті посіяти паніку, недовіру до влади та розколоти суспільство [10].

Попри різний баланс оборонного й наступального виміру, обидві моделі широко використовують інструменти державно-приватного партнерства. В Ізраїлі приватний сектор, передусім потужна індустрія кібербезпеки та високих технологій – є одним з ключових «стовпів» національної моделі, адже значна частина інновацій, технологічних рішень та людського капіталу зосереджена саме в комерційних компаніях, стартапах, науково-дослідних центрах [32]. Держава створює для них умови (податкові стимули, кластери

типу «кібер-парків», підтримку експорту) і водночас активно залучає до виконання державних контрактів, спільних проєктів у сфері захисту критичної інфраструктури, розробки систем моніторингу, штучного інтелекту та аналізу великих даних. В Україні державно-приватна взаємодія також інтенсивно розвивається, особливо після 2022 року, коли ІТ-компанії, волонтерські хакерські спільноти, громадські організації й медіа стали невід'ємною частиною загальнонаціонального спротиву [2].

Окремо слід порівняти підходи до протидії дезінформації та до роботи з суспільною думкою. В Ізраїлі значна частина зусиль у цій сфері має закритий або напівзакритий характер, оскільки йдеться про операції спецслужб, спроможності армії оборони Ізраїлю у сфері психологічних операцій, а також про контроль над інформаційним простором під час проведення військових операцій [50]. При цьому важливо підкреслити, що ізраїльська держава активно комунікує свою позицію на зовнішніх аудиторіях, використовуючи дипломатичні канали, медіа, соціальні мережі, працюючи з провідними глобальними платформами. Україна, зі свого боку, у відповідь на російську агресію зуміла розгорнути масштабну державну й громадянську інформаційну кампанію, спрямовану на мобілізацію внутрішньої підтримки та формування сприятливого міжнародного іміджу [7].

Ще один вимір порівняльного аналізу – ступінь цифрової зрілості та інтеграції інформаційної безпеки в ширшу стратегію цифрової трансформації. В Ізраїлі цифрова економіка і сектор високих технологій давно стали «локомотивами» розвитку, що створило сприятливі умови для будівництва комплексної системи кібербезпеки [45]. В Україні цифрова трансформація набрала особливих темпів останніми роками, зокрема через запровадження електронних сервісів на кшталт «Дії», розвиток систем електронного врядування, цифрових послуг для громадян і бізнесу [21]. Це, безперечно, створює нові можливості, але одночасно відкриває і нові площини для кібератак, що змушує українську державу швидко інтегрувати стандарти кіберзахисту в усі етапи цифрових реформ [25]. Важливо зазначити, що обидві

держави надають великого значення міжнародному співробітництву, але в різних форматах і з різною інтенсивністю. Ізраїль активно співпрацює зі США, низкою європейських держав, НАТО (у форматі партнерства), а також розвиває глобальні експортні ринки для своїх кібертехнологій та рішень у сфері безпеки [53]. Україна, своєю чергою, включає інформаційну безпеку в ширший контекст євроатлантичної інтеграції: йдеться про співпрацю з ЄС у рамках цифрової політики, участь у механізмах ЄС і НАТО з кіберзахисту, спільні навчання, підтримку з боку окремих держав, від надання обладнання до обміну експертизою і спільних проєктів з протидії дезінформації [19]. У цьому контексті модель України є більш «відкритою» та інтеграційною: інформаційна безпека розглядається як спільне благо демократичної спільноти, що протистоїть авторитарним і ревізіоністським режимам.

Водночас необхідно акцентувати, що у процесі подальшої розбудови української моделі важливо не лише переймати окремі елементи ізраїльського досвіду, але й критично осмислювати їх у світлі українських реалій. Наприклад, в Ізраїлі ефективність системи інформаційної безпеки значною мірою забезпечена високим рівнем довіри між суспільством, державними інституціями та армією, а також обов’язковою військовою службою, яка створює потужний кадровий резерв у сфері технологій і безпеки [75]. Україна, хоча й демонструє високий рівень суспільної мобілізації, не має такої ж уніфікованої системи підготовки фахівців [22]. Саме тому одним із ключових завдань української держави є інституціоналізація системного навчання у сфері кібер- та інформаційної безпеки, інтеграція цих компетенцій у вищу освіту, створення спеціалізованих навчальних центрів і програм національного масштабу.

Ще однією принциповою відмінністю є рівень централізації. Ізраїль через компактність території та уніфіковану структуру державного управління має змогу реалізувати високу ступінь централізації у сфері кіберзахисту [30]. Україна ж, як велика держава з численними органами виконавчої влади та глибоким процесом децентралізації, потребує моделі, що поєднуватиме

надійний центральний контроль із гнучкістю на регіональному рівні [25]. У цьому контексті перспективним є розвиток регіональних центрів кіберзахисту, які могли б діяти за уніфікованими протоколами, але мати власні оперативні можливості та ресурси. Також важливою є подальша цифровізація регіональних органів влади та формування локальних стратегій інформаційної безпеки, інтегрованих із загальнодержавною системою. Крім того, в Ізраїлі важливу роль відіграє інноваційна інфраструктура, зокрема кластери на кшталт CyberSpark у Беер-Шеві, що об'єднують університети, військові структури та провідні компанії [46]. Такі хаби забезпечують швидке впровадження технологічних рішень, обмін інформацією та кадрову підготовку в режимі реального часу. Україна також розвиває подібні центри, зокрема ІТ-кластери у Львові, Києві, Дніпрі, проте їхній зв'язок із сектором національної безпеки поки є менш інституціоналізованим [19]. Тому перспективним напрямом може стати створення спеціалізованих кіберкластерів саме у співпраці з Міністерством оборони, Держспецзв'язку та університетським сектором, а також інтеграція таких центрів у європейські мережі досліджень і кіберцентрів.

Надзвичайно важливим є також питання інформаційної стійкості суспільства. Ізраїль, маючи постійний досвід перебування під загрозою, сформував культуру стійкості як на рівні громадян, так і на рівні інституцій [74]. Громадяни звикли до швидкого реагування на ризики, а інформаційні кампанії держави наголошують на необхідності критичного мислення, відповідального споживання новин та розумінні тактики ворога. В Україні процес формування такої культури набув безпрецедентних масштабів після 2022 року: населення значною мірою навчилося фільтрувати інформацію, знижувати вплив панічних повідомлень, критично реагувати на провокації [4]. Проте для системності необхідна довгострокова державна політика з розвитку медіаграмотності, підтримки незалежних медіа, а також викладання основ інформаційної безпеки на всіх рівнях освіти.

Важливим елементом порівняння є підходи до взаємодії з глобальними цифровими платформами. Ізраїль активно працює з такими компаніями, як Meta, Google та інші, для швидкого блокування екстремістського контенту, видалення матеріалів, що загрожують національній безпеці [49]. Після подій 7 жовтня 2023 року ця співпраця стала ще більш інтенсивною. Україна також веде активний діалог із соціальними мережами, особливо у питаннях протидії російській дезінформації, але на практиці ефективність взаємодії часто обмежена складністю глобальних алгоритмів і нерівномірністю реакцій платформ [17]. Тому для України необхідно посилювати свою участь у європейських ініціативах, пов'язаних з регулюванням платформ (Digital Services Act, Code of Practice on Disinformation). Крім того, порівняння моделей Ізраїлю та України у сфері інформаційної безпеки дає змогу виявити важливу відмінність у підходах до прогнозування та превенції загроз. Ізраїль, як правило, робить ставку на раннє виявлення та попередження атак, що зумовлено як розвиненими розвідувальними можливостями, так і технологічними інструментами аналізу ризиків [30]. У 2022-2024 роках ізраїльські служби неодноразово публічно заявляли про нейтралізацію складних спроб кібератак іранських хакерських груп. Україна також поступово зосереджується на превентивному підході, про що свідчать нові проєкти раннього виявлення загроз, системи моніторингу критичної інфраструктури й аналізу інформаційних операцій у реальному часі [1].

Загалом, порівняльний аналіз моделей Ізраїлю та України у сфері інформаційної безпеки дозволяє дійти кількох узагальнюючих висновків. По-перше, обидві держави вибудували системи, що формуються в умовах «екзистенційної» загрози, але Ізраїль має значно триваліший досвід, більш усталені інституції та високу ступінь інтеграції інформаційної безпеки в загальну воєнно-політичну доктрину. Україна ж перебуває в стадії інтенсивного становлення, коли нормативні рамки, інституційна структура та практики взаємодії держави, бізнесу й громадянського суспільства одночасно формуються та проходять «бойове випробування». По-друге, ізраїльська

модель більш відверто робить ставку на наступальні інструменти й технологічне лідерство [8], тоді як українська модель, принаймні на нинішньому етапі, залишається переважно оборонною, спираючись на мобілізаційний потенціал суспільства та потужну підтримку союзників. По-третє, досвід Ізраїлю є цінним для України з погляду будівництва єдиного центру координації, розвитку державно-приватного партнерства, інституційної культури безпеки та підготовки кадрів, однак безпосереднє копіювання ізраїльської моделі є неможливим через відмінності у політико-правовому середовищі, міжнародних зобов'язаннях і стратегічних пріоритетах. У підсумку можна стверджувати, що українська система інформаційної безпеки еволюціонує у напрямі гібридної моделі, яка поєднує уроки ізраїльського досвіду з вимогами європейської інтеграції та власною практикою протидії російській агресії, що, у свою чергу, формує унікальний приклад адаптивної безпекової архітектури у XXI столітті.

3.3. Напрямки імплементації ізраїльського досвіду в Україні: стратегічні, правові та організаційні рекомендації

Насамперед слід підкреслити, що імплементація ізраїльського досвіду у сфері інформаційної безпеки в Україні є не просто корисним аналітичним завданням, а стратегічною необхідністю, зумовленою як агресивним зовнішнім середовищем, так і глибокою трансформацією внутрішньої політико-правової системи держави. У цьому контексті досвід Ізраїлю, котрий протягом останніх десятиліть створив одну з найефективніших та найінтегрованіших систем кібер- і інформаційної безпеки у світі, виступає унікальним джерелом стратегічних рішень. Водночас важливо враховувати не лише окремі інституційні чи технічні механізми, але й принципи організації, підходи до міжсекторальної взаємодії, моделі координації та нормативно-правового забезпечення. Усе це дозволяє сформулювати три ключові напрями імплементації ізраїльських практик в Україні: стратегічний, правовий та

організаційний, кожен із яких потребує окремого осмислення і практичних рекомендацій.

Стратегічний напрямок базується на розумінні того, що Ізраїль створив цілісну систему інформаційної безпеки не як сукупність розрізнених інституцій, а як інтегрований безпековий комплекс, у якому стратегія, політика, технології та людський потенціал працюють на досягнення єдиної мети – забезпечення стійкості держави [8]. В Україні також необхідно переходити від фрагментованого підходу до моделі, яка б об'єднувала зусилля різних державних органів та недержавних акторів. По-перше, доцільним є формування Національної стратегії інформаційної безпеки нового покоління, яка базувалася б на сучасних викликах 2022-2025 років, включно з масованими російськими дезінформаційними кампаніями, інформаційно-психологічними операціями та кібератаками на енергетичний сектор. Власне, події 2024 року, коли Україна зазнала низки складних кібертерактів проти систем управління критичною інфраструктурою, зокрема на енергетичних та телекомунікаційних об'єктах, показали, що стратегічне планування має включати не лише реагування, але й випереджальні заходи. По-друге, стратегічно важливим є впровадження моделі ризик-орієнтованого управління, яка є ядром ізраїльського підходу [56]. Вона передбачає не лише оцінку загроз, але й побудову сценаріїв, постійне тестування стійкості (stress-testing), проведення національних навчань типу «Cyber Dome», які в Ізраїлі відбуваються щороку та залучають усі ключові міністерства [30].

Крім цього, стратегічна імплементація має враховувати ізраїльську концепцію «інформаційної оборони» як елементу загальної стратегії національної безпеки [69]. Згідно з цією концепцією, інформаційна безпека не обмежується кіберзахистом або протидією дезінформації, а охоплює широкий спектр таких напрямів, як контроль за безпекою цифрового простору, стійкість суспільних інститутів, підтримка інформаційної автономії, незалежність стратегічних комунікацій. Для України, яка сьогодні перебуває в епіцентрі глобальної інформаційної війни, надзвичайно цінним є саме інтегральний

підхід Ізраїлю, що дозволяє розглядати інформаційну сферу не як другорядний вимір, а як критичний елемент державної оборони.

Правовий напрямок імплементації ізраїльського досвіду пов'язаний із необхідністю суттєвого оновлення законодавства України у сфері інформаційної безпеки. Ізраїль забезпечує свою інформаційну стійкість завдяки чітким правовим рамкам, у яких визначені функції органів влади, процедури взаємодії, стандарти відповідальності та механізми контролю [72]. Закон «Про національну кібербезпеку» Ізраїлю, ухвалений із широким суспільним і політичним консенсусом, створив єдину правову архітектуру, що зводить докупи обов'язки як державного сектору, так і приватних компаній [40]. В Україні аналогічні кроки вже були розпочаті, але, без сумніву, потребують прискорення та структурного доопрацювання. У цьому контексті доцільним є ухвалення комплексного «Коду інформаційної безпеки України», який би, подібно до ізраїльських практик, поєднував норми, що регулюють кіберзахист, інформаційний суверенітет, протидію дезінформації, стратегічні комунікації, а також діяльність суб'єктів критичної інфраструктури.

Особливо важливим є імплементація ізраїльського принципу регуляторної чіткості. В Ізраїлі будь-який суб'єкт, що працює у сфері інформаційних послуг, має чітко визначені обов'язки та стандарти безпеки [1]. Наприклад, компанії, які здійснюють обробку великих масивів персональних даних, підлягають суворим правилам аудиту та регулярним перевіркам з боку Урядового управління кібербезпеки. В Україні цей підхід може бути застосований через систему «обов'язкових базових стандартів інформаційної стійкості», що охоплювали б банківський сектор, телекомунікації, транспорт, енергетику та інші ключові галузі. Не менш важливою правовою рекомендацією є імплементація механізмів відповідальності за недотримання вимог у сфері інформаційної безпеки. У 2023 році Ізраїль запровадив оновлені положення щодо відповідальності державних і приватних структур за порушення вимог кіберзахисту, що суттєво підвищило рівень дисципліни у сфері інформаційних операцій [49] . Україна могла б адаптувати ці положення,

зокрема встановивши більш жорсткі санкції за невиконання рішень компетентних органів під час реагування на кризові інциденти.

Організаційний напрямок імплементації передбачає адаптацію структурних та інституційних рішень, що сформували основу ізраїльської системи. Центральним інституційним елементом є створення Ізраїльського національного кібердиректорату (INCD), який об'єднав функції спостереження, аналізу, координації та оперативного реагування [11]. Україна вже має відповідні інституції – Державну службу спеціального зв'язку та захисту інформації, Центр протидії дезінформації, Національний координаційний центр кібербезпеки. Однак, між ними все ще зберігається фрагментарність повноважень і недостатня централізація. У цьому аспекті корисним буде впровадження моделі «єдиного центру стратегічного управління інформаційною безпекою», що координував би дії не лише державних агентств, а й приватного сектору та громадських організацій. Окремої уваги потребує імплементація ізраїльської моделі державно-приватного партнерства, яка базується на постійній взаємодії між державою та інноваційним технологічним сектором. Ізраїльський «CyberSpark» у Беер-Шеві, створений у співпраці з провідними університетами та високотехнологічними компаніями, є прикладом середовища, де наука, бізнес та армія формують спільні проєкти у сфері інформаційної безпеки [32]. В Україні подібні технопарки можуть бути створені на базі Києва, Львова чи Харкова, що дозволить суттєво підвищити інноваційність та кадрову забезпеченість цієї сфери.

Водночас організаційні рекомендації мають включати розвиток людського капіталу. Ізраїль відомий високоякісною системою підготовки кадрів, яка інтегрує військову, академічну та приватну освіту. Зокрема, програма «8200 Alumni», тобто мережа фахівців, які пройшли службу в елітному підрозділі військової розвідки «Unit 8200», забезпечує створення висококваліфікованих стартапів та інноваційних рішень у сфері інформаційної безпеки [46]. Україна може адаптувати цей досвід, створивши спеціальні

урядові програми підготовки та перепідготовки кадрів, а також запровадивши практику стажувань у національних та міжнародних центрах кіберзахисту. Крім того, доцільним є інтегрування навчальних курсів з інформаційної безпеки у шкільну та університетську освіту, адже, як показує ізраїльський досвід, грамотність населення у сфері цифрової безпеки є вагомим чинником стійкості держави. Сучасні події підтверджують важливість таких заходів. Наприклад, у 2024 році Ізраїль оперативно нейтралізував масштабну атаку на системи управління водопостачанням, що було здійснено іранськими хакерськими групами [49]. Успіх став можливим завдяки високому рівню міжвідомчої координації та оперативності реагування. Україна, яка регулярно зіштовхується з кібератаками російських груп, має потенціал створити подібні механізми шляхом посилення координаційних функцій завдяки створенню єдиного центру кризового реагування.

Зрештою, важливим напрямком організаційної імплементації є розвиток системи стратегічних комунікацій. Ізраїльський уряд активно застосовує технології кризових комунікацій, інформаційного менеджменту та протоколів публічного інформування, що дозволяє мінімізувати паніку, протидіяти дезінформації та підтримувати суспільну довіру навіть у періоди ескалації, як це стало очевидно під час подій 2023–2024 років [50]. Україні потрібно адаптувати ці практики, розширивши функції Центру стратегічних комунікацій при РНБО та забезпечивши його сучасними аналітичними інструментами, зокрема системами моніторингу соціальних мереж та платформами аналізу великих даних.

Одночасно варто наголосити, що імплементація ізраїльського досвіду має супроводжуватися створенням системи постійного моніторингу ефективності запроваджених рішень. В Ізраїлі кожна стратегія чи нормативно-правовий акт у сфері інформаційної безпеки супроводжується чіткими індикаторами оцінювання, регулярними аудитами та аналізом на предмет адаптації до нових викликів [46]. Україна, яка перебуває у стані тривалої війни та щоденно стикається зі швидко змінними типами загроз, потребує

аналогічного механізму. Запровадження системи оцінювання відповідності стандартам інформаційної безпеки для органів влади, бізнесу та критичної інфраструктури дозволить підвищити рівень відповідальності та забезпечить зворотний зв'язок для коригування політики. Більш того, створення спеціальних незалежних експертних груп за прикладом ізраїльських advisory boards, що складаються з учених, представників технологічних компаній та колишніх військових аналітиків, могло б стати важливим елементом забезпечення об'єктивності моніторингу [8]. Додатково Україна може використати ізраїльську модель розбудови інформаційної обороноздатності на місцевому рівні. В Ізраїлі муніципалітети мають власні плани реагування на кіберінциденти, а їхні співробітники проходять спеціальні тренінги [30]. Так, після серії атак у 2022–2023 роках на муніципальні системи Тель-Авіва, Хайфи та Ашдода, уряд Ізраїлю запровадив програму з обов'язкової локальної кіберпідготовки для органів самоврядування [49]. Для України, яка має велику територію та різноманітні регіональні ризики, децентралізація заходів інформаційної безпеки може суттєво підвищити загальну стійкість держави. Запровадження регіональних центрів кіберзахисту, що діяли б під координацією національного центру, сприятиме більш ефективному реагуванню на локальні загрози та зменшить навантаження на центральні органи влади.

Не менш значущою є імплементація культурно-комунікаційного виміру ізраїльського досвіду, який передбачає формування суспільної культури стійкості, довіри та відповідального ставлення до цифрової безпеки. В Ізраїлі протягом останніх двох десятиліть уряд послідовно розвиває просвітницькі програми, що охоплюють школи, університети та громадські організації [36]. Завдяки цьому значна частина населення володіє базовими навичками цифрової гігієни, що суттєво зменшує ефективність інформаційно-психологічних атак. В Україні такі програми розвиваються, однак їх масштаб і глибина поки що недостатні. З огляду на це, доцільним є запуск довгострокової державної інформаційно-освітньої кампанії, яка пояснювала б громадянам

ризики, моделі поведінки в умовах інформаційних загроз та методи розпізнавання дезінформації. У цьому контексті можна навести приклад подій 2023 року, коли ізраїльські урядові структури провели масштабну кампанію протидії іранським дезінформаційним операціям, у межах якої громадянам регулярно надсилали повідомлення через SMS-інформування, соціальні мережі та мобільні додатки [49]. Це дозволило значно підвищити рівень обізнаності населення й нейтралізувати панічні настрої, які намагалися спровокувати ворожі актори. Для України аналогічні механізми можуть бути інтегровані у систему державних сервісів, наприклад у «Дію», що забезпечить охоплення мільйонів громадян.

З огляду на важливість усього спектра організаційних заходів, варто окремо звернути увагу на розвиток інноваційної інфраструктури, яка стала ключовим чинником успіху Ізраїлю. Протягом останніх років Ізраїль посідає провідні позиції у світових рейтингах стартап-екосистем, а близько 15% усіх інновацій у сфері кібербезпеки походять саме з ізраїльських компаній [46]. Результативність ізраїльської моделі пов’язана зі створенням сприятливих умов для досліджень, венчурних інвестицій, експериментальних центрів та інституцій, які поєднують державу й бізнес [32]. Для України, яка займає стратегічне положення у Східній Європі та має значний кадровий потенціал у сфері ІТ, розвиток національного інноваційного середовища у сфері інформаційної безпеки стане одним із найважливіших кроків на шляху до самодостатності.

Ще одним напрямком імплементації ізраїльського досвіду є посилення військово-цифрової взаємодії, оскільки Ізраїль чітко демонструє, що межа між традиційною обороною та інформаційною безпекою зникає. В Ізраїлі кіберпідрозділи інтегровані у структури оборонного планування, що дозволяє оперативно реагувати на загрози, які супроводжують сучасні бойові дії [75]. Для України, яка веде повномасштабну війну, важливо адаптувати подібні практики — зокрема посилити цифрову компоненту оборонних стратегій, забезпечити пріоритетне фінансування кіберпідрозділів та створити

сприятливі умови для співпраці між Збройними Силами України й приватними технологічними компаніями. Останній важливий блок рекомендацій стосується міжнародного співробітництва, яке в Ізраїлі є одним із ключових інструментів забезпечення інформаційної безпеки. Ізраїль активно бере участь у глобальних та регіональних ініціативах, зокрема у співпраці зі США, Великою Британією, Кана дою, державами ЄС та НАТО з метою обміну розвідувальними даними, технологіями, методологіями реагування на загрози [53]. Для України, яка вже стала важливою частиною глобальної системи кіберстійкості, доцільним є розширення участі у багатосторонніх форматах — таких як Cyber Defence Pledge НАТО, проєкти ЄС у сфері кіберзахисту (наприклад, EU Cyber Solidarity Act), а також партнерські програми з Ізраїлем.

Підсумовуючи, можна стверджувати, що стратегічні, правові та організаційні рекомендації на основі ізраїльського досвіду становлять важливий орієнтир для України, яка перебуває на шляху побудови сучасної системи інформаційної безпеки. Застосування цих підходів створить умови для ефективної протидії гібридним загрозам, забезпечення стійкості критичної інфраструктури, зміцнення довіри громадян до державних інституцій та інтеграції України у глобальну архітектуру цифрової безпеки. Такий комплексний шлях дозволить Україні не лише адаптувати найкращі світові практики, але й у перспективі стати одним із лідерів у сфері інформаційної безпеки у Європі.

Висновки до розділу 3

Зазначимо, що сучасна національна система інформаційної безпеки України перебуває у стані глибокої трансформації, спричиненої як ескалацією зовнішніх загроз, так і внутрішньою потребою у модернізації механізмів державної політики. З одного боку, Україна суттєво просунулась у напрямі формування стійкої архітектури кіберзахисту, удосконалення нормативно-правової бази та розвитку міжвідомчої координації. З іншого боку, наявні проблеми: фрагментованість управлінських рішень, недостатній рівень

інституційної узгодженості, обмежене фінансування, а також нерівномірність розвитку цифрової інфраструктури, все ще стримують ефективність реагування на гібридні загрози. Крім того, практична реалізація стратегічних документів нерідко ускладнюється бракованими процедурами взаємодії між державним сектором та бізнесом, що, відповідно, знижує рівень оперативності реагування на кібератаки та інформаційні операції.

Порівняльний аналіз української та ізраїльської моделей інформаційної безпеки засвідчує, що, незважаючи на спільність викликів, ці системи розвивалися за різними логіками. Ізраїль, маючи тривалу історію існування в умовах постійних загроз, сформував високоефективну централізовану модель, де ключову роль відіграють цілісний нормативний каркас, чітка вертикаль управління та тісна інтеграція оборонного сектору, академії й технологічних компаній. Україна ж поки що лише наближається до подібного рівня координації, хоча війна з РФ значно пришвидшила інституційні зміни й формування партнерств.

Отже, напрями імплементації ізраїльського досвіду мають бути багаторівневими. Стратегічно Україні варто зміцнити централізовану систему управління інформаційною безпекою та запровадити довгострокові програми розвитку інновацій і кіберстійкості. З правової точки зору, важливо створити комплексний, узгоджений набір законодавчих актів, які регламентують роль усіх суб’єктів сектора. Організаційно ж пріоритетом має стати розбудова ефективних механізмів державного-приватного партнерства, інституціоналізація спільних навчальних платформ та запровадження системи швидкого реагування, що, безумовно, підвищить стійкість держави до сучасних гібридних загроз.

ВИСНОВКИ

У результаті дослідження особливостей організації та функціонування системи інформаційної безпеки Ізраїлю, а також можливостей адаптації ізраїльського досвіду для удосконалення національної системи інформаційної безпеки України, зроблено наступні висновки:

1. Визначено, що поняття «інформаційна безпека» у міжнародних відносинах за останні десятиліття істотно трансформувалося. Сьогодні, у контексті стрімкої цифровізації, гібридних загроз і зростання ролі інформаційного простору як інструменту впливу, концепт «інформаційної безпеки» охоплює як технологічні, так і політичні, правові, комунікаційні та психологічні виміри безпеки. При цьому, як свідчить аналіз міжнародних практик, сучасна система глобального забезпечення інформаційної безпеки формується під впливом діяльності міжнародних організацій: ООН, ОБСЄ, НАТО, ЄС, які, кожна в межах власної компетенції, створюють норми, механізми взаємодії та рамки відповідальності держав за поведінку в кібер- та інформаційному просторі. Загалом дослідження дозволило встановити, що основні підходи до формування міжнародної системи забезпечення інформаційної безпеки можна умовно поділити на три групи. По-перше, це нормативний підхід, який передбачає створення міжнародно-правових документів, стандартів, конвенцій і рекомендацій щодо відповідальної поведінки держав. По-друге, інституційний, зорієнтований на зміцнення спеціалізованих структур, центрів реагування та міждержавних платформ координації. По-третє, стратегічний, який спрямований на формування довгострокових політик, що поєднують превентивні, захисні та реактивні заходи. У цьому контексті міжнародні моделі все частіше базуються на концепціях «стійкості» (resilience), «колективної відповідальності» та «спільної кібероборони», що, зрештою, формує нову конфігурацію міжнародної безпекової взаємодії.

2. З іншого боку, визначення теоретичних засад і ключових моделей розбудови національних систем інформаційної безпеки дозволило

переконатися, що сучасні держави застосовують різні архітектури управління залежно від історичного досвіду, рівня загроз, технічних можливостей і політичної культури. Так, у світовій практиці простежуються централізовані, мережеві та гібридні моделі забезпечення інформаційної безпеки, кожна з яких має свої переваги й обмеження. Централізована модель забезпечує чіткість управління, проте нерідко страждає від надмірної бюрократизації. Мережева, навпаки, передбачає широку взаємодію міждержавних та недержавних акторів, що підвищує її гнучкість, хоча інколи знижує керованість. Гібридна модель, яка сьогодні є найбільш поширеною, поєднує елементи обох, забезпечуючи баланс між оперативністю та інституційною стійкістю. Ці моделі дозволяють державам адаптуватися до новітніх технологічних тенденцій, від штучного інтелекту до квантових комунікацій, і передбачати виникнення нових типів інформаційних загроз.

3. У результаті дослідження ізраїльської системи інформаційної безпеки, було доведено, що вона є однією з найефективніших і інституційно розвиненіших у світі. Інституційна складова Ізраїлю включає Національний кібердиректорат, службу «Шабак», розвідувальну службу «Моссад», Міністерство оборони, підрозділи Армії оборони Ізраїлю та низку спеціалізованих аналітичних центрів. Кожен із цих суб’єктів виконує визначені функції, а міжвідомча взаємодія забезпечується через стандартизовані процедури обміну даними, спільні операційні групи та єдині центри реагування на інциденти. Як свідчить досвід Ізраїлю, ефективна координація неможлива без чіткої регламентації повноважень, а також без розмежування відповідальності між органами безпеки, урядовими установами та приватним сектором.

Нормативно-правова складова системи Ізраїлю, своєю чергою, відзначається послідовністю й багаторівневістю. Вона включає військову доктрину, національну кіберстратегію, законодавство про захист критичної інфраструктури, норми щодо діяльності спецслужб, а також регуляції приватних компаній у сфері кіберстійкості. Зазначене правове поле створює

умови для збалансованого поєднання безпеки, прав людини та економічних інтересів, що є однією з головних причин високої ефективності ізраїльської моделі.

4. Важливо підкреслити, що виявлені практичні кейси функціонування системи інформаційної безпеки Ізраїлю демонструють її гнучкість, технологічну інноваційність і здатність до швидкого реагування. Вони охоплюють приклади державно-приватного партнерства, зокрема, співпрацю між Національним кібердиректоратом і провідними технологічними компаніями; діяльність військово-наукових кластерів, які створюють нові технології для кібероборони; а також ефективні моделі міжвідомчої взаємодії, що забезпечують уніфіковану реакцію на складні інформаційні інциденти. Зокрема, механізми раннього виявлення загроз та централізованого реагування довели свою результативність у протидії кібератакам на критичну інфраструктуру та органи державної влади.

5. Порівняння ізраїльської та української моделей засвідчило суттєві відмінності у рівні інституційної зрілості, ступені централізації управління та спроможності до стратегічного планування. Україна, перебуваючи в умовах тривалої збройної агресії з боку РФ, формує власну систему інформаційної безпеки під тиском безпрецедентних викликів, що, з одного боку, стимулює швидкі реформи, але, з іншого, виявляє структурні слабкі місця, пов’язані з обмеженими ресурсами, недостатньою координацією та фрагментованістю нормативної бази. Нинішній стан української системи демонструє значний прогрес у сфері кіберзахисту, проте залишається недостатньо сформованим у напрямах захисту інформаційного простору, протидії дезінформації, розвитку кадрового потенціалу та створення механізмів системної співпраці з приватним сектором. Отже, напрями імплементації ізраїльського досвіду в українську практику мають включати, передусім, інституційну консолідацію та створення чіткої вертикалі управління інформаційною безпекою, що зменшить дублювання повноважень і підвищить ефективність реагування. Крім того, слід адаптувати ізраїльську модель державно-приватного

партнерства у сфері кіберзахисту, зокрема шляхом розвитку кластерів інновацій, спільних навчальних платформ і механізмів оперативного обміну інформацією. Не менш важливими є вдосконалення законодавства з акцентом на захист критичної інфраструктури, розбудова системи кадрової підготовки та, зрештою, підвищення стійкості суспільства до інформаційних впливів шляхом розвитку медіаграмотності, стратегічних комунікацій та національних наративів. У сукупності ці заходи можуть наблизити Україну до формування такої моделі інформаційної безпеки, яка відповідатиме сучасним міжнародним стандартам, забезпечуватиме стійкість у довгостроковій перспективі та сприятиме підвищенню рівня національної безпеки в умовах продовження геополітичних загроз..

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналітична записка з питань порівняльного законодавства щодо правових засад забезпечення та організації системи кібербезпеки та захисту державних інформаційних ресурсів у ЄС, державах-членах ЄС, а також в США, Ізраїлі, Південній Кореї. *Дослідницька служба Верховної Ради України.* Київ, 2024. 20 с. URL: https://research.rada.gov.ua/uploads/documents/33398.pdf (Last accessed: 07.10.2025).

2. Бен-Ізраїль І., Сердіо Дж., Ема А., Фрідман Л., Ієнка М. Tech titans, cyber commons and the war in Ukraine: An incipient shift in international relations. 2023. URL: https://scholar.google.com/citations?user=GIrTDM0AAAAJ&hl=iw (дата звернення: 07.10.2025).

3. Бєлєвцева В. В. Основи правового регулювання інформаційної сфери у державі Ізраїль. *Інформація і право.* 2024. № 1(48). С. 162–169. URL: http://il.ippi.org.ua/article/view/300802 (дата звернення: 07.10.2025).

4. Білоус Л. В. Інформаційна безпека України в умовах воєнного стану: історіографія проблеми. *Міжнародний науковий журнал «Інтернаука».* 2025. № 1. DOI: https://doi.org/10.25313/2520-2057-2025-1-10614. URL: https://www.inter-nauka.com/issues/2025/1/ (дата звернення: 07.10.2025).

5. Босак І. М. Інформаційна безпека України: загрози та методи протидії. *Київський економічний науковий журнал*. 2025. № 9. С. 33–38. DOI: https://doi.org/10.32782/2786-765X/2025-9-4.

6. Войтовський К. Досвід Ізраїлю щодо формування стратегії національної безпеки. *NISS.* 2022. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/dosvid-izrayilyu-shchodo-formuvannya-stratehiyi-natsionalnoyi (дата звернення: 07.10.2025).

7. Галіпчак В. Д. Державно-правовий механізм інформаційної безпеки України в умовах російської агресії. *Політикус : наук. журнал*. 2023. № 5. С. 19–24. DOI: https://doi.org/10.24195/2414-9616.2023-5.3. URL: http://politicus.od.ua/index.php/2023-ukr?id=66 (дата звернення: 07.10.2025).

8. Голдман Е. О. Lessons From Israel’s Rise as a Cyber Power. Lawfare. 2024. URL: https://www.lawfaremedia.org/article/lessons-from-israel-s-rise-as-a-cyber-power (дата звернення: 07.10.2025).

9. Дзеньків В. Кібербезпека в умовах сучасних загроз: ізраїльський досвід і його застосування в Україні. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Вип. 84. ч. 3. С. 77–83. DOI: 10.24144/2307-3322.2024.84.3.12. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/09/14-2.pdf (дата звернення: 07.10.2025).

10. Ейхенсер К. Е. Ukraine, Cyberattacks, and the Lessons for International Law. *American Journal of International Law.* 2022. № 116. С. 145–149. URL: https://scholar.google.com/citations?user=q-pEIsoAAAAJ&hl=en (дата звернення: 07.10.2025).

11. Живило Є. О., Докіль В. М. Досвід Ізраїля та Республіки Корея щодо механізмів державного забезпечення та організації системи кібербезпеки. *Наукові інновації та передові технології.* 2025. № 5(10). С. 120–139. DOI: https://doi.org/10.52058/3041-1793-2025-5(10)-120-139. URL: https://perspectives.pp.ua/index.php/niu/article/download/23696/23669/29698 (дата звернення: 07.10.2025).

12. Залєвська І. І., Удренас Г. І. Інформаційна безпека України в умовах російської військової агресії. *Південноукраїнський правничий часопис.* 2022. № 1–2. С. 20–26. DOI: https://doi.org/10.32850/sulj.2022.1-2.4. URL: http://www.sulj.oduvs.od.ua/archive/2022/1-2/6.pdf (дата звернення: 07.10.2025).

13. Кібербезпека в охороні здоров’я: глобальні тенденції та ізраїльський досвід. *Блог Офісу з питань економіки та торгівлі Посольства Держави Ізраїль в Україні.* 17.03.2025. URL: https://itrade.gov.il/ukraine/2025/02/12/кібербезпека-в-охороні-здоровя-глоб (дата звернення: 07.10.2025).

14. Кобець Т. Аналіз загроз когнітивній безпеці українського суспільства: класифікаційні підстави. *Вісник Прикарпатського університету. Серія: Політологія.* 2024. Вип. 21. С. 67–72. URL:

https://journals.pnu.if.ua/index.php/politology/article/view/182/178 (дата звернення: 07.10.2025).

15. Кочетков М. О. Інформаційна безпека України: стратегічні пріоритети та інституційні інструменти забезпечення. *Державне управління: удосконалення та розвиток.* 2024. № 3. URL: https://www.dy.nayka.com.ua/?op=1&z=2891 (дата звернення: 07.10.2025).

16. Кочубей Л., Некряч А. Державна інформаційна політика України в умовах євроінтеграції. *Публічне управління і політика.* 2025. № 4 (8). С. 1–9. URL: https://www.researchgate.net/publication/391834174_DERZAVNA_INFORMACIJNA_POLITIKA_UKRAINI_V_UMOVAH_EVROINTEGRACII (дата звернення: 07.10.2025).

17. Крап А. Дезінформація як загроза демократії та державному управлінню. *Український політико-правовий дискурс*. 2025. № 9. URL: https://zenodo.org/records/15108404 (дата звернення: 07.10.2025).

18. Крушеніцький V. Foreign experience in ensuring national security in the public information sphere. *Scientific Bulletin of Sivershchyna. Series: Law.* 2025. № 3 (26). С. 19–28. URL: https://sjlaw.pau.edu.ua/wp-content/uploads/2025/07/2.-Krushenitskyi-V-1.pdf (дата звернення: 07.10.2025).

19. Марчук О. Державна політика кібербезпеки: Україна та міжнародний досвід. *Інформаційні технології та телекомунікації*. 2025. URL: https://itta.info/derzhavna-polityka-kiberbezpeky-ukraina-ta-mizhnarodnyy-dosvid/ (Last accessed: 07.10.2025).

20. Милосердна І. М. Інформаційна безпека як елемент національної безпеки: теоретичний вимір та особливості впровадження. *Політикус : наук. журнал.* 2024. № 4. С. 179–185. URL: http://politicus.od.ua/4_2024/28.pdf (дата звернення: 07.10.2025).

21. Міщенко, Л.О., Хурдей, В.Д. Цифровізація публічного управління як чинник нейтралізації загроз національним інтересам. *Дніпровський науковий часопис публічного управління, психології, права та соціальних наук*,

2025. URL: http://chasopys-ppp.dp.ua/index.php/chasopys/article/view/768 (дата звернення: 07.10.2025).

22. Ніцевич О. В. Інформаційна безпека України в умовах воєнного стану. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2025. Т. 8, № 1. С. 166–177. URL: https://journals.lvduvs.lviv.ua/index.php/law/article/view/971 (дата звернення: 07.10.2025).

23. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 груд. 2021 р. № 685/2021 «Про Стратегію інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/show/685/2021 (дата звернення: 07.10.2025).

24. Радковський Ю. Приклад для України: Як в Ізраїлі реформують розвідувальні та спеціальні служби. *Defence-UA.* 2022. URL: https://defence-ua.com/weapon_and_tech/jak_v_izrajili_reformujut_rozviduvalni_ta_spetsialni_sluzhbi-5668.html (дата звернення: 07.10.2025).

25. Скиба О. В. Інституційні механізми розвитку системи інформаційної безпеки України в умовах цифрової трансформації. *Публічне управління та митне адміністрування.* 2023. № 4 (35). С. 45–53. DOI: https://doi.org/10.32836/2310-9653/2023.4.7. URL: https://customs-admin.umsf.in.ua/journal/article/view/1131 (дата звернення: 07.10.2025).

26. Трудолюбов М. Israel as a Security Model for Ukraine. *Wilson Center.* 2023. URL: https://www.wilsoncenter.org/blog-post/israel-security-model-ukraine (дата звернення: 07.10.2025).

27. Шапіро Д. Б., Раков Д. Zelenskyy wants Ukraine to be «a big Israel». *Here's a road map. Atlantic Council.* 2022. URL: https://www.atlanticcouncil.org/blogs/new-atlanticist/zelenskyy-wants-ukraine-to-be-a-big-israel-heres-a-road-map/ (дата звернення: 07.10.2025).

28. Шевчук М. Сучасні виклики і загрози в сфері інформаційної безпеки держави. *Актуальні проблеми вітчизняної юриспруденції.* 2024. № 6.

С. 160–166. URL: http://www.apnl.dnu.in.ua/6_2024/6_2024.pdf#page=160 (дата звернення: 07.10.2025).

29. Якубович М. Принципи оборони Ізраїлю в Україні. *CPD.* 2022. URL: https://cpd.gov.ua/articles/czpd_analizuye-6-2/ (дата звернення: 07.10.2025).

30. Annual Report 2022. *Israel National Cyber Directorate.* 2023. URL: https://www.gov.il/BlobFolder/reports/new-annual-reports/en/annual-reports_eng_main-annual-report-2022-eng.pdf (Last accessed: 07.10.2025).

31. Annual Summary 2020. *Israel National Cyber Directorate.* 2021. URL: https://www.gov.il/en/pages/annualsummary2020 (Last accessed: 07.10.2025).

32. Arvatz A. The Battle for Your Computer: Israel and the Growth of the Global Cyber-Security Industry. Hoboken: Wiley, 2023. 320 p. URL: https://www.wiley.com/The%2BBattle%2Bfor%2BYour%2BComputer%3A%2BIsrael%2Band%2Bthe%2BGrowth%2Bof%2Bthe%2BGlobal%2BCyber-Security%2BIndustry-p-00393049 (Last accessed: 07.10.2025).

33. Cyber and Information Systems – Annual Report 2024. *State Comptroller of Israel.* 2024. URL: https://library.mevaker.gov.il/sites/DigitalLibrary/Documents/2024/2024.11-Cyber/EN/2024.11-Cyber-Taktzirim-All-EN.pdf

34. Cyber and Information Systems – Audit Report 2022. *State Comptroller of Israel.* 2022. URL: https://library.mevaker.gov.il/sites/DigitalLibrary/Documents/2022/Cyber/2022.Cyber-001-EN.pdf

35. Cyber defence. *NATO official topic.* Brussels: North Atlantic Treaty Organization, 30 July 2024. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence (Last accessed: 07.10.2025).

36. Cyber For All Campus. Home – Cyber For All. 2023. URL: https://www.cyberforall.co.il/en (Last accessed: 07.10.2025).

37. Cyber incidents in Israel down 18 pct in 2022: national agency. Xinhua News Agency. 13.03.2023. URL:

https://english.news.cn/20230314/f7516c9834f0447d99618aedadd53db1/c.html (Last accessed: 07.10.2025).

38. Cyber Power – Tier Two. *International Institute for Strategic Studies.* London, 2021. URL: https://www.iiss.org/research-paper/2021/06/cyber-power---tier-two/ (Last accessed: 07.10.2025).

39. Cyber Week 2022 at TAU: Combating «Real and Growing» Threats. *Tel Aviv University.* 23.06.2022. URL: https://tautrust.org/cyber-week-2022-at-tau-combating-real-and-growing-threats/ (Last accessed: 07.10.2025).

40. Cybersecurity 2022 – Legal Guide to Israel. *Law.co.il.* Tel Aviv, 2022. URL: https://www.law.co.il/media/computer-law/2022_cybersecurity_legal_guide_to_israel.pdf (Last accessed: 07.10.2025).

41. Cybersecurity in Israel: Fortifying Digital Defences Amid Elevated Risks. *Global X ETFs.* 2022. URL: https://globalxetfs.eu/cybersecurity-in-israel-fortifying-digital-defences-amid-elevated-risks/ (Last accessed: 07.10.2025).

42. Danchuk V. Integration of blockchain technologies into cybersecurity systems for critical infrastructure objects: prospects and challenges. Bulletin of Cherkasy State Technological University. 2024. Vol. 29. №. 4. URL: https://bulletin-chstu.com.ua/en/journals/tom-29-4-2024/integratsiya-blokcheyn-tekhnologiy-u-sistemi-zabezpechennya-kiberbezpeki-dlya-ob-yektiv-kritichnoyi-infrastrukturi-perspektivi-ta-vikliki (Last accessed: 07.10.2025).

43. Digitalisation and Cyber Security in the Energy Sector: A Comparative Analysis between Germany and Israel. Deutsche Energie-Agentur (dena). Berlin, 2025. URL: https://energypartnership-israel.org/fileadmin/israel/newsroom/Digitalisation_and_Cyber_Security_in_the_Energy_Sector.pdf (Last accessed: 07.10.2025).

44. Engaging with Artificial Intelligence (AI). *Israel National Cyber Directorate.* Jerusalem, 2024. URL: https://www.gov.il/en/pages/engaging_with_artificial_intelligence_ai_2024 (Last accessed: 07.10.2025).

45. Fisher E., Cohen E. The Israeli High-Tech Industry. *The Palgrave International Handbook of Israel.* 2023. C. 1-13. DOI: 10.1007/978-981-16-2717-0_59-1.

46. Freilich C. D., Cohen M. S., Siboni G. Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power. Oxford: Oxford University Press, 2023. 422 p. URL: https://books.google.com/books/about/Israel_and_the_Cyber_Threat.html?id=TSnFEAAAQBAJ (Last accessed: 07.10.2025).

47. Freilich C., Cohen M., Siboni G. Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power. 2023. 441 p. DOI: 10.1093/oso/9780197677711.001.0001.

48. Global Cybersecurity Index 2020. Geneva: ITU, 2021. 148 p. (Country profiles, including Israel). *International Telecommunication Union (ITU).* URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (Last accessed: 07.10.2025).

49. In the Midst of the «Iron Swords» War – Annual Report of the Israel National Cyber Directorate 2023. *Israel National Cyber Directorate.* Jerusalem, 2024. URL: https://www.gov.il/en/pages/booklet_yearly_summary_2023 (Last accessed: 07.10.2025).

50. Influence Operations Against Israeli Economic and Security Interests (special publication). *INSS.* 2025. URL: https://www.inss.org.il/wp-content/uploads/2025/02/special-publication-18022025-1.pdf

51. Israel Artificial Intelligence Partnering Opportunities. *U.S. Department of Commerce.* 29.01.2024. URL: https://www.trade.gov/market-intelligence/israel-artificial-intelligence-partnering-opportunities (Last accessed: 07.10.2025).

52. Israel Cybersecurity Strategy 2025: A Strategic Gateway for U.S. Exporters. *U.S. Department of Commerce.* 21.04.2025. URL: https://www.trade.gov/market-intelligence/israel-cybersecurity-strategy-2025-strategic-gateway-us (Last accessed: 07.10.2025).

53. Israel International Cyber Strategy. *Israel National Cyber Directorate.*

2021. URL: https://www.gov.il/BlobFolder/news/international_strategy/en/Israel%20International%20Cyber%20Strategy.pdf

54. Israel International Cyber Strategy: International Engagement for Global Resilience. *Israel National Cyber Directorate (INCD).* Jerusalem, 2021. URL: https://www.gov.il/BlobFolder/news/international_strategy/en/Israel%20International%20Cyber%20Strategy.pdf (Last accessed: 07.10.2025).

55. Israel International Cyber Strategy: International Engagement for Global Resilience. *Israel National Cyber Directorate.* Jerusalem, 2021. 32 p. URL: https://www.gov.il/BlobFolder/news/international_strategy/en/Israel%20International%20Cyber%20Strategy.pdf (Last accessed: 07.10.2025).

56. Israel National Cyber Security Strategy 2025. *Israel National Cyber Directorate (INCD).* Jerusalem, 23 March 2025. URL: https://www.gov.il/en/pages/cyber_strategy_2025 (Last accessed: 07.10.2025). gov.il+1

57. Israel National Cybersecurity Strategy, 2025–2028. *Israel National Cyber Directorate.* Jerusalem, 2025. URL: https://en-cyber.tau.ac.il/home/NationalCyberSecurityStrategy (Last accessed: 07.10.2025).

58. Israel's Cyber Success Faces Risks from AI. The Jerusalem Post. *Jerusalem Post.* 15.11.2025. URL: https://www.jpost.com/business-and-innovation/article-873912 (Last accessed: 07.10.2025).

59. Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations / Cyber Defense Project (CDP). Zürich : Center for Security Studies (CSS), ETH Zürich, 2020. 24 p.

60. Israeli cyber startup Noma Security raises $100 million in private funding round. *Reuters.* 31.07.2025. URL: https://www.reuters.com/world/middle-east/israeli-cyber-startup-noma-security-raises-100-million-private-funding-round-2025-07-31/ (Last accessed: 07.10.2025).

61. Lessons from Israel's Rise as a Cyber Power. *Lawfare.* 2024. URL:

https://www.lawfaremedia.org/article/lessons-from-israel-s-rise-as-a-cyber-power (Last accessed: 07.10.2025).

62. Matania E., Podhorzer O., Daniel N. The Elusive Presence of Technology in Israel's Strategic Security Thinking. *Strategic Assessment.* 2023. Vol. 25. № 3. URL: https://www.inss.org.il/wp-content/uploads/2023/01/Adkan25.3_Eng_Matania-et-al.pdf (Last accessed: 07.10.2025).

63. National Cyber Security Index. NCSI: Israel. 2023. URL: https://ncsi.ega.ee/ncsi-index/?type=c&archive=1 (Last accessed: 07.10.2025).

64. National Cyber Security Strategy (February 2025). *Israel National Cyber Directorate.* 2025. URL: https://www.gov.il/BlobFolder/news/cyber_strategy_2025/he/israel_national_cyber security_strategy_feb2025.pdf (Last accessed: 07.10.2025).

65. National Cybersecurity Strategy 2025–2028. *Israel National Cyber Directorate.* Jerusalem: Prime Minister's Office, 2025. URL: https://www.gov.il/en/pages/cyber_strategy_2025 (Last accessed: 07.10.2025).

66. OECD Policy Framework on Digital Security. *OECD.* Paris: OECD Publishing, 2022. 84 p. URL: https://www.oecd.org/en/publications/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c.html (Last accessed: 07.10.2025).

67. Pidbereznykh I., Koval O., Solomin Y., Kryvoshein V., Plazova T. Ukrainian policy in the field of information security. *Amazonia Investiga*. 2022. Vol. 11, No. 60. P. 206–213. DOI: https://doi.org/10.34069/AI/2022.60.12.22. URL: https://amazoniainvestiga.info/index.php/amazonia/article/view/2226 (Last accessed: 07.10.2025).

68. Schenker J. L. Key Takeaways from CyberTechGlobal Tel Aviv 2022. The Innovator. 2022. URL: https://theinnovator.news/key-takeaways-from-cybertechglobal-tel-aviv-2022/ (Last accessed: 07.10.2025).

69. Shabtai S. The New National Cyber Strategy: Israel's Updated Cyber Security Concept. *BESA Center Perspectives Paper* №. 2346. 2025. URL:

https://besacenter.org/wp-content/uploads/2025/07/2346-Shabtai-The-new-national-cyber-strategy-1.pdf (Last accessed: 07.10.2025).

70. Sharma R. K. Cybersecurity in Israel. In: Kumaraswamy P. R. The Palgrave International Handbook of Israel. Singapore : Palgrave Macmillan, 2025. DOI: 10.1007/978-981-16-2717-0_115-1. URL: https://link.springer.com/referenceworkentry/10.1007/978-981-16-2717-0_115-1 (Last accessed: 07.10.2025).

71. Spyer J., Kagan B. Israel and Ukraine Face Shared Cyber Threats. Foundation for Defense of Democracies. 13.11.2023. URL: https://www.fdd.org/analysis/2023/11/13/israel-and-ukraine-face-shared-cyber-threats/ (Last accessed: 07.10.2025).

72. Stancu A.-I., Pavel T. Unveiling Israel's Cyber Legal Landscape: A Comprehensive Analysis of Cybersecurity Regulations and Policies. Perspectives of Law and Public Administration. 2023. Vol. 12. Iss. 4. P. 643–657. URL: https://www.researchgate.net/publication/377110754_Unveiling_Israel%27s_Cyber_Legal_Landscape_A_Comprehensive_Analysis_of_Cybersecurity_Regulations_and_Policies (Last accessed: 07.10.2025).

73. Summary of the Third Annual Event of the OECD Global Forum on Digital Security for Prosperity, hosted virtually by Israel, 7–9 June 2021. *OECD.* Paris: OECD, 2023. (DSTI/CDEP/SDE(2022)5/FINAL). URL: https://one.oecd.org/document/DSTI/CDEP/SDE(2022)5/FINAL/en/pdf (Last accessed: 07.10.2025).

74. Tabansky L. Cybersecurity in Israel: Strategy, Organization, and Future Challenges.The Oxford Handbook of Cyber Security. 2021. P. 631-648. DOI: 10.1093/oxfordhb/9780198800682.013.57.

75. Tabansky L. Israel Defense Forces and National Cyber Defense. *Connections: The Quarterly Journal.* 2020. Vol. 19. № 1. С. 45-62. DOI: 10.11610/Connections.19.1.05.

76. The Annual Report of the National Cyber Directorate 2023. *Israel National Cyber Directorate.* 2024. URL:

https://www.gov.il/en/pages/booklet_yearly_summary_2023 (Last accessed: 07.10.2025).

77. The Cyber Defense Index 2022/23. *MIT Technology Review Insights.* Cambridge, MA, 2023. URL: https://mittrinsights.s3.amazonaws.com/CDIreport.pdf (Last accessed: 07.10.2025).

78. The Israeli Cyber Emergency Response Team (CERT): Principles of Operation. *Inter-American Development Bank; Israel National Cyber Directorate.* 2024. URL: https://publications.iadb.org/publications/english/document/The-Israeli-Cyber-Emergency-Response-Team-CERT-Principles-of-Operation-Cybersecurity-Best-Practices.pdf

79. The Israeli National AI Program – Artificial Intelligence in Israel. *Israeli National AI Program.* 2023. URL: https://aiisrael.org.il/ (Last accessed: 07.10.2025).

80. Voo J., Hemani I., Cassidy D. National Cyber Power Index 2022. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard University, 2022. 92 p. URL: https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf (Last accessed: 07.10.2025).

АНОТАЦІЯ

Гончаренко В.С. Система інформаційної безпеки Ізраїлю: досвід для України (магістерська робота). Харків: ХНУ імені В. Н. Каразіна, 2025. 87 с. (рукопис).

Кваліфікаційна робота магістра присвячена визначенню особливості організації та функціонування системи інформаційної безпеки Ізраїлю, а також можливостей адаптації ізраїльського досвіду для удосконалення національної системи інформаційної безпеки України. Об’єкт дослідження – система забезпечення інформаційної безпеки держави. Предмет дослідження – система функціонування інформаційної безпеки Ізраїлю та виявлення досвіду її діяльності щодо імплементації в Україні.

У першому розділі розглянуто еволюцію поняття «інформаційної безпеки» у сучасних міжнародних відносинах та основні підходи до формування міжнародної системи її забезпечення; визначено теоретичні засади та ключові моделі розбудови національних систем інформаційної безпеки

У другому розділі розкрито інституційну та нормативно-правову складові системи інформаційної безпеки Ізраїлю.

У третьому розділі виявлено практичні кейси функціонування системи інформаційної безпеки Ізраїлю, зокрема механізми нормативно-правового регулювання, міжвідомчої координації та державно-приватного партнерства; встановлено специфіку моделей Ізраїлю та України у сфері інформаційної безпеки, сучасний стан і ключові проблеми української системи та виявити напрями імплементації ізраїльського досвіду.

Ключові слова: інформаційна безпека, кібербезпека Ізраїлю, національна кіберстратегія, Національне кіберуправління Ізраїлю, модель багаторівневого захисту, військово-цифрова доктрина.

ANNOTATION

Honcharenko V.S. Israel's Information Security System: Experience for Ukraine (master’s work). Kharkiv: V. N. Karazin Kharkiv National University, 2025. 87 p. (manuscript).

The master's qualification work is devoted to determining the peculiarities of the

organization and functioning of the Israeli information security system, as well as the possibilities of adapting the Israeli experience to improve the national information security system of Ukraine. The object of the study is the system of ensuring the state's information security. The subject of the study is the system of functioning of Israel's information security and identifying the experience of its implementation in Ukraine.

The first section considers the evolution of the concept of «information security» in modern international relations and the main approaches to the formation of an international system of its provision; the theoretical principles and key models of the development of national information security systems are determined.

The second section reveals the institutional and regulatory components of the Israeli information security system.

The third section identifies practical cases of the functioning of the Israeli information security system, in particular the mechanisms of regulatory and legal regulation, interagency coordination and public-private partnership; identifies the specifics of the Israeli and Ukrainian models in the field of information security, the current state and key problems of the Ukrainian system and identifies areas for implementing Israeli experience.

Keywords: information security, Israeli cybersecurity, national cyber strategy, Israeli National Cyber Directorate, multi-level protection model, military digital doctrine.

ВІДГУК

на кваліфікаційну роботу магістра
студента 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»
освітньо-професійної програми
«Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут
міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Гончаренко Владислава Сергійовича
на тему «Система інформаційної безпеки Ізраїлю: досвід для України»

1.Актуальність теми зумовлена зростанням масштабів гібридних загроз, які трансформують сучасний безпековий простір та створюють нові виклики для держав, що перебувають у стані активної протидії зовнішній агресії. Україна, яка з 2014 року і особливо після повномасштабного вторгнення Росії у 2022 році стикається з безперервними кібератаками, дезінформаційними кампаніями, маніпуляцією громадською думкою та спробами підриву критичної інфраструктури, потребує ефективної моделі зміцнення власної інформаційної стійкості. У цьому контексті ізраїльський досвід є надзвичайно цінним, оскільки Ізраїль протягом десятиліть формував одну з найбільш результативних систем інформаційної безпеки у світі, що поєднує жорсткі нормативно-правові механізми, розвинену міжвідомчу координацію та інноваційне державно-приватне партнерство. Крім того, актуальність теми підсилюється тим, що Україна активно модернізує власну систему інформаційної безпеки відповідно до стандартів ЄС і НАТО. Саме тому аналіз ізраїльської моделі дозволяє не лише визначити практики, що можуть бути адаптовані до українських реалій, але й сформувати комплексні рекомендації щодо посилення кіберзахисту, упередження дезінформації та забезпечення стійкості критичної інфраструктури. Отже, тема є важливою як у науковому, так і в практичному вимірі.

2. Позитивні аспекти в роботі. Зміст роботи повністю відповідає обраній темі. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел. Позитивними рисами кваліфікаційної роботи магістра є системність та послідовність викладення матеріалу.

3. Недоліки роботи. В той же час, автору слід було б приділити більше уваги ілюстративній частині роботи, однак це не впливає на роботу вцілому.

4. Практична цінність висновків і рекомендацій. полягає в тому, що вони дають змогу органам влади України, по-перше, сформувати більш цілісну та

проактивну модель реагування на гібридні загрози, використовуючи ізраїльський досвід інтеграції військових, технологічних і цивільних інструментів захисту. По-друге, запропоновані висновки дозволяють удосконалити систему кібероборони шляхом розширення партнерства держави з приватним сектором, що, як показує приклад Ізраїлю, істотно підвищує стійкість критичної інфраструктури. Крім того, результати можуть бути застосовані для розроблення сучасних протоколів кризового менеджменту та комунікацій, що, відповідно, забезпечить швидшу й ефективнішу координацію між усіма суб'єктами національної безпеки. Запропоновані у кваліфікаційній роботі магістра теоретичні положення та висновки можуть бути використані у навчальному процесі Харківського національного університету імені В.Н. Каразіна та інших вищих навчальних закладів при розробці та викладанні дисциплін, за програмами підготовки магістрів міжнародних відносин, суспільних комунікацій та регіональних студій.

5. Загальна оцінка дипломної роботи та її допуск/не допуск до захисту перед ЕК. Кваліфікаційна робота магістра Гончаренко Владислава Сергійовича на тему «Система інформаційної безпеки Ізраїлю: досвід для України» заслуговує на позитивну, а її автор гідний присвоєння кваліфікації магістра міжнародних відносин, суспільних комунікацій та регіональних студій.

Керівник кваліфікаційної роботи,
кандидат політичних наук, доцент,
доцент кафедри міжнародних відносин,
міжнародної інформації та безпеки
Харківського національного

університету імені В.Н. Каразіна Пересипкіна І. В.

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
студента 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»
освітньо-професійної програми
«Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут
міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Гончаренко Владислава Сергійовича
на тему «Система інформаційної безпеки Ізраїлю: досвід для України»

1. Актуальність теми зумовлена зростанням масштабів та складності гібридних загроз, що дедалі більше впливають на національну безпеку держав, зокрема України. Ізраїль, який протягом десятиліть перебуває в умовах постійної зовнішньої небезпеки, виробив унікальну модель комплексного захисту інформаційного простору, що поєднує технологічну інноваційність, інституційну узгодженість та високий рівень суспільної стійкості. Саме тому вивчення його досвіду набуває особливої ваги в сучасних умовах, коли Україна стикається з інтенсивними кібератаками, інформаційно-психологічними операціями та спробами дестабілізації з боку РФ. Зокрема, важливим є аналіз взаємодії військових, розвідувальних і цивільних структур Ізраїлю, впровадження передових технологій штучного інтелекту та систем раннього виявлення загроз, а також формування культури інформаційної безпеки на рівні громадянського суспільства. Крім того, ізраїльська модель демонструє ефективність принципу «превентивності», який може бути корисним для України в умовах постійної ескалації цифрових ризиків. Таким чином, дослідження даної теми має не лише теоретичне, а й вагоме практичне значення, оскільки дозволяє адаптувати найкращі міжнародні практики до українського контексту та сприяти зміцненню національної стійкості.

2. Характеристика якості виконання кожного розділу роботи. У першому розділі «ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ» розглянуто еволюцію поняття «інформаційної безпеки» у сучасних міжнародних відносинах та основні підходи до формування міжнародної системи її забезпечення; визначено теоретичні засади та ключові моделі розбудови національних систем інформаційної безпеки

У другому розділі «СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІЗРАЇЛЮ» розкрито інституційну та нормативно-правову складові системи інформаційної безпеки Ізраїлю.

У третьому розділі «ВИКОРИСТАННЯ ІЗРАЇЛЬСЬКОГО ДОСВІДУ У ФОРМУВАННІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ» виявлено

практичні кейси функціонування системи інформаційної безпеки Ізраїлю, зокрема механізми нормативно-правового регулювання, міжвідомчої координації та державно-приватного партнерства; встановлено специфіку моделей Ізраїлю та України у сфері інформаційної безпеки, сучасний стан і ключові проблеми української системи та виявити напрями імплементації ізраїльського досвіду

3. Ступінь обґрунтованості висновків роботи. Висновки достатньо обґрунтовані та відповідають поставленим завданням у кваліфікаційній роботі.

4. Використання в дипломній роботі останніх досліджень. Варто відзначити, що автором проаналізовано значний обсяг фактологічного матеріалу. Був здійснений детальний аналіз обраної проблематики, наукові методи використані коректно. Проаналізовано великий спектр вітчизняної та зарубіжної наукової літератури.

5. Позитивні сторони роботи. Зміст роботи повністю відповідає обраній темі. Робота складається зі вступу, трьох розділів, висновків і списку використаних джерел. В дипломній роботі присутня системність та послідовність викладення матеріалу.

6. Недоліки роботи. Доцільно було б більше уваги приділити теоретичній частині дослідження, однак це не впливає негативно на дипломну роботу в цілому.

7. Практичне значення. Практичне значення отриманих результатів щодо вивчення системи інформаційної безпеки Ізраїлю для органів влади України полягає не лише у можливості адаптації успішних підходів, але й у формуванні цілісного бачення того, як держава може ефективно діяти в умовах постійних гібридних загроз.

8. Загальна оцінка кваліфікаційної роботи. Кваліфікаційна робота магістра Гончаренко Владислава Сергійовича на тему «Система інформаційної безпеки Ізраїлю: досвід для України» заслуговує на позитивну, а її автор гідний присвоєння кваліфікації магістра міжнародних відносин, суспільних комунікацій та регіональних студій.

Рецензент:
кандидат політичних наук, доцент,
доцент кафедри політології,
соціології і культурології
Харківського національного педагогічного
університету імені Г. С. Сковороди КАЛЮЖНА Юлія Іванівна

Підпис [illegible] засвідчується зав. [illegible]

04.12.2025