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: **«ІНФОРМАЦІЙНИЙ ВИМІР НАЦІОНАЛЬНОЇ БЕЗПЕКИ ВЕЛИКОЇ БРИТАНІЇ»**

Виконала:

студентка 2-го курсу, групи УМІБ–61

спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»

ОПП «Міжнародна інформаційна безпека»

Сободєєва Анастасія Олександрівна

(прізвище, ім’я, по батькові)

Керівник:

д.політ.н., доц. Вінникова Наталія Анатоліївна

(науковий ступінь, вчене звання, прізвище, ім’я, по батькові)

Рецензент:

к. держ. упр., доц. Гришина Наталія Михайлівна

(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**

**завідувач кафедри**

_____ **Наталія ВІННИКОВА**

(Підпис) (ім'я, прізвище)

«2» червня 2025 року
(зі змінами від 10.09.2025; 06.10.2025)

**ЗАВДАННЯ**

**на кваліфікаційну роботу магістра**

Сободєєвої Анастасії Олександрівни

(прізвище, ім'я та по батькові)

1.Тема роботи «Інформаційний вимір національної безпеки Великої Британії» керівник роботи д.п.н., проф. Вінникова Наталія Анатоліївна

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «02» червня 2025 року № 4001-5/1324 (зі змінами від «10» вересня 2025 року № 4001-5/3049; «6» жовтня 2025 року № 4001-5/3656.

2. Строк подання здобувачем вищої освіти роботи 21 листопада 2025 р.

3. Перелік питань, які потрібно розробити:

1. Інституційна архітектура та ключові державні органи у сфері інформаційної та кібербезпеки.

2. Нормативно-правове забезпечення інформаційної безпеки: національні стратегії та міжнародні стандарти.
3. Політичні інструменти, механізми управління ризиками та системи підзвітності у сфері інформаційної безпеки.
4. Основні загрози та виклики у сфері інформаційної та кібербезпеки Великої Британії.
5. Взаємодія Великої Британії з іншими акторами міжнародних відносин у сфері інформаційної безпеки.
6. Перспективи розвитку національної інформаційної політики та кіберстратегії Великої Британії з урахуванням сучасних геополітичних трендів.

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 | 12.05.2025-30.06.2025 |
| 2 | Підготовка вступу і розділу 1 КРМ | 22.09.2025-30.09.2025 |
| 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: 02 червня 2025 року

**Здобувач вищої освіти** _____ Анастасія СОБОДЄЄВА

(підпис) (ім’я, прізвище)

**Керівник роботи** _____ Наталія ВІННИКОВА

(підпис) (ім’я, прізвище)

# ЗМІСТ

# ВСТУП

У сучасному світі, в умовах стрімкої цифровізації суспільства та зростання кіберзагроз інформаційна безпека стала ключовим чинником національної безпеки сучасних держав. Інформаційний вимір охоплює не лише технічний аспект, а й політичний, соціальний, правовий і комунікаційний рівні, що визначають стійкість державного управління. Велика Британія є однією з провідних держав у формуванні комплексної системи інформаційної безпеки.

У 2024–2025 рр. Велика Британія зіткнулася зі стрибком складних кіберінцидентів і інформаційних загроз, що напряму зачіпають демократію, економіку та критичні послуги. На цьому тлі питання інформаційної безпеки набуло статусу ключового виміру національної та міжнародної безпеки, оскільки ризики для виборчої інфраструктури, ланцюгів постачання та цифрових платформ виявили системні вразливості інституційного та нормативного характеру. Зрештою, у 2025 р. уряд оприлюднив оновлені рамки безпеки та економіки кіберсектора, що засвідчило перехід від реактивного до проактивного регулювання й потребу в інтегрованій політиці стійкості, яка поєднує правові, технологічні та комунікаційні інструменти. Сукупність цих чинників обґрунтовує своєчасність дослідження інформаційного виміру національної безпеки Великої Британії, з акцентом на оцінюванні ефективності чинних стратегій, інституційної спроможності та можливостей їхнього вдосконалення.

Проблематика інформаційного виміру національної безпеки Великої Британії активно досліджується у працях вітчизняних та зарубіжних науковців. Серед зарубіжних авторів значний внесок зробив Девід Оманд [55]. В українській науковій думці питання інформаційної безпеки як складової національної безпеки висвітлюють, зокрема, Г. Почепцов та В. Бурячок, які досліджують концепти інформаційного простору, кіберзагроз та

гібридних війн [4,6].

**Метою** нашого дослідження є визначення інформаційного виміру національної безпеки Великої Британії.

Для досягнення мети у роботі поставлено наступні **завдання**:

1. Встановити теоретичні основи поняття «інформаційна безпека» та її місце в системі національної безпеки.
2. Визначити нормативно-правову базу Великої Британії у сфері інформаційної безпеки.
3. Виявити основні інформаційні загрози, що постають перед Великою Британією у XXI столітті.
4. Визначити ефективність реалізації стратегічних документів у сфері інформаційної безпеки.
5. Сформувати рекомендації щодо удосконалення політики інформаційної безпеки та можливого використання британського досвіду в Україні.

**Об’єктом** дослідження є національна безпека Великої Британії.

**Предметом** дослідження виступає інформаційний вимір національної безпеки Великої Британії.

Теоретико-методологічною основою дослідження стали праці українських та зарубіжних учених у галузі міжнародної інформаційної безпеки, теорії національної безпеки та міжнародних відносин, а також ключові концепції стратегічного управління та забезпечення інформаційної безпеки. Зокрема, робота спирається на підходи комплексного управління державними та суспільними ресурсами, теорію інформаційного протиборства, модель управління ризиками у сфері інформаційної безпеки, а також положення національних та міжнародних стратегічних документів щодо забезпечення інформаційної безпеки.

У дослідженні застосовано такі **методи**:

– історико-порівняльний, для аналізу еволюції підходів Великої Британії до інформаційної безпеки;

– системний, для розгляду інформаційного виміру як частини загальної системи національної безпеки;

– інституційний, для вивчення діяльності державних органів у сфері кібер- та інформаційної безпеки;

– Метод аналізу документу

Інформаційну базу склали офіційні документи уряду Великої Британії, аналітичні звіти, наукові публікації, а також матеріали періодичних видань і офіційних ресурсів.

Результати дослідження можуть бути використані для вдосконалення освітніх програм з міжнародної інформаційної безпеки, розробки рекомендацій для державних органів України щодо формування політики інформаційної стійкості, а також для підготовки аналітичних звітів у сфері національної безпеки. Отримані висновки можуть слугувати базою для подальших порівняльних досліджень політик інформаційної безпеки країн ЄС та НАТО.

**Гіпотеза** нашого дослідження полягає в тому, що комплексна інтеграція інформаційного виміру у систему національної безпеки Великої Британії, заснована на поєднанні технічних, правових і стратегічних інструментів, забезпечує підвищення стійкості держави до інформаційних загроз і може бути ефективною моделлю для інших демократичних країн.

**Апробація** результатів дослідження була проведена на всеукраїнському науково-практичному круглому столі «Стратегічні напрями зовнішньої політики та дипломатії країн світу».

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, який налічує близько 80 найменувань.

Загальний обсяг роботи становить приблизно 74 сторінки, з яких основного тексту 62 сторінки.

# РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОГО ВИМІРУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

## 1.1 Поняття та сутність інформаційного виміру національної безпеки

У XXI столітті інформаційний простір став ключовим чинником формування національної безпеки. Його роль зросла через глобальну цифровізацію, розвиток мережевих технологій, стрімке поширення соціальних медіа, а також появу нових форм загроз таких як кіберзлочинність, інформаційні махінації, маніпуляції громадською думкою тощо. Відповідно, поняття інформаційного виміру національної безпеки охоплює весь комплекс відносин, процесів і механізмів, пов'язаних із формуванням, передачею, захистом і використанням інформації в інтересах суспільства та держави.

Термін «інформаційна безпека» у науковій літературі має міждисциплінарний характер. Згідно з визначенням британського дослідника Девіда Оманда, колишнього директора Центру урядових комунікацій, інформаційна безпека це не лише технічна категорія, а передусім здатність держави адаптуватися до змін, зберігати стабільність під впливом зовнішніх інформаційних тисків і приймати стратегічні рішення в умовах невизначеності [55].

Автор підкреслює, що інформаційна безпека має бути інтегрованою складовою політичної культури управління, адже її порушення безпосередньо впливає на державну стабільність і довіру суспільства до влади.

Подібної думки дотримується Бен Б'юкенен, дослідник Гарвардського університету, який у праці «Хакери і держави» наголошує, що у цифрову епоху межа між кібербезпекою та інформаційною безпекою фактично стирається. Кібератаки, шпигунство та інформаційні маніпуляції стають не лише питанням технічного захисту, а й політичним інструментом впливу, який формує міжнародну поведінку держав [5].

Інформаційний аспект національної безпеки включає кілька важливих

елементів: технологічний, політичний, правовий і соціальний. З технологічної точки зору це захист важливих інформаційних систем, мереж, баз даних, комунікацій та телекомунікацій. На політичному рівні це розробка законів, стратегій, установ та процесів, які дозволяють реагувати на загрози. Соціальний аспект стосується здатності людей розрізняти правдиву та неправдиву інформацію, бути обізнаними і вірити у офіційні джерела, що допомагає суспільству зупинити дезінформацію.

У цьому контексті важливо відзначити саме британський досвід, який вважається одним із найпослідовніших у світі. У Національній кіберстратегії Великої Британії 2022 року уряд визначив п’ять головних пріоритетів, серед яких посилення кіберстійкості держави, розвиток технологічного потенціалу, протидія інформаційним загрозам і забезпечення довіри громадян до цифрових сервісів [10].

Документ підкреслює, що забезпечення інформаційної безпеки має бути обов’язком усіх: уряду, бізнесу, університетів та громадян. Серед організацій, які відповідальні за інформаційну безпеку в Британії, зокрема згадують Національний центр кібербезпеки, Центр урядових комунікацій та Національні кіберсили, які створили разом з Міністерством оборони. За дослідженням Королівського Об'єднаного інституту оборонних досліджень, британська стратегія ґрунтується на ідеї «всебічного суспільного підходу», який передбачає участь уряду, приватних підприємств та громадських організацій у забезпеченні кібер- та інформаційної безпеки.

У науковій літературі існують різні підходи до визначення сутності інформаційного виміру. Джозеф Най у праці «Кіберсила» розглядає інформацію як форму влади: контроль над нею визначає політичний вплив держави у глобальній системі. Він стверджує, що інформаційна безпека  це не лише захист, а й стратегічна можливість для проєкції «м’якої сили» [52].

Джейсон Ліндсей у статті «Кібербезпека» пропонує технократичний підхід, у якому кібер- та інформаційна безпека є системою управління ризиками для збереження цілісності інформації.

На думку українського дослідника Георгія Почепцова, інформаційна безпека це не лише захист від фейків чи кібератак, а передусім «здатність держави та суспільства підтримувати стійку картину реальності, не дозволяючи противнику змінювати її через інформаційні маніпуляції» [4].

Такий підхід наближає українське розуміння до британського, де питання безпеки в інформаційному просторі розглядається як технічне, так і стратегічне, як частина більш широкої системи управління ризиками та формування національної стійкості.

Отже, інформаційний аспект національної безпеки це багатовимірна категорія, яка поєднує технічні, політичні, правові та соціальні елементи. Його суть полягає не тільки у запобіганні загрозам, а й у створенні умов для стабільної роботи держави у цифровому середовищі. Велика Британія має ефективну модель цього аспекту, де стратегічне планування, взаємодія інституцій і суспільна відповідальність об’єднуються в єдину систему.

## 1.2 Інформаційна безпека як складова міжнародної безпеки

Сучасні міжнародні відносини зазвичай вважаються інформаційно залежними. Інформація стає стратегічним ресурсом, а її контроль фактором впливу в політиці, економіці та армії. У цьому контексті інформаційна безпека є не лише частиною внутрішнього управління держави, а й важливою складовою міжнародної безпеки. Вона включає різноманітні міжнародні правила, установи та механізми, які призначені для запобігання, виявлення та реагування на загрози, що мають транскордонний характер.

Проблема інформаційної безпеки вийшла на міжнародний рівень у середині 1990-х років, коли Генеральна Асамблея ООН уперше включила питання «досягнення міжнародної інформаційної безпеки» до порядку денного. У резолюціях ГА ООН № 53/70 (1998), № 68/243 (2013) та № 74/29 (2019) підкреслюється необхідність вироблення універсальних правил поведінки держав у кіберпросторі та обміну інформацією щодо кіберзагроз [68].

Ці документи заклали основу для формування глобального режиму

інформаційної безпеки, заснованого на принципах суверенітету, невтручання у внутрішні справи та міжнародного співробітництва.

Однією з найактивніших організацій, які формують стандарти міжнародної кібер та інформаційної безпеки, є Організація Північноатлантичного договору. Починаючи з 2002 року, кібербезпека офіційно визнана елементом колективної оборони Альянсу. У Стратегії НАТО з кібероборони 2022 року наголошено, що «кіберзагрози можуть мати наслідки, еквівалентні збройному нападу», а отже, кіберпростір визнано окремою операційною сферою оборони поряд із сушею, морем, повітрям і космосом [49].

Цей підхід демонструє перехід від технічного розуміння інформаційної безпеки до геополітичного.

Значну роль у формуванні експертної та правової бази відіграє Центр передового досвіду з кібероборони НАТО, розташований у Таллінні. Саме він у 2013–2017 роках розробив «Талліннський посібник з міжнародного права, що застосовується до кібероперацій», який став основоположним документом для тлумачення правил ведення кіберконфліктів. Цей документ визнає, що держави мають право на самооборону у випадку масштабних кібератак, але також зобов’язані дотримуватись принципів пропорційності та уникати втручання у внутрішні справи інших країн.

Європейський Союз також активно інтегрує питання інформаційної безпеки у свою зовнішню та безпекову політику. У 2020 році ЄС ухвалив оновлену Стратегію кібербезпеки для цифрового десятиліття, де визначено, що стійкий цифровий простір є основою демократії, економічного розвитку та суверенітету держав-членів.

Важливим напрямом є розвиток програми «Інструментарій кібердипломатії», яка забезпечує спільні дипломатичні реакції ЄС на кібератаки, у тому числі через санкційні механізми [12].

На регіональному рівні активну роль відіграє Організація з безпеки і співробітництва в Європі, яка з 2013 року впроваджує набір довірчих заходів у

сфері кібербезпеки, спрямованих на підвищення прозорості, обмін інформацією та запобігання ескалації конфліктів у кіберпросторі. Вони включають повідомлення про кіберінциденти, створення контактних пунктів та взаємне інформування про національні стратегії.

На думку Джозефа Ная, інформаційна безпека є фундаментом нової форми влади, яка поєднує технологічні можливості держав із їхніми політичними й дипломатичними ресурсами. Держава, що контролює інформаційні потоки, може впливати не лише на поведінку своїх громадян, а й на міжнародні відносини, поширюючи наративи та цінності [52].

Схожу думку висловлює Бен Б'юкенен, зазначаючи, що кібератаки та інформаційні операції дедалі частіше стають частиною державної політики, і тому інформаційна безпека повинна розглядатися як складова стратегічної стабільності у світі. Він називає це «цифровою холодною війною», у якій головна боротьба точиться не за територію, а за контроль над даними, технологіями та свідомістю людей [5].

З точки зору британських аналітичних центрів, інформаційна безпека це один із ключових напрямів міжнародного партнерства. Королівський інститут міжнародних відносин у звіті «Кібербезпека та геополітика» підкреслює, що без спільних підходів демократичних держав до інформаційної безпеки існує ризик фрагментації глобального кіберпростору. Автори наголошують, що міжнародна співпраця має базуватися на принципах прозорості, верховенства права та поваги до прав людини [23].

Британський досвід показує, як ефективно можна інтегрувати національну інформаційну безпеку в міжнародні структури. Велика Британія, яка є членом НАТО, G7 та Співдружності націй, активно участь у створенні різноманітних міжнародних форматів співпраці в сфері кібер- та інформаційної безпеки. Наприклад, у 2021 році Лондон започаткував «Стратегію Британської кібер безпеки для розвитку», яка має на меті допомогти країнам-партнерам підвищити свої кіберспроможності та забезпечити захист демократичних інститутів.

Для України питання міжнародної інформаційної безпеки набуло особливо гострого значення після початку російської агресії у 2014 році. Відтоді Україна стала полігоном для нових форм гібридних загроз, зокрема кібератак на державні установи, інформаційних операцій, кампаній з дезінформації та втручання у виборчі процеси. Ці виклики сприяли активнішій участі України у міжнародних ініціативах таких як співпраця з НАТО, ЄС, ОБСЄ, а також долученню до Київської ініціативи щодо інформаційної стійкості, започаткованої разом із партнерами з Великої Британії, Канади та Польщі [40].

Українські науковці, зокрема Георгій Почепцов і Віталій Бурячок, розглядають міжнародну інформаційну безпеку як «мережеву архітектуру», де поєднуються державні, приватні та суспільні ініціативи. За їхніми словами, рівень інформаційної безпеки на глобальному рівні визначається не лише технічними стандартами, але й здатністю країн координувати свої дії та забезпечувати єдиний підхід у боротьбі з інформаційними загрозами [4,6].

Отже, інформаційна безпека є важливою частиною міжнародної безпеки, оскільки інформаційні загрози мають транскордонний характер, і їх не можна нейтралізувати окремо від національних зусиль.

Сучасна система глобальної інформаційної безпеки створюється через діяльність міжнародних організацій, таких як ООН, НАТО, ЄС, ОБСЄ, а також завдяки участі ведучих країн: Великої Британії, США, Канади у розробці загальних стратегій і правил поведінки у кіберпросторі. Британський досвід, що базується на принципах партнерства, прозорості та суспільної відповідальності, є одним із найефективніших прикладів поєднання національної та міжнародної політики інформаційної безпеки.

## 1.3 Теоретико-методологічні підходи до аналізу інформаційного виміру національної безпеки

Дослідження інформаційного аспекту національної безпеки потребує широкого підходу, бо ця галузь поєднує багато факторів: політичні,

технологічні, правові, соціальні та психологічні. Інформаційна безпека одночасно є предметом державного управління, інструментом міжнародної політики та темою наукових досліджень у теоріях безпеки, міжнародних відносинах, комунікації та стратегічних дослідженнях.

Системний підхід розглядає інформаційну безпеку як частина національної безпеки, де технологічні, правові, інституційні та соціальні аспекти взаємодіють один з одним. Така позиція не дозволяє розглядати окремі засоби безпеки окремо, а враховує всю систему, як ціле, її розвиток та наслідки взаємодії окремих частин, таких як військові, політичні, економічні та соціальні. У сучасному світі до цих підсистем додається ще один важливий елемент, а саме інформаційний. Теоретично це розуміння базується на тому, що безпека це складне явище, і зміни в одному аспекті (наприклад, в інформаційному) можуть впливати на інші аспекти (економічний, політичний, суспільний), призводячи до серії наслідків.

Аналітична операціоналізація системного підходу зазвичай включає три рівні. На мікрорівні аналізуються окремі організації, процеси та технології (наприклад, підрозділи, які реагують на інциденти, процедури управління вразливостями, локальні правила комунікації), що дозволяє оцінити роботу основних елементів системи. На мезорівні увага звертається до взаємодії між різними секторами: державних органів, операторів критичної інфраструктури, цифрових платформ, академічних інститутів та професійних груп де важливими є стандартизовані засоби передачі даних, загальні навчання та узгоджені процедури реагування на інциденти. На макрорівні оцінюються стратегії, закони, міжнародні зобов’язання, а також соціальні аспекти, особливо довіра та ставлення до ризиків, без яких неможлива підтримка суспільства у діях з безпеки.

Методичний інструментарій системного підходу включає: картування системи із фіксацією акторів, повноважень та потоків; побудову причинно-наслідкових петель для виявлення точок важеля; сценарне моделювання та стрес-тестування з акцентом на каскадні наслідки а також матриці

взаємозалежностей, що дозволяють оцінити перехресний вплив регуляторних змін (наприклад, посилення вимог до ланцюгів постачання телекомунікацій) на декілька секторів одночасно. Така комбінація дає можливість переходити від опису інцидентів до аналізу структурних причин уразливості та обґрунтування системних інтервенцій.

Для оцінювання системної стійкості доцільно застосовувати багаторівневі метрики. До вхідних належать частка витрат на безпеку, охоплення підготовкою персоналу, ступінь контрактної «прошитості» вимог до постачальників. Процесні метрики відбивають якість операцій, середній час виявлення й відновлення, інтенсивність та своєчасність обміну розвідданими про кіберзагрози між державою і приватним сектором. Вихідні метрики фіксують вплив у публічній площині: частка інцидентів без тривалих перерв у наданні послуг, довіра громадян до цифрових сервісів уряду, стабільність виборчих процесів. Важливо, що остання група метрик «переводить» технічні зусилля в категорії суспільної легітимності — ключового ресурсу безпеки [55].

Застосування до кейсу Великої Британії передбачає, по-перше, чітке окреслення меж аналізу (кіберзахист державного сектору, критична інфраструктура, виборчі процеси, регуляція цифрових платформ, стратегічні комунікації); по-друге, картування ключових потоків (оперативна кіберінформація, нормативні та публічні сигнали, міжнародні канали); по-третє, аналіз петель зворотного зв’язку, що формують траєкторію довіри та спроможності системи; і, по-четверте, виявлення «вузьких місць» (залежність від окремих постачальників, прогалини у платформенній регуляції, кадрові обмеження) та визначення точок важеля. Такий алгоритм узгоджується з логікою британських стратегічних документів, що інтегрують технічні, правові та соціальні інструменти стійкості.

Вартість системного підходу полягає в тому, що він дозволяє розуміти, як загрози можуть впливати через межі країн та як вони пов'язані між собою. Крім того, він допомагає зрозуміти додаткові наслідки, які часто мають більше впливу, ніж сама технічна шкода (наприклад, вплив на репутацію, політику,

економіку). Однак у цьому підході є певні обмеження. Наприклад, потрібні якісні дані про зв'язки та зміни, що відбуваються. Також може виникнути проблема, коли спрощений підхід приводить до неправильного розуміння складних ситуацій. Інша проблема, це відхилення між ідеальною моделлю та реальними умовами, які підтримуються не достатніми ресурсами або волею влади. Тому краще поєднувати системний аналіз з інституційним, політичним та комунікаційним підходами, щоб узгодити результати з реальними ситуаціями та сприйняттям суспільства.

Інституційно-політичний підхід виходить із того, що інформаційна безпека є насамперед функцією державного управління, де результат визначається не лише рівнем технічного захисту, а й архітектурою інститутів, розподілом повноважень, якістю координації, регуляторними механізмами та суспільною довірою до рішень. У цій логіці «безпека» інтерпретується як стан керованості ризиків і здатність уряду підтримувати суспільну впевненість через прозорі правила, відповідальність та ефективні процедури реагування [55].

Рівні аналізу:

- Макрорівень охоплює стратегічні та правові рамки (стратегії, закони, стандарти, міжнародні зобов'язання), які задають цілі, принципи й інструменти політики.
- Мезорівень фокусується на міжвідомчій взаємодії та державно-приватних партнерствах: формалізованих каналах обміну даними, спільних навчаннях, кризових штабах та секторальних форумах.
- Мікрорівень стосується практик окремих органів і регуляторів: процедур інцидент-респонсу, аудиту та нагляду, механізмів публічної комунікації, що перетворюють нормативні настанови на операційну спроможність [36].

Аналітично доцільно розрізняти чотири фази: ідентифікація проблеми та сек'юритизація (формулювання екзистенційної значущості загроз для критичних функцій); дизайн інструментів (вимоги до ланцюгів постачання, обов'язки повідомлення про інциденти, регулювання платформ); імплементація

та координація (протоколи обміну, спільні навчання, кризові комунікації); оцінювання та підзвітність (аудити, показники стійкості, публічні звіти, парламентський контроль). Британська практика характеризується поєднанням «м'яких» інструментів (стандарти, партнерства) із «твердими» регуляторними важелями (обов'язкові вимоги, санкції, нагляд) [23].

Інституційно-політичний підхід підкреслює, що без довіри політика безпеки не може бути ефективною. За думкою Д. Оманда, безпека це головним чином стан впевненості суспільства, коли основні ризики добре контролюються, з цього витікає необхідність прозорості, послідовності та відповідальності під час подій та кризових ситуацій [55].

Перевага цього підходу полягає в тому, щоб пояснити, чому однакові технічні методи можуть давати різні результати в різних умовах: вирішальним є взаємодія інституцій, правові стимули й культура відповідальності. Проте існують певні обмеження: може виникнути ризик надмірного оптимізму щодо законодавства (переоцінка його впливу без відповідних ресурсів), складність приписування відповідальності у системах з багатьох учасників, а також залежність від політичних коливань та рівня довіри. Отже, інституційний аналіз краще поєднувати з системним (щоб врахувати зв'язки між різними секторами), сек'юрітизаційним (для аналізу легітимності інструментів) та технічним або ризик-орієнтованим.

Соціально-комунікаційний підхід розглядає інформаційну безпеку як частину процесів взаємодії та соціальних механізмів, які забезпечують довіру. У цьому підході важливо не тільки захист комунікаційних каналів, а й те, як текст, образ, історія та платформи впливають на сприйняття ризиків, легітимність установ та поведінку суспільства. Безпека у цій концепції це здатність керувати середовищем інформації та стійкість людей до впливу. Також це здатність держави забезпечувати чітку, своєчасну і зрозумілу комунікацію, яка поєднується з інфраструктурою перевірки фактів, медіаграмотності та регулювання соціальних платформ.

По-перше, у межах досліджень «інформаційного безладу» вирізняють

дезінформацію, місінформацію та малінформацію як різні за наміром і наслідками явища, що поширюються мережевими каналами та потребують багаторівневих відповідей, а саме від платформної модерації до інформаційної освіти [70].

По-друге, комунікаційна школа наголошує на боротьбі за «картину світу» аудиторій: стратегічні комунікації мають підтримувати стабільні когнітивні рамки, які знижують чутливість суспільства до маніпуляцій і підвищують готовність до захисних практик [4].

По-третє, прикладні дослідження фіксують селективні ефекти платформної архітектури (алгоритмічні рекомендації, мережеві каскади), що посилюють видимість координованої неавтентичної поведінки та впливових операцій; відтак потрібна комбінація технологічних, поведінкових і нормативних інструментів протидії [49].

Британська модель поєднує взаємодію уряду, приватних платформ, академії та громадянського суспільства зі стратегічними комунікаціями державного сектора. Регуляторна рамка інтегрує вимоги прозорості та відповідальності платформ; паралельно урядові стратегії передбачають розвиток механізмів виявлення та стримування впливових операцій, а також підтримку фактчекінгових ініціатив під час виборчих циклів [10].

Підхід залежить від доступності даних і готовності платформ до співпраці, існує ризик надмірної модерації та нормативної невизначеності. Це зумовлює потребу поєднувати соціально-комунікаційний підхід із системним (для врахування міжсекторних залежностей) та інституційно-політичним (для закріплення процедур, підзвітності й правових гарантій), а також здійснювати незалежний аудит інтервенцій.

Узагальнюючи, три розглянуті підходи утворюють повну аналітичну структуру для оцінки інформаційного аспекту національної безпеки. Системний підхід розглядає інформаційну безпеку як частина державної безпеки, де технічні, правові, організаційні та соціальні елементи взаємозв’язані між собою через мережі зв’язків і впливу. Він виявляє зв’язки між різними секторами і

навіть каскадні наслідки злочинів. Інституційно-політичний підхід розглядає ці зв’язки у контексті державного управління та суспільної політики, акцентує увагу на структурі установ, поділі повноважень, координації та регулювальних механізмів, що дозволяє перетворити стратегічні рішення на реальну дію. Соціально-комунікаційний підхід доповнює попередні два, пояснюючи, як комунікації, платформи та наративи впливають на довіру, розуміння ризиків і поведінку людей, а відтак, на довіру до підхідних рішень. Всього це створює загальну рамку, яка дає: структурну уяву про систему (хто з ким зв’язаний, яким чином та через що); можливість контролю через установчі механізми (стандартів, нагляд, державно-приватні взаємодії, процедури реагування); стійкість суспільства завдяки прозорим комунікаціям, управлінню через платформи та розумінню медіа.

**Висновки до розділу 1**

У першому розділі визначено основні поняття та розкрито складний характер інформаційного виміру національної безпеки. Показано, що інформаційна безпека перевищує простий технічний захист систем і включає правові, інституційні та соціальні аспекти, які впливають на управління ризиками, законність діяльності держави, стабільність важливих функцій суспільства та здатність держави діяти у міжнародному середовищі.

У розділі роз’яснено важливість міжнародного контексту для розуміння інформаційної безпеки та розглянуто роль Великої Британії у євроатлантичних структурах безпеки.

Встановлено, що національні підходи ефективні лише в взаємодії з міжнародними нормами, процедурами та механізмами, які допомагають збільшити координацію, сумісність, відповідальність та ефективність у сфері інформаційної безпеки.

Теоретична основа розділу ґрунтується на трьох взаємозв'язаних підходах.

Системний підхід дає загальне уявлення про інформаційну безпеку як частину державної безпеки, показує зв'язки між різними секторами, наслідки

інцидентів та можливості підвищити стабільність. Інституційно-політичний підхід зосереджується на управлінні державою і публічній політиці, розкриває роль інституцій, розподіл прав, координацію між агентами, регуляторні методи та взаємодію між державою та приватним сектором. Соціально-комунікаційний підхід пояснює, як засоби комунікації, навчальні матеріали та ресурси впливають на сприйняття ризиків, поведінку людей, довіру до інституцій та вплив на ефективність управлінських рішень.

Застосування розглянутих підходів до прикладу Великої Британії є відповідною методологічно.

Інституційна структура країни, яка включає агентства, що забезпечують комунікації, кібербезпеку, регулювання та виконавчу владу, демонструє співпрацю між стратегією, операціями, нормами та публічною відповідальністю. Інтеграція різних інструментів забезпечує поступовий перехід від реакційного стилю до управління ризиками та формування підтримки суспільства.

Гіпотеза, сформульована у вступі, про те, що ефективність інформаційного виміру національної безпеки залежить від якості матеріальної зв’язки, зрілої комунікаційної стратегії та правових норм, отримала теоретичне підґрунтя.

Далі цю гіпотезу потрібно перевірити за допомогою аналізу документів, інституційних ролей, емпіричних подій та оцінки ефективності за ключовими показниками.

Підсумовуючи все зазначене, перший розділ виконав дві основні функції: по-перше, визначив концептуальну базу та методологічні принципи дослідження, по-друге, розкрив логіку подальших аналізів, які будуть включати вивчення взаємозв’язків між інституційною архітектурою, процесами управління ризиками, комунікаційними стратегіями та реальними результатами забезпечення інформаційної безпеки в Великій Британії.

# Розділ 2. ІНФОРМАЦІЙНИЙ ВИМІР НАЦІОНАЛЬНОЇ БЕЗПЕКИ ВЕЛИКОЇ БРИТАНІЇ

## 2.1. Інституційна архітектура та нормативно-правові рамки інформаційної безпеки Великої Британії

Інституційна структура інформаційної безпеки Великої Британії побудована за принципами «всеурядового» і «суспільно орієнтованого» підходів. Ці підходи об'єднують стратегічне планування, оперативну готовність та регуляторний контроль у єдину систему, яка підлягає контролю. Основним документом є «Національна кіберстратегія 2022 року», що визначає мету держави у кіберпросторі, її основні напрямки, роль ключових органів, способу співпраці з приватним сектором та напрямки міжнародного співробітництва. У стратегії підкреслюється важливість одночасного захисту на всіх рівнях, розвитку національних можливостей та про активної зовнішньої політики у сфері кібер- та інформаційної безпеки.

Операційне ядро системи становлять Центр урядового зв’язку та Національний центр кібербезпеки, інтегровані інституційно й функціонально. Національний центр кібербезпеки виконує роль технічного авторитету і «єдиної точки контакту» держави з бізнесом та операторами критичної інфраструктури: розробляє керівництва і стандарти, забезпечує запобігання, виявлення та реагування на інциденти, координує обмін розвідданими про кіберзагрози та розвиває інструменти активного кіберзахисту. Такий розподіл функцій формує наскрізну вертикаль від вироблення стандартів до практичного менеджменту інцидентів і повернення досвіду у політику [10].

Однією з частин архітектури є Національні кіберсили - партнерство між різними відомствами, що відповідає за дії в кіберпросторі та через нього, з метою запобігання, протидії та захисту національних інтересів. Встановлення цієї системи як стабільної структури говорить про те, що країна переходить від просто відповіді на події до того, щоб керувати застосуванням державної сили в

цифровому середовищі, у дотриманні національних та міжнародних прав.

Стратегічна організація безпеки державних установ здійснюється у рамках урядових структур, які відповідають за узгодження політики, стандартів та відповідальності.

Це визначене у «Урядовій стратегії кібербезпеки на 2022–2030 роки», яка встановлює вимоги щодо управління ризиками, звітності про інциденти, незалежного аудиту, відповідальності керівництва та показників, які вимірюють ефективність (наприклад, час виявлення та відновлення проблем, рівень зрілості заходів, відповідність вимогам постачальників). Постійні звіти про виконання стратегій підтримують прозорість та дозволяють оцінювати досягнення за визначеними показниками [9].

Нормативно-правова система підтримує інституційну структуру за допомогою жорстких регуляторних інструментів. У сфері електронних комунікацій діють закон і кодекс практик щодо безпеки телекомунікацій, які встановлюють обов’язкові організаційні та технічні заходи, вимоги до моніторингу, повідомлення про компрометації, аудит відповідності та оцінку постачальників. Разом з тим режим онлайн-безпеки, який перебуває під наглядом профільного регулятора, встановлює поетапні обов’язки для провайдерів платформних послуг: оцінку ризиків, системний дизайн безпеки, звітність, нагляд і можливість застосування санкцій у разі невиконання вимог. Всі ці правила забезпечують передбачуваність і контрольованість регуляторного середовища для держави та ринку.

Взаємодія держави з приватним сектором є інституціоналізованою через формалізовані механізми: обмін розвідданими про загрози, секторальні хаби, спільні навчання та «вшивання» вимог кіберстійкості у державні закупівлі й комерційні контракти. Така конфігурація скорочує часові лаги реагування, підвищує відтворюваність найкращих практик і зміцнює довіру між державою та бізнесом у питаннях критичних послуг.

Міжнародний контур політики доповнює національні механізми. На рівні Організації Північноатлантичного договору визначено засади кібероборони,

взаємодії союзників і сумісності підходів до захисту мереж та операцій. В європейському вимірі діє санкційний режим протидії зловмисним кібератакам, який створює інструменти спільної дипломатичної відповіді на загрози, що мають значний вплив на безпеку держав. Для Сполученого Королівства це означає узгодження стандартів, колективне стримування та підвищення легітимності заходів у багатосторонньому форматі [48].

Узагальнюючи, інституційна структура Великої Британії поєднує стратегічну організацію на рівні уряду, технічний центр з компетентністю та реагуванням, можливості вести активні кібероперації та багаторівневий контроль, який підтримується комплексом правових правил і процесів публічного звітності. Впровадження з євроатлантичними стандартами, санкційними інструментами, а також формальна співпраця з приватним сектором забезпечує управління ризиками, стійкість важливих функцій і відповідність міжнародним нормам.

Крім основних державних органів, у системі інформаційної безпеки Великої Британії виділяються регіональні та секторні хаби, які забезпечують координацію між урядом, місцевою владою та критичними галузями економіки. Наприклад, окремі галузеві центри відповідальні за енергетику, транспорт та охорону здоров’я, що дозволяє адаптувати стандарти безпеки до специфіки сектору. Ці хаби працюють у тісній взаємодії з приватними компаніями та надають експертну підтримку у випадках кіберінцидентів, а також здійснюють регулярні оцінки кіберстійкості.

Додатково, регуляторні механізми передбачають використання публічних настанов і керівництв щодо кіберзахисту для всіх організацій державного та приватного секторів. Вони включають рекомендації з управління вразливостями, підготовки персоналу, оцінки постачальників і процедур реагування на інциденти. Підхід «захист за дизайном» і інтеграція вимог у державні закупівлі та контракти дозволяють підвищувати рівень безпеки ще на етапі планування та реалізації проєктів.

Важливою складовою є також система навчання та підвищення

кваліфікації фахівців державного і приватного секторів. Програми тренінгів, спільні навчання та моделювання кіберінцидентів забезпечують узгодженість дій та швидкість реагування на кризові ситуації. Це створює наскрізну систему безпеки, де стратегічна політика, технічна компетенція та підзвітність поєднуються у єдину модель управління інформаційними ризиками на національному рівні.

Таким чином, інституційна та нормативно-правова структура Великої Британії забезпечує комплексний підхід до інформаційної безпеки, поєднуючи стратегічне управління, оперативне реагування, нормативні вимоги, навчання персоналу та координацію з приватним сектором і міжнародними партнерами. Цей підхід дозволяє не лише зменшувати ймовірність інцидентів, а й оперативно локалізувати наслідки, підвищуючи стійкість критичних функцій держави та довіру суспільства.

## 2.2 Інструменти політики, процеси управління ризиками та публічна підзвітність

Практична модель забезпечення інформаційної безпеки у Великій Британії складається з комбінації «твердих» нормативно-правових інструментів, обов'язкових вимог, регуляторного нагляду, санкцій та «м'яких» управлінських та технічних засобів: керівництва, фреймворків оцінки ризиків, сервісів активного захисту. Разом вони утворюють єдину систему управління ризиками та циклів підзвітності. Основні напрями, принципи підходу, що відкриті для всіх і спрямовані на суспільство, а також розподіл ролей держави, підприємств і громадянського суспільства визначені в Національній кіберстратегії 2022 року і деталізовані в стратегічних документах для державного сектору.

Ключовим техніко-операційним інструментом є програма «Активний кіберзахист» Національного центру кібербезпеки, що знижує шкоду від масових «товарних» атак за допомогою масштабованих сервісів (захист доменної інфраструктури, виявлення фішингу, очищення шкідливого хостингу, раннє попередження). Логіка програми полягає у виконанні «малих дій у

великому масштабі», які в сукупності істотно зменшують поверхню ураження як у державному, так і в приватному секторах; у державному секторі ці сервіси прямо інтегровані в процеси кіберстійкості, передбачені урядовою стратегією [32].

Другим системоутворювальним елементом є «Рамка оцінювання кібербезпеки» від технічного авторитету, яка пропонує цілісну систему цілей, принципів і «індикаторів належної практики» для організацій, що забезпечують життєво важливі функції. Вона використовується як для самооцінювання, так і для незалежної перевірки зрілості контролів, спрямованої на управління ризиками до «прийнятного» рівня. На рівні державної політики структура Рамки оцінювання кібербезпеки узгоджується зі стратегічними цілями, забезпечуючи порівнянність результатів між секторами критичних послуг.

Нормативно-правова частина інструментарію охоплює секторальні режими. У сфері електронних комунікацій Закон про безпеку телекомунікацій і Кодекс практик установлюють юридично зобов’язальні вимоги до постачальників мереж і послуг: від управління вразливостями, моніторингу до оцінювання постачальників і інцидент-репортингу. Уряд регулярно оновлює підзаконні акти та керівництва з урахуванням еволюції загроз і технологій, зберігаючи режим обов’язковості та наглядової спроможності [65].

Для платформного середовища діє режим онлайн-безпеки під наглядом профільного регулятора, який поєднує ризик-орієнтовані обов’язки провайдерів (оцінювання та зменшення ризиків, безпека за задумом, прозорість, звітність) із поетапним упровадженням кодексів практики та вимог до захисту дітей. Регулятор публікує «дорожні карти» і бюлетені для індустрії, що дозволяє відслідковувати виконання обов’язків і формалізує канали підзвітності [54].

У секторах сутнісних послуг застосовуються регламенти про мережі та інформаційні системи, які встановлюють обов’язки щодо управління ризиками та повідомлення про інциденти для операторів життєво важливих послуг та надавачів цифрових сервісів; галузеві керівництва детальніше роз’яснюють ці обов’язки (наприклад, для сфер охорони здоров’я та водопостачання). Це

встановлює зв’язок з роллю технічного авторитету, який виступає як консультативний і перевірочний центр.

Важливим елементом режиму реагування залишається захист персональних даних: наглядовий орган наголошує на необхідності оцінки ризиків та повідомлення про інциденти із персональними даними протягом установлених строків, а також на наданні поетапної інформації, коли повна картина події ще не зібрана. Практика правозастосування і публічні роз’яснення формують дисципліну своєчасного інцидент-репортингу та підзвітності обробників даних.

Управління ризиками у державному секторі відповідно до урядової стратегії охоплює повний цикл. Включає в себе визначення та реєстрацію ризиків, оцінку ефективності контрольних заходів, профілактичні міри, зокрема через сервіси захисту. Також передбачає виявлення загроз, реагування, а саме визначення середнього часу виявлення та відновлення. Після подій проводиться аналіз і звітність про події. Річні звіти про виконання Національної кіберстратегії дозволяють оцінювати результати та забезпечують прозорість, враховуючи як відомчі, так і міжвідомчі пріоритети національної безпеки.

Публічна підзвітність реалізується через кілька каналів: по-перше, регулярні «прогрес-звіти» та відкриті матеріали центральних органів влади; по-друге, регуляторні документи і комунікації наглядових органів (коди практик, дорожні карти, бюлетені); по-третє, публічні керівництва та колекції методичних матеріалів технічного авторитету. У сукупності це створює передбачувану архітектуру прозорості, в межах якої як держава, так і приватні суб’єкти верифікують виконання обов’язків і підтверджують результативність інтервенцій [54].

Нарешті, інструментарій політики продовжує еволюціонувати під впливом оперативної обстановки. Актуальні звернення урядовців до бізнесу щодо приєднання до сервісів раннього попередження та підвищення готовності, а також новини регуляторного поля і практики розслідувань підкреслюють домінування ризик-орієнтованої логіки, де пріоритетами залишаються

скорочення часу реагування, прозорість та зменшення системного ризику для критичних функцій і прав громадян.

Британська система поєднує масштабовані технічні сервіси, уніфіковані рамки оцінювання, юридично обов'язкові вимоги для критичних інфраструктур і платформ, а також зрозумілі канали публічної підзвітності. Саме така комбінація дозволяє зменшувати ймовірність інцидентів, локалізувати їхні наслідки та підтримувати суспільну довіру як базову умову ефективності інформаційної безпеки.

Додатково, британська система інформаційної безпеки передбачає інтеграцію навчання та підвищення кваліфікації персоналу як ключовий елемент управління ризиками. Це включає регулярні тренінги для державних службовців, керівників критичних операторів та фахівців приватного сектору, симуляції кіберінцидентів, а також міжвідомчі навчальні вправи, які імітують реальні кібератаки та інциденти дезінформації. Такі заходи дозволяють оцінити готовність персоналу до реагування, відпрацювати координацію дій та скоротити час реагування на реальні загрози.

Особливу увагу приділено спільним платформам обміну розвідданими та координаційним хабам, які забезпечують швидкий обмін інформацією про кіберзагрози між державними органами, секторальними операторами та приватними компаніями. Це дозволяє мінімізувати часові лаги реагування на нові атаки, підвищує відтворюваність найкращих практик і зміцнює довіру між державою та бізнесом у питаннях критичних послуг.

У межах секторальної безпеки застосовуються інструменти незалежного аудиту та сертифікації, що дозволяють перевіряти ефективність заходів кіберзахисту та відповідність вимогам стандартів безпеки. Наприклад, для операторів критичних інфраструктур здійснюються регулярні перевірки готовності, оцінка відповідності протоколам кіберстійкості та аналіз інцидентів за минулі періоди. Подібні практики сприяють формуванню єдиного стандарту безпеки, який може застосовуватись у різних секторах [11].

Важливим аспектом є взаємодія з громадянським суспільством та

забезпечення прозорості інформаційної політики. Регулярні публічні матеріали, відкриті звіти та рекомендації для бізнесу й населення дозволяють формувати культуру кіберстійкості на рівні громадян, підвищують обізнаність про потенційні загрози та зменшують ризик соціальної інженерії. Також державні кампанії підвищують обізнаність щодо захисту персональних даних, відповідального використання цифрових сервісів та правил безпечної поведінки онлайн.

Ця комплексна конфігурація дозволяє не лише мінімізувати ризики інцидентів, а й забезпечує безперервне вдосконалення системи кіберзахисту та зміцнення суспільної довіри як ключового елемента національної безпеки.

## 2.3. Міжнародна взаємодія та зовнішній вимір інформаційної безпеки Великої Британії

Міжнародна кооперація є ключовою передумовою ефективності інформаційної безпеки Великої Британії, оскільки характер загроз: від державного кіберзухвальства до транснаціональної дезінформації та програм-вимагачів виходить за межі юрисдикцій і секторів. Уряд системно поєднує спроможності розвідки та кіберзахисту з дипломатичними інструментами, санкційною політикою та участю у партнерських форматах, що прямо закріплено у стратегічних засадничих документах останніх років.

Зокрема, «Національна кіберстратегія 2022» визначає Велику Британію «відповідальною демократичною кібердержавою» та передбачає активну міжнародну взаємодію для встановлення правил належної поведінки у кіберпросторі, притягнення порушників до відповідальності та розбудови глобальної стійкості до інформаційних атак [10].

Оновлене бачення пріоритетів зовнішньої політики та безпеки «Інтегрований огляд 2023», висвітлює більш суперечливий світ, у якому операції впливу, іноземне втручання в демократичні процеси та кіберзагрози поєднуються в єдиний спектр гібридного протистояння. У документі наголошується на розвитку суспільної та інституційної стійкості, включаючи такі ініціативи, як «Робоча група із захисту демократії», а також на зміцненні

міжнародного партнерства для протидії державним та недержавним суб’єктам у цифровому середовищі [27].

У «Національній кіберстратегії 2025» ця логіка продовжена з акцентом на національну конкурентоспроможність, критичні технології та резилієнтність як спільний знаменник безпеки та розвитку, що вимагає синхронізації з союзниками [47].

Санкційний інструментарій посідає окреме місце у зовнішньому вимірі інформаційної безпеки. ЄС у 2019 р. започаткував горизонтальний санкційний режим за значні кібернапади, що загрожують Союзу або його державам-членам. Хоча Сполучене Королівство після так званого брекзиту використовує власні правові механізми, саме європейський режим створив прецедент секторальної відповідальності за кіберзлочини та державне кіберзухвальство і став довідковою точкою для партнерів [12].

На практиці Лондон регулярно здійснює цільові обмежувальні заходи проти державних та афілійованих структур, відповідальних за зловмисну кібердіяльність, у тому числі за втручання у роботу демократичних інституцій прикладом є публічне покладення відповідальності на пов’язані з КНР організації у 2024 р.. [67].

Окремий тематичний вектор це протидія програмам-вимагачам у міжнародних коаліціях. Велика Британія є активним учасником Ініціативи протидії програмам-вимагачам, що просуває відмову від викупів як норму поведінки та координацію правоохоронних і дипломатичних дій. Відповідні спільні заяви 2024 р. відображають консолідацію підходів партнерів.

На національному рівні дискусія щодо законодавчого обмеження виплат у публічному секторі, яка триває станом на 2025 р., демонструє поєднання внутрішньої політики зі зовнішньою коаліційною лінією.

Зовнішній вимір інформаційної безпеки невіддільний від внутрішнього регуляторного курсу, націленого на стримування шкідливого контенту і протидію іноземному втручанню в онлайн-середовищі. «Закон про безпеку в Інтернеті 2023» закріпив регуляторну роль держави і передбачив обов’язки

платформ щодо запобігання незаконному контенту та контенту, шкідливому для дітей. У межах акту враховано також незаконну, спонсоровану дезінформацію та новий склад «іноземного втручання». Втілення акту відбувається поетапно, а політичний та експертний дискурс підкреслює його значення для виборчої цілісності та інформаційної стійкості [56].

Системність британського підходу забезпечується горизонтальними урядовими стратегіями кіберстійкості державного сектору та щорічними звітами про виконання Національної кіберстратегії, де окремо висвітлюються міжнародні компоненти: від стандартів обміну розвідданими до технічної допомоги партнерам і спільних попереджень для критичних секторів. Практична імплементація цих підходів простежується на рівні центральних та місцевих органів влади, що створює «внутрішній базис» для зовнішніх зобов’язань і зворотний зв’язок політики та практики.

Окрім коаліційних форматів і санкційних механізмів, Велика Британія активно впроваджує механізми транснаціонального обміну розвідданими про кіберзагрози. Це включає участь у спеціалізованих міжнародних робочих групах і спільних операційних центрах, де відбувається швидке поширення інформації про атаки на критичну інфраструктуру, нові шкідливі програми та кампанії дезінформації. Такий підхід дозволяє не лише реагувати на вже здійснені атаки, а й прогнозувати потенційні загрози та координувати профілактичні дії між державами [3].

Особливу увагу приділено розбудові кіберстійкості союзників та партнерів, у тому числі через надання технічної допомоги, навчання персоналу та консультаційні програми з впровадження стандартів кіберзахисту. Ці заходи сприяють формуванню єдиного безпекового простору у межах союзницьких та партнерських структур, що підвищує колективну здатність протидіяти гібридним загрозам та зменшує ризики для власної інфраструктури.

Велике значення мають міжнародні координаційні ініціативи протидії програмам-вимагачам, участь у яких демонструє принципову позицію Сполученого Королівства щодо неприйнятності викупів і стимулює

стандартизацію міжнародних процедур реагування. Це включає спільні правоохоронні операції, обмін досвідом та формування рекомендацій щодо управління ризиками для державного та приватного секторів.

Британська стратегія також передбачає поєднання зовнішньої політики з внутрішніми регуляторними інструментами, такими як Закон про безпеку в Інтернеті 2023 року, що забезпечує захист від незаконного контенту, іноземного втручання та шкідливої дезінформації. Поєднання міжнародної та внутрішньої політики дозволяє країні контролювати потоки загроз, підвищує ефективність дипломатичних та санкційних заходів і формує передбачуване середовище для бізнесу та громадян.

Крім того, британський підхід передбачає регулярну оцінку ефективності міжнародної взаємодії, включаючи аналіз спільних навчань, обмін даними про інциденти та результати координаційних заходів. Це дозволяє коригувати стратегії, оперативно реагувати на зміни у загрозовому середовищі та зміцнювати довіру до партнерів.

Таким чином, міжнародний вимір інформаційної безпеки Великої Британії реалізується через комплексну систему дій, що об’єднує коаліційні формати, технічну та нормативну підтримку союзників, санкційні та правозастосовні механізми, а також інтеграцію внутрішніх регуляторних заходів. Така багаторівнева стратегія дозволяє не лише реагувати на кіберзагрози, а й запобігати їх ескалації, підтримуючи демократичні цінності та міжнародну легітимність дій Сполученого Королівства.

У підсумку, міжнародна політика Великої Британії в інформаційному вимірі є багаторівневою: вона поєднує союзницькі рамки, коаліційні формати боротьби з кіберзлочинністю та державним кіберзухвальством, санкційні й правозастосовні механізми, а також внутрішнє регулювання цифрових платформ. Саме зв’язок зовнішньої та внутрішньої політики формує сприятливість не тільки реагувати на інциденти, а й запобігати ескалації інформаційних загроз, зберігаючи демократичну легітимність і союзницьку синергію.

**Висновки до розділу 2**

Аналіз інституційної, регуляторної та операційної структури інформаційної безпеки у Великій Британії дозволяє сформулювати низку ключових висновків щодо унікальності та ефективності британської моделі. У розділі було виявлено, що інформаційний вимір у Великій Британії є не додатковим, а наскрізним та інтегрованим компонентом національної безпеки, що відображає фундаментальний перехід від пасивного захисту до активного стратегічного управління ризиками в цифровому середовищі. Це передбачає комплексний підхід, який поєднує державне стратегічне планування, технічну експертизу та багатосторонню міжнародну співпрацю.

Перш за все, інституційна архітектура демонструє високий ступінь централізації технічної експертизи, зосередженої в Центрі урядових комунікацій та Національному центрі кібербезпеки, та водночас децентралізацію відповідальності за впровадження, яка реалізується через принципи підходів «всього уряду» та «орієнтованого на суспільство». Стратегічне планування інтегровано на найвищому рівні (Національна кіберстратегія 2022), забезпечуючи узгодженість цілей між відомствами та секторами. Крім того, створення Національних кіберсил сигналізує про зсув до управління використанням державної влади в кіберпросторі, легітимізуючи здатність Великої Британії брати участь у операціях активного стримування відповідно до національного та міжнародного права.

На додаток до інституційної бази, операційна модель безпеки є унікальним поєднанням обов'язкових регуляторних важелів, таких як Закон про безпеку телекомунікацій, та гнучких методологічних рамок, що забезпечують глибоку інтеграцію кіберзахисту в процеси управління. Ключовим системним елементом є Структура оцінки кібербезпеки, яка пропонує єдину систему показників зрілості контролю, що дозволяє порівнювати рівень управління ризиками в різних критично важливих секторах послуг. Ключовим операційним досягненням є програма активного кіберзахисту Національного центру кібербезпеки, яка є прикладом інноваційного підходу до зниження системного

ризику за допомогою масштабованих технічних послуг, що значно зменшують вплив на всіх учасників. Важливо, що інституціоналізація співпраці з приватним сектором шляхом обміну розвідувальними даними та інтеграції вимог до кіберстійкості зміцнює довіру громадськості. Зрештою, багаторівнева підзвітність, що реалізується шляхом обов'язкового звітування про інциденти та публікації щорічних «звітів про хід», забезпечує прозорість та формує дисципліну своєчасного звітування про події, що є передумовою ефективного управління кризами.

Зовнішній вимір інформаційної безпеки невіддільний від внутрішньої стійкості, оскільки британський уряд розглядає кіберпростір як поле постійної геополітичної конфронтації. Велика Британія активно використовує свою перевагу в кіберрозвідці для просування міжнародних норм та притягнення винних до відповідальності, позиціонуючи себе як «відповідальна демократична кібердержава». Ця роль посилюється завдяки синергії коаліційних форматів: узгодження принципів кіберзахисту з Організацією Північноатлантичного договору, активна участь у транснаціональних ініціативах, таких як протидія програмам-вимагачам, та узгодження з режимом санкцій Європейського Союзу. Внутрішнє законодавство, зокрема Закон про кібербезпеку 2023 року, також має прямий зовнішній вимір, оскільки його положення щодо боротьби з іноземним втручанням та дезінформацією безпосередньо сприяють глобальній інформаційній стійкості.

Таким чином, інституційна, регуляторна та операційна база Великої Британії передбачає комплексний, багаторівневий підхід до інформаційної безпеки. Британська модель успішно поєднує технічну компетентність (Національний центр кібербезпеки, Національні кіберсили) з управлінською підзвітністю (Структура оцінки кібербезпеки, щорічні звіти), а також внутрішню стійкість з активною зовнішньою політикою стримування. Це дозволяє Сполученому Королівству не лише мінімізувати ймовірність інцидентів та стримувати їхні наслідки, але й діяти як відповідальний лідер, формуючи норми поведінки в сучасному дедалі суперечливішому

кіберпросторі.

# Розділ 3. ОЦІНКА ЕФЕКТИВНОСТІ БРИТАНСЬКОЇ МОДЕЛІ, ПЕРСПЕКТИВИ ЇЇ РОЗВИТКУ ТА ПРАКТИЧНЕ ЗАСТОСУВАННЯ ДОСВІДУ ДЛЯ УКРАЇНИ

## 3.1. Діагностика ефективності системи інформаційної безпеки Великої Британії

Оцінка ефективності державної політики у сфері інформаційної безпеки в умовах сучасних гібридних загроз вимагає виходу за межі традиційного розуміння безпеки як стану захищеності периметра та переходу до концепції динамічної стійкості. У випадку Сполученого Королівства Великої Британії та Північної Ірландії, яке у своїх засадничих документах, зокрема у Національній кіберстратегії дві тисячі двадцять другого року, декларує амбіцію утвердження статусу провідної відповідальної демократичної кібердержави, діагностика ефективності потребує застосування комплексного багаторівневого підходу. Цей підхід має базуватися на глибокому, системному аналізі співвідношення між стратегічними цілями, закладеними у доктринальних документах уряду, та реальними емпіричними показниками операційної стійкості, інституційної спроможності та соціальної довіри, що фіксуються у щорічних звітах наглядових органів. Діагностика ефективності британської моделі у рамках цього магістерського дослідження проводиться за методологією аналізу розриву спроможностей, що дозволяє виявити та критично осмислити розбіжності між нормативним дизайном системи безпеки та практикою її повсякденного функціонування в умовах реальних загроз. Для об’єктивізації аналізу ефективності функціонування системи інформаційної безпеки Сполученого Королівства доцільно виокремити інтегровану групу критеріїв, що охоплюють операційно-технічні, інституційно-управлінські та соціально-політичні аспекти, кожен з яких має свої індикатори вимірювання.

Фундаментальним параметром діагностики виступає критерій операційної резилієнтності, або стійкості, який відображає здатність

національної критичної інфраструктури, державного сектору та бізнесу витримувати кібератаки, локалізувати їх руйнівні наслідки та відновлювати штатне функціонування у мінімально можливі терміни. Аналіз звітних документів британського уряду, зокрема звітів Кабінету Міністрів та профільних парламентських комітетів за період з дві тисячі двадцять другого по дві тисячі двадцять п'ятий роки, дозволяє констатувати високу ефективність технічної компоненти системи, що підтверджується конкретними статистичними показниками та успішністю реалізації національних проєктів. Зокрема, впровадження та масштабування програми «Активний кіберзахист», що реалізується Національним центром кібербезпеки, стало революційним кроком у зміні глобальної парадигми державного управління Інтернетом, переходу від пасивної ролі надання порад до безпосередніх проактивних дій держави у цифровому просторі. Ця програма базується на філософії захисту більшості громадян автоматизованими засобами, не вимагаючи від них спеціальних технічних знань.

Згідно з річним оглядом діяльності Національного центру кібербезпеки за дві тисячі двадцять третій рік, завдяки інструментам програми «Активний кіберзахист», таким як сервіс примусового видалення шкідливого контенту, було автоматично нейтралізовано понад два мільйони триста тисяч шкідливих кампаній, що включали фішингові сайти, сервери управління бот-мережами та шахрайські ресурси [42].

Сполучене Королівство демонструє унікальний для світової практики підхід, коли держава бере на себе функцію своєрідного системного адміністратора національного масштабу, очищуючи національний сегмент мережі Інтернет від фішингу та шкідливого програмного забезпечення на рівні інтернет-провайдерів та системи доменних імен. Крім того, високу ефективність демонструють спеціалізовані сервіси для державного сектору, такі як «Перевірка пошти» та «Веб-перевірка», які дозволили знизити кількість успішних компрометацій урядових доменів на значний відсоток порівняно з попередніми періодами. Важливим елементом операційної стійкості стало

впровадження у дві тисячі двадцять третьому році нової схеми аудиту кібербезпеки державного сектору під назвою «GovAssure». Ця ініціатива змінила підхід до перевірки захищеності міністерств і відомств, відмовившись від формального заповнення опитувальників на користь незалежного аудиту третьою стороною відповідно до суворих критеріїв Рамки оцінювання кібербезпеки. Це дозволило уряду отримати об'єктивну картину вразливостей та перейти до ризик-орієнтованого управління безпекою, де ресурси спрямовуються на захист найбільш критичних активів [8].

Поряд з суто технічними та операційними показниками, важливим критерієм оцінки є інституційна когерентність, що відображає якість управлінської архітектури, відсутність дублювання функцій та ефективність міжвідомчої координації. Унікальність та ефективність британської моделі полягає у її гібридній природі, де Національний центр кібербезпеки структурно є частиною розвідувальної служби Центру урядового зв’язку. Така архітектура забезпечує прямий доступ фахівців із захисту до закритих розвідувальних даних про наміри та можливості іноземних противників, що дозволяє формувати попередження про загрози ще до початку активної фази атак [17].

Ця інтеграція дозволяє Сполученому Королівству стабільно утримувати лідерські позиції у сфері міжнародного позиціонування та дипломатії. Згідно з рейтингом Глобального індексу кібербезпеки Міжнародного союзу електрозв'язку та авторитетним рейтингом «Кіберсил» Белферовського центру Гарвардської школи імені Кеннеді, Сполучене Королівство стабільно входить до п'ятірки провідних кібердержав світу першого рівня, поступаючись лише Сполученим Штатам Америки за сукупним ресурсним потенціалом, але випереджаючи більшість країн Європейського Союзу за рівнем стратегічної інтеграції та злагодженості дій [31].

Це свідчить про високу ефективність зовнішньополітичного треку інформаційної безпеки, зокрема у формуванні міжнародних коаліцій атрибуції кібератак та використанні механізмів публічного покладання відповідальності на ворожі держави, такі як російська федерація, Китайська Народна Республіка,

Іран та Корейська Народно-Демократична Республіка.

Однак, незважаючи на високі макропоказники та міжнародне визнання, детальний аналіз внутрішніх процесів та звітів контролюючих органів виявляє низку глибоких системних проблем. Ці проблеми ставлять під загрозу довгострокову стійкість моделі та дозволяють діагностувати критичні зони вразливості, які можуть бути використані супротивниками. Найбільш гострою проблемою, що загрожує ефективності всієї архітектури безпеки, є хронічний дефіцит кваліфікованих кадрів у державному секторі, який набув ознак системної кризи людського капіталу. Звіт Об'єднаного комітету парламенту зі стратегії національної безпеки, опублікований у дві тисячі двадцять третьому році, містить жорстку критику уряду, прямо вказуючи на те, що державні органи не здатні конкурувати з приватним сектором за рівнем оплати праці та умовами роботи фахівців з кібербезпеки [33].

Проблема має глибокий структурний характер, оскільки висококласні фахівці Національного центру кібербезпеки та Центру урядового зв’язку, отримавши унікальний досвід роботи з передовими технологіями та допуск до державної таємниці, масово переходять у приватні технологічні компанії, банківський сектор або консалтинг, де рівень фінансової винагороди часто у три-чотири рази перевищує ставки державної служби. Це призводить до постійної ротації кадрів, втрати інституційної пам'яті та неможливості сформувати стійкі команди для реалізації довгострокових проєктів. Згідно з дослідженням Департаменту науки, інновацій та технологій, загальний розрив у кібернавичках на ринку праці Сполученого Королівства складає близько одинадцяти тисяч двохсот осіб щорічно, і половина підприємств країни відчуває нестачу фахівців для базового технічного захисту [15].

Нестача фахівців особливо гостро відчувається на рівні регіональних органів влади, муніципалітетів та у секторі охорони здоров'я, що гальмує впровадження складних систем захисту і робить ці критично важливі сфери легкою здобиччю для зловмисників, які використовують програми-вимагачі. Таким чином, без вирішення кадрової кризи навіть найдосконаліші стратегії

ризикують залишитися декларативними документами через фізичну відсутність людського капіталу для їх практичної імплементації на місцях.

Другим критичним аспектом діагностики, що суттєво знижує загальний рівень національної безпеки, є наявність значного технологічного боргу та вразливість застарілих інформаційних систем, так званих «успадкованих систем». Звіт Національного офісу аудиту визначає застарілі IT-системи як один із ключових ризиків для операційної спроможності Міністерства оборони та інших відомств [41].

Значна частина баз даних та систем управління логістикою Міністерства оборони, Міністерства внутрішніх справ та Національної служби охорони здоров'я базується на архітектурі, розробленій ще на початку двохтисячних років. Такі системи часто вже не підтримуються виробниками, не отримують оновлень безпеки та технічно не можуть підтримувати сучасні протоколи шифрування чи багатофакторної автентифікації. Масштабна атака програми-вимагача WannaCry у дві тисячі сімнадцятому році, яка паралізувала роботу лікарень по всій країні, та наступні атаки на постачальників медичних послуг, зокрема інцидент із компанією Synnovis у дві тисячі двадцять четвертому році, продемонстрували, що медичний сектор залишається «м'яким підчерев'ям» британської безпеки через фрагментарність інфраструктури та застаріле обладнання.

Ситуація із технологічною вразливістю ускладнюється ризиками ланцюгів постачання та залежністю від іноземних виробників телекомунікаційного обладнання. Незважаючи на політичне рішення уряду про повне видалення обладнання китайської компанії Huawei з мереж п'ятого покоління до дві тисячі двадцять сьомого року, прийняте відповідно до Закону про безпеку телекомунікацій дві тисячі двадцять першого року, процес заміщення відбувається повільно і створює значне фінансове навантаження на операторів зв'язку. За оцінками експертів телекомунікаційної групи, вартість заміни обладнання сягає сотень мільйонів фунтів стерлінгів, що відволікає ресурси від інноваційного розвитку. Залежність від іноземних апаратних

компонентів, особливо у сфері напівпровідників, залишається критично високою, що створює потенційні ризики апаратних втручань, шпигунства та віддаленого впливу на критичну інфраструктуру у випадку геополітичного загострення [60].

Отже, технічна модернізація у Сполученому Королівстві відбувається асинхронно, коли передові наступальні та розвідувальні можливості спецслужб співіснують із архаїчними та вразливими системами цивільного управління, що створює небезпечні прогалини в загальному периметрі національної безпеки.

Наступним важливим діагностичним аспектом є регуляторна дилема та колізія із фундаментальними правами людини, що яскраво виявилася під час розробки та імплементації Закону про безпеку в Інтернеті дві тисячі двадцять третього року. Цей процес висвітлив глибоку інституційну проблему пошуку балансу між вимогами національної безпеки, захистом суспільства від шкідливого контенту та правом громадян на приватність. Закон надає незалежному регулятору Ofcom широкі повноваження вимагати від платформ обміну повідомленнями та соціальних мереж впровадження технологій сканування контенту для виявлення терористичних матеріалів та матеріалів сексуального насильства над дітьми. Проте така вимога вступає у прямий технологічний та етичний конфлікт із технологією наскрізного шифрування, яка гарантує, що повідомлення можуть прочитати лише відправник та отримувач. Провідні глобальні технологічні компанії, власники популярних месенджерів WhatsApp та Signal, публічно заявили про готовність залишити ринок Великої Британії, ніж погодитися на послаблення протоколів шифрування, що створило б небезпечний прецедент для авторитарних режимів у всьому світі. Ця ситуація чітко діагностує межі суверенного регулювання в епоху транснаціональних платформ, оскільки навіть така потужна у цифровому та економічному вимірі держава, як Сполучене Королівство, стикається з об'єктивними труднощами у нав'язуванні своїх національних правил глобальним цифровим корпораціям. Це створює реальний ризик того, що законодавство залишиться частково недієвим або призведе до міграції

користувачів у тіньові засоби комунікації, які є повністю непідконтрольними державному моніторингу, що лише ускладнить роботу правоохоронних органів [37].

Спроба вирішити проблеми інформаційної безпеки суто національними законодавчими інструментами наштовхується на глобальний, безкордонний характер архітектури мережі Інтернет та опір приватного сектору, який захищає свою бізнес-модель та довіру користувачів.

Крім того, незважаючи на створення окремого роду військ Національних кіберсил та офіційну декларацію доктрини активного стримування у кіберпросторі, ефективність цих інструментів залишається предметом дискусій через проблему політичної атрибуції та недостатній стримуючий ефект. Звіти Парламентського комітету з розвідки та безпеки, зокрема доповідь щодо діяльності Китаю, свідчать, що ворожі держави продовжують проводити масштабні кампанії кібершпигунства, крадіжки інтелектуальної власності та втручання у демократичні процеси, не відчуваючи достатнього тиску від британських контрзаходів [28].

Проблема полягає у значному часовому розриві між фактом атаки та її офіційною атрибуцією. Процес збору неспростовних технічних доказів, їх верифікації розвідувальними спільнотами та політичного узгодження публічної заяви про звинувачення, часто у тісній координації з партнерами розвідувального альянсу П'ять очей, займає місяці, а іноді й роки. За цей час інформаційний та деструктивний ефект від атаки вже досягається супротивником, а санкційна або дипломатична відповідь сприймається громадськістю та агресором як запізніла та слабка. Крім того, доктринальні «червоні лінії» для застосування наступальних кіберможливостей Національних кіберсил залишаються розмитими та непублічними, що знижує їх превентивний потенціал, оскільки супротивник не має чіткого розуміння невідворотності покарання за свої дії у цифровому просторі [38].

Підсумовуючи діагностику ефективності системи інформаційної безпеки, можна стверджувати, що модель Великої Британії перебуває на стадії складної

трансформаційної зрілості. До беззаперечних сильних сторін системи належить унікальна інтегрована інституційна модель, яка ефективно усуває бар'єри між зовнішньою розвідкою та внутрішнім захистом, висока ефективність автоматизованих засобів захисту національного масштабу у боротьбі з масовими загрозами, а також наявність чіткої стратегічної візії та розвиненої нормативної бази. Однак ці значні досягнення частково нівелюються критичними зонами ризику, такими як імплементаційний розрив, коли амбітна стратегія стикається з гострим дефіцитом ресурсів та кадрів для реалізації на місцях, асиметрія захисту між захищеним центральним урядом та вразливими регіональними структурами, а також регуляторна невизначеність механізмів контролю інформаційного простору. Таким чином, діагноз системи можна сформулювати як стратегічно досконалу, але операційно перенапружену архітектуру, яка потребує негайних дій для усунення дисбалансів. Ефективність британської моделі у середньостроковій перспективі значною мірою залежатиме від здатності уряду вирішити внутрішні структурні проблеми, зокрема кадрову кризу та технологічний борг, швидше, ніж еволюціонують зовнішні загрози та адаптуються супротивники. Для України цей досвід є критично важливим джерелом уроків, оскільки він наочно демонструє, що саме лише створення потужних централізованих інституцій недостатньо без паралельної побудови стійкої екосистеми освіти, технологічної модернізації та ефективного, взаємовигідного державно-приватного партнерства.

## 3.2. Обґрунтування резервів зростання та перспективи оптимізації британської моделі

Базуючись на результатах комплексної, багатофакторної діагностики, проведеної у попередньому підрозділі магістерського дослідження, яка висвітлила наявність глибинних структурних диспропорцій між амбітними стратегічними цілями уряду Сполученого Королівства та його поточними операційними можливостями в умовах перманентної ескалації гібридних загроз, ми вважаємо за необхідне перейти до фундаментального наукового обґрунтування резервів зростання системи. На наше глибоке переконання, в

умовах технологічної сингулярності, пов’язаної з бурхливим розвитком штучного інтелекту, квантових обчислень та автоматизованих інструментів кібератак, британська модель інформаційної безпеки потребує не просто косметичного вдосконалення чи точкових корекцій, а якісного, парадигмального фазового переходу. Цей перехід має відбутися від застарілої концепції «статичної фортеці», яка передбачає захист периметра, до інноваційної біологічної метафори «динамічної імунної системи», яка здатна адаптуватися до мутацій загроз у режимі реального часу, навчатися на власних помилках та діяти на випередження. У цьому контексті перспективи оптимізації моделі вбачаються нами не в екстенсивному нарощуванні бюджетів чи механічному збільшенні штату кіберполіції, що є тупиковим шляхом в умовах дефіциту кадрів, а в інтелектуалізації процесів управління, посиленні наступальних спроможностей як інструменту стратегічного стримування та формуванні глобальних технологічних альянсів. Нижче ми детально обґрунтовуємо ключові резерви зростання, які, на нашу думку, здатні забезпечити якісний стрибок у ефективності функціонування досліджуваного об'єкта, перетворюючи Сполучене Королівство з пасивного споживача безпеки на архітектора глобального цифрового порядку.

Першим, найбільш фундаментальним та технологічно ємним резервом зростання ефективності британської системи, на наш погляд, є радикальна зміна філософії аудиту та моніторингу безпеки: від дискретного, періодичного контролю до безперервного алгоритмічного нагляду та управління ризиками у реальному часі. Проведений нами аналіз показує, що існуюча практика використання Рамки оцінювання кібербезпеки, попри свою методологічну стрункість та універсальність, страждає від критичного недоліку — статичності у часі. Оцінка захищеності критичної інфраструктури, що проводиться раз на рік або навіть рідше, створює небезпечну ілюзію безпеки, оскільки ландшафт загроз змінюється щогодини, а нові вразливості нульового дня з’являються щодня. Ми вважаємо, що стратегічний резерв оптимізації криється у повномасштабному впровадженні концепції «Безпека як код» та інструментів

автоматизованого комплаєнсу. Це передбачає інтеграцію спеціалізованих сенсорів безпеки та агентів збору телеметрії безпосередньо в архітектуру інформаційних систем державних органів, операторів енергетичних мереж, транспортних хабів та фінансових установ. Такий архітектурний зсув дозволить Національному центру кібербезпеки отримувати знеособлені метадані про стан захищеності національних активів у режимі реального часу, формуючи динамічну карту ризиків усієї держави.

Цей підхід, який ми пропонуємо концептуалізувати як «цифровий паноптикон національної безпеки», дозволить здійснити перехід від реагування на інциденти постфактум, коли збитки вже завдано, до предиктивного усунення вразливостей ще до того, як ними скористаються зловмисники. Наукове обґрунтування цього резерву базується на кібернетичній теорії складних систем та законі необхідного розмаїття Ешбі: система управління повинна мати не меншу швидкість реакції та складність, ніж керована система або середовище, що на неї впливає. Оскільки сучасні кібератаки здійснюються бот-мережами зі швидкістю світла, людська реакція є апріорі недостатньою. Практична реалізація цього резерву вимагає від уряду Сполученого Королівства значної політичної волі для стандартизації протоколів обміну даними між приватним сектором та державою. Це, безумовно, викличе дискусії щодо приватності та комерційної таємниці, однак в умовах тотальної кібервійни це є безальтернативним шляхом для виживання. Ми пропонуємо розглядати впровадження національної платформи обміну телеметрією як створення «цифрової нервової системи» держави, здатної відчувати біль (атаку) і миттєво посилати сигнал до м’язів (засобів захисту) [9].

Розвиваючи думку про необхідність доктринальної трансформації, ми вбачаємо колосальний, досі не розкритий повною мірою резерв зростання у площині глибокої інтеграції оборонних та наступальних кіберможливостей, що дозволить реалізувати концепцію повного спектра кіберсили. Наш аналіз діяльності новостворених Національних кіберсил свідчить про те, що потенціал активного стримування використовується не на повну потужність через

доктринальну невизначеність, юридичні перепони та певну політичну обережність Лондона. Ми глибоко переконані, що в сучасних геополітичних умовах, коли межа між миром та війною у кіберпросторі стерта, класична концепція «стримування через заперечення» (тобто побудова настільки сильного захисту, що атака стає економічно невигідною) вже не є достатньою. Агресивні дії державних акторів, таких як російська федерація чи Китайська Народна Республіка, демонструють готовність інвестувати будь-які ресурси для досягнення стратегічних цілей, ігноруючи економічну доцільність. Тому перспектива оптимізації британської моделі лежить у переході до стратегії «постійної взаємодії» та «оборони на передових рубежах», яка була успішно апробована Кіберкомандуванням Сполучених Штатів Америки. Ця стратегія передбачає безперервний тиск на інфраструктуру супротивників у їхніх власних мережах, виявлення та нейтралізацію загроз ще на етапі їх формування на серверах зловмисників.

Обґрунтуванням цього підходу є теза про те, що національна безпека у двадцять першому столітті досягається не пасивним очікуванням удару за високими стінами фаєрволів, а нав'язуванням супротивнику власної волі, перехопленням ініціативи та змушуванням його витрачати левову частку ресурсів на власний захист, а не на планування атак. Ми пропонуємо розглядати резерв зростання у створенні єдиних міжвідомчих ситуаційних центрів, так званих ф'южн-центрів, де аналітики Національного центру кібербезпеки, які бачать вхідні атаки, та оператори Національних кіберсил, які мають інструменти для удару у відповідь, працюватимуть у єдиному інформаційному та операційному контурі. Виявлена спроба атаки на британську критичну інфраструктуру має автоматично, з мінімальною затримкою, генерувати варіанти пропорційної кінетичної, цифрової або когнітивної відповіді по джерелу загрози. Реалізація цього резерву дозволить Сполученому Королівству сформувати репутацію гравця, атака на якого гарантовано призводить до неприйнятних, асиметричних збитків для агресора, що є сутністю сучасного стримування. Це вимагає розробки нових правил

ведення бою, які б чітко регламентували автоматизовану відповідь, залишаючись у правовому полі міжнародного гуманітарного права [39].

Критично важливим резервом, який вимагає глибокого стратегічного осмислення та довгострокового планування, є досягнення технологічного суверенітету в умовах незворотної глобалізації ланцюгів постачання. Наш аналіз вказує на те, що критична залежність від іноземних напівпровідників, телекомунікаційного обладнання та хмарних платформ є «ахіллесовою п'ятою» британської безпеки, яка потенційно може нівелювати всі зусилля із програмного захисту. В епоху, коли апаратні закладки та «чорні ходи» можуть бути інтегровані на рівні архітектури мікропроцесора, жоден антивірус не здатен гарантувати безпеку. Однак ми тверезо оцінюємо реальність і розуміємо, що повна технологічна автаркія для держави розміром зі Сполучене Королівство є економічно неможливою утопією. Тому перспектива оптимізації, на нашу думку, полягає у реалізації моделі «керованої взаємозалежності» та стратегії «френдшорінгу» (перенесення виробництва та розробки критичних компонентів до країн, що входять до альянсу довірених партнерів, таких як «П'ять очей»).

Резерв зростання ми вбачаємо у перетворенні положень Національної напівпровідникової стратегії з декларації намірів на конкретні, фінансово забезпечені інвестиційні проєкти зі створення фабрик подвійного призначення та дизайн-центрів на території Сполученого Королівства. Особливий акцент має бути зроблений на збереженні та розвитку інтелектуального потенціалу навколо архітектури ARM (Advanced RISC Machine), яка є британським національним надбанням. Крім того, слід звернути пильну увагу на резерв у сфері розробки квантових технологій, зокрема постквантової криптографії. Враховуючи реальну загрозу появи у найближче десятиліття квантових комп'ютерів, здатних миттєво зламати сучасні алгоритми шифрування на яких тримається вся світова фінансова система та державна таємниця, Сполучене Королівство має унікальний історичний шанс стати світовим лідером у впровадженні квантово-стійких алгоритмів. Інвестиції у цей напрям сьогодні

стануть гарантією інформаційного суверенітету завтра, дозволяючи захистити дані, які мають довготривалу цінність. Ми вважаємо, що саме технологічне лідерство у вузьких, але критичних нішах, а не лише регуляторні обмеження, здатне забезпечити довгострокову безпеку національних інтересів [16].

Окремої, детальної уваги заслуговує резерв оптимізації регуляторного середовища та правового поля, особливо у контексті стрімкого, експоненціального розвитку генеративного штучного інтелекту. Наш аналіз процесу імплементації Закону про безпеку в Інтернеті виявив ригідність та інерційність традиційних законодавчих механізмів, які часто застарівають ще на етапі парламентських слухань, до моменту набуття чинності. У світі, де нові версії великих мовних моделей з’являються щомісяця, закон не встигає за кодом. Ми обґрунтовуємо нагальну необхідність переходу до моделі «адаптивного, експериментального регулювання» через механізми «регуляторних пісочниць». Цей підхід дозволяє тестувати інноваційні безпекові рішення, алгоритми модерації контенту та методи протидії дезінформації у контрольованому середовищі у тісній співпраці з технологічними компаніями та громадянським суспільством без ризику порушення жорсткого законодавства.

Перспектива розвитку британської моделі вбачається нами у стратегічному позиціонуванні Лондона як глобального арбітра та центру компетенцій з безпеки штучного інтелекту. Успіх глобального саміту у Блетчлі-Парку продемонстрував наявність у Сполученого Королівства значного політичного та дипломатичного капіталу для виконання такої ролі модератора між жорстким регуляторним підходом Європейського Союзу та ліберальним підходом Сполучених Штатів. Резерв зростання полягає у створенні та розміщенні на британській території міжнародного інституту сертифікації та аудиту алгоритмів штучного інтелекту на предмет їх безпеки, етичності та відсутності упередженості. Експортуючи свої стандарти безпеки штучного інтелекту, Сполучене Королівство фактично поширюватиме свою юридичну та ціннісну юрисдикцію на глобальний цифровий простір, що є вищою формою

реалізації національних інтересів через інструменти м'якої сили та інтелектуального лідерства [14].

Не менш значущим, а можливо і вирішальним в умовах когнітивної війни, на наше переконання, є резерв соціальної мобілізації, формування культури безпеки та когнітивної стійкості нації. Технічна діагностика показує, що програмні та апаратні засоби захисту досягли межі своєї ефективності, зловмисники все частіше атакують не комп'ютер, а людину за клавіатурою. Людський фактор залишається слабкою ланкою системи, але ми пропонуємо змінити вектор розгляду цієї проблеми: замість того, щоб розглядати користувача як джерело ризику, слід перетворити його на «першу лінію оборони» та «розподілений сенсор безпеки».

Перспектива оптимізації полягає у впровадженні загальнонаціональної системи кібербезпеки та громадянської оборони у кіберпросторі. Це може бути реалізовано через створення національної платформи винагород за виявлення вразливостей у державних сервісах, де тисячі етичних хакерів, студентів та дослідників зможуть легально та контрольовано тестувати державні системи на міцність, отримуючи за це визнання та винагороду.

Також величезний резерв криється у докорінній реформі системи освіти: кібергігієна та медіаграмотність мають перестати бути факультативними дисциплінами і стати наскрізною компетенцією, інтегрованою у всі навчальні програми, від початкової школи до університетів та курсів підвищення кваліфікації державних службовців. Ми обґрунтовуємо це тим, що в умовах тотальної когнітивної війни, де полем битви є свідомість громадян, здатність критично мислити, розпізнавати дезінформацію, перевіряти джерела та розуміти механізми маніпуляції стає таким же критичним елементом національної безпеки, як і наявність ядерної зброї чи протиракетної оборони. Стійке суспільство, яке не піддається на провокації та паніку, є найкращим запобіжником проти гібридної агресії [45].

Варто також наголосити на резерві оптимізації архітектури державно-приватного партнерства, яке у британській моделі хоч і є розвиненим, але часто

носить формальний характер періодичного обміну інформацією. Ми бачимо перспективу у переході до моделі «операційної інтеграції» та «спільної відповідальності». Це означає, що представники ключових технологічних компаній, телекомунікаційних операторів та системно важливих банків мають не просто отримувати розсилки від регулятора, а фізично працювати у єдиних ситуаційних центрах разом з офіцерами розвідки та урядовцями під час кризових ситуацій. Такий підхід, частково апробований у фінансовому секторі через механізми обміну даними про шахрайство, має бути масштабований на енергетику, транспорт, водопостачання та охорону здоров'я. Це дозволить усунути бюрократичні бар'єри та затримки при обміні чутливою інформацією, забезпечить миттєву синхронізацію дій держави та бізнесу і дозволить створити єдиний фронт протидії. Обґрунтуванням є чіткі розуміння того, що левова частка критичної інфраструктури (понад вісімдесят відсотків) перебуває у приватній власності, і держава фізично не може захистити її без глибокої довіри, обміну даними та інтеграції з власниками активів [26].

Нарешті, стратегічним резервом, що виходить за межі національних кордонів, є інтернаціоналізація британських стандартів безпеки як потужний інструмент геополітичного впливу та формування альянсів. Сполучене Королівство за останні роки розробило одні з найкращих у світі методологій, такі як Рамка оцінювання кібербезпеки, стандарти безпеки Інтернету речей та методики атрибуції державних кібератак. Перспектива оптимізації полягає у активному, агресивному просуванні цих стандартів як основи для національних систем кібербезпеки країн Співдружності націй, країн, що розвиваються, та партнерів по НАТО. Допомагаючи партнерам будувати сумісні, інтероперабельні системи захисту, Лондон не лише підвищує глобальний рівень безпеки та зменшує простір для дій кіберзлочинців, але й створює величезні ринки збуту для власної індустрії кібербезпеки та консалтингу. Ми вважаємо, що активна «кібердипломатія» та роль «нормативного підприємця» здатні перетворити Сполучене Королівство на архітектора нової системи колективної цифрової безпеки, альтернативної моделям цифрового

авторитаризму та суверенного інтернету, які просувають Китай та росія. Це дозволить Британії не лише захистити себе, а й формувати правила гри у глобальному масштабі [59].

Узагальнюючи проведене комплексне обґрунтування, ми приходимо до логічного висновку, що перспективи оптимізації британської моделі інформаційної безпеки є багатовимірними, взаємопов'язаними і вимагають безпрецедентної синергії технологічних інновацій, управлінських реформ та дипломатичних зусиль. Ключові резерви зростання знаходяться не стільки у площині екстенсивного нарощування ресурсів, скільки у площині підвищення адаптивності системи, інтелектуалізації процесів, швидкості прийняття рішень та глибини довіри між всіма стейкхолдерами.

Реалізація запропонованих напрямів трансформації дозволить Сполученому Королівству не лише зберегти статус лідера, але й задати нові еталонні стандарти ефективності для всього демократичного світу. Для України, яка сьогодні перебуває на вістрі жорсткого гібридного протистояння і фактично є полігоном для випробування новітніх кіберзагроз, глибоке розуміння цієї еволюції британської моделі є безцінним джерелом знань. Воно вказує на те, що майбутнє національної безпеки лежить не у товщині цифрових стін а у швидкості реакції, колективному інтелекті, технологічному суверенітеті та непорушній суспільній довірі.

## 3.3. Напрями залучення міжнародного досвіду Великої Британії у вітчизняну систему національної безпеки

Проведений у попередніх розділах нашого дослідження системний, компаративний та багаторівневий аналіз архітектоніки системи національної безпеки Сполученого Королівства Великої Британії та Північної Ірландії дозволяє зробити однозначний висновок про її високу релевантність для потреб реформування українського сектору безпеки і оборони [18].

В умовах безпрецедентної за масштабами, жорстокістю та технологічною складністю повномасштабної збройної агресії Російської Федерації, яка трансформувалася у першу в історії людства тотальну війну гібридного типу, де

кібернетичний, інформаційний та кінетичний театри бойових дій злилися в єдиний простір конфлікту, вітчизняна модель безпеки зіткнулася з екзистенційними викликами. Ці виклики вимагають не косметичних змін чи ситуативного латання дірок, а глибинної, парадигмальної перебудови самих основ державного управління безпекою [63,35].

Ця війна супроводжується безпрецедентними за масштабом, складністю та скоординованістю кібернетичними атаками на енергетичну інфраструктуру, масованими інформаційно-психологічними операціями, спрямованими на підрив соціальної єдності, та спробами цифрової блокади державних інституцій [57].

Україна сьогодні перебуває в унікальній ситуації: маючи колосальний практичний бойовий досвід, який вивчають військові академії всього світу, вона все ще зберігає рудименти пострадянської бюрократичної системи управління, яка характеризується надмірною зарегульованістю, каральним ухилом у відносинах з приватним сектором та реактивним підходом до загроз. У цьому контексті досвід Сполученого Королівства, яке є визнаним глобальним лідером у сфері стратегічного планування, розвідки та кібербезпеки, пропонує готову, верифіковану часом та кризами матрицю побудови стійкої демократичної держави [33,6].

Залучення цього досвіду має відбуватися шляхом складної інтелектуальної адаптації британських принципів до українського контексту воєнного та післявоєнного часу. Ми пропонуємо розглянути комплексну програму імплементації британського досвіду, розгорнуту у площині філософії урядування, інституційного дизайну та нормативно-правового регулювання.

Фундаментальним концептуальним уроком, який Україна має засвоїти з британського досвіду, є зміна самої онтології безпеки. У Сполученому Королівстві протягом останнього десятиліття відбувся остаточний відхід від вузькопрофільного розуміння інформаційної безпеки як суто технічної дисципліни, спрямованої на захист секретних даних, до широкої концепції «національної кіберсили» та «національної стійкості». В Україні ж досі, попри

прогрес останніх років, домінує парадигма «технічного захисту інформації», успадкована від радянських спецслужб, де головним критерієм є відповідність формальним вимогам атестації, а не реальна здатність системи витримати удар [69].

Ми обґрунтовуємо необхідність закріплення в українському доктринальному полі, зокрема у новій редакції Стратегії національної безпеки та Стратегії кібербезпеки, британського принципу «безпека як екосистема». Цей принцип передбачає, що держава не може бути єдиним провайдером безпеки в умовах, коли дев'яносто відсотків критичної інфраструктури перебуває у приватній власності, а інформаційний простір контролюється транснаціональними технологічними платформами [46].

Запозичення британського підходу вимагає від українського керівництва визнання того факту, що національна безпека є продуктом спільного виробництва держави, бізнесу, академічної спільноти та громадянського суспільства. Практична імплементація цього напряму має розпочатися з перегляду базових дефініцій у Законі України «Про національну безпеку України» та Законі України «Про основні засади забезпечення кібербезпеки України», зміщуючи акценти з контролю та нагляду на партнерство, обмін інформацією та спільне реагування [69].

Аналіз інституційної моделі Сполученого Королівства вказує на ключову роль Національного центру кібербезпеки як єдиного входу для всіх питань безпеки. В Україні функції, які у Британії виконує Національний центр кібербезпеки, розпорошені між Державною службою спеціального зв'язку та захисту інформації, Службою безпеки України, Кіберполіцією та Радою національної безпеки і оборони. Така архітектура, хоч і забезпечує систему стримувань і противаг, часто призводить до дублювання функцій, розмивання відповідальності та конкуренції відомств за бюджети та вплив, замість конкуренції за ефективність. Особливо гостро це відчувається у взаємодії з приватним сектором, який змушений звітувати про інциденти кільком органам одночасно, часто наражаючись на слідчі дії замість отримання технічної

допомоги [25].

Ми пропонуємо провести глибинну інституційну реформу, метою якої є створення в Україні Національного агентства цифрової стійкості (умовна назва), побудованого за лекалами британського Національного центру кібербезпеки. Цей орган не повинен бути черговим силовим монстром. Ключова інновація британського досвіду, яку необхідно імплементувати, полягає у поєднанні під одним дахом доступу до високочутливої розвідувальної інформації (завдяки інтеграції з розвідувальним співтовариством) та відкритої, сервісної культури взаємодії з суспільством. Новостворений орган має бути позбавлений правоохоронних функцій (права на обшуки, затримання, виїмку серверів), що є критично важливим для формування довіри з боку IT-індустрії та міжнародних партнерів [2].

Його мандат має охоплювати три стратегічні завдання, запозичені з британської практики. По-перше, це функція «Національного технічного авторитету». Це означає, що саме цей орган, а не слідчі органи, встановлює стандарти криптографічного захисту, архітектури безпечних мереж та хмарних сервісів. При цьому, слідуючи британському прикладу, ці стандарти мають бути не імперативними бюрократичними інструкціями, а гнучкими фреймворками, які адаптуються під специфіку бізнесу. По-друге, це функція управління інцидентами національного масштабу. Україні необхідна єдина диспетчерська служба для кіберпростору, яка координує дії під час масованих атак, подібних до тих, що відбувалися на початку вторгнення. По-третє, це функція проактивної розвідки загроз. Використовуючи досвід британського Центру урядового зв’язку, новий український орган має отримати законодавче право на аналіз метаданих трафіку на магістральних каналах (без доступу до змісту комунікацій) для виявлення аномалій та патернів атак ворожих спецслужб.

Найбільш складним, але необхідним напрямом залучення британського досвіду є докорінна зміна регуляторної моделі. Українська система захисту інформації, що базується на атестації систем раз на 3-5 років, є морально

застарілою і не відповідає динаміці сучасних загроз [6].

Британський досвід пропонує альтернативу у вигляді Рамки оцінювання кібербезпеки. Це методологія, яка оцінює не наявність паперів, а реальну здатність організації функціонувати під тиском [44].

Ми пропонуємо розробити та імплементувати «Національний стандарт кіберстійкості», який буде повною адаптацією британської Рамки оцінювання кібербезпеки до українського законодавства. Цей стандарт має стати обов'язковим для всіх об'єктів критичної інфраструктури. Його ключова відмінність полягатиме у принципі «управління за результатами». Регулятор встановлює цілі безпеки (наприклад, «забезпечити неможливість несанкціонованої зміни даних»), а суб'єкт господарювання сам обирає технічні засоби для досягнення цієї цілі. Це стимулює інновації та дозволяє використовувати найсучасніші рішення, а не лише ті, що мають застарілі сертифікати.

Крім того, критично важливим є запозичення британського досвіду у сфері регулювання Інтернету речей. Закон Сполученого Королівства про безпеку продуктів та телекомунікаційну інфраструктуру забороняє продаж пристроїв зі стандартними паролями та зобов'язує виробників вказувати термін підтримки оновлень безпеки. Враховуючи, що Україна стає полігоном для кібервійни, мільйони незахищених камер спостереження, роутерів та смарт-пристроїв у домівках українців є потенційним ресурсом для ворожих бот-мереж. Ми пропонуємо внести зміни до Закону України «Про технічні регламенти та оцінку відповідності», запровадивши жорсткі вимоги кібербезпеки для будь-якого обладнання, що підключається до мережі Інтернет та імпортується в Україну. Це створить «цифровий санітарний кордон», що ускладнить діяльність ворожих спецслужб [1].

Окремим вектором нормативної роботи має стати адаптація британського досвіду захисту ланцюгів постачання. Закон про безпеку телекомунікацій дав британському уряду повноваження забороняти використання обладнання «високоризикових постачальників» (зокрема, Huawei) у мережах 5G. Україні,

яка перебуває у стані війни, необхідно розробити аналогічний механізм «скринінгу технологій». Ми пропонуємо прийняти Закон «Про безпеку критичних ланцюгів постачання», який надасть Раді національної безпеки і оборони повноваження проводити аудит програмного та апаратного забезпечення, що використовується на об’єктах критичної інфраструктури, на предмет наявності «закладок» та зв’язків з країною-агресором. Це має стосуватися не лише прямого імпорту з РФ, але й програмного забезпечення, розробленого компаніями, чиї центри розробки знаходяться у ворожих юрисдикціях.

Британська програма «Активний кіберзахист» є революційним прикладом того, як держава може захищати громадян автоматизовано, без їхньої активної участі [64].

В Україні захист громадянина у кіберпросторі досі є його приватною справою. Ми вважаємо за необхідне змінити цю парадигму, запозичивши технологічну архітектуру Британської програми «Активний кіберзахист».

По-перше, це стосується створення «Національного захищеного DNS» (PDNS). У Британії цей сервіс блокує запити державних службовців до шкідливих доменів. В Україні, враховуючи рівень загроз, доцільно розгорнути такий сервіс не лише для держорганів, а й для всіх шкіл, лікарень, об’єктів енергетики та водопостачання. Технічно це реалізується через співпрацю з провайдерами: запити до відомих шкідливих сайтів (бази яких формуються розвідкою) просто не обробляються. Це дозволить відсікти до 70% масових фішингових атак на критичну інфраструктуру.

По-друге, імплементація сервісу «Takedown». Британський Центр національної комп'ютерної безпеки Великобританії автоматизував процес надсилання скарг хостинг-провайдерам щодо фішингових сайтів, що імітують державні сервіси. В Україні цей процес часто є ручним і бюрократизованим. Створення автоматизованої платформи, яка б від імені держави Україна генерувала юридично обґрунтовані вимоги до Google, Microsoft, Amazon та інших провайдерів щодо блокування російської пропаганди та фішингу,

дозволило б значно очистити інформаційний простір. Досвід Британії показує, що авторитет державної агенції дозволяє скоротити час блокування шкідливого ресурсу з кількох діб до кількох годин [43].

По-третє, впровадження системи перевірки електронних листів та стандартів для всього державного сектору. На п’ятому році цифровізації в Україні все ще існують державні органи, які використовують незахищені поштові сервери або публічні поштові сервіси для службового листування. Запозичення британського протоколу захисту електронної пошти, який унеможливлює підробку адреси відправника (спуфінг), є критично важливим для протидії російським ІПСО, які часто розсилають фейкові накази нібито від імені міністерств чи Генштабу.

Унікальність британської моделі полягає не лише у силі спецслужб, а й у силі контролю над ними. Діяльність розвідувальних та безпекових органів перебуває під пильним наглядом Парламентського комітету з розвідки та безпеки та незалежних комісарів. В Україні парламентський контроль за сектором безпеки часто носить формальний характер. Ми вважаємо, що ефективність нової системи безпеки неможлива без довіри, а довіра неможлива без контролю [63].

Ми пропонуємо імплементувати в Україні інститут Незалежного комісара з питань інформаційної безпеки та розвідки, який би мав повний доступ до секретних матеріалів та право перевіряти законність дій спецслужб у кіберпросторі (наприклад, правомірність втручання у приватне життя громадян під час контррозвідувальних заходів). Річні звіти цього Комісара (у розсекреченій частині) мають бути публічними. Це дозволить збалансувати посилення повноважень спецслужб в умовах війни з гарантіями дотримання прав людини, що є обов’язковою умовою нашого руху до Європейського Союзу.

Також доцільно запровадити практику публікації щорічних звітів про стан кібербезпеки держави, аналогічних «Щорічний звіт» британського Центру національної комп'ютерної безпеки Великобританії [43].

Українське суспільство має право знати не лише про кількість відбитих атак, а й про системні проблеми, дефіцит кадрів та реальні ризики. Відверта розмова уряду з суспільством про вразливості, як це роблять у Лондоні, не послаблює владу, а навпаки, мобілізує суспільство та бізнес на допомогу державі.

Окремим, надзвичайно актуальним вектором є запозичення досвіду регулювання соціальних мереж. Британський Електронний акт безпеки 2023 став піонерським актом, що поклав відповідальність на платформи за психологічну та фізичну безпеку користувачів. В Україні, де соціальні мережі Telegram, TikTok, Facebook стали основними каналами отримання інформації, проблема дезінформації та ворожого впливу стоїть надзвичайно гостро [24].

Ми пропонуємо розробити український аналог цього закону, адаптований до умов війни. Ключовою ідеєю має стати не цензура контенту (що є неприйнятним для демократії), а регулювання алгоритмів та відповідальність платформ. Закон має зобов’язати платформи з певною кількістю українських користувачів відкрити фізичні представництва в Україні для юридичної взаємодії. Також необхідно запровадити вимоги до прозорості алгоритмів рекомендацій та механізмів модерації. Платформи повинні звітувати, скільки ресурсів вони витрачають на модерацію українського сегменту, та як вони протидіють мережам ботів. У разі невиконання вимог щодо видалення явно злочинного контенту (наприклад, закликів до повалення конституційного ладу, коригування вогню), до платформ мають застосовуватися важкі фінансові санкції, співмірні з британськими (до 10% від глобального обороту) [7].

Разом з тим, українська версія закону має містити чіткі запобіжники проти зловживань владою. Визначення того, що є дезінформацією, не може бути прерогативою виконавчої влади. Тут доцільно використати британську модель співрегулювання, коли стандарти розробляються спільно регулятором, індустрією та громадянським суспільством.

Аналіз британської стратегії національної безпеки переконливо доводить, що у двадцять першому столітті справжній суверенітет держави визначається

не лише наявністю боєздатних збройних сил, а й рівнем володіння критичними технологіями. Сполучене Королівство, усвідомлюючи ризики технологічної залежності від потенційних супротивників, активно реалізує політику «суверенних спроможностей» у таких сферах, як штучний інтелект, квантові обчислення та напівпровідники. Для України, яка перебуває у стані високотехнологічної війни на виснаження, запозичення цього досвіду є питанням фізичного виживання нації. Ми пропонуємо імплементувати британську модель державної підтримки інновацій подвійного призначення, яка реалізується через Фонд стратегічних інвестицій у національну безпеку.

Україні необхідно створити аналогічний суверенний венчурний фонд або спеціалізований інвестиційний механізм під егідою Міністерства стратегічних галузей промисловості та Міністерства оборони. Завданням цього фонду має стати не просто грантова підтримка стартапів, як це робить нинішній Фонд розвитку інновацій, а входження держави у капітал компаній, що розробляють критично важливі технології: засоби радіоелектронної боротьби, захищені системи зв’язку, алгоритми шифрування, системи аналізу великих даних та автономні платформи. Британський досвід показує, що держава може виступати «якірним інвестором», який бере на себе первинні ризики розробки технологій, що є занадто складними або довгостроковими для приватного венчурного капіталу. Це дозволить Україні зберегти права інтелектуальної власності на критичні розробки всередині країни та запобігти їх витоку за кордон.

Окремим вектором технологічної адаптації має стати розвиток національної екосистеми штучного інтелекту для цілей безпеки. Сполучене Королівство позиціонує себе як глобальний лідер у безпечному використанні штучного інтелекту, створивши Інститут безпеки штучного інтелекту. Україні доцільно створити аналогічний центр компетенцій, який би фокусувався на прикладному використанні штучного інтелекту в оборонній сфері: для аналізу супутникових знімків, виявлення дезінформаційних кампаній, автоматизованого пошуку вразливостей у коді державних реєстрів та

прогнозування дій ворога. Важливо також запозичити британські етичні рамки та протоколи безпеки при використанні таких технологій, щоб автоматизація не призвела до втрати людського контролю над летальними системами чи системами прийняття стратегічних рішень.

Діагностика британської моделі виявила, що її головною конкурентною перевагою є не техніка, а люди. Система підготовки кадрів у Сполученому Королівстві побудована на тісній інтеграції академічної освіти, практичних потреб спецслужб та індустрії. В Україні ж спостерігається розрив між теоретичною підготовкою в університетах та реальними потребами сектору безпеки. Ми пропонуємо докорінно реформувати підхід до освіти у сфері кібербезпеки, використовуючи програму сертифікації освітніх ступенів Національним центром кібербезпеки як еталон.

Суть пропозиції полягає у запровадженні державного стандарту якості освітніх програм з кібербезпеки, який розробляється та контролюється не лише Міністерством освіти і науки, а й безпосередньо суб'єктами забезпечення кібербезпеки: Службою безпеки України, Державною службою спеціального зв'язку та Кіберполіцією. Університети, чиї програми пройдуть таку «бойову акредитацію», мають отримувати пріоритетне державне фінансування, доступ до закритих полігонів для тренувань та гарантоване працевлаштування випускників. Це дозволить відсіяти неякісні освітні продукти та сконцентрувати ресурси на підготовці еліти кіберзахисту. Крім того, слід масштабувати британську ініціативу «КіберПерші», яка виявляє талановитих підлітків ще у школі, надає їм стипендії та менторську підтримку від офіцерів спецслужб, формуючи кадровий резерв на десятиліття вперед.

Ще більш актуальним для України є запозичення британського досвіду формування Кіберрезерву. В умовах війни в Україні стихійно виник потужний волонтерський рух у кіберпросторі, відомий як «ІТ-армія». Однак для довгострокової стійкості держави цей рух потребує інституалізації та введення у правове поле. Британська модель Кіберрезерву передбачає, що цивільні фахівці високого класу (архітектори хмарних систем, пентестери, аналітики

даних) укладають контракт з Міністерством оборони, проходять перевірку на благонадійність та періодичні тренування, залишаючись працювати у приватному секторі. У разі виникнення кризової ситуації національного масштабу вони можуть бути мобілізовані для виконання специфічних завдань. Україні необхідно прийняти Закон «Про кіберрезерв», який би легалізував статус «цифрових резервістів», надав їм соціальні гарантії, аналогічні військовослужбовцям, та визначив механізм їх залучення до кібероперацій без необхідності фізичної присутності в окопах. Це дозволить державі ефективно використовувати колосальний інтелектуальний потенціал українського IT-сектору, не руйнуючи при цьому економіку.

Успіх Сполученого Королівства на міжнародній арені базується на активній кібердипломатії та просуванні концепції «відповідальної демократичної кібердержави». Британія не лише захищається, а й формує глобальний порядок денний, встановлює норми поведінки та будує альянси. Україна, маючи унікальний статус жертви першої повномасштабної кібервійни та держави, що успішно протистоїть цифровій наддержаві, має повне право претендувати на роль регіонального лідера у питаннях безпеки. Залучення британського досвіду тут полягає у переході від дипломатії запитів про допомогу до дипломатії пропозиції рішень [18].

Ми пропонуємо створити в структурі Міністерства закордонних справ України спеціалізований Департамент цифрової дипломатії та санкційної політики, який працюватиме у тісній зв’язці з розвідувальним співтовариством. Його завданням має стати імплементація британської тактики публічної атрибуції кібератак. Україна повинна навчитися перетворювати технічні дані про російські атаки на політичну зброю. Це вимагає впровадження стандартів цифрової криміналістики, які визнаються судами Сполученого Королівства та країн Європейського Союзу. Коли українські фахівці надають докази атаки, вони мають бути бездоганними з юридичної точки зору, щоб на їх основі партнери могли запроваджувати санкції.

Також доцільно ініціювати створення під егідою України та Великої

Британії постійно діючого міжнародного механізму обміну знаннями про гібридні загрози «Київського діалогу з кіберстійкості». У рамках цього формату Україна могла б передавати партнерам унікальні дані про тактику, техніки та процедури російських хакерів, вразливості російського обладнання та методи протидії інформаційним операціям. Це перетворить український бойовий досвід на валюту, якою ми можемо «платити» за військову та фінансову підтримку, зміцнюючи свою суб'єктність. Крім того, Україна має активно долучатися до британських ініціатив щодо боротьби з найманцями у кіберпросторі та розповсюдженням шпигунського програмного забезпечення, позиціонуючи себе як форпост цифрової демократії.

**Висновки до розділу 3**

У третьому розділі магістерської роботи здійснено комплексну аналітичну оцінку ефективності функціонування системи інформаційної безпеки Сполученого Королівства Великої Британії та Північної Ірландії, визначено стратегічні резерви її подальшого розвитку та обґрунтовано пріоритетні напрями імплементації британського досвіду у вітчизняну практику національної безпеки. Проведена діагностика дозволила констатувати, що британська модель перебуває на стадії високої інституційної зрілості, яка характеризується глибокою інтеграцією розвідувальних та захисних спроможностей, наявністю чіткої стратегічної візії та розвиненою нормативно-правовою базою. Ключовим фактором ефективності системи визначено унікальну архітектуру, в якій Національний центр кібербезпеки виступає єдиним технічним авторитетом, поєднуючи доступ до закритої інформації з відкритою сервісною моделлю взаємодії з приватним сектором. Водночас аналіз виявив низку структурних диспропорцій, які стримують реалізацію потенціалу моделі, зокрема критичний дефіцит кваліфікованих кадрів у державному секторі, наявність значного технологічного боргу у вигляді застарілих інформаційних систем та складність регулювання транснаціональних цифрових платформ національними законодавчими інструментами. Встановлено, що стратегічно досконала архітектура безпеки

стикається з операційними обмеженнями на етапі практичної реалізації, що створює ризики імплементаційного розриву.

На основі виявлених проблемних аспектів було науково обґрунтовано резерви зростання та перспективи оптимізації британської моделі, які полягають у переході від статичної парадигми захисту периметра до динамічної концепції імунної системи держави. Доведено, що ключовим вектором розвитку є заміна дискретних механізмів аудиту безпеки на системи безперервного автоматизованого моніторингу в режимі реального часу, що дозволить мінімізувати час реакції на інциденти. Також обґрунтовано необхідність глибшої інтеграції оборонних та наступальних кіберможливостей для реалізації стратегії активного стримування, коли безпека гарантується здатністю завдавати асиметричних збитків інфраструктурі агресора. Окремий акцент зроблено на важливості досягнення технологічного суверенітету через розвиток національної індустрії напівпровідників та штучного інтелекту, а також на необхідності масштабування культури кібергігієни серед населення як фундаменту когнітивної стійкості нації.

Центральним елементом розділу стала розробка науково обґрунтованих пропозицій щодо адаптації британського досвіду в Україні. Визначено, що механічне копіювання нормативних актів є неефективним без зміни самої філософії державного управління у сфері безпеки. Запропоновано здійснити трансформацію вітчизняної системи шляхом створення єдиного національного технічного авторитету, який буде інституційно відділений від репресивних функцій та сфокусований на наданні сервісної підтримки об’єктам критичної інфраструктури. Аргументовано доцільність повної відмови від застарілої системи атестації інформаційних систем на користь ризик-орієнтованого підходу, що базується на адаптації британської Рамки оцінювання кібербезпеки.

Критично важливим визнано впровадження в Україні національної системи активного кіберзахисту, яка передбачає створення захищених сервісів доменних імен та фільтрації трафіку на рівні магістральної інфраструктури, що

дозволить автоматизовано блокувати масові загрози без участі користувачів. Також розроблено рекомендації щодо інституалізації відносин з цивільними фахівцями через створення законодавчо врегульованого Кіберрезерву та впровадження механізмів автоматичної синхронізації санкцій з Великою Британією за кіберагресію. Реалізація запропонованих заходів дозволить Україні здійснити перехід від реактивної моделі ліквідації наслідків атак до проактивної моделі управління національною стійкістю, що є необхідною умовою для перемоги у гібридній війні та подальшої інтеграції до євроатлантичного безпекового простору.

# ВИСНОВКИ

Проведене у межах магістерської роботи комплексне, системне та багатовимірне дослідження інформаційного виміру національної безпеки Сполученого Королівства Великої Британії та Північної Ірландії дозволяє стверджувати, що в сучасних геополітичних умовах, які характеризуються безпрецедентною турбулентністю, розмиванням кордонів між миром і війною та стрімкою технологічною акселерацією, інформаційна безпека остаточно трансформувалася з допоміжної технічної функції у фундаментальний атрибут державного суверенітету та ключовий фактор виживання нації. Глибокий аналіз еволюції британської моделі дає підстави констатувати зміну самої онтологічної парадигми безпеки: відбувся незворотний перехід від статичної концепції захисту периметра інформаційних систем до динамічної, адаптивної стратегії управління національною стійкістю. Теоретичне осмислення цієї трансформації, здійснене у роботі, переконливо доводить, що сучасна безпека є складним, багатошаровим феноменом, який охоплює не лише технічну захищеність телекомунікаційних мереж, баз даних та критичної інфраструктури, а й когнітивну стійкість суспільства до деструктивного інформаційного впливу, стабільність демократичних інститутів та здатність держави проєктувати силу у глобальному цифровому просторі. Ми дійшли обґрунтованого висновку, що ефективність державної політики у цій сфері залежить не стільки від наявності високих технологічних бар'єрів чи обсягів фінансування, скільки від якості інституційного дизайну, архітектури управління та, що найважливіше, від рівня довіри між урядом, приватним сектором та громадянським суспільством, що дозволяє розглядати національну безпеку як продукт спільного виробництва всіх відповідальних суб'єктів соціуму.

Детальний аналіз нормативно-правового базису та стратегічного планування Великої Британії дає змогу виокремити унікальну рису

британського підходу, а саме його високу адаптивність та стратегічну гнучкість, що є критично важливою перевагою в умовах невизначеності. Фундаментом цієї системи виступає не просто набір законів, а цілісна екосистема, вершиною якої є Національна кіберстратегія. Цей документ не обмежується декларацією намірів, а закріплює амбіцію держави утвердитися у статусі відповідальної демократичної кібердержави, здатної не лише захищати власні інтереси, а й формувати глобальні правила гри у кіберпросторі. Характерною особливістю британського правового регулювання є вдалий, прагматичний баланс між жорсткими імперативними нормами для критичної інфраструктури, втіленими у законодавстві про безпеку телекомунікацій, та гнучкими, орієнтованими на результат механізмами регулювання цифрового контенту, що реалізуються через новітнє законодавство про безпеку в Інтернеті. Особливої уваги та наукового визнання заслуговує той факт, що британська правова система однією з перших у світі відмовилася від застарілого бюрократичного підходу «безпека як відповідність паперам» на користь прогресивного ризик-орієнтованого підходу «безпека як результат». Впровадження Рамки оцінювання кібербезпеки як універсального національного стандарту дозволило державі перейти від формального контролю наявності сертифікатів до реальної, вимірюваної оцінки операційних спроможностей організацій протистояти атакам, виявляти інциденти та відновлювати функціонування, що значно підвищило загальний рівень національної стійкості.

Необхідність побудови такої складної та гнучкої архітектури продиктована радикальною, якісною зміною ландшафту загроз, що постають перед Сполученим Королівством та всім демократичним світом у двадцять першому столітті. Наше дослідження переконливо свідчить про еволюцію загроз від спорадичних, розрізнених дій кіберзлочинців, мотивованих фінансовою вигодою, до скоординованих, довготривалих гібридних кампаній, що плануються, фінансуються та проводяться ворожими державними акторами. Ключовими опонентами у цій «сірій зоні» конфлікту виступають авторитарні

режими, насамперед Російська Федерація та Китайська Народна Республіка, які використовують кібершпигунство, саботаж критичної інфраструктури та інформаційно-психологічні операції як асиметричні інструменти геополітичного впливу для нівелювання конвенційної військової переваги Заходу. Загрози набули небезпечного конвергентного характеру, коли технічна кібератака на енергетичну мережу чи банківський сектор супроводжується масованою, таргетованою дезінформаційною кампанією для провокування соціальної паніки, хаосу та підриву довіри до уряду. Крім того, поява нових векторів атак, пов'язаних із використанням штучного інтелекту для автоматизації злому, створення синтетичного контенту (діпфейків) та обходу традиційних систем захисту, створює екзистенційні виклики, які вимагають від держави випереджаючого розвитку контрзаходів, постійної адаптації оборонних стратегій та інвестування у проривні технології.

Оцінюючи ефективність реалізації стратегічних документів та функціонування інституційної моделі Сполученого Королівства, ми можемо діагностувати її як інституційно зрілу, стратегічно виважену, але водночас операційно напружену. Беззаперечним досягненням та еталонним прикладом для наслідування є створення Національного центру кібербезпеки, який, об'єднавши під одним дахом функції технічної розвідки, аналізу загроз та цивільного захисту, став взірцем ефективної державної агенції нового типу. Ця інституційна інновація дозволила реалізувати революційну програму активного кіберзахисту, яка, працюючи на рівні інфраструктури, довела свою високу ефективність у автоматизованому блокуванні мільйонів масових загроз ще до того, як вони досягнуть кінцевого користувача, фактично створивши невидимий «цифровий купол» над країною. Водночас, наш критичний аналіз виявив низку системних диспропорцій, які стримують повну реалізацію потенціалу моделі. Зокрема, існує критичний розрив між високим рівнем експертизи центральних органів влади та спецслужб і недостатньою спроможністю регіональних структур, муніципалітетів і малого бізнесу забезпечити належний рівень захисту. Хронічний дефіцит кваліфікованих

кадрів у державному секторі, спричинений неконкурентними умовами оплати праці порівняно з приватним сектором, та критична залежність від застарілих, успадкованих інформаційних систем залишаються «ахіллесовою п'ятою» британської оборони, що вказує на необхідність глибшої інтеграції з приватним сектором та докорінного реформування кадрової політики.

Екстраполюючи результати аналізу британського досвіду на українські реалії, ми дійшли фундаментального висновку, що механічне перенесення норм, правил чи організаційних структур є недоцільним і навіть шкідливим без глибинної трансформації самої філософії управління національною безпекою. В умовах повномасштабної війни та постійної загрози з боку агресора, Україна потребує переходу від реактивної моделі «гасіння пожеж» до проактивної моделі управління ризиками та побудови національної стійкості. Пріоритетним напрямом такої трансформації, на наше переконання, має стати створення єдиного національного технічного авторитету, інституційно та ментально відокремленого від репресивних, слідчих та каральних функцій. Цей орган має стати не черговим регулятором, а сервісним центром для критичної інфраструктури та бізнесу, надаючи допомогу, експертизу та дані розвідки для захисту. Це дозволить відновити втрачену довіру бізнесу до держави, подолати бар'єри у комунікації та налагодити ефективний двосторонній обмін інформацією про загрози в режимі реального часу.

Критично важливим вбачається впровадження в Україні національної екосистеми активного кіберзахисту, адаптованої до умов воєнного часу. Це передбачає розгортання захищених сервісів доменних імен та фільтрації трафіку на рівні магістральної інфраструктури держави для автоматизованого блокування відомих загроз без необхідності активних дій з боку користувача. Такий підхід «безпека за замовчуванням» дозволить значно знизити навантаження на команди реагування та мінімізувати людський фактор як джерело вразливостей. Особливої уваги в контексті українських реалій заслуговує необхідність інституалізації відносин між державою та високопатріотичною спільнотою IT-фахівців через створення законодавчо

врегульованого Кіберрезерву. Це дозволить легалізувати величезний інтелектуальний потенціал українського суспільства, який проявив себе у перші дні війни, та системно спрямувати його на захист національних інтересів, не руйнуючи при цьому економічний потенціал ІТ-галузі.

У зовнішньополітичній площині ми обґрунтовуємо необхідність поглиблення стратегічного партнерства з Великою Британією не лише як з донором допомоги, а як з ключовим союзником у кіберпросторі. Доцільним є створення механізму автоматичної синхронізації санкційних режимів проти кіберагресорів та активне залучення України до міжнародних коаліцій з атрибуції кібератак, що дозволить перетворити технічні дані про російські злочини на політичні та економічні наслідки для агресора. Підсумовуючи, можна стверджувати, що унікальний сплав безпрецедентного українського бойового досвіду, здобутого у протистоянні з технологічно розвиненим ворогом, та передових британських інституційних практик і стандартів здатен створити якісно нову, гібридну архітектуру безпеки. Ця архітектура не лише забезпечить стійкість української держави перед обличчям поточних та майбутніх загроз, а й може стати експортним зразком для побудови систем колективної безпеки в Європі та світі. Таким чином, мета магістерського дослідження досягнута, а отримані результати формують надійне підґрунтя для подальших державних рішень у сфері національної безпеки.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Гнатюк С. О., Сидоренко В. А. Сучасні тенденції кібербезпеки критичної інфраструктури: порівняльний аналіз Великої Британії та України. *Кібербезпека: освіта, наука, техніка*. 2019. № 2 (6). С. 22–35. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/72 (дата звернення: 12.11.2025).
2. Бузаров А. Стратегічна підтримка України Великою Британією в умовах протидії російській агресії. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2023. URL: https://journals.chnu.edu.ua/mediaforum/article/view/883/921.
3. Кіянка І., Шараськін А. Виклики національної безпеки в контексті Європейської інтеграції: досвід Великобританії. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2023. № 1 (35). URL: https://relint.vnu.edu.ua/index.php/relint/uk/article/view/320/295.
4. Почепцов Г. Як держава вибудовує своє пропагандистське щастя. *StopFake*. 2021. URL: https://www.stopfake.org/uk/yak-derzhava-vibudovuye-svoye-propagandistske-shhastya/ (дата звернення: 14.10.2025).
5. Buchanan B. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA: Harvard University Press, 2020. 432 p.
6. Buryachok V., Tolubko V. *Information and Cyber Security: Sociotechnical Aspects*. Kyiv: DUT, 2023.
7. Cabinet Office. *Fact Sheet: Online Safety Bill – Suicidal Content*. London: UK Government, 2023.
8. Cabinet Office. *GovAssure: A new cyber security assurance regime for government*. London: GOV.UK, 2023. URL: https://www.gov.uk/government/news/government-launches-new-cyber-security-measures-to-tackle-ever-growing-threats--2 (дата звернення: 15.11.2025).

9. Cabinet Office. *Government Cyber Security Strategy: 2022–2030 implementation update*. London: HM Government, 2023. URL: https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf (дата звернення: 10.11.2025).
10. Cabinet Office. *National Cyber Strategy 2022*. London: HM Government, 2022. 130 p. URL: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 (дата звернення: 12.10.2025).
11. Chatham House. *Cyber Security and the UK's Integrated Review Refresh*. Research Paper. London: Royal Institute of International Affairs, 2023.
12. Council of the European Union. Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. *Official Journal of the European Union*. 2019. 17 May. (L 129 I). P. 13–19. URL: https://eur-lex.europa.eu/eli/dec/2019/797/oj (дата звернення: 17.10.2025).
13. Crandall M., Allan K. Small States and Big Tech: The Case of Estonia and Ukraine. *Digital Policy, Regulation and Governance*. 2024. Vol. 26, No. 2. P. 145–162.
14. Department for Science, Innovation and Technology. *A pro-innovation approach to AI regulation: government response*. London: UK Government, 2024. (CP 1019).
15. Department for Science, Innovation and Technology. *Cyber security skills in the UK labour market 2024*. London: UK Government, 2024. URL: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024/cyber-security-skills-in-the-uk-labour-market-2024 (дата звернення: 19.11.2025).
16. Department for Science, Innovation and Technology. *National Semiconductor Strategy*. London: UK Government, 2023. URL: https://www.gov.uk/government/publications/national-semiconductor-strategy/national-semiconductor-strategy (дата звернення: 17.11.2025).

17. Devanny J., Martin C. The National Cyber Security Centre: A Survey of the First Five Years. *Intelligence and National Security*. 2023. Vol. 38, No. 5. P. 743–761. DOI: https://doi.org/10.1080/02684527.2023.2176874.
18. Dubov D. Cyber Diplomacy: The UK Experience and Lessons for Ukraine. *Strategic Panorama*. 2024. No. 1. P. 45–58.
19. Dunn Cavelty M., Wenger A. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*. 2022. Vol. 43, No. 1. P. 6–32.
20. European Union Agency for Cybersecurity (ENISA). *Threat Landscape 2023*. Athens: ENISA, 2023.
21. Foreign, Commonwealth & Development Office. *UK sanctions regime for cyber-attacks*. London: FCDO, 2023.
22. Geltzer J. A. Constructing the Cyber Threat: The Role of Government and Industry in Defining the Problem. *Journal of Strategic Studies*. 2022. Vol. 45, No. 2. P. 215–238.
23. Hakmeh J., Shires J., Tanczer L. M. et al. *A principles-based approach to cyber capacity-building*. London: Chatham House, 2024. 44 p. URL: https://www.chathamhouse.org/sites/default/files/2024-06/2024-06-25-principles-based-approach-cyber-capacity-building-hakmeh-et-al.pdf (дата звернення: 18.10.2025).
24. Hansen S. O. Regulating the Digital Domain: The Impact of the UK Online Safety Act. *Journal of Cyber Policy*. 2024. Vol. 9, No. 1. P. 112–130.
25. Hnatyuk S., Sydorenko V. Modern Trends in Cybersecurity of Critical Infrastructure: UK and Ukraine Comparative Analysis. *Cybersecurity: Education, Science, Technique*. 2023. Vol. 4. P. 22–35.
26. House of Commons Science, Innovation and Technology Committee. *Governance of artificial intelligence: interim report*. Ninth Report of Session 2022–23. London, 2023. (HC 1769).
27. *Integrated Review Refresh 2023: Responding to a more contested and volatile world*. GOV.UK, 2023. URL:

https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world

28. Intelligence and Security Committee of Parliament. *China*. London: HMSO, 2023. (HC 1605). P. 45–48.
29. Intelligence and Security Committee of Parliament. *Russia*. London: HMSO, 2023. (HC 632).
30. International Institute for Strategic Studies. *Cyber Capabilities and National Power: A Net Assessment*. London: IISS, 2024.
31. International Telecommunication Union. *Global Cybersecurity Index 2024*. Geneva: ITU Publications, 2024.
32. Introduction to Active Cyber Defence. *NCSC.GOV.UK*. URL: https://www.ncsc.gov.uk/section/active-cyber-defence/introduction (дата звернення: 10.10.2025).
33. Joint Committee on the National Security Strategy. *A hostage to fortune: ransomware and UK national security*. First Report of Session 2023–24. London: House of Commons, 2023. URL: https://committees.parliament.uk/publications/42493/documents/211438/default/ (дата звернення: 20.11.2025).
34. Kello L. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2023.
35. Lewis J. A. *Cyber War and Ukraine*. Center for Strategic and International Studies, 2022.
36. Lindsay J. R. Cybersecurity: Start Here. *International Studies Review*. 2015. Vol. 17, No. 3. P. 411–445.
37. Milmo D. WhatsApp and Signal unite against online safety bill. *The Guardian*. 2023. 17 April. URL: https://www.theguardian.com/technology/2023/apr/18/whatsapp-signal-unite-against-online-safety-bill-privacy-messaging-apps-safety-security-uk (дата звернення: 20.11.2025).
38. Ministry of Defence & GCHQ. *National Cyber Force: Responsible Cyber*

*Power in Practice*. London: UK Government, 2023. URL: https://assets.publishing.service.gov.uk/media/642a8886fbe620000c17dabe/Responsible_Cyber_Power_in_Practice.pdf (дата звернення: 20.11.2025).

39. Ministry of Defence. *Defence Command Paper 2023: Defence's response to a more contested and volatile world*. London: UK Government, 2023. (CP 901).
40. Ministry of Foreign Affairs of Ukraine. *Kyiv hosted the first Kyiv International Cyber Resilience Forum 2024: "Resilience at The Cyberwar"*. Kyiv: MFA of Ukraine, 2024. URL: https://mfa.gov.ua/en/news/u-kiyevi-vidbuvsya-pershij-kiyivskij-mizhnarodnij-forum-z-kiberbezpeki-2024-stijkist-pid-chas-kibervijni (дата звернення: 19.10.2025).
41. National Audit Office. *The Digital Strategy for Defence: A review of early progress*. London: NAO, 2023. (HC 1530).
42. National Cyber Security Centre. *Active Cyber Defence: The Sixth Year*. London: NCSC, 2023. URL: https://www.ncsc.gov.uk/files/ACD6-full-report.pdf (дата звернення: 20.11.2025).
43. National Cyber Security Centre. *Annual Review 2023: Making the UK the safest place to live and work online*. London: NCSC, 2023.
44. National Cyber Security Centre. *Cyber Assessment Framework (CAF) version 3.1*. London: NCSC, 2022.
45. National Cyber Security Centre. *Cyber Security Awareness and Culture: A Guide for Organisations*. London: NCSC, 2024.
46. National Security and Defence Council of Ukraine. *Cybersecurity Strategy of Ukraine*. Kyiv: NSDC, 2021.
47. *National Security Strategy 2025: Security for the British People in a Dangerous World*. GOV.UK, 2025. URL: https://www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world-html (дата звернення: 11.10.2025).
48. NATO Cooperative Cyber Defence Centre of Excellence. *The Tallinn Manual*

*2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2023.

49. NATO StratCom COE. *Annual Report*. Riga: NATO StratCom COE, 2022.
50. North Atlantic Treaty Organization. *Cyber defence*. Brussels: NATO, [s.a.]. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence (дата звернення: 16.10.2025).
51. Nye J. S. The End of Cyber-Anarchy? How to Build a New Digital Order. *Foreign Affairs*. 2022. Vol. 101, No. 1. P. 32–42.
52. Nye J. S., Jr. *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010. 30 p. URL: https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/cyber-power.pdf (дата звернення: 13.10.2025).
53. O'Grady S. *The UK's Cyber Power Strategy: Ambition vs Reality*. Chatham House Research Paper. London: Chatham House, [s.a.].
54. Ofcom's approach to implementing the Online Safety Act. *Ofcom*. URL: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/roadmap-to-regulation (дата звернення: 10.10.2025).
55. Omand D. *How Spies Think: Ten Lessons in Intelligence*. London: Penguin/Viking, 2020. URL: https://www.researchgate.net/publication/358902140_How_Spies_Think_Ten_Lessons_in_Intelligence (дата звернення: 15.10.2025).
56. *Online Safety Act 2023*. Legislation.gov.uk. 2023. URL: https://www.legislation.gov.uk/ukpga/2023/50 (дата звернення: 19.10.2025).
57. Pocheptsov G. *Information Warfare and Cognitive Resilience in Ukraine*. Kyiv: National Defence University of Ukraine, 2023.
58. Rid T. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux, 2020.
59. Royal United Services Institute. *The Future of UK Cyber Power: Strategy, Capabilities and Influence*. RUSI Conference Report. London: RUSI, 2024.
60. Royal United Services Institute. *The Silent Threat: Legacy IT in UK Critical*

*Infrastructure*. RUSI Occasional Papers. London: RUSI, 2024.

61. Schneider J. Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy. *Journal of Cybersecurity*. 2023. Vol. 9, No. 1. P. 1–12.
62. Schneier B. *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. New York: W. W. Norton & Company, 2018.
63. State Service of Special Communications and Information Protection of Ukraine. *Report on Russian Cyber Aggression against Ukraine*. Kyiv: SSSCIP, 2023.
64. Tanczer L. M. UK Active Cyber Defence: A public good for the private sector? *Journal of Cyber Policy*. 2023. Vol. 8, No. 3. P. 342–362.
65. *Telecommunications Security Code of Practice*. GOV.UK, 2022. URL: https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf (дата звернення: 10.10.2025).
66. UK Parliament. *The UK's international counter-ransomware strategy*. House of Commons Library Research Briefing. London: HMSO, 2023.
67. *UK sanctions China state-affiliated actors after malicious cyber activity*. GOV.UK, 2024. URL: https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity (дата звернення: 19.10.2025).
68. United Nations. General Assembly. *Resolution 74/29: Developments in the field of information and telecommunications in the context of international security*. New York: United Nations, 2019. URL: https://docs.un.org/en/A/RES/74/29 (дата звернення: 18.10.2025).
69. Verkhovna Rada of Ukraine. *Law of Ukraine on National Security of Ukraine*. Kyiv: VRU, 2018.
70. Wardle C., Derakhshan H. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Strasbourg: Council of Europe, 2017.
71. Yuzkova O. Implementing European and British Standards of Critical

Infrastructure Protection in Ukraine. *Law and Security*. 2023. Vol. 4. P. 112–119.

## АНОТАЦІЯ

Сободєєва А.О. Інформаційний вимір національної безпеки Великої Британії (магістерська робота). Харків: ХНУ імені В. Н. Каразіна, 2025. 74 с. (рукопис).

Магістерська робота присвячена дослідженню інформаційного виміру національної безпеки Великої Британії. Визначено теоретичні засади інформаційної безпеки, сутність кіберзагроз та гібридних викликів сучасного геополітичного простору; розглянуто роль міжнародних інституцій та нормативно-правове регулювання у сфері глобальної кібербезпеки.

Визначено еволюцію стратегій кібербезпеки Великої Британії; виокремлено інституційний механізм та основні інструменти протидії кібератакам і дезінформації; досліджено концепцію «відповідальної кібердержави» та підходи Британії до регулювання цифрового простору.

Розглянуто співробітництво між Великою Британією та Україною у сфері кіберзахисту в умовах російської агресії; проаналізовано британську допомогу у зміцненні кіберстійкості України; сформульовано рекомендації щодо імплементації британського досвіду для вдосконалення системи національної безпеки України.



**Ключові слова:** міжнародна інформаційна безпека, кібербезпека, стратегія кібербезпеки, Велика Британія, гібридна війна, дезінформація, критична інфраструктура, українсько-британське співробітництво.


---


## ANNOTATION

Sobodieieva A.O. Information dimension of national security of Great Britain (master'swork). Kharkiv: V. N. Karazin Kharkiv National University, 2025. 74 p. (manuscript).

The master's thesis is devoted to the study of the information dimension of national security of Great Britain. The theoretical foundations of information security, the essence of cyber threats and hybrid challenges of the modern geopolitical space are determined; the role of international institutions and regulatory regulation in the field of global cybersecurity is considered.

The evolution of the UK's cybersecurity strategies is determined; the institutional mechanism and main tools for countering cyber-attacks and disinformation are identified; the concept of a "responsible cyber state" and Britain's approaches to regulating the digital space are studied.

Cooperation between Great Britain and Ukraine in the field of cyber defense in the context of Russian aggression is considered; British assistance in strengthening Ukraine's cyber resilience is analyzed; recommendations are formulated for the implementation of British experience to improve the national security system of Ukraine.



**Keywords:** international information security, cybersecurity, cybersecurity strategy, Great Britain, hybrid warfare, disinformation, critical infrastructure, Ukrainian-British cooperation.

**ВІДГУК**

керівника кваліфікаційної роботи магістра
студентки 2–го курсу, групи УМІБ–61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Навчально-науковий інститут
«Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В. Н. Каразіна
Сободєєвої Анастасії Олександрівни

на тему **«Інформаційний вимір національної безпеки Великої Британії»**

1. **Актуальність дослідження** зумовлена стрімкою цифровізацією суспільства та зростанням кіберзагроз, які перетворюють інформаційну безпеку на ключовий чинник національної безпеки сучасних держав. Авторка переконливо показує, що інформаційний вимір охоплює не лише технічний, а й політичний, соціальний, правовий та комунікаційний рівні, які визначають стійкість державного управління. Особливої ваги набуває аналіз британського досвіду: у 2024–2025 рр. країна зіткнулася зі стрибком складних кіберінцидентів, що зачіпають демократію, економіку та критичні послуги, а уряд у 2025 р. оприлюднив оновлені рамки кібербезпеки, засвідчивши перехід від реактивного до проактивного регулювання. Такий контекст робить дослідження своєчасним і значущим, адже воно спрямоване на оцінку ефективності стратегій, інституційної спроможності та можливостей удосконалення політики інформаційної безпеки.

2. **Сильними сторонами** роботи є її комплексність та багатовимірність, що поєднує теоретичний аналіз із глибоким емпіричним матеріалом, а також системність викладу, яка забезпечує логічну послідовність аргументації. Авторка переконливо показує трансформацію інформаційної безпеки з технічної функції у фундаментальний атрибут державного суверенітету, діагностує зміну парадигми від статичного захисту до динамічної стратегії управління національною стійкістю та підкреслює значення когнітивної стійкості суспільства. Важливою перевагою є практична спрямованість роботи: запропоновані рекомендації щодо адаптації британського досвіду для України, включно зі створенням національного технічного авторитету та впровадженням екосистеми активного кіберзахисту. Міжнародний вимір дослідження, увага до партнерства з Великою Британією та участі у глобальних коаліціях, а також інноваційність ризик-орієнтованого підходу «безпека як результат» надають роботі високої наукової та прикладної цінності.

3. Запропоновані авторкою **заходи та пропозиції** вирізняються системністю й практичною спрямованістю. Авторка не лише здійснила комплексну діагностику британської моделі інформаційної безпеки, але й запропонувала конкретні напрями її адаптації до українських реалій. Особливої уваги заслуговує ідея створення єдиного національного технічного авторитету, відокремленого від каральних функцій та орієнтованого на сервісну підтримку критичної інфраструктури, що відповідає сучасним міжнародним стандартам.

Важливим є також акцент на впровадженні ризик-орієнтованого підходу до оцінювання кібербезпеки, який дозволяє перейти від формальної атестації до реальної перевірки операційних спроможностей. Практичну цінність має пропозиція щодо створення національної системи активного кіберзахисту та інституалізації співпраці з ІТ-спільнотою через Кіберрезерв, що сприятиме мобілізації суспільного потенціалу у сфері безпеки. Перспективним виглядає й механізм автоматичної синхронізації санкційних режимів із Великою Британією, який посилює зовнішньополітичний вимір захисту. Сукупність цих заходів формує цілісну концепцію переходу України від реактивної моделі реагування до проактивної моделі управління національною стійкістю, що має стратегічне значення для перемоги у гібридній війні та інтеграції до євроатлантичного безпекового простору.

4. **Недоліки роботи.** Попри комплексне обґрунтування та високий рівень наукової аргументації, у роботі простежуються окремі недоліки, що знижують її практичну завершеність. Зокрема, рекомендації здобувачки залишаються переважно на концептуальному рівні й не супроводжуються розгорнутою оцінкою ризиків їхньої імплементації. Створення єдиного національного технічного авторитету потребує значних кадрових та фінансових ресурсів, що в умовах дефіциту кваліфікованих фахівців може стати серйозним бар'єром. Впровадження системи активного кіберзахисту на рівні магістральної інфраструктури вимагає масштабних інвестицій та узгодження з приватними провайдерами, що ускладнює швидку реалізацію. Крім того, робота зосереджена переважно на британському досвіді, тоді як ширший порівняльний контекст та емпіричні приклади з інших країн могли б посилити універсальність висновків.

5. **Загальний висновок і оцінка кваліфікаційної роботи, присвоєння кваліфікації.** Представлена магістерська кваліфікаційна робота є самостійним комплексним дослідженням інформаційного виміру національної безпеки Великої Британії, що поєднує теоретичний аналіз, інституційний та нормативно-правовий огляд із практичною оцінкою ефективності державної політики. Авторка переконливо доводить трансформацію інформаційної безпеки з допоміжної технічної функції у фундаментальний атрибут державного суверенітету та ключовий чинник стійкості демократичних інститутів. Важливою перевагою роботи є поєднання глибокого аналізу британської моделі з розробкою практичних рекомендацій для України, що надає дослідженню прикладної цінності та стратегічної перспективи. Робота відповідає вимогам, що висуваються до кваліфікаційних робіт магістра, а її авторка Сободєєва Анастасія Олександрівна, заслуговує на оцінку 93 бали «відмінно» та присвоєння кваліфікації магістра за спеціальністю 291 «Міжнародні відносини, суспільні комунікації та регіональні студії».

Керівник кваліфікаційної роботи,
доктор політичних наук, доцент
завідувач кафедри міжнародних відносин
Навчально-наукового інституту
«Каразінський інститут міжнародних відносин та
туристичного бізнесу» Харківського національного
університету імені В.Н. Каразіна Наталія ВІННИКОВА

**РЕЦЕНЗІЯ**

на кваліфікаційну роботу магістра
студента 2–го курсу, групи УМІБ–61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Навчально-науковий інститут
«Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В. Н. Каразіна
Сободєєвої Анастасії Олександрівни

на тему «**ІНФОРМАЦІЙНИЙ ВИМІР НАЦІОНАЛЬНОЇ БЕЗПЕКИ ВЕЛИКОЇ БРИТАНІЇ**»

1. Актуальність теми кваліфікаційної роботи зумовлена тим, що інформаційний вимір національної безпеки сьогодні є одним із ключових компонентів стійкості держави в умовах гібридних загроз, зростання масштабів кібератак, іноземного втручання та дезінформаційних операцій. Велика Британія, як одна з провідних демократичних держав і цифрових економік світу, активно формує комплексну систему кібер- та інформаційної безпеки, що поєднує інституційні механізми, технологічні інструменти та міжвідомчу координацію. Реалізація цього дослідження дозволяє глибше зрозуміти підходи, моделі й інструменти кіберзахисту та інформаційної політики в контексті сучасних безпекових викликів.

2. Характеристика якості виконання кожного розділу роботи

У першому розділі роботи автором розкрито теоретико-методологічні засади дослідження інформаційної безпеки держави, подано еволюцію поняття «інформаційна безпека» та визначено ключові загрози, притаманні сучасному інформаційному середовищу. Концептуальна база, на яку спирається автор, викладена чітко, логічно та з урахуванням підходів провідних міжнародних організацій.

Другий розділ присвячений аналізу інституційної архітектури та нормативно-правових механізмів забезпечення інформаційної безпеки у Великій Британії. Ґрунтовно розкрито функціонування Кабінету міністрів та інших органів, що формують національну кіберполітику. Окремо заслуговує на увагу детальний огляд стратегічних документів, зокрема *Національної кіберстратегії 2022*. Загалом цей розділ вирізняється системністю та широким використанням первинних джерел.

У третьому розділі автором проведено комплексний аналіз політик, інструментів і практик управління ризиками, механізмів відповідальності та реагування на інформаційні загрози. Особливо цікавим є огляд сучасних підходів до протидії дезінформації, захисту критичної інфраструктури й управління інцидентами. У розділі подано авторське бачення викликів та перспектив розвитку британської моделі інформаційної безпеки, що є сильним елементом роботи.

3. Ступінь обґрунтованості висновків роботи
Висновки, сформульовані автором, є логічними, аргументованими та повністю відповідають поставленим меті й завданням. Вони спираються на широку джерельну базу та сучасні міжнародні практики. Особливо важливо, що у висновках подано конкретні рекомендації щодо вдосконалення інформаційної політики та можливостей адаптації британського досвіду в інших державах.

4. Характеристика ілюстративної частини роботи у роботі відсутня ілюстративна частина.

Ілюстративна частина у роботі відсутня. Включення схем інституційної взаємодії, графічних моделей загроз або статистичних даних могло б посилити наочність викладеного матеріалу.

5. Використання останніх досліджень, передових методів і технологій

У роботі використано широкий спектр актуальних джерел, включно з британськими урядовими звітами, аналітичними документами НАТО та ЄС, сучасними академічними дослідженнями. Автор вміло залучає міждисциплінарні підходи, спирається на новітні концепції кібер- й інформаційної безпеки, що свідчить про високий рівень опанування теми.

6. Позитивні сторони роботи. До позитивних сторін роботи можна віднести послідовність розгортання дослідження, широкий спектр джерельної бази, зокрема використання актуальних дослідницьких напрацювань за цією проблематикою, чітку авторську позицію щодо досліджуваної проблеми.

7. Недоліки роботи. Попри високий рівень виконання, окремі аспекти роботи можна вдосконалити. Доцільно було б розширити емпіричну базу, зокрема додати статистичні дані щодо кіберінцидентів, структури загроз або бюджетів безпекових програм. Крім того, включення ілюстративного матеріалу сприяло б кращому сприйняттю складних структурних елементів британської системи кібербезпеки.

8. Практичне значення роботи полягає в тому, що її результати можуть бути використані у формуванні державної інформаційної політики, при розробці стратегічних документів у сфері національної безпеки, кіберзахисту та протидії дезінформації. Матеріали дослідження можуть також знайти застосування у навчальних курсах, присвячених міжнародним відносинам, міжнародній тінформаційні безпеці, міжнародним комунікаціям.

9. Загальна оцінка кваліфікаційної роботи. Кваліфікаційна робота Сободєєвої Анастасії Олександрівни «Інформаційний вимір національної безпеки Великої Британії» є самостійним, ґрунтовним і актуальним дослідженням, що комплексно розкриває специфіку британської моделі інформаційної та кібербезпеки. Отримані результати доповнюють сучасні наукові підходи до

вивчення системи національної безпеки, зокрема в частині інституційної взаємодії та стратегічного реагування на загрози. За рівнем науково-методологічної обґрунтованості та аргументованістю положень робота заслуговує на високу позитивну оцінку.

**Рецензент:**
доцент кафедри права,
національної безпеки та
європейської інтеграції
навчально-наукового інституту
«Інститут державного управління»
кандидат наук з державного управління, доцент Наталія ГРИШИНА