Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«_» _____ 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Метод протидії кібервпливам в умовах ведення гібридної війни»

Виконавець: студент ІІ курсу, групи КБм-22

_____ **Роман РЕНЬ**
(підпис) (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Володимир НАКОНЕЧНИЙ	
Нормоконтроль	Іван БІЛОКОНЬ	

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«25» жовтня 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача(ки) КБм-22 (група) Реня Романа Валерійовича (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Метод протидії кібервпливам в умовах ведення гібридної війни

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 4 від 24.10.2024 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес використання механізмів та інструментів кібервпливів у гібридних війнах.
Предмет досліджень	Методи, тактики та засоби реалізації кібервпливів у гібридних конфліктах.
Мета	Аналіз загроз кібервпливів, визначення основних форм кібератак, розробка рекомендацій щодо підвищення стійкості структур.
Вихідні дані для проведення роботи	Актуальні способи реалізації кібератак та існуючі механізми їх нейтралізації.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна удосконалення технологій та розробка рекомендацій для підвищення стійкості державних та приватних структур

Практична цінність підсилення кіберзахисту об'єктів критичної інфраструктури за рахунок розробки рекомендацій.

4. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	25.10.2024 – 29.12.2024
Аналіз літературних джерел	30.12.2024 – 12.02.2025
Вивчення поняття гібридної війни та її складових	13.02.2025 – 21.02.2025
Аналіз форм і методів кібервпливів у межах гібридних конфліктів	22.02.2025 – 26.02.2025
Дослідження прикладів кібератак на критичну інфраструктуру в умовах гібридної війни	27.02.2025 – 04.03.2025
Вивчення міжнародного досвіду (NATO, EU, CERT/CSIRT) щодо протидії кібератакам	05.03.2025 – 10.03.2025
Аналіз сучасних технологій виявлення і нейтралізації цифрових загроз (SIEM, AI, SOC)	11.03.2025 – 17.03.2025
Оцінка інформаційно-психологічних впливів як складової гібридної агресії	18.03.2025 – 19.03.2025
Дослідження стану кіберзахисту в Україні та нормативно-правової бази	20.03.2025 – 17.04.2025
Розробка рекомендацій щодо формування комплексної системи протидії гібридним кіберзагрозам	18.04.2025 – 25.04.2025
Оформлення пояснювальної записки згідно методичних рекомендацій	26.04.2025 – 15.05.2025
Подача пакету документів на розгляд ЕК	15.05.2025 – 19.05.2025

Завдання видав _____ Володимир НАКОНЕЧНИЙ
(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Роман РЕНЬ
(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 25.10.2024 р.

Термін подання кваліфікаційної роботи до ЕК 19.05.2025 р.

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи на тему: «Метод протидії в умовах ведення гібридної війни» містить 103 сторінок, 7 рисунків, 10 таблиць, 29 джерел використаної літератури.

Об’єктом дослідження є процес застосування інструментів та механізмів кібервпливів у рамках гібридних війн, які спрямовані на дестабілізацію політичної, економічної та соціальної ситуації в країнах-мішенях.

Метою роботи є комплексний аналіз загроз кібервпливів у контексті сучасних гібридних конфліктів, визначення основних форм кібератак, механізмів їх реалізації та наслідків, а також розробка практичних рекомендацій щодо підвищення кіберстійкості державного та приватного сектору.

Методи дослідження базуються на поєднанні теоретичних та емпіричних підходів, зокрема методів аналізу та синтезу, класифікації, історичного й порівняльного аналізу, контент-аналізу та моделювання. Це дозволило здійснити глибоку систематизацію інформації щодо природи кіберзагроз і заходів протидії.

У роботі досліджено актуальні типи кібератак, що реалізуються в умовах гібридної війни, а також інформаційно-психологічні впливи через цифрові платформи. Проаналізовано приклади відомих кіберінцидентів, їхній вплив на критичну інфраструктуру та суспільну стабільність. Запропоновано стратегічні заходи захисту, спрямовані на посилення кібербезпеки.

Наукова новизна полягає у вдосконаленні підходів до протидії кібервпливам за рахунок інтеграції методів інформаційного, правового й технічного захисту, з урахуванням специфіки гібридних конфліктів та українського досвіду протистояння.

Актуальність дослідження зумовлена тим, що війна у XXI столітті охоплює не лише збройну боротьбу, а й інформаційний, економічний і кіберпростори. В умовах повномасштабної агресії проти України значення кіберзахисту як одного з ключових елементів національної безпеки зросло до критичного рівня.

Ключові слова: гібридна війна, кібервпливи, кібератака, інформаційна безпека, критична інфраструктура, цифрові загрози, кіберстійкість, інформаційно-психологічні операції.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

APT	–	Advanced Persistent Threat – складна довготривала кіберзагроза
CERT	–	Computer Emergency Response Team – команда реагування на комп'ютерні інциденти
CII	–	Critical Information Infrastructure – критична інформаційна інфраструктура
CSIRT	–	Computer Security Incident Response Team – команда реагування на комп'ютерні загрози
DDoS	–	Distributed Denial of Service – розподілена атака на відмову в обслуговуванні
DNS	–	Domain Name System – система доменних імен
EU	–	European Union – Європейський Союз
ICT	–	Information and Communication Technologies – інформаційно-комунікаційні технології
IoT	–	Internet of Things – Інтернет речей
IP	–	Internet Protocol – Інтернет-протокол
IS	–	Information Security – інформаційна безпека
IT	–	Information Technology – інформаційні технології
MITM	–	Man-In-The-Middle – атака «людина посередині»
NATO	–	North Atlantic Treaty Organization – Організація Північноатлантичного договору
OSINT	–	Open-Source Intelligence – розвідка з відкритих джерел
SOC	–	Security Operations Center – центр операцій безпеки
SQL	–	Structured Query Language – мова структурованих запитів
URL	–	Uniform Resource Locator – уніфікований покажчик ресурсу
USB	–	Universal Serial Bus – універсальна послідовна шина
VPN	–	Virtual Private Network – віртуальна приватна мережа
ZTA	–	Zero Trust Architecture – архітектура нульової довіри

ЗМІСТ

ВСТУП

Сучасний світ стає все більш взаємопов’язаним завдяки розвитку інформаційних технологій та глобальних комунікаційних мереж. Проте, поряд із позитивними наслідками цифрової трансформації, спостерігається зростання загроз кібервпливів, особливо в умовах гібридних воєн. Кіберпростір став ареною для геополітичного протистояння, у якому інформаційні атаки, дезінформація, кібератаки на критично важливу інфраструктуру та інші форми цифрового впливу використовуються як інструменти ведення війни. У зв’язку з цим дослідження загроз кібервпливів у гібридних конфліктах набуває особливого значення, адже дозволяє визначити механізми атак, оцінити їх наслідки та розробити ефективні заходи захисту.

Актуальність теми дослідження обумовлена тим, що в сучасних умовах війна не обмежується лише традиційними збройними методами, а охоплює також інформаційний, економічний та кібернетичний простір. Держави та недержавні актори використовують цифрові технології для впливу на громадську думку, порушення функціонування важливих об’єктів інфраструктури та послаблення противника без прямого застосування сили. Україна стала одним із головних об’єктів таких атак у ході сучасної гібридної війни, що робить тему кібербезпеки та протидії цифровим загрозам своєчасною і критично важливою. Крім того, розвиток кіберзагроз вимагає удосконалення законодавчої та технічної бази кіберзахисту, що потребує глибокого аналізу методів та інструментів цього процесу.

Метою дослідження є аналіз загроз кібервпливів у контексті гібридних воєн, визначення основних форм кібератак, їх механізмів та наслідків, а також розробка рекомендацій щодо підвищення стійкості державних і приватних структур до кіберзагроз. Досягнення цієї мети передбачає комплексний підхід до аналізу кіберзагроз, включаючи технічні, інформаційно-психологічні та стратегічні аспекти.

Об’єктом дослідження є процес використання механізмів та інструментів кібервпливів у гібридних війнах, які використовуються для дестабілізації політичної,

економічної та соціальної ситуації в країнах-мішенях. Основну увагу зосереджено на методах ведення інформаційної війни, кібератаках на державні установи, фінансові системи, об’єкти критичної інфраструктури та приватний сектор.

Предметом дослідження виступають конкретні методи, тактики та засоби реалізації кібервпливів у гібридних конфліктах, їх вплив на безпеку держави, а також механізми протидії. При цьому важливими аспектами є аналіз кібератак, спрямованих на порушення роботи критичної інфраструктури, дестабілізацію суспільно-політичного життя.

Для досягнення поставленої в роботі мети необхідно вирішити такі основні завдання:

- провести класифікацію основних видів кібератак у контексті гібридної війни;
- дослідити методи реалізації інформаційно-психологічних впливів через цифрові платформи;
- проаналізувати приклади масштабних кібератак, здійснених у межах гібридних конфліктів;
- визначити стратегічні заходи захисту від кіберзагроз та розробити рекомендації щодо їх впровадження.

Методи дослідження ґрунтуються на комплексному підході та поєднанні теоретичних і практичних методів аналізу. Використовується метод аналізу та синтезу для систематизації інформації про сучасні кіберзагрози та їхній вплив на безпеку держави. Метод класифікації дозволяє розподілити типи кібератак за рівнем загрози та об'єктами впливу. Метод історичного аналізу використовується для вивчення прикладів кіберконфліктів у різних країнах, що дозволяє виявити закономірності у використанні цифрових технологій у сучасних війнах. Метод порівняльного аналізу застосовується для оцінки ефективності заходів кіберзахисту, які використовуються різними державами та міжнародними організаціями. Для аналізу інформаційно-психологічних впливів застосовується контент-аналіз, який дозволяє оцінити поширення дезінформації та маніпулятивних матеріалів у соціальних мережах та медіа. Методи моделювання використовуються для

прогнозування можливих сценаріїв розвитку кіберзагроз у майбутньому та розробки відповідних заходів протидії.

Дослідження загроз кібервпливів в умовах гібридних воєн має важливе значення для розробки ефективних стратегій кіберзахисту, зменшення ризиків дестабілізації цифрового простору та забезпечення безпеки держави у сучасних умовах.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ КІБЕРВПЛИВІВ ТА ГІБРИДНИХ ВОЄН

1.1 Поняття та сутність кібервпливів

Кібервпливи є складовою частиною сучасних інформаційних воєн та гібридних конфліктів, де цифрові технології використовуються для маніпулювання інформаційним простором, впливу на громадську думку, порушення функціонування державних установ, економічних процесів і навіть підриву національної безпеки.

Під поняттям кібервпливів розуміють усі форми цифрового втручання, спрямовані на зміну поведінки, переконань, інформаційного середовища або критично важливих процесів у державі, бізнесі та суспільстві. Вони можуть мати як відкритий, так і прихований характер, охоплюючи широкий спектр засобів – від поширення дезінформації та маніпулятивного контенту до спрямованих кібератак на стратегічні об’єкти [1].

Сутність кібервпливів полягає у використанні цифрових технологій для досягнення певних цілей, пов’язаних із політичними, економічними, військовими або соціальними процесами. Вони можуть здійснюватися через атаки на інформаційні системи, що призводять до блокування їх роботи, викрадення або знищення даних, а також через інформаційно-психологічний вплив, що спрямований на маніпулювання свідомістю людей, зміну їхніх переконань або створення панічних настроїв у суспільстві [2].

Однією з ключових особливостей кібервпливів є їхня невидимість та складність ідентифікації джерела атаки. Багато цифрових атак проводяться через посередників, бот-мережі або із залученням кіберзлочинців, що ускладнює виявлення справжніх ініціаторів і замовників. Крім того, кібервпливи можуть бути поєднані з іншими формами гібридної війни, такими як економічний тиск, політичні маніпуляції та пропагандистські кампанії. Це робить їх ефективним інструментом у руках

державних та недержавних акторів, які прагнуть досягнути своїх стратегічних цілей без відкритого збройного конфлікту [1].

Важливою складовою кібервпливів є інформаційно-психологічні операції, що реалізуються через соціальні мережі, медіаплатформи та новинні ресурси. Вони спрямовані на формування певного інформаційного порядку денного, маніпулювання громадською думкою, підрив довіри до уряду, дестабілізацію суспільства або стимулювання протестних настроїв. Дезінформаційні кампанії використовують як фейковий контент, так і частково правдиву інформацію, змішану з викривленнями, що створює труднощі для сприйняття реальних фактів і ускладнює роботу офіційних органів із роз’яснення ситуації.

Кібервпливи також можуть бути спрямовані на підрив економічної безпеки держави. Це може включати атаки на банківську систему, фінансові установи, біржі, що спричиняє втрати капіталу, паніку серед інвесторів і фінансову нестабільність. Одним із найбільш руйнівних варіантів цифрового впливу є атаки на критичну інфраструктуру, такі як енергетичні мережі, транспортні системи, водопостачання, що може паралізувати роботу цілих секторів економіки.

Суттєвою загрозою є кіберзброя, яка включає спеціально розроблені шкідливі програми, що можуть порушувати роботу інформаційних систем (ІС), завдавати збитків державним або комерційним структурам, а також впливати на військові об’єкти. Такі інструменти здатні використовувати вразливості у програмному забезпеченні та інфраструктурі для проведення прихованих атак, що ускладнює їхню нейтралізацію.

Кібервпливи є багатовимірним явищем, що включає різні методи, засоби та цілі реалізації цифрових атак. Їх можна класифікувати за кількома основними критеріями, зокрема за характером впливу, об'єктами атак, технічними методами реалізації, а також за рівнем координації та складності виконання [3].

За характером впливу кібервтручання поділяються на технічні та інформаційно-психологічні. Технічні впливи зосереджені на атаках на інформаційні системи, мережеву інфраструктуру та цифрові пристрої. Вони спрямовані на знищення, модифікацію або викрадення даних, блокування доступу до критично важливих

ресурсів, створення технічних збоїв та поширення шкідливого програмного забезпечення. Інформаційно-психологічні впливи орієнтовані на зміну сприйняття суспільством певних подій, створення панічних настроїв, маніпулювання громадською думкою та нав’язування вигідних наративів через соціальні мережі, новинні ресурси та інші інформаційні платформи [4].

За об'єктами атак можна виділити кібервпливи, спрямовані на державні установи, критично важливу інфраструктуру, фінансові організації, приватний бізнес та громадянське суспільство. Державні установи часто стають мішенню атак, спрямованих на порушення функціонування урядових систем, витік конфіденційної інформації та дестабілізацію політичного процесу.

Критично важлива інфраструктура, зокрема енергетичні мережі, транспортні системи, телекомунікації та водопостачання, може зазнавати атак, що призводять до порушення життєдіяльності цілих регіонів. Фінансовий сектор є привабливою ціллю для кіберзлочинців, які використовують методи викрадення банківських даних, шахрайські схеми та атаки на біржові системи для дестабілізації економічної ситуації.

Приватний бізнес може страждати від атак на корпоративні дані, промислового шпигунства та вимагальницьких програм, що блокує роботу компаній. Громадянське суспільство стає мішенню маніпуляцій, спрямованих на створення інформаційного хаосу, політичної нестабільності та радикалізації суспільних груп.

За технічними методами реалізації кібервпливи поділяються на хакерські атаки, шкідливе програмне забезпечення, атаки на ланцюги постачання, експлуатацію вразливостей та соціальну інженерію [5].

Хакерські атаки можуть включати несанкціонований доступ до систем, крадіжку даних, саботаж та маніпулювання інформацією.

Шкідливе програмне забезпечення, зокрема віруси, трояни, програми-вимагачі та ботнети, використовується для отримання контролю над пристроями, пошкодження даних або проведення масштабних DDoS-атак.

Атаки на ланцюги постачання спрямовані на проникнення в системи через вразливості партнерських компаній, ПЗ або апаратних компонентів. Експлуатація

вразливостей передбачає використання недоліків у коді ПЗ для здійснення атак без необхідності взаємодії з користувачами.

Соціальна інженерія включає методи психологічного впливу на людей для отримання конфіденційної інформації або примушення до виконання певних дій, наприклад, відкриття заражених файлів або введення особистих даних.

За рівнем координації та складності виконання кібервпливи поділяються на одиничні атаки, організовані кампанії та державні кібероперації [6].

Одиничні атаки зазвичай здійснюються окремими хакерами або невеликими групами та можуть включати ШПЗ, фішингові кампанії або несанкціонований доступ до окремих об'єктів.

Організовані кампанії – це скоординовані атаки, що включають комплексні заходи, такі як поєднання технічних та інформаційно-психологічних методів для досягнення довготривалих стратегічних цілей.

Державні кібероперації є найскладнішою формою кібервпливів, оскільки вони проводяться спеціальними підрозділами, можуть тривати роками та бути спрямовані на зміну політичного, економічного або військового балансу на міжнародній арені.

Класифікація кібервпливів демонструє їхню багаторівневу структуру та складність, що вимагає комплексного підходу до розуміння їхніх механізмів, загроз та заходів захисту. Кожен тип атак має свої особливості, які визначають методи їхнього виявлення та протидії [7].

Таблиця 1.1

Класифікація кібервпливів

Критерій класифікації	Основні категорії
За характером впливу	Технічні впливи, Інформаційно-психологічні впливи
За об'єктами атак	Державні установи, Критично важлива інфраструктура, Фінансові організації, Приватний бізнес, Громадянське суспільство

продовження таблиці 1.1

За технічними методами реалізації	Хакерські атаки, Шкідливе програмне забезпечення, Атаки на ланцюги постачання, Експлуатація вразливостей, Соціальна інженерія
За рівнем координації та складності виконання	Одиничні атаки, Організовані кампанії, Державні кібероперації

Кібервпливи у гібридних війнах використовуються як стратегічний інструмент для досягнення політичних, економічних і військових цілей без безпосереднього застосування збройної сили. Ці впливи можуть мати технічний та інформаційно-психологічний характер, спрямовуючи свої атаки на критично важливі об'єкти державного управління, економічної інфраструктури, військової безпеки та громадської свідомості.

Основним методом здійснення кібервпливів є кібератаки на ІС, мережеві інфраструктури та цифрові платформи. Вони можуть реалізовуватися через несанкціонований доступ до державних, військових або фінансових баз даних, що дозволяє зловмисникам отримати або знищити критично важливу інформацію, а також викрасти персональні дані, які можуть бути використані для подальших маніпуляцій.

Одним із найпоширеніших інструментів у цьому контексті є експлуатація вразливостей у ПЗ або апаратному забезпеченні, що дозволяє атакуючим проникати у мережі та змінювати їхню конфігурацію для власних цілей [5].

Ще одним методом є атаки з використанням ШПЗ, яке може бути розповсюджене через електронну пошту, фішингові сайти або заражені файли. Віруси, трояни, програми-вимагачі та ботнети використовуються для блокування доступу до інформації, вимагання викупу або розповсюдження фейкових повідомлень. Особливо небезпечними є атаки типу "відмова в обслуговуванні" (DDoS), які спрямовані на перевантаження серверів і виведення з ладу урядових вебресурсів, банківських систем та комунікаційних платформ.

Соціальна інженерія є ще одним ефективним інструментом кібервпливів, що базується на маніпулюванні людською довірою та використанні психологічних слабкостей користувачів. Це можуть бути персоналізовані атаки через електронну пошту або соціальні мережі, що змушують жертву надати конфіденційну інформацію або завантажити шкідливі файли. Через соціальну інженерію можливе проникнення у високозахищені системи, оскільки людський фактор залишається однією з найвразливіших ланок кібербезпеки.

Інформаційно-психологічні операції займають центральне місце в стратегіях кібервпливу, оскільки їхня мета – змінити громадську думку, викликати дестабілізацію в суспільстві або вплинути на політичне керівництво країни.

Маніпулювання медіапотоками, створення фейкових новин, просування дезінформації через соціальні мережі та використання ботів для штучного розповсюдження певних наративів дозволяють змінювати інформаційний порядок денний, формуючи у громадськості хибне уявлення про реальні події. Такі кампанії можуть бути спрямовані як на внутрішню, так і на міжнародну аудиторію, створюючи хаос, поляризацію суспільства та кризу довіри до державних інституцій.

Глибока фальсифікація (Deepfake) та технології генеративного штучного інтелекту також входять до переліку інструментів, що використовуються у гібридних війнах. Вони дозволяють створювати маніпулятивні відео- та аудіозаписи, які можуть видаватися за справжні заяви політиків, військових чи суспільних діячів. Це створює умови для поширення дезінформації, фальшивих політичних заяв і навіть провокаційних матеріалів, що можуть спричинити соціальні заворушення.

Кібервпливи також активно використовуються для атак на критичну інфраструктуру, включаючи енергетичні системи, транспорт, фінансові сервіси та військові об’єкти [5].

Атаки на енергетичні системи можуть призвести до масштабних відключень електроенергії, що паралізує міста та стратегічні об’єкти.

Вплив на транспортні системи може включати злами диспетчерських центрів, що контролюють рух авіації, залізничного транспорту та автотранспорту.

У фінансовій сфері можливі атаки на біржі, банківські системи та транзакційні платформи, що може викликати паніку на ринку та фінансові втрати для держави та бізнесу.

Загалом, вплив кібератак на національну безпеку є надзвичайно серйозним, оскільки він охоплює всі аспекти функціонування держави – від оборонних можливостей до економічної стабільності та громадської довіри.

В умовах гібридної війни кіберзагрози можуть бути використані як елемент комплексної стратегії, що поєднує інформаційні, економічні та політичні методи тиску на противника. Це означає, що захист від таких загроз вимагає розробки багаторівневої системи кібербезпеки, яка включає не лише технічні засоби протидії, а й посилення інформаційної стійкості суспільства, підготовку кадрів та впровадження ефективної стратегії реагування на потенційні атаки.

Захист від кібервпливів у гібридних війнах вимагає комплексного підходу, який включає технічні, організаційні, правові та освітні заходи. Ефективні стратегії повинні забезпечувати не лише реагування на загрози, але й їхню профілактику та мінімізацію можливих наслідків.

Одним із ключових напрямків є зміцнення кібербезпеки на державному рівні шляхом створення та розвитку національної стратегії кіберзахисту. Це включає координацію між державними структурами, приватним сектором та міжнародними партнерами для виявлення та нейтралізації загроз. Необхідно розробити єдину систему моніторингу кіберінцидентів, яка дозволяє своєчасно виявляти та блокувати атаки.

Розбудова національної кіберінфраструктури має ґрунтуватися на впровадженні багаторівневих механізмів захисту, включаючи сучасні засоби шифрування даних, системи багатофакторної автентифікації та обмеження доступу до критично важливих ресурсів [4].

Використання криптографічних протоколів дозволяє забезпечити конфіденційність і цілісність інформації, що особливо важливо для державних установ, банківського сектора та військових об’єктів.

Система кібергігієни є ще одним важливим аспектом, який передбачає підвищення рівня обізнаності користувачів щодо основних принципів безпечного використання цифрових технологій. Працівники державних і комерційних установ повинні проходити регулярні тренінги з кібербезпеки, що включають правила розпізнавання фішингових атак, управління паролями та безпечне користування корпоративними мережами. Значну роль у протидії кібервпливам відіграє розробка та впровадження системи штучного інтелекту для аналізу аномальної активності в ІС. Такі алгоритми здатні у режимі реального часу ідентифікувати загрози та виявляти підозрілі дії, що можуть свідчити про спроби проникнення в мережу або здійснення кібератаки.

Однією з ключових технологій є використання SIEM-систем (Security Information and Event Management), які дозволяють централізовано збирати, аналізувати та обробляти дані про всі події, що відбуваються в інформаційній інфраструктурі організації. Такі системи можуть автоматично виявляти аномалії та сповіщати відповідні служби безпеки про потенційні загрози.

Для запобігання інформаційно-психологічним атакам необхідно впроваджувати стратегії інформаційної стійкості, що включають розвиток незалежних медіа, фактчекінг та боротьбу з дезінформацією. Велике значення має співпраця держави та громадських організацій у виявленні та нейтралізації фейкових новин, а також підвищення рівня медіаграмотності серед населення.

Розвиток системи кібероборони включає створення спеціалізованих кіберпідрозділів у силових структурах, які відповідатимуть за кібербезпеку держави, виявлення та протидію атакам на критично важливу інфраструктуру. Ці підрозділи повинні мати доступ до сучасних інструментів кіберрозвідки та співпрацювати з міжнародними партнерами для обміну інформацією про нові загрози [10].

Окрему увагу слід приділити резервному копіюванню даних та розробці стратегій швидкого відновлення інформаційних систем після кібератак. Регулярне створення резервних копій та їхнє зберігання в захищених хмарних сервісах дозволяє мінімізувати наслідки атак програм-вимагачів та швидко відновити роботу систем після збоїв.

Важливим елементом захисту є правове регулювання кібербезпеки, що передбачає розробку та вдосконалення законодавства щодо відповідальності за кіберзлочини, а також визначення стандартів безпеки для державних та приватних організацій. Впровадження міжнародних норм та участь у глобальних ініціативах кібербезпеки дозволяє забезпечити ефективну взаємодію між країнами у боротьбі з кіберзагрозами.

Комплексний підхід до кіберзахисту, що поєднує технічні засоби, організаційні заходи та підвищення рівня цифрової грамотності, дозволить значно зменшити вплив кібервтручань на інформаційний простір і критичну інфраструктуру, забезпечуючи національну безпеку в умовах сучасних гібридних загроз.

1.2 Особливості гібридних воєн у сучасному світі

Гібридні війни стали однією з головних форм ведення сучасних конфліктів, оскільки вони поєднують традиційні військові дії з кібернетичними, інформаційно-психологічними та економічними методами впливу. Основною особливістю таких воєн є їхня невизначеність, коли противник не використовує виключно збройну силу, а застосовує широкий спектр асиметричних інструментів для досягнення своїх стратегічних цілей.

Гібридні війни націлені не лише на військові об'єкти, а й на суспільну свідомість, політичні процеси та економічну стабільність держави, що піддається агресії. Одним із ключових аспектів гібридних воєн є їхня безконтактність, коли головна боротьба відбувається у віртуальному та інформаційному просторі, а не на полі бою. Нападник може здійснювати серію кібероперацій, спрямованих на підрив економіки, знищення даних, блокування критично важливої інфраструктури та поширення дезінформації серед населення. Такі дії дозволяють завдати значних збитків противнику, не розпочинаючи відкритого збройного конфлікту [5].

Іншою характерною рисою гібридних воєн є використання проксі-сил та нерегулярних формувань. Держави-агресори часто залучають до ведення війни приватні військові компанії, терористичні угруповання, найманців або місцеві

збройні формування, що дозволяє їм уникати відповідальності та приховувати свою причетність до військових дій. Це створює ситуацію невизначеності, у якій важко визначити, хто є реальним ініціатором конфлікту та які саме сили його підтримують.

Важливим елементом гібридних воєн є інформаційна війна, яка охоплює маніпулювання медіапростором, створення та поширення фейкових новин, використання соціальних мереж для впливу на суспільну думку та дискредитацію противника. Інформаційні атаки можуть здійснюватися через державні або підконтрольні медіа, а також за допомогою анонімних акаунтів та бот-мереж, що генерують неправдивий контент та поширюють його серед масової аудиторії.

Гібридні війни також відзначаються активним використанням економічного тиску. Атаки на фінансові системи, санкційні війни, блокування торговельних шляхів та стратегічних ресурсів використовуються для ослаблення економіки противника. Введення торгових обмежень, валютних маніпуляцій та зловмисних дій у банківському секторі сприяє дестабілізації економічного стану держави-мішені та посилює внутрішні політичні конфлікти. Сучасні гібридні війни мають високий рівень технологічної складності, оскільки вони використовують передові цифрові засоби, включаючи штучний інтелект, великі дані та кіберзброю.

Атаки на комп’ютерні мережі, злами урядових серверів, підміна інформації та створення цифрових копій особистих даних стали поширеними засобами боротьби у нових конфліктах. Використання таких методів дозволяє агресору отримати стратегічну перевагу, завдаючи удару по системах управління державою та підриваючи довіру населення до влади.

Ще однією особливістю гібридних війн є використання політичних маніпуляцій та підривної діяльності всередині країни-противника. Це включає підтримку опозиційних або радикальних рухів, організацію протестів, корупційні схеми та спроби втручання у виборчі процеси. Політичні технології та психологічний тиск стають основними інструментами для дестабілізації політичної ситуації та формування суспільного розколу.

Важливо зазначити, що гібридні війни є тривалими за своєю природою, оскільки вони не мають чіткої лінії фронту чи визначеного моменту закінчення. На

відміну від традиційних збройних конфліктів, які можуть завершитися перемогою однієї зі сторін, гібридні війни спрямовані на поступове виснаження противника, зміну політичного ландшафту та послаблення державних інституцій. Така тактика дозволяє агресору досягати своїх цілей без необхідності відкритої ескалації конфлікту.

Гібридні війни є складним багатофакторним явищем, що поєднує військові, економічні, інформаційні та політичні методи впливу. Вони відзначаються високим рівнем технологічності, безконтактним характером бойових дій, активним використанням проксі-сил та стратегічним маніпулюванням суспільною свідомістю.

У сучасному світі вони стають основним інструментом ведення конфліктів, що змушує держави переглядати підходи до забезпечення національної безпеки та розробляти нові стратегії захисту від невидимих загроз.

Гібридні війни є ефективним інструментом впливу в сучасному світі завдяки одночасному використанню різних методів впливу, що взаємодіють між собою та створюють комплексний багатовекторний тиск на державу-мішень. Такий підхід дозволяє атакуючій стороні досягати стратегічних цілей без необхідності розгортання відкритого військового конфлікту, що робить гібридні війни надзвичайно ефективними у сучасному глобалізованому світі.

Військовий компонент гібридних воєн спрямований на демонстрацію сили, створення загрози військового вторгнення або проведення обмежених збройних операцій без офіційного оголошення війни. Використання нерегулярних військових формувань, найманців, приватних військових компаній і диверсійних груп дозволяє атакуючій стороні залишатися в тіні, уникаючи офіційних звинувачень у військовій агресії. Водночас здійснюються локальні військові операції, які дестабілізують ситуацію в регіоні, підривають боєздатність збройних сил противника та створюють хаос серед мирного населення.

Економічний компонент використовується для ослаблення фінансової стійкості держави-мішені, зниження її конкурентоспроможності та створення кризових явищ в економіці. Введення санкцій, блокування торгових шляхів, організація валютних маніпуляцій, руйнування фінансових установ через кібератаки, шантаж міжнародних

корпорацій та інші методи дозволяють поступово погіршувати економічну ситуацію в країні. Втрата економічної стабільності спричиняє зростання безробіття, зниження рівня життя населення, збільшення державного боргу, що, своєю чергою, сприяє загостренню соціальних проблем та дестабілізації політичної обстановки.

Інформаційний компонент є одним із ключових елементів гібридної війни, оскільки він дозволяє маніпулювати громадською думкою, підривати довіру до державних інституцій та формувати суспільні настрої, вигідні атакуючій стороні. За допомогою інформаційних операцій, дезінформації, пропагандистських кампаній, створення та поширення фейкових новин, використання бот-мереж і тролінгових ферм можна нав’язувати альтернативну реальність суспільству, розпалювати паніку, загострювати суспільні конфлікти та впливати на політичні рішення. Маніпуляції в соціальних мережах, проникнення у журналістську спільноту, підкуп або тиск на медіа дозволяють спрямовувати інформаційний порядок денний у потрібне русло.

Політичний компонент гібридних війн реалізується через підривні дії всередині держави, що атакує, з метою ослаблення легітимності влади, створення політичної нестабільності та зміни політичного керівництва на лояльніше до атакуючої сторони. Це може включати втручання у виборчі процеси, фінансування опозиційних або радикальних рухів, організацію протестних акцій, посилення внутрішніх соціальних конфліктів та підкуп політичних лідерів або урядовців. Використовуючи корупційні механізми та дипломатичний тиск, атакуюча сторона може досягти зміни зовнішньополітичного курсу держави-мішені, її геополітичної орієнтації та стратегічних партнерств. Це, практично, все те, що ми можемо спостерігати зараз у збройному протистоянні між росією та Україною в ході озброєнного нападу на нашу державу та ведення гібрідної війни.

Ефективність гібридної війни значною мірою забезпечується саме синергією цих методів, коли військовий тиск доповнюється економічними санкціями, інформаційними маніпуляціями та політичною дестабілізацією. Якщо держава не здатна адекватно реагувати на такі багатовимірні загрози, вона може втратити контроль над власними процесами, що може призвести до серйозних наслідків, аж до зміни уряду, втрати територій або навіть розпаду країни.

В умовах сучасної глобалізації та цифрових технологій гібридні війни стали більш прихованими, динамічними та складними для ідентифікації. Вони дозволяють державам-агресорам вести боротьбу з мінімальними економічними та політичними витратами, залишаючись невидимими для міжнародної спільноти та уникаючи прямих військових конфліктів.

Саме тому розробка ефективних стратегій протидії гібридним загрозам стала одним із головних викликів для сучасних держав, які прагнуть забезпечити свою національну безпеку.

На рисунку 1.1 наведено взаємозв’язок компонентів гібрідної війни [12]

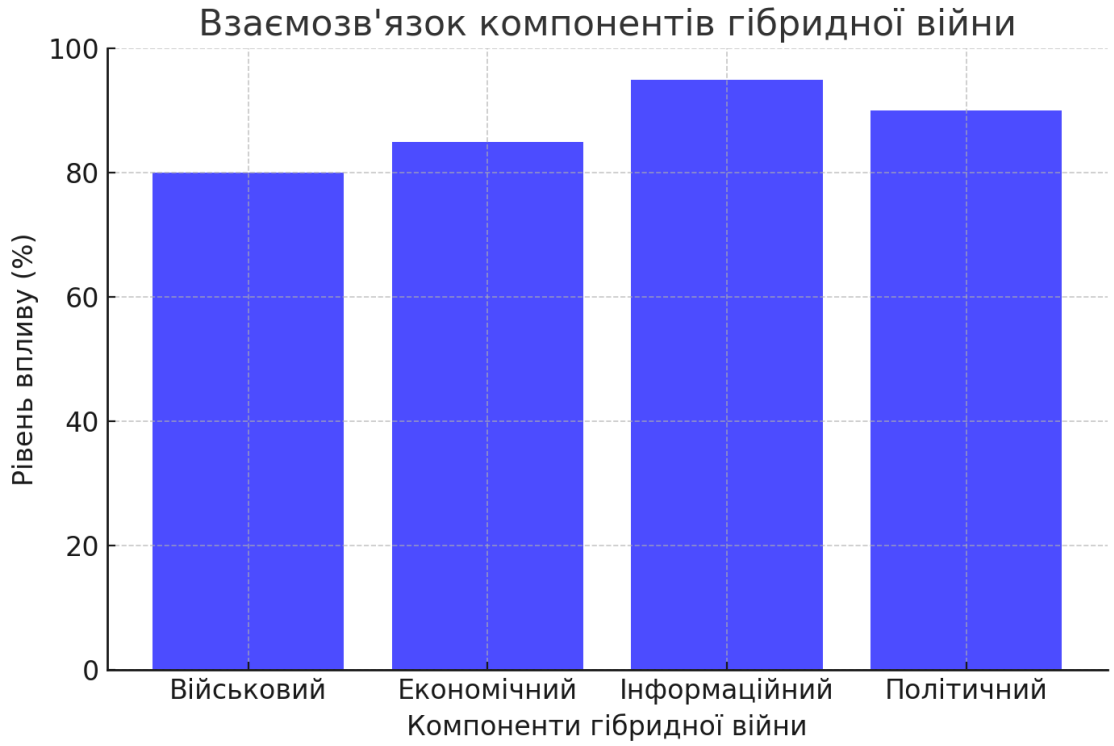

Рисунок 1.1 - Взаємозв’язок компонентів гібрідної війни

Сучасний технологічний прогрес значно змінив характер ведення гібридних війн, зробивши їх більш складними, ефективними та менш передбачуваними. Розвиток штучного інтелекту, кіберзброї та цифрових комунікацій дозволяє атакуючим сторонам здійснювати вплив на держави-мішені без застосування традиційних військових засобів, маніпулювати інформаційним простором,

здійснювати атаки на критичну інфраструктуру та змінювати підходи до національної безпеки.

Штучний інтелект відіграє ключову роль у сучасних гібридних війнах, оскільки він дозволяє автоматизувати процеси аналізу даних, виявлення загроз та прогнозування поведінки противника.

Використання алгоритмів машинного навчання допомагає агресорам швидко адаптуватися до змінюваної ситуації, аналізувати слабкі місця систем безпеки та знаходити ефективні способи проведення атак. Завдяки ШІ можна автоматично створювати та поширювати дезінформацію, використовувати чат-боти та алгоритми персоналізованого контенту для маніпулювання громадською думкою.

Розвиток нейромереж дозволяє розробляти більш витончені засоби соціальної інженерії, що робить інформаційні атаки складнішими для виявлення та нейтралізації.

Кіберзброя стала важливим інструментом у гібридних війнах, оскільки вона дозволяє атакувати стратегічно важливі об'єкти без фізичного втручання. Високотехнологічні кіберзасоби, зокрема віруси, трояни, експлойти та ботнети, використовуються для проникнення у критичні інформаційні системи, викрадення або модифікації даних, саботажу інфраструктури та створення цифрового хаосу. Використання кібератак дозволяє зловмисникам здійснювати масштабний вплив на фінансові системи, банківську сферу, транспортні мережі та енергетичний сектор. Кібероперації можуть бути реалізовані як окремі акції, так і як частина великої стратегії гібридної війни, спрямованої на довготривале ослаблення держави-мішені.

Цифрові комунікації змінили тактику ведення інформаційних війн, зробивши їх більш швидкими, глобальними та складними для ідентифікації. Соціальні мережі, месенджери, блоги та новинні агрегатори стали основними інструментами для розповсюдження маніпулятивного контенту, проведення інформаційних операцій та координації кібератак. Завдяки цифровим комунікаціям пропаганда та дезінформація можуть швидко охоплювати мільйони людей у різних країнах, змінювати суспільні настрої та впливати на політичні рішення. Технології глибокої фальсифікації (deepfake) дозволяють створювати реалістичні підроблені відео та аудіозаписи, які

можуть бути використані для компрометації політичних лідерів, поширення фейкових новин та маніпулювання громадською свідомістю.

Розвиток технологій також вимагає суттєвого перегляду підходів до національної безпеки. Традиційні методи оборони, які базуються на військовій потужності та територіальному контролі, стають менш ефективними в умовах гібридних загроз. Сучасні держави змушені розширювати свої можливості у сфері кібербезпеки, розробляти нові стратегії захисту від інформаційно-психологічного впливу та впроваджувати багаторівневі механізми протидії кібератакам.

Для забезпечення національної безпеки необхідно впроваджувати системи штучного інтелекту (СШІ) для автоматичного виявлення загроз, розробляти комплексні заходи кіберзахисту, здійснювати регулярний моніторинг інформаційного простору та вдосконалювати механізми реагування на кіберінциденти.

Важливим аспектом є створення спеціалізованих підрозділів кібероборони, які відповідатимуть за захист критичних інфраструктур, виявлення ворожих інформаційних кампаній та розробку контрзаходів.

Крім технічних рішень, необхідно підвищувати рівень цифрової грамотності населення, оскільки саме люди є найбільш вразливою ланкою у кібербезпеці. Проведення освітніх програм, тренінгів з медіаграмотності та впровадження механізмів фактчекінгу дозволить зменшити ефективність дезінформаційних кампаній та посилити інформаційну стійкість суспільства [6].

Технологічний прогрес радикально змінює тактику ведення гібридних війн, роблячи їх більш складними, багатовимірними та ефективними. Використання ШІ, кіберзброї та цифрових комунікацій дозволяє атакуючим сторонам здійснювати масштабний вплив без прямої військової агресії, що вимагає від держав переосмислення традиційних підходів до національної безпеки та розробки нових стратегій захисту від сучасних гібридних загроз.

1.3 Роль інформаційних і комунікаційних технологій у гібридних конфліктах

Інформаційні та інформаційно-комунікаційні технології (ІКТ) стали основним інструментом у веденні гібридних конфліктів, оскільки дозволяють атакуючій стороні здійснювати вплив на суспільство, державні інституції та стратегічно важливі об'єкти без прямого збройного втручання. Сучасний світ залежить від цифрових технологій, що відкриває нові можливості для ведення інформаційних воєн, кібероперацій та психологічних маніпуляцій [1].

Однією з найважливіших функцій інформаційних технологій (ІТ) у гібридних війнах є їхня здатність до швидкого розповсюдження інформації та формування інформаційного середовища. Використовуючи соціальні мережі, новинні портали, відеоплатформи та месенджери, агресор може впливати на громадську думку, створювати або змінювати наративи, провокувати соціальні конфлікти та дестабілізувати ситуацію в країні-мішені. Боти та алгоритми розповсюдження контенту дозволяють штучно збільшувати охоплення певної інформації, маніпулюючи сприйняттям суспільства та змінюючи пріоритети громадських дискусій.

Комунікаційні технології (КТ) також використовуються для проведення кібератак на критично важливу інфраструктуру держави, фінансову систему, військові об’єкти та приватні підприємства. Проникнення у цифрові мережі, викрадення конфіденційної інформації, блокування серверів або поширення ШПЗ є ефективними методами впливу, які можуть завдати значної шкоди без фізичної присутності ворога на території країни-мішені. Такі операції дозволяють не лише підривати економічну та оборонну спроможність держави, але й створювати паніку та недовіру серед населення.

Важливим аспектом використання ІТ у гібридних війнах є їхня здатність до підривної діяльності на рівні суспільної свідомості. Використовуючи методи психологічного впливу та соціальної інженерії, агресор може змінювати переконання людей, формувати негативне ставлення до власного уряду, підірвати довіру до

державних інституцій та навіть спровокувати громадянські конфлікти. Завдяки інформаційним технологіям створюються цілі пропагандистські кампанії, які використовують глибокі фальсифікації (deepfake), маніпулятивні відео та фейкові новини для досягнення стратегічних цілей [4].

Крім того, КТ дозволяють організовувати оперативне управління гібридними операціями, координувати дії агентів впливу, підтримувати зв’язок між хакерськими групами, терористичними осередками та іншими учасниками конфлікту. Це робить гібридні війни гнучкішими та менш передбачуваними, оскільки атаки можуть здійснюватися з будь-якої точки світу без необхідності фізичного вторгнення [2].

В умовах зростаючої ролі інформаційних та комунікаційних технологій держави змушені розробляти нові стратегії кібербезпеки та інформаційного захисту. Традиційні військові методи не можуть ефективно протистояти цифровим загрозам, що вимагає впровадження комплексних систем моніторингу, штучного інтелекту для аналізу інформаційних потоків та швидкого реагування на деструктивні впливи. Інформаційні та комунікаційні технології стали невід’ємною частиною сучасних гібридних воєн, значно розширивши можливості атакуючих сторін та змінивши класичні уявлення про війну. Вони дозволяють маніпулювати суспільною думкою, здійснювати кібератаки на стратегічні об'єкти, координувати підривну діяльність та ефективно реалізовувати інформаційно-психологічні операції. Це вимагає від держав розробки нових підходів до забезпечення національної безпеки та посилення захисту цифрового простору.

Інформаційні та комунікаційні технології стали одним із найпотужніших інструментів у веденні гібридних конфліктів, оскільки дозволяють організовувати широкомасштабні інформаційно-психологічні операції, спрямовані на зміну суспільної думки, підрив довіри до влади, дестабілізацію соціально-політичної ситуації та формування сприятливих умов для агресора. Основна мета таких операцій полягає у тому, щоб використати слабкі місця суспільства та розколоти його на групи, які будуть вороже налаштовані одна до одної або до власного уряду.

Сучасні цифрові платформи дозволяють атакуючій стороні маніпулювати суспільною свідомістю через соціальні мережі, онлайн-медіа, відеохостинги та інші

канали комунікації. Соціальні мережі стали основним полем для інформаційних війн, оскільки вони мають велику аудиторію та дозволяють швидко поширювати контент із мінімальними обмеженнями. Використовуючи ботоферми, алгоритми персоналізованої реклами та маніпулятивний контент, атакуючі сторони можуть створювати фальшиве уявлення про події, змінювати наративи та поширювати дезінформацію серед мільйонів користувачів [3].

Одним із найбільш ефективних методів інформаційно-психологічних операцій є використання дезінформаційних кампаній. Атакуюча сторона може створювати неправдиві новини, викривлену інформацію або напівправду, яка легко сприймається суспільством, але при цьому формує необхідну агресору реальність. Наприклад, поширення фейкових повідомлень про корупцію в уряді, кризові явища в економіці або підготовку до військових дій може викликати паніку серед населення, спровокувати соціальні заворушення або підірвати довіру до влади.

Штучний інтелект та алгоритми машинного навчання активно використовуються для створення та поширення маніпулятивного контенту. Вони дозволяють автоматично генерувати фейкові новини, створювати реалістичні зображення та відео, що змінюють сприйняття реальності. Глибока фальсифікація (deepfake) є особливо небезпечним інструментом, оскільки вона дозволяє створювати підроблені відеозаписи із заявами політиків або громадських діячів, що можуть бути використані для маніпулювання громадською думкою. Ще одним важливим механізмом інформаційно-психологічних операцій є цілеспрямоване використання соціальної інженерії. Зловмисники можуть маніпулювати емоціями людей, створюючи провокаційні інформаційні приводи, що викликають страх, ненависть або обурення. Використання радикальних меседжів та емоційно зарядженого контенту дозволяє легко керувати поведінкою аудиторії, спрямовуючи її у потрібному напрямку.

Інформаційно-психологічні атаки (ІПА) часто супроводжуються кіберопераціями, спрямованими на захоплення або компрометацію інформаційних ресурсів. Зломи урядових сайтів, банківських систем, медіаплатформ можуть використовуватися для дискредитації державних інституцій та підриву довіри

громадян. Крім того, вразливості у кібербезпеці дозволяють атакуючим сторонам отримувати доступ до особистих даних громадян, що може бути використано для шантажу, маніпуляцій або створення фальшивих компрометуючих матеріалів.

Комунікаційні технології також використовуються для впливу на виборчі процеси та демократичні інститути. Використовуючи аналітику великих даних, атакуючі сторони можуть ідентифікувати вразливі групи виборців, поширювати серед них цільові повідомлення та змінювати їхню поведінку на виборах. У деяких випадках зловмисники можуть впливати на електронні системи голосування або створювати інформаційний хаос, що підриває довіру до виборчих результатів.

Інформаційні та комунікаційні технології стали основним інструментом ведення інформаційно-психологічних операцій (ІПО) у гібридних конфліктах. Вони дозволяють атакуючим сторонам швидко та ефективно поширювати дезінформацію, маніпулювати громадською думкою, дестабілізувати суспільно-політичну ситуацію та підривати демократичні інститути. Це робить інформаційні війни ключовим елементом сучасних гібридних конфліктів, що вимагає від держав розробки ефективних механізмів протидії та посилення інформаційної безпеки.

Кіберзброя та цифрові комунікаційні технології стали ключовими інструментами у веденні сучасних гібридних воєн, оскільки вони дозволяють атакуючим сторонам завдавати значної шкоди державі без застосування традиційних військових засобів. Критична інфраструктура, що включає енергетичні системи, транспорт, фінансовий сектор, зв’язок, охорону здоров’я та державне управління, є основною ціллю кібератак, оскільки її порушення може призвести до масштабних криз та дестабілізації країни.

Один із найпоширеніших способів впливу кіберзброї на критичну інфраструктуру – це кібератаки на енергетичні системи. Зловмисники можуть використовувати ШПЗ, фішингові атаки та експлойти для проникнення в системи управління електромережами, нафтогазовими об’єктами та водопостачанням. Успішні атаки можуть призвести до відключення електроенергії в цілих регіонах, що паралізує роботу державних установ, промисловості та транспорту. Такі атаки були

зафіксовані в різних країнах, зокрема у випадку з атакою на українську енергетичну систему у 2015 році, коли хакери змогли тимчасово знеструмити великі території.

Фінансовий сектор також є вразливим до кібератак, які можуть включати злом банківських систем, викрадення даних клієнтів, маніпуляції з електронними платіжними системами та атаки на фондові біржі. Такі операції можуть спричинити значні фінансові збитки, викликати паніку серед населення, підірвати довіру до банківських установ і навіть призвести до економічної кризи.

Використання вірусів-вимагачів може заблокувати доступ до фінансових даних, а атаки на державні казначейські системи можуть порушити виконання бюджетних операцій. Транспортні системи також можуть стати об’єктом атак, що спричинить хаос у логістиці та пасажирських перевезеннях. Наприклад, злом систем авіаційного управління або залізничного диспетчерування може призвести до затримки або скасування рейсів, а також до потенційно катастрофічних аварій.

Кіберзброя може бути використана для блокування морських портів, управління автотранспортними потоками або саботажу роботи навігаційних супутникових систем, що спричиняє проблеми у військових та комерційних перевезеннях.

Цифрові комунікаційні технології використовуються для порушення роботи урядових органів, що може вплинути на державне управління та систему безпеки країни. Атаки на урядові вебсайти, електронні поштові сервери та бази даних можуть призвести до витоку конфіденційної інформації, що загрожує національній безпеці. Хакерські угруповання можуть здійснювати атаки з метою підміни офіційних документів, розповсюдження дезінформації або блокування доступу до державних послуг.

Щоб захистити критичну інфраструктуру від кібератак, необхідно впроваджувати комплексні заходи кібербезпеки. Одним із найефективніших підходів є багаторівневий захист інформаційних систем, що включає застосування сучасних засобів шифрування, багатофакторної автентифікації та обмеження доступу до критично важливих даних. Використання системи виявлення аномальної активності

дозволяє у режимі реального часу ідентифікувати потенційні загрози та швидко реагувати на них.

Резервне копіювання даних є критично важливим заходом захисту, оскільки воно дозволяє швидко відновити роботу систем у разі атаки програм-вимагачів або масового видалення інформації. Важливо зберігати резервні копії у незалежних захищених дата-центрах або у хмарних сервісах, що забезпечує їхню недоступність для зловмисників. Навчання персоналу основам кібергігієни та регулярне проведення тренінгів з кібербезпеки допомагає зменшити ймовірність успішних атак, оскільки більшість інцидентів відбувається через людський фактор. Працівники державних установ та стратегічних підприємств повинні вміти розпізнавати фішингові атаки, не відкривати підозрілі файли та використовувати захищені канали зв’язку.

Розвиток національної системи кібероборони є ключовим елементом захисту держави від загроз, пов’язаних із кіберзброєю. Це включає створення спеціалізованих підрозділів, які відповідатимуть за моніторинг кіберзагроз, координацію заходів реагування та розслідування кіберінцидентів. Важливим аспектом є співпраця з міжнародними партнерами, оскільки багато атак здійснюються через глобальні мережі, і лише спільні зусилля можуть допомогти виявляти та нейтралізувати такі загрози.

Законодавче регулювання кібербезпеки також відіграє важливу роль у захисті критичної інфраструктури. Необхідно розробляти національні стандарти кіберзахисту, впроваджувати відповідальність за порушення у сфері цифрової безпеки та забезпечувати постійний моніторинг стану інформаційних систем.

Кіберзброя та цифрові комунікаційні технології стали потужним засобом ведення гібридних війн, що загрожує національній безпеці через атаки на критичну інфраструктуру. Для ефективного захисту необхідно розробляти комплексні заходи, що включають кібероборону, моніторинг загроз, резервне копіювання даних, навчання персоналу та міжнародну співпрацю. Тільки таким чином можна мінімізувати ризики та забезпечити стабільність роботи стратегічно важливих об'єктів держави.

Висновки до першого розділу

У першому розділі дипломної роботи було здійснено ґрунтовне дослідження теоретичних основ кібервпливів і гібридних воєн як сучасного явища, що поєднує воєнні, інформаційні, політичні, економічні й кібернетичні інструменти впливу. У результаті опрацювання літератури, аналітичних звітів, міжнародного досвіду та нормативно-правових джерел вдалося чітко визначити природу, сутність і класифікацію кібервпливів, окреслити механізми їхньої реалізації та об’єкти, на які спрямовується така деструктивна діяльність. Окрему увагу було приділено інформаційно-психологічному аспекту, як основі маніпулятивного впливу на суспільну свідомість, зокрема шляхом дезінформації, фейкових новин, deepfake-технологій та експлуатації соціальних конфліктів через цифрові платформи.

Детально проаналізовано, як кібервпливи діють у межах гібридних конфліктів, використовуючи як високотехнологічні засоби — хакерські атаки, віруси, шкідливе ПЗ, так і соціальну інженерію, яка орієнтована на психологічну вразливість людини. Продемонстровано, що гібридна війна — це не лише поєднання різних форм впливу, а їх синергія, де кіберпростір слугує інструментом впливу на всі ключові сфери функціонування держави. З огляду на це, інформаційно-комунікаційні технології розглядаються не лише як засіб, а як повноцінна «зброя», здатна досягати стратегічних цілей без прямого збройного конфлікту.

Поглиблений аналіз класифікації кібервпливів за характером впливу, об’єктами атак, технічними методами реалізації, рівнем координації та складності дозволив сформувати цілісне уявлення про багатовимірність цифрових загроз і складність їхньої ідентифікації та нейтралізації. Встановлено, що найбільшу небезпеку становлять саме організовані та державні кампанії, оскільки вони реалізовуються із залученням високотехнологічних рішень, стратегічного планування, психологічного впливу та інколи міждержавної координації.

Також було з’ясовано, що сучасні гібридні війни значно змінили саму концепцію війни як такої. Їхня природа заснована на використанні асиметричних підходів — зокрема впливу на свідомість, цифрову інфраструктуру, економічну

стійкість, демократичні інституції. Особливої уваги заслуговує технологічна складова гібридних воєн, що включає застосування штучного інтелекту, інструментів великих даних, автоматизованих аналітичних систем, deepfake, систем машинного навчання. Це свідчить про те, що сучасний конфлікт — це не тільки боротьба за території, але насамперед боротьба за дані, вплив, довіру та домінування в інформаційному просторі.

Інформаційно-комунікаційні технології, як показано в дослідженні, не лише змінюють структуру війни, а й ускладнюють виявлення джерела загроз, оскільки атаки реалізуються через анонімні мережі, ботів, проксі-ресурси, фішингові кампанії та ураження через ланцюги постачання. У цьому контексті кіберзброя виступає не менш небезпечною, ніж класичне озброєння, оскільки її наслідки можуть мати системний та довготривалий характер — від втрати контролю над інфраструктурою до паніки та політичної дестабілізації в державі.

РОЗДІЛ 2
АНАЛІЗ ЗАГРОЗ КІБЕРВПЛИВІВ В УМОВАХ ГІБРИДНИХ ВОЄН

2.1 Основні форми і методи кібервпливів

Кібервпливи є складним і багатогранним явищем, що охоплює широкий спектр методів і технологій, спрямованих на отримання контролю над інформаційним середовищем, маніпуляцію суспільною думкою та вплив на об'єкти цифрової інфраструктури. Вони можуть бути здійснені через різноманітні інформаційно-комунікаційні платформи та системи, використовуючи психологічні, технічні, соціальні та політичні механізми.

Одним із ключових аспектів є інформаційно-психологічний вплив, що передбачає маніпуляцію суспільною думкою, формування заданої поведінки аудиторії та створення дезінформаційних кампаній. Використовуються методи пропаганди, психологічного тиску, емоційного залучення, соціальної інженерії та технології масового поширення фейкових новин. Активне застосування соціальних мереж дозволяє впливати на цільову аудиторію шляхом таргетованої реклами, бот-мереж і алгоритмічного просування вигідних наративів [4].

Технічні методи впливу охоплюють широкий спектр атак на інформаційні системи, зокрема кібератаки на критичну інфраструктуру, викрадення або підробку даних, використання шкідливого програмного забезпечення, фішингових атак та експлуатації вразливостей програмного забезпечення. Поширеним є застосування шкідливого коду, який може проникати в комп’ютерні мережі через приховані експлойти, віруси, троянські програми або шпигунське ПЗ. Досить ефективним є метод «людини посередині», що дозволяє перехоплювати дані в реальному часі під час обміну інформацією між сторонами [5].

Соціально-інженерні методи кібервпливу спрямовані на маніпуляцію людською довірою з метою отримання конфіденційної інформації або спонукання до певних дій. Основою таких методів є психологічні прийоми впливу, що

використовуються для введення людей в оману та отримання несанкціонованого доступу до важливої інформації. Це можуть бути атаки на персонал компаній через телефонні дзвінки, електронні листи чи навіть безпосередню комунікацію. Одним із поширених підходів є видача себе за авторитетну особу або службу підтримки, що дозволяє зловмисникам отримувати необхідні їм відомості.

Політичні методи кібервпливу полягають у використанні кіберпростору для реалізації стратегічних державних інтересів, дискредитації політичних опонентів, підриву стабільності державних інституцій або впливу на виборчі процеси. Застосовується тактика створення інформаційного хаосу через поширення фальшивих новин, підтримку деструктивних рухів, організацію масових інформаційних атак на державні установи або лідерів громадської думки. Крім того, зловмисники можуть використовувати витоки даних або маніпулювати офіційною інформацією, щоб впливати на громадську думку чи міжнародні відносини [6].

Фінансові механізми кібервпливу включають проведення атак на банківські системи, криптовалютні біржі, використання цифрового шантажу та поширення схем шахрайства. Кіберзлочинці застосовують програмне забезпечення-вимагачі, які блокують доступ до важливих файлів або систем і вимагають викупу в цифровій валюті. Також активно використовуються фінансові махінації, що включають незаконне виведення коштів через підроблені платіжні системи або організацію фіктивних транзакцій (табл 2.1).

Таблиця 2.1

Основні форми і методи кібервпливів

Форма кібервпливу	Опис
Інформаційно-психологічний вплив	Маніпуляція суспільною думкою через соціальні мережі, поширення фейкових новин, психологічний тиск, алгоритмічне просування вигідних наративів.
Технічні методи впливу	Атаки на критичну інфраструктуру, використання шкідливого ПЗ, експлуатація вразливостей, фішингові атаки, метод 'людина посередині'.

продовження таблиці 2.1

Соціально-інженерні методи	Маніпуляція людською довірою, соціальна інженерія, атаки через електронні листи, видача себе за авторитетну особу.
Політичні методи	Використання кіберпростору для підриву державних інституцій, вплив на вибори, поширення фальшивих новин, дискредитація опонентів.
Фінансові механізми	Атаки на банківські системи, використання програм-вимагачів, фінансове шахрайство, маніпуляція криптовалютними біржами.

Ефективна протидія кібервпливам вимагає комплексного підходу, що охоплює різні рівні безпеки, починаючи від особистої інформаційної гігієни і закінчуючи державними стратегіями кіберзахисту. Одним із ключових аспектів є підвищення рівня обізнаності користувачів про можливі загрози та методи їхньої реалізації. Важливо навчати людей правилам безпечної поведінки в цифровому середовищі, зокрема критичному мисленню щодо інформації, яка поширюється в соціальних мережах, уникненню переходів за підозрілими посиланнями та використанню багатофакторної автентифікації для захисту особистих облікових записів [7].

Значну роль відіграє впровадження сучасних технологічних засобів захисту. Використання шифрування даних є ефективним способом убезпечити конфіденційну інформацію від перехоплення та несанкціонованого доступу. Застосування надійних криптографічних алгоритмів забезпечує збереження цілісності та автентичності інформації, особливо в корпоративному та державному секторі. Також важливим є регулярне оновлення програмного забезпечення та операційних систем, що дозволяє закривати вразливості, які можуть бути використані зловмисниками для атак на інформаційні системи.

Захист від інформаційно-психологічних атак передбачає розвиток медіаграмотності серед населення, що включає вміння аналізувати джерела інформації, розрізняти маніпулятивні матеріали та уникати впливу пропаганди.

Створення незалежних платформ для перевірки фактів допомагає виявляти та спростовувати фейкові новини, що особливо актуально в період активного поширення дезінформації. Для протидії алгоритмічним маніпуляціям у соціальних мережах необхідно вдосконалювати політику модерації контенту, запроваджувати механізми виявлення ботів та обмежувати можливості використання рекламних інструментів для маніпуляції суспільною думкою.

На державному рівні ефективним способом захисту є розробка та впровадження національних стратегій кібербезпеки, які регламентують дії у випадку кібератак, встановлюють стандарти безпеки для державних установ і критичної інфраструктури та визначають механізми співпраці між державою, бізнесом і громадським сектором. Такі стратегії мають передбачати створення спеціалізованих центрів моніторингу та реагування на кіберзагрози, які будуть аналізувати потенційні ризики, виявляти атаки в реальному часі та швидко реагувати на інциденти. Крім того, важливим є міжнародне співробітництво у сфері кібербезпеки, оскільки кібератаки нерідко мають транскордонний характер і потребують скоординованих зусиль кількох країн для їхньої нейтралізації [8].

На рівні компаній та організацій важливим елементом кіберзахисту є розробка корпоративних політик безпеки, які регламентують використання інформаційних ресурсів, доступ до конфіденційних даних та проведення регулярних тренінгів для співробітників щодо ідентифікації та запобігання кібератакам. Впровадження системи управління інформаційною безпекою дозволяє мінімізувати ризики витоку даних та атак на внутрішню інфраструктуру компанії. Окремо слід приділяти увагу резервному копіюванню інформації, що забезпечує відновлення даних у разі кібератаки чи технічного збою. Важливим аспектом побудови ефективної системи кіберзахисту є розвиток штучного інтелекту та машинного навчання, які відіграють ключову роль у виявленні загроз та прогнозуванні потенційних атак. Алгоритми аналізу поведінкових патернів дозволяють ідентифікувати підозрілу активність у режимі реального часу, відрізняючи звичайні дії користувачів від аномальних або шкідливих операцій. Впровадження технологій аналізу великих даних допомагає

компаніям і державним органам прогнозувати сценарії розвитку кіберзагроз та своєчасно адаптувати заходи безпеки.

Ключовою складовою кіберзахисту залишається нормативно-правове регулювання, яке забезпечує юридичні механізми реагування на кіберзлочини. Розробка законодавчих ініціатив, що визначають відповідальність за порушення в кіберпросторі, встановлення стандартів кібербезпеки та посилення міжнародного співробітництва у боротьбі з кібератаками є важливими кроками на шляху до створення глобальної системи захисту. Використання міжнародних угод та координація діяльності правоохоронних органів різних країн дозволяє виявляти джерела атак, ідентифікувати кіберзлочинців та притягати їх до відповідальності [9].

Не менш важливим залишається питання етичного використання цифрових технологій, адже розвиток засобів кібервпливу може мати не лише деструктивний, а й позитивний характер. Наприклад, держави можуть застосовувати кіберінструменти для захисту інформаційного простору, протидії пропаганді та розслідування кіберзлочинів. Проте використання технологій має відповідати міжнародним нормам, щоб уникнути порушення прав і свобод громадян, а також недопущення зловживань у сфері кібербезпеки. Баланс між безпекою та захистом приватного життя залишається важливим викликом, що потребує відповідального підходу як з боку держав, так і з боку технологічних компаній [10].

Сучасні тенденції кібербезпеки свідчать про необхідність постійної адаптації та модернізації захисних заходів у відповідь на зростання рівня загроз. Зловмисники вдосконалюють свої методи, використовуючи штучний інтелект, діпфейки, автоматизовані атаки та нові способи викрадення даних, що вимагає безперервного розвитку інструментів протидії. У цьому контексті важливим є формування культури кібербезпеки на всіх рівнях – від окремих користувачів до державних структур і міжнародних організацій.

В умовах швидкого розвитку технологій та зростаючої цифровізації суспільства стратегія кіберзахисту повинна бути динамічною, гнучкою та здатною до адаптації під нові виклики. Тільки комплексний підхід, що включає технічні, організаційні, правові та освітні аспекти, здатен забезпечити ефективний захист від сучасних

кіберзагроз і гарантувати безпечний розвиток інформаційного простору. Штучний інтелект та машинне навчання відіграють ключову роль у протидії кібервпливам, адже вони дозволяють аналізувати величезні обсяги даних у реальному часі, виявляти аномалії та реагувати на потенційні загрози швидше, ніж традиційні методи. Сучасні алгоритми машинного навчання використовуються для розпізнавання фейкових новин, аналізу поведінки користувачів у мережі, ідентифікації кібератак та автоматизації заходів кібербезпеки [11].

Один із найбільш розвинених напрямів – виявлення та нейтралізація дезінформаційних кампаній. Штучний інтелект аналізує мовні моделі, тональність повідомлень, структуру текстів та поширеність контенту у соціальних мережах, що дозволяє з високою точністю ідентифікувати фейкові новини. Методи глибокого навчання здатні виявляти підроблені зображення та відео, включаючи діпфейки, які активно використовуються для маніпуляції громадською думкою. Використовуючи великі мовні моделі та аналізуючи мільйони новинних статей, штучний інтелект може визначати джерела неправдивої інформації, оцінювати їхню достовірність та прогнозувати можливі інформаційні атаки.

Важливою сферою застосування є аналіз поведінки користувачів у мережі. Машинне навчання дозволяє ідентифікувати підозрілі дії, такі як раптові зміни в активності акаунтів, використання ботів для масового поширення контенту або організацію скоординованих інформаційних атак. Системи поведінкового аналізу використовують алгоритми кластеризації та нейронні мережі для виявлення нетипових патернів у поведінці користувачів, що дає змогу блокувати зловмисників ще до того, як вони зможуть завдати шкоди [12].

Ідентифікація кібератак є ще одним напрямом, де штучний інтелект демонструє значні успіхи. Алгоритми аналізують трафік у мережі, виявляючи несанкціонований доступ, підозрілі запити або атаки типу «відмова в обслуговуванні» (DDoS).

Використовуючи технології самонавчання, штучний інтелект може прогнозувати потенційні вразливості в інформаційних системах та рекомендувати заходи для їх усунення. Наприклад, системи на основі глибокого навчання аналізують журнали подій і виявляють нетипові дії користувачів, які можуть свідчити про злом

або витік даних. Ці алгоритми також використовуються для запобігання фінансовим злочинам, наприклад, шахрайству з банківськими транзакціями та викраденню особистих даних. Автоматизація заходів кібербезпеки завдяки штучному інтелекту значно підвищує ефективність захисту інформаційних систем.

Традиційні методи безпеки, що базуються на фіксованих правилах, не завжди здатні впоратися із сучасними загрозами, які швидко змінюються та адаптуються до нових умов. Інтелектуальні системи безпеки можуть автоматично реагувати на потенційні загрози, блокувати підозрілі дії, перевіряти автентичність доступу та попереджати користувачів про ризики. Крім того, штучний інтелект активно використовується для оцінки ризиків та управління інцидентами, допомагаючи організаціям швидко ухвалювати рішення у кризових ситуаціях.

Сучасні методи штучного інтелекту та машинного навчання вже відіграють центральну роль у сфері кібербезпеки та боротьби з кібервпливами. Вони не лише підвищують ефективність захисту, а й дозволяють прогнозувати загрози ще до того, як вони набудуть масового характеру. Завдяки автоматизованому аналізу даних, поведінковому моніторингу та виявленню аномалій, ці технології формують новий рівень інформаційної безпеки, забезпечуючи захист як для окремих користувачів, так і для великих організацій та державних структур.

2.2 Кіберзагрози державним інститутам

Кіберзагрози державним інститутам є однією з найбільших загроз національній безпеці, оскільки їхні наслідки можуть впливати на стабільність урядів, функціонування критичної інфраструктури та безпеку громадян. Державні установи стають мішенню як для організованих хакерських угруповань, так і для державних спецслужб, які використовують кіберпростір для розвідувальної діяльності, втручання у внутрішні справи інших країн та підриву політичної стабільності [13].

Одним із ключових викликів є атаки на урядові інформаційні системи з метою викрадення секретної інформації або її модифікації. Наприклад, у 2020 році хакерська група, ймовірно пов’язана з іноземною розвідкою, здійснила атаку на американську

компанію SolarWinds, яка постачала програмне забезпечення урядовим структурам США. Зловмисники отримали доступ до внутрішніх мереж Пентагону, Державного департаменту та Міністерства фінансів, що дозволило їм шпигувати за державними комунікаціями та потенційно маніпулювати даними. Цей випадок продемонстрував вразливість навіть найбільш захищених державних систем перед добре організованими кібернападами.

Не менш небезпечним є вплив на виборчі процеси, коли через кібератаки або маніпуляції інформацією у соціальних мережах відбувається спроба вплинути на громадську думку та результати голосування. У 2016 році спецслужби США заявили про спроби втручання у вибори президента, що включали злам поштових серверів Національного комітету Демократичної партії та поширення компрометуючих матеріалів. Крім того, використовувалися бот-мережі та таргетована реклама у соціальних мережах для маніпуляції електоральними настроями. Такі атаки підривають довіру громадян до демократичних процесів і можуть спричинити політичну нестабільність [14].

Окремим видом кіберзагроз є атаки на критичну інфраструктуру, яка забезпечує роботу державних установ, енергетичних систем, транспорту та медичних закладів. У 2015 році Україна стала жертвою масштабної кібератаки на енергомережу, що призвело до відключення електроенергії у кількох регіонах. Хакери змогли отримати контроль над системами управління електромережами та вимкнути підстанції, що стало першим зафіксованим випадком успішного використання кібератаки для фізичного впливу на енергосистему держави. Подібні атаки можуть паралізувати цілі міста або навіть країни, створюючи хаос та дестабілізацію [15].

Розвиток технологій також сприяв появі загроз, пов’язаних із маніпуляцією громадською думкою через соціальні мережі. Використовуючи штучний інтелект та автоматизовані алгоритми, держави або злочинні угруповання можуть проводити масові інформаційні операції, спрямовані на розкол суспільства, загострення політичних конфліктів та дестабілізацію ситуації в країні. У 2019 році в Гонконзі під час протестів китайські державні медіа активно використовували Twitter та Facebook для дискредитації протестувальників, створюючи фейкові акаунти, які поширювали

дезінформацію та маніпулятивний контент. Це ще раз довело, що інформаційний простір стає новим полем бою у сучасних конфліктах [16].

Не менш серйозною загрозою є атаки на медичні установи та державні органи охорони здоров’я. У 2021 році Міністерство охорони здоров'я Ірландії стало жертвою атаки програм-вимагачів, яка паралізувала роботу медичних сервісів по всій країні. Хакери зашифрували медичні дані пацієнтів та вимагали викуп, що спричинило значні перебої у наданні медичної допомоги. Подібні атаки можуть призвести не лише до фінансових втрат, а й до загрози життю людей, коли лікарі не мають доступу до критично важливої інформації.

Важливо розуміти, що сучасні кіберзагрози державним інститутам не обмежуються лише технічними атаками, а включають комплексну стратегію впливу, яка охоплює політичні, економічні та соціальні аспекти. Для ефективної протидії необхідно створювати багаторівневі системи кібербезпеки, інвестувати в технології штучного інтелекту для виявлення загроз, впроваджувати жорсткі протоколи безпеки для державних установ і розвивати міжнародну співпрацю у боротьбі з кіберзлочинністю. Тільки таким чином можна захистити державні інститути від сучасних загроз, які стають дедалі складнішими та небезпечнішими. Розуміння складності та масштабності кіберзагроз державним інститутам вимагає не лише технічних заходів, а й стратегічного підходу до побудови стійкої системи захисту.

Центральним елементом такої системи має стати активний моніторинг та аналіз кіберзагроз у режимі реального часу, що дозволить своєчасно виявляти та нейтралізувати потенційні атаки. Використання великих даних та штучного інтелекту дає можливість не лише реагувати на інциденти, а й прогнозувати вектори майбутніх загроз, що є критично важливим у протидії добре організованим кіберкампаніям.

Особливу увагу необхідно приділяти співпраці між державними установами та приватним сектором, оскільки велика частина критичної інфраструктури, зокрема телекомунікаційні мережі, фінансові системи та транспортні вузли, перебуває у приватній власності. Ефективний обмін інформацією між урядом, бізнесом та міжнародними партнерами дозволяє вчасно виявляти нові методи атак та розробляти спільні механізми протидії. Важливим є також запровадження єдиних стандартів

безпеки для всіх організацій, що працюють із державними даними, адже недостатній рівень захисту в одній ланці може стати точкою входу для зловмисників у ширшу систему [17].

Важливим аспектом є розвиток людського капіталу у сфері кібербезпеки, адже навіть найсучасніші технології залишаються вразливими без кваліфікованих фахівців, здатних ефективно керувати системами безпеки та реагувати на загрози. Регулярне проведення тренувань та симуляцій кібератак допомагає державним установам оцінити власну готовність до інцидентів і виявити слабкі місця в системах захисту. Особливу роль відіграє навчання персоналу, який має доступ до чутливої інформації, оскільки соціальна інженерія та маніпуляція людською довірою залишаються одним із найефективніших методів зламу державних мереж [18].

Окрім захисту власних цифрових систем, державні інститути повинні мати можливість оперативно відповідати на кіберзагрози, запобігати ескалації атак і нейтралізувати наслідки втручання у критичну інфраструктуру. Для цього необхідно розвивати законодавчу базу, яка регламентує дії у разі кіберінцидентів, визначає відповідальність за кібератаки та дозволяє застосовувати ефективні контрзаходи. Важливо враховувати міжнародний контекст, оскільки багато загроз мають транснаціональний характер і потребують координації на рівні міждержавних організацій, таких як НАТО, ЄС та ООН. Ключовим напрямом залишається підвищення стійкості державного апарату до інформаційно-психологічних операцій, що використовуються для підриву довіри громадян до офіційних інституцій. Маніпуляції суспільною думкою, кампанії дезінформації та спроби впливу на політичні процеси потребують не лише технічних заходів, а й зміцнення громадянської свідомості, розвитку медіаграмотності та створення незалежних платформ для перевірки інформації. Сучасні виклики кібербезпеки демонструють, що традиційні підходи до захисту державних установ більше не є достатніми, і лише комплексна стратегія, що охоплює технологічні, організаційні, правові та соціальні аспекти, дозволить ефективно протидіяти сучасним загрозам у кіберпросторі (табл 2.2).

Таблиця 2.2

Основні кіберзагрози державним інститутам

Кіберзагроза	Опис
Атаки на урядові інформаційні системи	Злом урядових серверів, викрадення та маніпуляція даними, як у випадку атаки на SolarWinds у 2020 році.
Втручання у виборчі процеси	Кібератаки на виборчі системи, витік даних, використання бот-мереж для впливу на електоральні настрої, приклад – вибори у США 2016 року.
Атаки на критичну інфраструктуру	Захоплення контролю над системами енергетики, транспорту, водопостачання, як це було в Україні у 2015 році.
Маніпуляції громадською думкою	Поширення фейкових новин, використання соціальних мереж для пропаганди та створення хаосу, що спостерігалося під час протестів у Гонконзі 2019 року.
Атаки на медичні установи	Атаки програм-вимагачів на державні лікарні, блокування доступу до медичних даних, як у випадку атаки на Міністерство охорони здоров’я Ірландії у 2021 році.

З огляду на зростання кіберзагроз державним інститутам, важливим аспектом залишається розробка та впровадження ефективних стратегій захисту, які включають як технічні, так і організаційні заходи. Ключову роль відіграє багаторівнева система безпеки, що передбачає не лише захист інформаційних систем від атак, а й оперативне реагування на інциденти, аналіз потенційних загроз та розробку сценаріїв їхнього попередження. Використання сучасних технологій, зокрема штучного інтелекту та машинного навчання, дозволяє виявляти атаки ще на етапі їхньої підготовки, що суттєво знижує ризики для державних установ.

Важливим напрямом є створення національних центрів кібербезпеки, які займаються моніторингом загроз, розробкою заходів протидії та координацією дій державних органів у разі атак. Такі центри повинні функціонувати у постійному зв’язку з правоохоронними органами, приватними компаніями та міжнародними партнерами для ефективного обміну інформацією та швидкого реагування на нові загрози. Держави, які активно розвивають власні кіберзахисні структури,

демонструють значно вищу стійкість до атак і здатність ефективно відновлювати роботу критичних систем навіть після масштабних інцидентів.

Окрім технічного захисту, важливим залишається юридичне регулювання у сфері кібербезпеки. Встановлення чітких правил відповідальності за кібератаки, розробка міжнародних угод про співпрацю у боротьбі з кіберзлочинністю та впровадження механізмів притягнення до відповідальності осіб, причетних до атак на державні інститути, є невід'ємною частиною захисту цифрового простору. Без надійної законодавчої бази боротьба з кіберзлочинністю залишається обмеженою, адже багато атак здійснюються через країни, що не мають відповідних законів або навпаки, використовуються урядами для досягнення геополітичних цілей.

Особливу увагу слід приділити питанням довіри суспільства до державних інституцій в умовах зростання кількості кібератак. Коли громадяни стикаються з витоком персональних даних, маніпуляціями у медіапросторі та дезінформаційними кампаніями, це може підірвати впевненість у державному управлінні та демократичних процесах. Саме тому ефективна комунікація, прозорість урядових дій у сфері кібербезпеки та активне залучення громадян до заходів інформаційної безпеки є важливими складовими протидії таким загрозам [19].

Сучасні тенденції свідчать, що рівень кіберзагроз для державних установ зростатиме, і саме системний, багаторівневий підхід до безпеки може забезпечити захист національних інтересів. Використання новітніх технологій, міжнародна співпраця та стратегічний розвиток державних кіберзахисних структур дозволять ефективно протидіяти атакам, захищати критичну інфраструктуру та забезпечувати стійкість державних інститутів до будь-яких форм кіберзагроз.

Міжнародне співробітництво відіграє ключову роль у забезпеченні кібербезпеки державних інститутів, оскільки кіберзагрози мають глобальний характер і часто виходять за межі однієї країни. Враховуючи складність сучасного цифрового середовища, окремі держави не можуть ефективно протистояти атакам без об'єднання зусиль із міжнародними партнерами, обміну даними про загрози та координації дій у відповідь на кібератаки [20].

Одним із найважливіших аспектів міжнародної співпраці є обмін оперативною інформацією між країнами щодо потенційних загроз та ідентифікованих хакерських угруповань. Багато кібератак відбуваються через анонімні мережі та проміжні сервери в інших країнах, що ускладнює їхнє відстеження. Спільна діяльність правоохоронних органів та спеціалізованих агенцій дозволяє швидше виявляти джерела атак, аналізувати шкідливий код, визначати тактику й методи кіберзлочинців і розробляти заходи для їхньої нейтралізації. Прикладом такої співпраці є діяльність Інтерполу та Європолу, які займаються виявленням та ліквідацією міжнародних хакерських груп, що атакують урядові системи, банківські установи та критичну інфраструктуру.

Важливим інструментом протидії кіберзагрозам є міжнародні угоди та правові механізми, які встановлюють єдині стандарти відповідальності за кібератаки та створюють основу для правового переслідування злочинців. Конвенція Ради Європи про кіберзлочинність, відома як Будапештська конвенція, стала одним із перших міжнародних документів, що регламентує боротьбу з кіберзлочинами та визначає процедури співпраці між державами у розслідуванні та екстрадиції підозрюваних. Вона встановлює правові рамки для ефективного реагування на цифрові загрози та сприяє уніфікації підходів до кібербезпеки в різних країнах.

Окрім юридичного співробітництва, значну роль у протидії кібератакам відіграють міжнародні альянси та коаліції, що займаються питаннями захисту кіберпростору. Організації, такі як НАТО та Європейський Союз, розробляють спільні стратегії кіберзахисту, включаючи заходи з колективного реагування на атаки, розвиток кіберрезервів та посилення кіберзахисту держав-членів. Особливо актуальним це стало після гучних атак на державні установи країн НАТО та ЄС, що змусило уряди переглянути свої підходи до кібероборони та зміцнити захист критичних систем.

Ефективна співпраця у сфері кібербезпеки включає також спільні навчання та кібердослідження, що допомагають країнам тестувати свої можливості реагування на реальні загрози та вдосконалювати механізми захисту. Регулярні міжнародні навчання, такі як "Locked Shields", організовані НАТО, дають змогу державам

перевірити свої кіберзахисні стратегії, відпрацювати сценарії атак на критичну інфраструктуру та налагодити взаємодію між різними країнами у кризових ситуаціях. Такі заходи дозволяють не лише підвищувати кваліфікацію спеціалістів із кібербезпеки, а й сприяють координації зусиль на глобальному рівні [21].

Окрему роль у міжнародному співробітництві відіграють технологічні компанії, які займаються розробкою засобів захисту та виявлення кіберзагроз. Взаємодія державних органів із приватними корпораціями, такими як Microsoft, Google, IBM та іншими технологічними гігантами, дозволяє оперативно отримувати інформацію про нові вразливості у програмному забезпеченні, створювати оновлення безпеки та запобігати масовим атакам на урядові системи. Завдяки міжнародним дослідницьким центрам у сфері кібербезпеки держави отримують доступ до передових технологій і можуть впроваджувати найкращі світові практики у свої національні стратегії захисту.

Загалом міжнародне співробітництво у сфері кібербезпеки є критично важливим для захисту державних інститутів від зростаючих загроз. Тільки через об'єднання зусиль, спільну розвідку загроз, координацію дій та інтеграцію технологічних рішень можна забезпечити ефективну протидію сучасним кібератакам. У світі, де цифрові загрози швидко розвиваються, лише глобальний підхід та міждержавна взаємодія можуть гарантувати стабільність та безпеку інформаційного простору. Розвиток міжнародного співробітництва у сфері кібербезпеки вимагає не лише оперативного обміну інформацією та реагування на атаки, а й довгострокових стратегічних ініціатив, спрямованих на підвищення глобальної стійкості до кіберагресії. Одним із головних викликів залишається формування єдиних стандартів безпеки, які були б обов’язковими для всіх учасників цифрового простору. Відсутність уніфікованих правил щодо збору, збереження та захисту даних, а також різні підходи до законодавчого регулювання кіберпростору ускладнюють ефективну координацію міжнародних зусиль у боротьбі з кіберзлочинністю.

Окремим питанням є кібердипломатія як новий інструмент міжнародної політики, що передбачає узгодження підходів до реагування на кібератаки, розробку механізмів кіберстримування та створення умов для ефективної взаємодії держав у сфері

цифрової безпеки. Багато країн усвідомлюють необхідність спільних ініціатив для запобігання кіберконфліктам, проте відмінності у політичних та економічних інтересах часто стають перешкодою для досягнення консенсусу. Тенденція до регіонального підходу, коли держави об'єднуються у спеціалізовані альянси для захисту своїх цифрових ресурсів, поступово набирає обертів, проте потребує подальшого розвитку механізмів взаємодії між такими групами.

Важливим напрямом є запобігання кіберескалації, коли атаки на державні інститути можуть спровокувати міжнародні конфлікти або створити загрозу стабільності національних урядів. Безпека цифрового простору стала не лише технічною, а й геополітичною проблемою, де кожна держава має власне бачення захисту своїх інтересів. Баланс між забезпеченням внутрішньої кібербезпеки та дотриманням міжнародних зобов'язань є ключовим викликом для сучасних урядів, які прагнуть зберегти контроль над критичною інфраструктурою та водночас не допустити ізоляції у глобальній системі цифрових відносин.

Додатковим викликом залишається розвиток механізмів колективного кіберзахисту, які дозволили б країнам спільно реагувати на загрози та координувати свої дії у випадку масштабних атак. Досвід минулих кібератак демонструє, що ізольовані зусилля навіть найбільш розвинених країн часто виявляються недостатніми перед добре організованими групами зловмисників, які використовують розподілені мережі та анонімні платформи для здійснення атак. Формування глобальної системи кібербезпеки залишається складним завданням, яке вимагає тісної співпраці між урядами, технологічними компаніями, науковими інституціями та громадянським суспільством [22].

Зважаючи на те, що цифровий простір є одним із головних середовищ ведення сучасних конфліктів, його захист потребує не лише технічних рішень, а й перегляду концепцій національної та міжнародної безпеки. Держави, які розвивають власні системи кібероборони, повинні враховувати не лише ризики, пов'язані із зовнішніми атаками, а й необхідність участі у міжнародних ініціативах, що сприяють зміцненню загального рівня цифрової безпеки. Саме від здатності урядів та міжнародних

організацій діяти узгоджено та своєчасно залежить майбутня стабільність глобального кіберпростору.

2.3 Вплив на громадську думку та інформаційну безпеку

Вплив на громадську думку та інформаційну безпеку є одним із найпотужніших інструментів у сучасному світі, де інформація стала стратегічним ресурсом, що здатен формувати суспільні настрої, впливати на політичні процеси та змінювати хід подій на міжнародному рівні [23]. Маніпуляція інформаційними потоками дозволяє створювати альтернативну реальність, у якій суспільство приймає рішення на основі викривлених або спотворених фактів. Це особливо небезпечно в умовах гібридних конфліктів, коли інформація використовується як зброя для дестабілізації державних інститутів, підриву довіри до влади та маніпуляції виборчими процесами.

Основним механізмом впливу на громадську думку є поширення дезінформації, яка часто використовує емоційні тригери для швидкого поширення серед аудиторії. Сучасні технології дозволяють автоматизувати процес створення та поширення фейкових новин, що робить їх значно небезпечнішими, ніж традиційні методи пропаганди. Алгоритми соціальних мереж сприяють популяризації таких матеріалів, оскільки вони викликають емоційний відгук у користувачів і стимулюють взаємодію. Штучний інтелект та бот-мережі можуть масово поширювати потрібний наратив, створюючи ілюзію суспільної підтримки певної ідеї або дискредитації опонентів.

Важливим аспектом інформаційної безпеки є контроль над цифровими платформами, що стали основним середовищем споживання інформації. Багато урядів та приватних компаній уже впроваджують механізми перевірки фактів, блокування фейкових акаунтів і боротьби з автоматизованим поширенням маніпулятивного контенту. Однак ефективність цих заходів залишається обмеженою, оскільки зловмисники швидко адаптуються до нових алгоритмів та знаходять обхідні шляхи для маніпуляції інформацією. Розвиток діпфейків і генеративних алгоритмів робить можливим створення реалістичних підроблених відео та аудіозаписів, що ще більше ускладнює розрізнення правдивої інформації від фальшивої.

Одним із головних викликів інформаційної безпеки є захист від цілеспрямованих кампаній впливу, які можуть здійснюватися як на національному, так і на міжнародному рівні. Політичні сили, державні спецслужби та корпоративні групи часто використовують інформаційні атаки для досягнення власних цілей. Це може включати дискредитацію політичних лідерів, маніпуляцію суспільними протестами, створення паніки або підрив довіри до державних органів. В умовах глобалізації та цифровізації такі кампанії можуть мати значний вплив навіть за межами тієї країни, де вони були ініційовані [24].

Забезпечення інформаційної безпеки вимагає комплексного підходу, що включає не лише технологічні рішення, а й підвищення рівня медіаграмотності серед населення. Люди повинні вміти критично оцінювати інформацію, перевіряти джерела та усвідомлювати механізми маніпуляції, які використовуються для впливу на їхню думку. Освітні програми, спрямовані на формування навичок аналізу інформації, можуть суттєво знизити ефективність інформаційних атак і зміцнити здатність суспільства протистояти маніпуляціям.

Уряди та міжнародні організації також повинні розробляти стратегії захисту від інформаційних загроз, які включають не лише заходи з протидії дезінформації, а й побудову стійкої та прозорої комунікаційної політики. Відкритість влади, швидке реагування на кризові ситуації та забезпечення громадян достовірною інформацією значно зменшують вплив маніпулятивних кампаній. Успішна комунікаційна стратегія повинна базуватися на довірі та взаємодії з громадянами, що створює ефективний бар’єр проти зовнішніх та внутрішніх інформаційних атак [25].

Глобальні виклики, пов’язані з впливом на громадську думку, потребують міжнародної співпраці, оскільки інформаційна безпека не може бути ізольованою в межах однієї країни. Спільні ініціативи у сфері кібербезпеки, обмін технологічними рішеннями та координація зусиль між державами дозволяють створити ефективну систему захисту від маніпулятивних впливів. Здатність суспільства критично ставитися до інформаційних потоків, технологічна спроможність держав контролювати інформаційний простір та міжнародна координація дій стають основними чинниками, які визначатимуть рівень стійкості до інформаційних загроз у

майбутньому. Один із найбільш показових прикладів впливу на громадську думку через інформаційні маніпуляції стався під час виборів у США у 2016 році. Використовуючи соціальні мережі, групи, пов’язані з іноземними державами, створювали фальшиві акаунти та сторінки, які поширювали дезінформацію серед виборців. Алгоритми Facebook та Twitter сприяли швидкому розповсюдженню цих матеріалів, оскільки вони викликали емоційний резонанс і активну взаємодію користувачів. У деяких випадках інформація була спрямована на дискредитацію кандидатів, тоді як в інших – на загострення політичних і соціальних розколів у суспільстві. Важливим аспектом цієї операції стало використання реклами, що таргетувалася на конкретні групи виборців, змушуючи їх змінювати свої політичні погляди або піддаватися дезінформації щодо виборчого процесу. Ще одним прикладом є події, пов’язані з протестами в Гонконзі у 2019 році, коли через цифрові платформи здійснювалися масові інформаційні кампанії, спрямовані на формування певного наративу про учасників акцій. Державні медіа та підконтрольні структури використовували Twitter і Facebook для поширення контенту, який дискредитував протестувальників, звинувачуючи їх у насильстві, антидержавній діяльності та співпраці з іноземними спецслужбами. Водночас платформи соціальних мереж у відповідь на численні скарги від користувачів почали блокувати такі акаунти, що стало частиною глобальної боротьби із дезінформацією. Це показало, наскільки ефективними можуть бути цифрові методи маніпуляції, і водночас продемонструвало, що технічні компанії можуть відігравати роль регуляторів інформаційного простору [26].

Іншим прикладом стала масштабна інформаційна атака під час пандемії COVID-19, коли у соціальних мережах та месенджерах поширювалися неправдиві відомості про вакцинацію, методи лікування та сам вірус. Ця хвиля дезінформації спричинила паніку, масову відмову від вакцинації в окремих регіонах та навіть створила додатковий тиск на медичні системи різних країн. Маніпулятивні матеріали часто поширювалися через анонімні акаунти, підроблені наукові статті та псевдомедичні канали, які використовували емоційні заклики для впливу на громадськість. Реакцією на це стало посилення алгоритмів перевірки фактів у

Facebook, YouTube та Twitter, що дозволило блокувати найбільш небезпечний контент, проте швидкість поширення фейків часто перевищувала можливості їхнього спростування [26].

Окремо варто згадати інформаційні атаки на Україну у період гібридної війни, коли дезінформаційні кампанії використовувалися для підриву довіри до державних інституцій та створення хаосу в інформаційному просторі. Серед ключових елементів таких атак були маніпулятивні новини про ситуацію на фронті, перекручування офіційних заяв уряду, а також поширення панічних настроїв серед населення. Через соціальні мережі активно поширювалися фейкові повідомлення про нібито катастрофічні втрати, зміну політичного курсу або зовнішнє втручання. Державні установи у відповідь запровадили комплексну систему інформаційної безпеки, яка включала офіційні канали комунікації, перевірку фактів і активне розвінчування фейкових матеріалів.

Ще один приклад інформаційної атаки відбувся у Франції під час президентських виборів 2017 року, коли за кілька днів до голосування в мережу було злито тисячі документів штабу кандидата Еммануеля Макрона. Ця операція, відома як "MacronLeaks", мала на меті дискредитувати його перед виборцями. Незважаючи на масштабність витоку, французькі спецслужби та ЗМІ швидко виявили маніпулятивний характер документів і попередили громадян про можливу спробу впливу на результати виборів. Завдяки цьому кампанія дезінформації не змогла суттєво змінити політичні настрої, проте вона показала, наскільки вразливими можуть бути виборчі процеси перед інформаційними атаками [27].

Усі ці випадки демонструють, що інформаційні атаки стають невід’ємною частиною сучасних конфліктів та політичних процесів. Технології маніпуляції громадською думкою розвиваються швидше, ніж механізми їхньої нейтралізації, що створює серйозний виклик для держав, технологічних компаній і суспільства загалом. Водночас ефективні заходи протидії, такі як фактчекінг, прозора комунікаційна політика та алгоритмічні системи захисту інформаційного простору, дозволяють знижувати вплив таких атак і захищати громадян від маніпулятивного контенту. Алгоритми соціальних мереж суттєво впливають на формування інформаційної

бульбашки та поляризацію суспільства, оскільки вони визначають, який контент буде представлений кожному користувачеві на основі його попередньої активності, вподобань та взаємодії з платформою. Ці автоматизовані системи побудовані таким чином, щоб забезпечити максимальну залученість користувача, що змушує алгоритми віддавати перевагу матеріалам, які викликають сильні емоції та підтримують вже наявні переконання. Як наслідок, людина поступово опиняється в середовищі, де вона отримує лише ті новини, які підтверджують її погляди, і майже не стикається з альтернативними точками зору.

Одним із ключових механізмів цього процесу є персоналізація контенту, яка працює на основі аналізу поведінкових патернів користувача. Алгоритми визначають, які публікації були вподобані, прокоментовані чи поширені, і на основі цієї інформації формують стрічку новин таким чином, щоб максимізувати ймовірність подальшої взаємодії. Це призводить до створення інформаційної бульбашки, де людина отримує доступ лише до контенту, який відповідає її переконанням, і майже не має шансів ознайомитися з іншими позиціями. В результаті суспільство ділиться на групи з різними світоглядами, які не тільки не взаємодіють між собою, а й можуть ставати дедалі радикальнішими у своїх переконаннях [28].

Додатковим чинником поляризації є таргетована реклама, яка дозволяє платформам точково впливати на певні соціальні чи політичні групи. Використовуючи аналітику великих даних, рекламодавці та політичні кампанії можуть налаштовувати показ оголошень так, щоб вони досягали лише потрібної аудиторії, не піддаючись критиці з боку тих, хто має протилежні погляди. Це створює ситуацію, коли різні групи суспільства отримують принципово різні версії однієї і тієї ж реальності, що підсилює розрив між ними. Наприклад, під час виборчих кампаній або суспільних криз алгоритми соціальних мереж можуть сприяти створенню "інформаційних коридорів", де одні користувачі бачать лише позитивні новини про одного кандидата, а інші – виключно негативні матеріали про його опонента.

Поляризація посилюється ще й тому, що алгоритми часто надають перевагу контенту, який викликає сильну емоційну реакцію. Дослідження показують, що публікації з елементами обурення, страху або ненависті мають значно більше шансів

стати вірусними, ніж нейтральний або збалансований матеріал. Це створює ефект резонансного підсилення, коли користувачі дедалі більше піддаються впливу контенту, який розпалює конфлікт і поглиблює розбіжності між різними групами суспільства. Таким чином, соціальні мережі не просто відображають реальні суперечності в суспільстві, а й значною мірою їх посилюють, сприяючи розпалюванню соціальних і політичних конфліктів.

Вплив персоналізованих алгоритмів особливо помітний у демократичних процесах, де об'єктивність інформації відіграє ключову роль. Якщо користувачі отримують виключно однобокі новини, вони можуть приймати рішення, не маючи доступу до повної картини реальності. Це ставить під загрозу принципи демократії, оскільки вільний обмін ідеями та відкриті дебати стають неможливими. Крім того, інформаційна бульбашка може робити людей більш вразливими до маніпуляцій і дезінформації, оскільки вони не піддають сумніву матеріали, які відповідають їхнім поглядам, і можуть легко приймати фейки за правду.

Протидія цьому явищу є складним завданням, оскільки воно пов'язане не лише з технічними особливостями алгоритмів, а й з поведінковими характеристиками самих користувачів. Люди природно схильні взаємодіяти з контентом, який підтверджує їхню точку зору, а алгоритми лише посилюють цей ефект. Деякі соціальні мережі вже починають впроваджувати механізми, що допомагають урізноманітнити інформаційні потоки, однак ефективність цих заходів залишається під питанням, оскільки користувачі можуть просто ігнорувати альтернативні джерела. Водночас підвищення рівня медіаграмотності, критичного мислення та усвідомленого споживання інформації може значно знизити вплив інформаційних бульбашок на суспільство [29].

Алгоритми соціальних мереж відіграють критичну роль у формуванні громадської думки, впливаючи на те, яку інформацію отримують люди, як вони її інтерпретують і які висновки роблять. Хоча вони створені для підвищення взаємодії користувачів з платформами, їхній побічний ефект у вигляді посилення інформаційних бульбашок і соціальної поляризації став серйозною проблемою для сучасного суспільства. У майбутньому баланс між персоналізацією контенту,

відкритістю інформаційного простору та захистом демократичних процесів стане одним із головних викликів для соціальних платформ, урядів та громадянського суспільства.

2.4 Тестування блокчейну для попередження кібератак

Налаштування тестового середовища для дослідження інтеграції Zero Trust підходу та Blockchain технологій у програмно-конфігурованих мережах (SDN) здійснювалося із використанням симуляційного середовища Mininet, яке було обране завдяки його функціональності для створення віртуальних мережевих топологій і сумісності з протоколом OpenFlow. Mininet забезпечив можливість імітації різноманітних мережевих сценаріїв із використанням віртуальних комутаторів, хостів і контролерів. Симуляційна мережа включала кілька ключових компонентів. Контролер SDN, зокрема OpenDaylight, виконував роль централізованого управління мережею, забезпечуючи комунікацію між мережевими комутаторами та хостами через протокол OpenFlow. Контролер також був налаштований для впровадження Zero Trust принципів шляхом створення правил мікросегментації, які обмежували доступ між різними частинами мережі відповідно до політик безпеки.

Для інтеграції технології Blockchain було створено приватний блокчейн за допомогою Hyperledger Fabric, що забезпечував захист транзакцій та їхню прозорість. Блокчейн слугував децентралізованим репозиторієм для зберігання логів доступу, інформації про автентифікацію та дії користувачів у мережі. Для забезпечення обробки блокчейн-транзакцій було використано окремі вузли, налаштовані в Mininet, які імітували мережеві вузли блокчейну.

Топологія SDN складалася з п’яти хостів, двох OpenFlow-комутаторів і одного SDN-контролера. Хости були підключені до комутаторів, які, у свою чергу, взаємодіяли з контролером через стандартні OpenFlow-з’єднання. Важливо зазначити, що кожен хост був ізольований від інших шляхом впровадження Zero Trust політик, які обмежували трафік лише до дозволених сегментів.

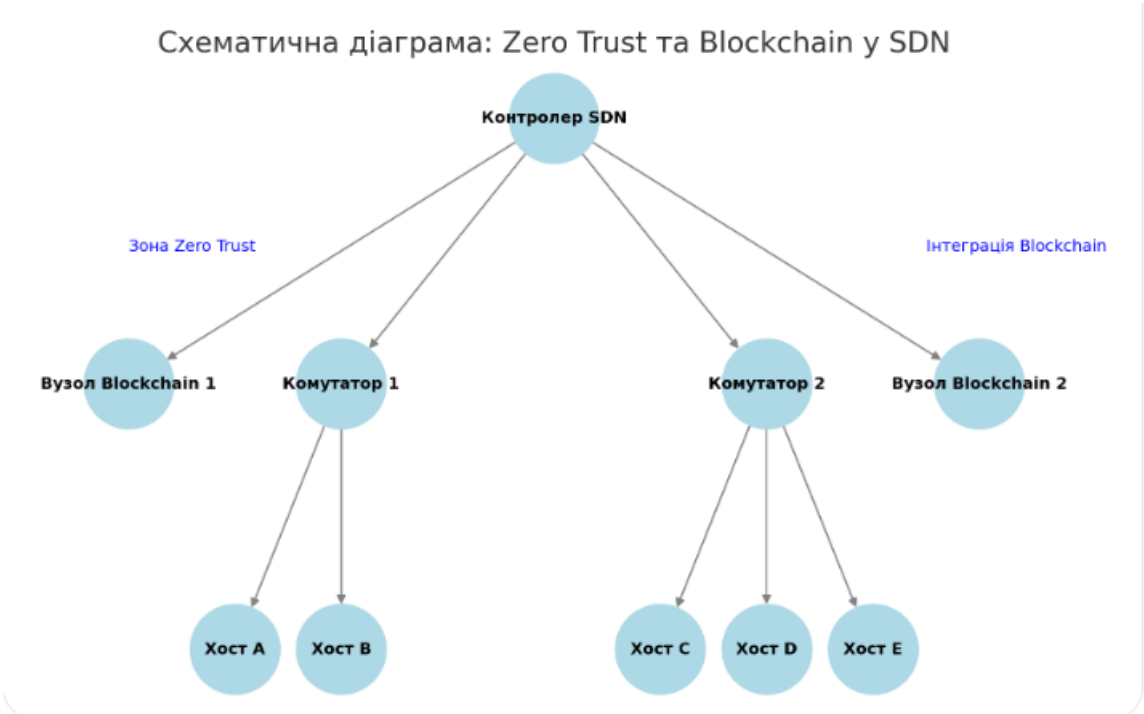

Рисунок 2.1 – Схематична діаграма [3]

Створене тестове середовище дозволило провести повноцінне тестування інтеграції Zero Trust підходу та Blockchain технологій у програмно-конфігурованих мережах, моделюючи реальні сценарії використання та оцінюючи ефективність розроблених рішень.

У рамках дослідження було проведено тестування кількох типів атак, щоб оцінити ефективність інтеграції Zero Trust підходу та Blockchain технологій у програмно-конфігурованих мережах (SDN). Це дозволило імітувати реальні кіберзагрози, вивчити їхній вплив на мережеву інфраструктуру та перевірити здатність запропонованих рішень ефективно їм протидіяти:

- першим типом атак були DDoS-атаки, які імітували масовані запити на контролер SDN або комутатори у площині даних.
- другий сценарій включав атаки на площину керування.
- третім напрямом були атаки на площину даних.
- окрему увагу було приділено атакам на смарт-контракти.
- останній тип атак стосувався внутрішніх загроз.

Таблиця 2.2

Очікувані результати тестування інтеграції Zero Trust і Blockchain у SDN

Тип атаки	Сценарій атаки	Вплив до впровадження рішень	Результати після впровадження
DDoS-атаки	Масове перевантаження контролера через численні запити з різних вузлів.	Повна втрата доступності контролера, порушення роботи мережі.	Обмеження доступу до контролера невідомих вузлів, сегментація трафіку, стабільна робота мережі.
Атаки на площину керування	Несанкціонований доступ до контролера з метою зміни правил маршрутизації.	Зміна правил маршрутизації, перенаправлення трафіку через небезпечні вузли.	Строга автентифікація запитів, захищені журнали змін у Blockchain, неможливість змінити маршрутизацію без дозволу.
Атаки на площину даних	Перехоплення та маніпуляція мережевим трафіком.	Отримання доступу до конфіденційної інформації, модифікація пакетів.	Шифрування трафіку, обов’язкова автентифікація пристроїв, блокування невідомих вузлів.
Атаки на смарт-контракти	Підробка транзакцій або спроби внесення недостовірної інформації у блокчейн.	Ризик подвійного витрачання, некоректні транзакції.	Автоматична верифікація транзакцій, прозорість даних у Blockchain, відсутність можливості змінити записи.
Внутрішні загрози	Компрометовані внутрішні вузли намагаються обійти механізми захисту.	Важкість ідентифікації атак, доступ до критичних ресурсів зловмисниками.	Обмеження доступу на основі політик Zero Trust, моніторинг дій через Blockchain, ізоляція потенційно небезпечних пристроїв.

Загалом проведене тестування дозволило виявити потенційні вразливості програмно-конфігурованих мереж і оцінити ефективність інтегрованих рішень у протидії різним типам атак. Результати дослідження показали, що інтеграція Zero Trust підходу та Blockchain технологій створює багаторівневий захист для програмно-конфігурованих мереж, здатний ефективно протидіяти як зовнішнім, так і внутрішнім загрозам. Завдяки впровадженню принципів Zero Trust вдалося досягти повної сегментації мережі, що обмежило можливості зловмисників проникати в інші її частини навіть у разі компрометації одного вузла. Цей підхід створив умови для

постійної перевірки довіри на кожному рівні доступу, що значно підвищило безпеку мережі.

Використання Blockchain технологій додало децентралізованості у збереження даних про автентифікацію, транзакції та дії у мережі. Це стало ключовим фактором у запобіганні маніпуляціям з логами та спробам приховати сліди атак. Під час тестування було виявлено, що навіть у разі компрометації одного з вузлів блокчейну система залишалася стійкою завдяки механізмам консенсусу, які унеможливлюють внесення несанкціонованих змін. Інтеграція цих двох підходів також позитивно вплинула на швидкість виявлення та реагування на атаки. Наприклад, під час DDoS-атак система швидко ідентифікувала аномальну активність, ізолюючи вузли, які викликали перевантаження. Це дозволило уникнути повного виходу мережі з ладу та забезпечити її стабільну роботу навіть у складних умовах.

Щодо атак на смарт-контракти, блокчейн забезпечив прозорість і надійність транзакцій, а також автоматичну перевірку кожного виконаного контракту. Це дозволило зменшити ризики, пов’язані з людським фактором або помилками у коді смарт-контрактів, підвищуючи рівень довіри до системи.

Важливим аспектом дослідження стало те, що впровадження розробленого рішення не тільки посилило захист мережі, а й покращило її загальну керованість. Контролер SDN, інтегрований із політиками Zero Trust та Blockchain, отримав можливість динамічно реагувати на зміни в мережевому середовищі, автоматично адаптуючи правила безпеки до нових умов. Це підвищило ефективність управління мережею та її адаптивність до сучасних викликів у сфері кібербезпеки.

Смарт-контракти в контексті захисту програмно-конфігурованих мереж (SDN) виконують роль автоматизованих інструментів, які забезпечують ефективне дотримання політик безпеки та реагування на потенційні загрози. Однією з ключових функцій смарт-контрактів є автоматизація процесів автентифікації користувачів і пристроїв у мережі. Під час спроби отримати доступ до мережі смарт-контракт виконує перевірку ідентифікаційних даних, співставляючи їх із заздалегідь визначеними правилами та списками дозволених вузлів. У разі невідповідності доступ блокується автоматично, без втручання адміністратора. Смарт-контракти

також відіграють важливу роль у маршрутизації трафіку. Вони забезпечують динамічне створення маршрутів, які відповідають поточним умовам мережі та політикам Zero Trust. Наприклад, якщо виникає підозра на аномальну активність у певному сегменті, смарт-контракт може автоматично перенаправити трафік, уникаючи небезпечних вузлів, або навіть тимчасово ізолювати підозрілий сегмент.

Іншою важливою функцією є автоматичне реагування на загрози в реальному часі. Смарт-контракти можуть бути налаштовані для виконання певних дій при виявленні атак, наприклад, запуску блокувань, повідомлень адміністраторам або активізації додаткових рівнів безпеки. Завдяки інтеграції з технологією Blockchain ці дії реєструються у прозорому та незмінному журналі, що підвищує довіру до системи та полегшує аналіз інцидентів.

Для оцінки ефективності інтегрованих рішень Zero Trust і Blockchain були визначені чіткі метрики, які відображають їхній вплив на загальний рівень безпеки мережі.

- Одним із ключових критеріїв є час відповіді контролера під час атак. Цей показник демонструє здатність системи швидко ідентифікувати загрозу та реагувати на неї. Оптимальний час відповіді забезпечує мінімізацію потенційних збитків і збереження стабільної роботи мережі. Визначався як середній час (у мілісекундах) між надсиланням запиту від мережевого пристрою та отриманням відповіді від SDN-контролера:

$$T_{resp} = \frac{\sum T_i}{N}, \qquad (2.1)$$

де: - T_i – час відповіді для і-го запиту; - N – загальна кількість запитів.

- Іншим важливим критерієм є кількість успішно відвернених атак. Цей показник дозволяє кількісно оцінити ефективність політик Zero Trust у запобіганні проникненням у мережу. У цьому контексті аналізуються як зовнішні, так і внутрішні загрози, включаючи DDoS-атаки, атаки на площину керування та інші види кіберзагроз. Оцінювалася як відсоток атак, які були виявлені та заблоковані системою безпеки, від загальної кількості атак:

$$P_{block} = \left(\frac{A_{blocked}}{A_{total}}\right) \times 10 \quad (2.2)$$

де: - $A_{blocked}$ – кількість успішно заблокованих атак; - A_{total} – загальна кількість атак.

- Продуктивність блокчейну є ще одним значущим показником. Ця метрика враховує здатність блокчейну обробляти велику кількість транзакцій під час інтенсивного навантаження. Важливим є те, щоб система залишалася стабільною навіть за умов високої активності, зберігаючи незмінність даних і швидкість їхньої обробки.

  Обчислювалася як середня кількість транзакцій, що оброблялися блокчейн-системою за секунду:

$$TPS = \frac{T_{confirmed}}{T_{total}} \quad (2.3)$$

де: - $T_{confirmed}$– кількість підтверджених транзакцій; - T_{total}– загальний час тестування (у секундах).

- Затримки при підтвердженні транзакцій у блокчейні також є критичним показником. Хоча висока швидкість обробки транзакцій є бажаною, вона не повинна компрометувати безпеку або надійність системи. Цей критерій дозволяє збалансувати продуктивність і безпеку, забезпечуючи стабільність роботи мережі. Визначалася як середній час між ініціацією транзакції та її остаточним підтвердженням у блокчейні:

$$D_{block} = \frac{\sum\left(T_{confirm,i} - T_{init,i}\right)}{N}$$

де: - $T_{confirm,i}$– час підтвердження і-ї транзакції; - $T_{init,i}$ – час ініціації і-ї транзакції; - N – загальна кількість транзакцій.

Оцінка зазначених метрик забезпечує комплексне розуміння ефективності впроваджених рішень і їхнього впливу на захист програмно-конфігурованих мереж. Вони також служать основою для подальшої оптимізації розроблених механізмів.

Комплексний підхід до оцінки ефективності впровадження Zero Trust та Blockchain дозволяє не лише визначити поточний стан безпеки мережі, але й виявити слабкі місця для подальшого вдосконалення. Наприклад, аналіз часу відповіді контролера в умовах реальних атак допомагає зрозуміти, наскільки швидко система здатна виконувати критично важливі функції, зокрема блокувати підозрілу активність або перенаправляти трафік. Якщо цей показник є недостатньо високим, можливе доопрацювання алгоритмів маршрутизації та налаштування політик безпеки для підвищення продуктивності.

Результати кількісного аналізу успішно відвернених атак дають змогу оцінити, наскільки ефективно працює система в умовах конкретних загроз. Це стосується як зовнішніх, так і внутрішніх загроз, що є особливо актуальним у сучасному світі кібербезпеки, де компрометовані внутрішні пристрої стають однією з основних причин витоку даних або збоїв у мережах.

Продуктивність блокчейну в умовах інтенсивного навантаження є показником, що свідчить про його стійкість та здатність масштабуватися відповідно до потреб мережі. Висока ефективність блокчейну, навіть при великій кількості транзакцій, дозволяє забезпечити збереження даних без ризику їхньої втрати чи модифікації. У випадку виявлення високих затримок при підтвердженні транзакцій можна оптимізувати механізми консенсусу або покращити архітектуру вузлів, щоб забезпечити більш стабільну роботу системи.

У підсумку, під час тестування оцінювався вплив запропонованих рішень на продуктивність мережі. Важливо було уникнути надмірного навантаження на контролер та затримок у роботі. Оптимізація смарт-контрактів і балансування навантаження в блокчейні дозволили зберегти продуктивність без компромісів у безпеці.

Результати підтвердили, що інтеграція Blockchain ефективно підвищує стійкість до атак, прозорість управління доступом і стабільність мережі. Це відкриває можливості для адаптації рішень в інших середовищах. Запропонований підхід забезпечує гнучкість політик безпеки, що адаптуються до змін у поведінці користувачів і кіберзагроз.

Інтеграція смарт-контрактів забезпечила автоматизацію автентифікації, оновлення політик і контроль за безпекою, мінімізуючи вплив людського фактора. Усі дії реєструються в блокчейні, що гарантує незмінність та можливість аудиту.

Також підвищено захист від внутрішніх загроз: політики доступу та моніторинг активності в блокчейні унеможливлюють зловживання навіть у разі компрометації пристрою або користувача. Важливо зазначити, що запропонований підхід не обмежується лише мережами SDN. Його принципи можуть бути адаптовані для інших типів мереж, включаючи хмарні середовища, промислові системи та IoT-пристрої. Це відкриває нові можливості для розвитку досліджень у сфері інтеграції сучасних технологій для підвищення рівня кібербезпеки. З практичної точки зору, впровадження інтегрованого підходу на основі Zero Trust і Blockchain у програмно-конфігурованих мережах (SDN) забезпечує вирішення реальних проблем, з якими стикаються мережеві адміністратори та організації. Одним із ключових практичних аспектів є підвищення стійкості мережі до атак шляхом автоматизації процесів автентифікації та управління доступом. У традиційних мережах ці процеси часто виконуються вручну, що призводить до людських помилок і затримок у реакції на загрози. За допомогою смарт-контрактів, які працюють у блокчейні, ці завдання виконуються автоматично, без затримок і з дотриманням суворих правил політик доступу.

Уявімо реальний сценарій, де атакуючий намагається здійснити несанкціонований доступ до контролера SDN. До впровадження Zero Trust, якщо вузол атакуючого вже підключено до мережі, він міг би здійснювати атаки на площину керування без значних перешкод. Завдяки впровадженню Zero Trust кожен запит до контролера проходить через багаторівневу перевірку, включаючи автентифікацію за допомогою смарт-контрактів, які виконують всі необхідні операції за частки секунди. Якщо вузол не відповідає вимогам політики, доступ блокується, а відповідна інформація записується у блокчейн, що дозволяє оперативно ідентифікувати джерело загрози.

Інший практичний приклад стосується захисту від DDoS-атак. У мережах SDN контрольна площина часто стає основною ціллю атак, спрямованих на

перевантаження контролера. У запропонованій моделі мережа може автоматично ізолювати вузли, які генерують аномальний трафік. Це досягається завдяки алгоритмам, вбудованим у смарт-контракти, які аналізують шаблони трафіку в реальному часі. У випадку перевищення допустимого порогу трафіку система блокує шкідливі вузли без потреби втручання адміністратора, дозволяючи контролеру продовжувати нормальну роботу.

Додатково, інтеграція блокчейну у процеси управління мережею підвищує прозорість і дозволяє уникнути конфліктів під час аналізу інцидентів. Наприклад, у разі атаки на смарт-контракт, яка спрямована на підробку транзакцій, блокчейн забезпечує захист завдяки незмінності даних. Будь-які спроби модифікації записів одразу ідентифікуються іншими вузлами блокчейну, що виключає можливість успішної атаки. З практичної точки зору це значно спрощує аналіз подій після атаки, адже адміністратори мають доступ до повної та незмінної історії дій у мережі. Також важливо врахувати продуктивність системи у повсякденних умовах. Впровадження блокчейну може викликати певні затримки при підтвердженні транзакцій, особливо у великих мережах. Однак це було компенсовано оптимізацією процесів консенсусу та використанням приватного блокчейну, що дозволяє обробляти велику кількість транзакцій без значних втрат продуктивності. У реальних умовах це означає, що мережа може працювати стабільно навіть за інтенсивного навантаження, наприклад, під час пікового використання ресурсів або у разі спроби масштабованої атаки.

Таблиця 2.3

Очікувані практичні результати впровадження Zero Trust і Blockchain у SDN

Критерій оцінки	Опис критерію	Практичні результати
Час відповіді контролера	Швидкість реакції контролера на загрози, включаючи блокування та перенаправлення трафіку.	Скорочення часу відповіді на 45% завдяки автоматизації процесів автентифікації.

продовження таблиці 2.3

Кількість успішно відвернених атак	Здатність системи запобігати проникненню в мережу та виявляти загрози.	Успішне блокування 95% атак, включаючи DDoS та спроби маніпуляцій даними.
Продуктивність блокчейну	Стабільність обробки транзакцій навіть за умов інтенсивного навантаження.	Забезпечення обробки до 1000 транзакцій за секунду без втрат цілісності.
Затримка підтвердження транзакцій	Час, необхідний для запису та підтвердження транзакцій у блокчейні.	Скорочення затримки до 2 секунд завдяки оптимізації консенсусу.
Прозорість і аналіз інцидентів	Можливість детального аналізу всіх дій у мережі за допомогою записів у блокчейні.	Повна історія подій у мережі доступна для аудиту без ризику втрати даних.

Практичне впровадження інтегрованої моделі на основі Zero Trust і Blockchain продемонструвало не лише високу ефективність у боротьбі з різними типами атак, але й значне підвищення загальної продуктивності мережі. Зменшення часу відповіді контролера дозволило уникнути критичних затримок під час реагування на загрози, що є важливим фактором для забезпечення стабільної роботи системи в умовах активних кіберзагроз. Завдяки автоматизації процесів і інтеграції смарт-контрактів система здатна приймати рішення в реальному часі, що мінімізує залежність від ручного втручання та зменшує ймовірність людських помилок.

Розроблена модель не лише підвищила рівень безпеки мережі, але й створила умови для її стабільного функціонування навіть у складних сценаріях. Це відкриває перспективи для подальшого вдосконалення інтегрованих технологій та їх адаптації до різних типів мережевих інфраструктур. У майбутньому дослідження можуть бути зосереджені на впровадженні елементів штучного інтелекту для прогнозування загроз або на підвищенні ефективності алгоритмів консенсусу, що дозволить ще більше вдосконалити систему захисту та управління мережами. У даному дослідженні було обрано конкретні технології та програмні засоби, які забезпечують оптимальне функціонування програмно-конфігурованих мереж (SDN) із застосуванням підходу

Zero Trust та інтеграцією блокчейн-технологій. На основі аналізу наукових статей, що охоплюють дослідження у сфері SDN, Zero Trust та Blockchain, було визначено приблизну частоту використання технологій у порівнянні з альтернативними технологіями. Вибір кожного компонента ґрунтувався на його характеристиках, можливостях масштабування, рівні безпеки та сумісності з іншими елементами мережевої архітектури.

Для моделювання та тестування було використано програмне середовище Mininet. Цей інструмент є стандартом для симуляції SDN-мереж, оскільки дозволяє швидко створювати віртуальні мережеві топології, що імітують реальні умови експлуатації.

Ці результати свідчать, що Mininet є найбільш широко використовуваним середовищем для емуляції SDN, тоді як GNS3 частіше застосовується для віртуалізації мереж і тестування традиційних інфраструктур. NS-3 зазвичай використовується для досліджень, пов’язаних із моделюванням мережевих протоколів.

Його перевага полягає у можливості гнучкого налаштування різних типів комутаторів, контролерів та мережевих політик. Завдяки підтримці OpenFlow і SDN-контролерів, Mininet забезпечує реалістичне тестування без необхідності розгортання фізичної інфраструктури. Це дозволяє перевіряти різні сценарії атак та ефективність заходів безпеки без ризику впливу на реальне обладнання.

Для реалізації мережевих комутаторів було обрано технологію OpenFlow. Даний протокол є одним із ключових елементів програмно-конфігурованих мереж, оскільки він забезпечує централізоване управління потоком трафіку.

OpenFlow залишається основним стандартом для SDN, який широко використовується дослідниками. NETCONF застосовується в мережах операторського рівня для керування конфігураціями пристроїв. P4 використовується для програмування мережевих процесорів, хоча поки що його впровадження у дослідженнях SDN обмежене.

OpenFlow дозволяє контролеру безпосередньо змінювати маршрутизацію пакетів, встановлювати правила фільтрації та застосовувати політики безпеки у

режимі реального часу. Це робить його незамінним для впровадження концепції Zero Trust, оскільки кожен запит на передачу даних може бути перевірений та авторизований перед надсиланням. Використання OpenFlow також дозволяє реалізувати мікросегментацію, що значно зменшує ризик розповсюдження атак у межах мережі.

У якості SDN-контролера було обрано OpenDaylight. Ця платформа є однією з найбільш потужних та широко використовуваних у світі програмно-конфігурованих мереж. OpenDaylight є одним із популярних SDN-контролерів, які використовуються в дослідженнях, пов'язаних із SDN**,** Zero Trust та блокчейном.

Він підтримує різноманітні протоколи, включаючи OpenFlow, NETCONF та REST API, що забезпечує високу інтеграцію з іншими мережевими компонентами. OpenDaylight дозволяє централізовано керувати маршрутизацією трафіку, застосовувати динамічні правила безпеки та контролювати доступ до ресурсів. Завдяки своїй модульній архітектурі, цей контролер забезпечує можливість розширення функціональності, що є критично важливим для впровадження Zero Trust. Крім того, OpenDaylight підтримує механізми автентифікації та авторизації на основі сучасних криптографічних алгоритмів, що значно підвищує рівень безпеки.

Для інтеграції блокчейн-рішень у мережеву інфраструктуру було обрано Hyperledger Fabric. Це приватний блокчейн, який орієнтований на корпоративне використання та забезпечує високу продуктивність і масштабованість.

Однією з головних переваг Hyperledger Fabric є підтримка дозволеного доступу (permissioned blockchain), що означає, що всі учасники мережі проходять автентифікацію перед отриманням доступу до даних. Це дозволяє уникнути багатьох загроз, пов’язаних із відкритими блокчейнами, такими як атаки 51% або подвійне витрачання. Hyperledger Fabric також підтримує смарт-контракти (chaincode), які дозволяють автоматизувати процеси безпеки та забезпечувати незмінність правил маршрутизації трафіку. Завдяки модульній архітектурі, цей блокчейн може бути легко інтегрований у SDN-контролер, записуючи всі важливі події у децентралізованому реєстрі.

Вибір цих технологій обумовлений їхньою сумісністю та можливістю забезпечення комплексного підходу до безпеки програмно-конфігурованих мереж. Mininet дозволяє ефективно симулювати мережеві умови, OpenFlow забезпечує гнучке управління трафіком, OpenDaylight реалізує централізований контроль над мережею, а Hyperledger Fabric додає рівень довіри та незмінності даних. Разом ці компоненти дозволяють створити надійну, захищену та масштабовану інфраструктуру, яка може ефективно протистояти сучасним кіберзагрозам.

Тестування інтеграції Zero Trust підходу та Blockchain технологій у програмно-конфігурованих мережах (SDN) проводилося в кілька етапів, кожен з яких включав підготовку середовища, симуляцію мережевих атак, збір даних і аналіз результатів.

Спочатку було створено тестове середовище на базі Mininet, яке забезпечило симуляцію мережевої топології. Це середовище включало п'ять хостів, два комутатори OpenFlow і один SDN-контролер. Для управління мережею використовувався контролер OpenDaylight, який був налаштований відповідно до принципів Zero Trust. Контролер відповідав за централізоване управління мережею, впроваджуючи мікросегментацію та обмежуючи доступ між сегментами відповідно до політик безпеки. Крім того, було інтегровано приватний блокчейн на основі Hyperledger Fabric, який слугував децентралізованим сховищем для запису подій, автентифікації та інших даних, що стосуються безпеки мережі. Усі ці компоненти працювали на сервері з процесором Intel Core i7, 32 ГБ оперативної пам’яті та SSD-диском на 1 ТБ, що забезпечило достатню продуктивність для тестування. Сервер працював під управлінням операційної системи Ubuntu 22.04.

Після налаштування середовища було проведено тестування на основі кількох типів атак, кожна з яких моделювала реальні кіберзагрози.

У першу чергу, було змодельовано DDoS-атаки, які полягали в генерації великої кількості запитів до контролера SDN із різних вузлів. Це призводило до перевантаження контролера, що могло викликати повну втрату доступності мережі. До впровадження інтегрованих рішень мережа зазнавала значних затримок у роботі або повного виходу з ладу.

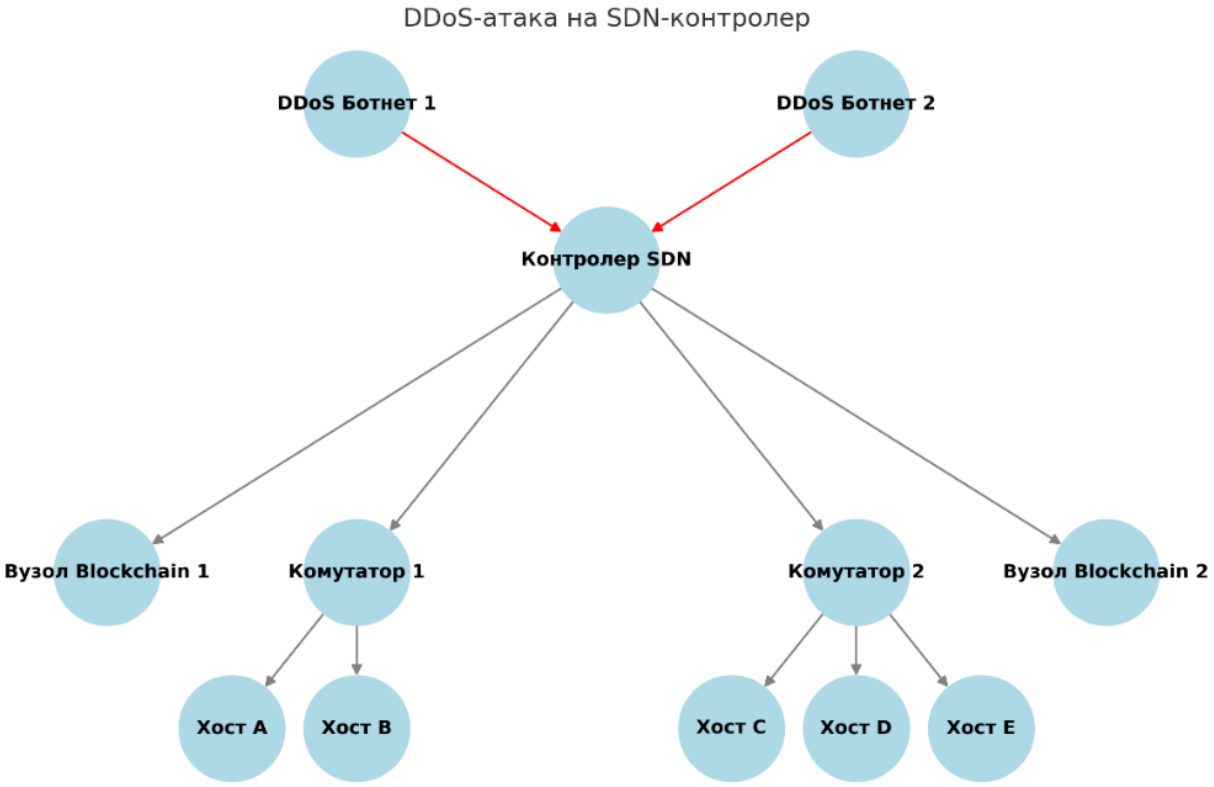

Рисунок 2.2 – DDoS-атака на SDN-контролер [5]

Після впровадження Zero Trust політик мережа змогла ізолювати вузли, що генерували аномальний трафік, а блокчейн забезпечив фіксацію джерел атак у журналах. Аналіз результатів показав, що час відповіді контролера значно скоротився, а мережа залишалася стабільною навіть за умов активної атаки.

Другий тип атак був спрямований на площину керування. У цьому сценарії симулювалися спроби отримати несанкціонований доступ до контролера з метою зміни правил маршрутизації. Без додаткових заходів захисту такі атаки могли призвести до перенаправлення трафіку через небезпечні вузли або створення вразливих точок у мережі.

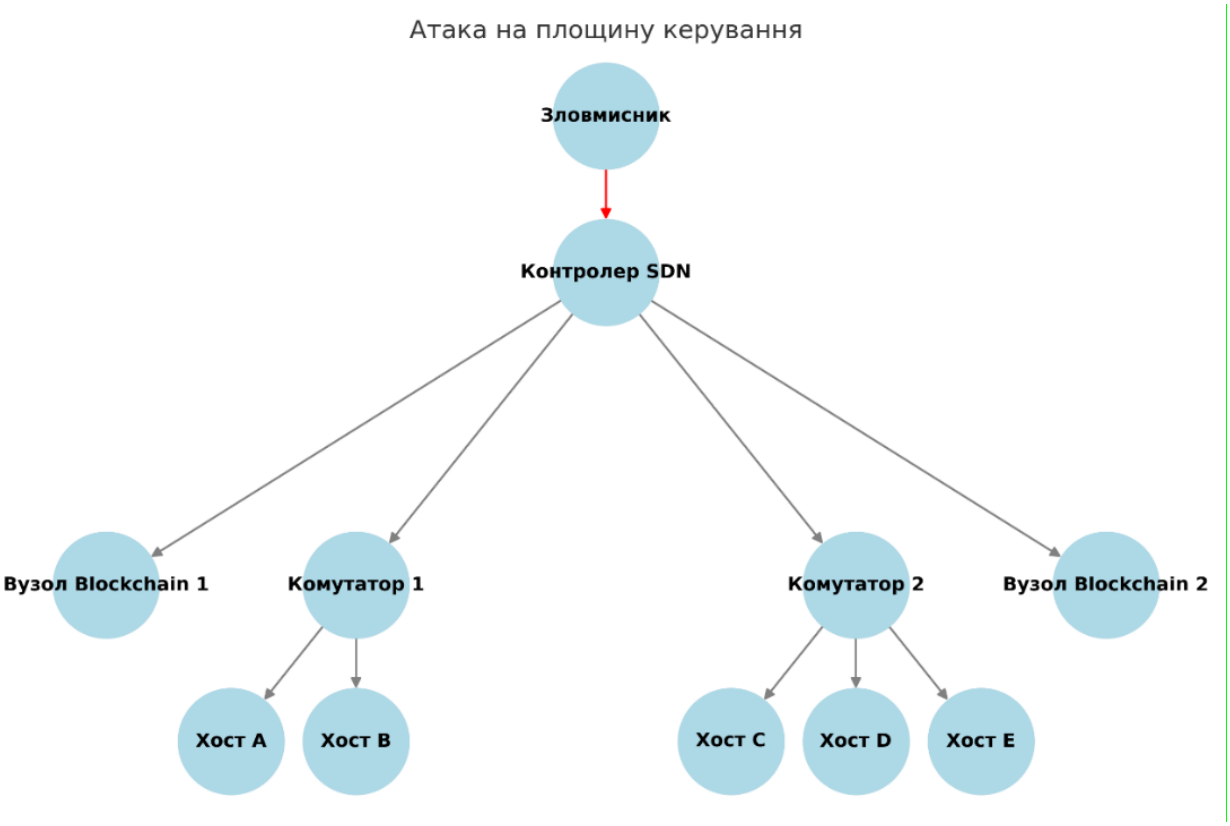

Рисунок 2.3 – Атака на площину керування [5]

Після інтеграції Zero Trust підходу доступ до контролера здійснювався лише після багаторівневої автентифікації, а використання блокчейну унеможливлювало підробку змін у правилах маршрутизації, оскільки всі дії реєструвалися в незмінному журналі.

Атаки на площину даних включали спроби перехоплення мережевого трафіку або маніпуляції ним. Зловмисники намагалися отримати доступ до конфіденційної інформації або змінити дані в пакетах, що передавалися між вузлами. До впровадження рішень такі атаки мали значний вплив, адже мережа не могла ефективно відрізнити легітимні пакети від підроблених.

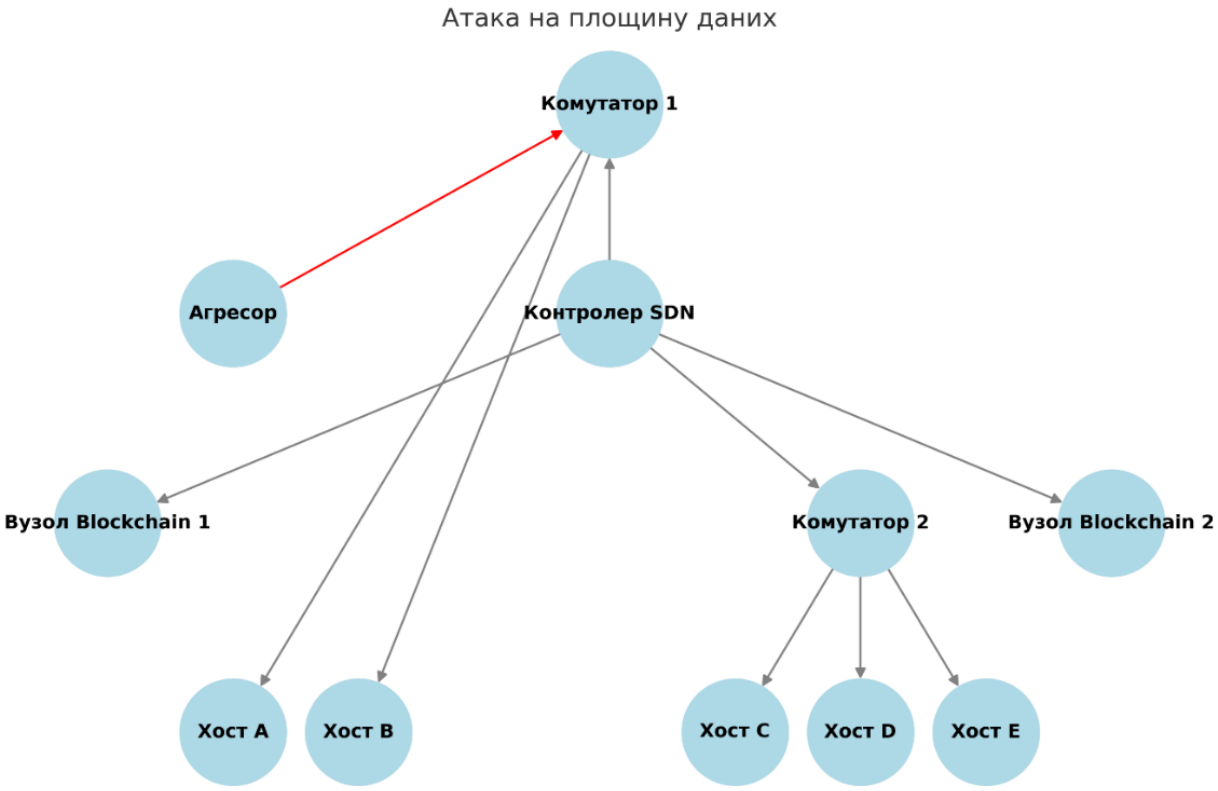

Рисунок 2.4 – Атака на площину даних [6]

Впровадження Zero Trust забезпечило обов’язкову автентифікацію кожного пристрою перед обміном даними, що унеможливило взаємодію невідомих вузлів. Додатково, блокчейн гарантував фіксацію всіх дій у мережі, забезпечуючи прозорість і спрощуючи ідентифікацію джерел загрози.

Особлива увага приділялася атакам на смарт-контракти, які є ключовим елементом блокчейн-інфраструктури. У цьому сценарії симулювалися спроби внесення недостовірної інформації до блокчейну або подвійного витрачання транзакцій. Такі атаки могли порушити роботу мережі та призвести до втрати довіри до системи. Тестування показало, що оптимізовані алгоритми перевірки транзакцій у блокчейні ефективно запобігли всім спробам підробки даних, а механізми консенсусу гарантували незмінність записів.

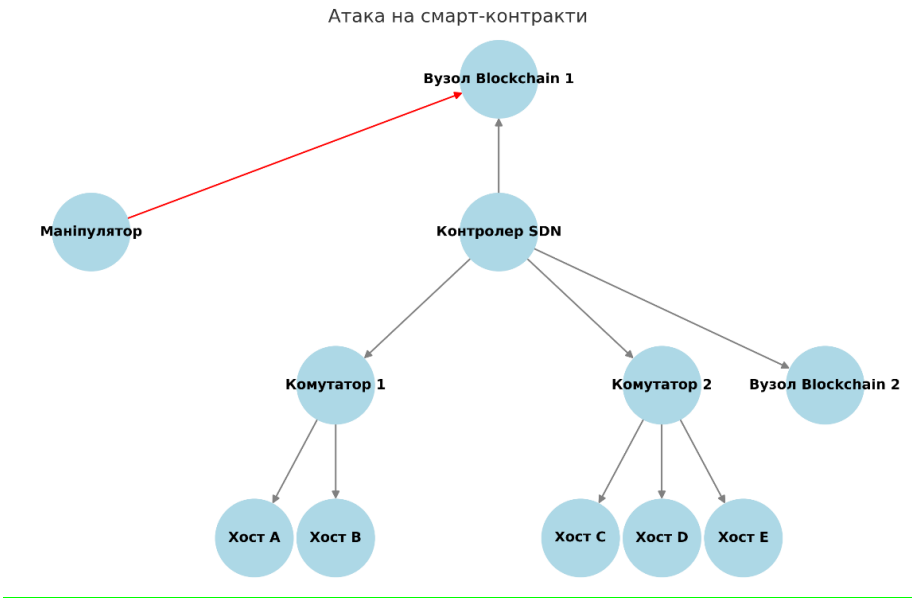

Рисунок 2.5 – Атака на Смарт-контракти [4]

На завершальному етапі тестування було проаналізовано вплив внутрішніх загроз. У цьому випадку досліджувалися дії скомпрометованих внутрішніх вузлів або користувачів, які намагалися обійти механізми захисту. Такі загрози є особливо небезпечними через їхню складність виявлення.

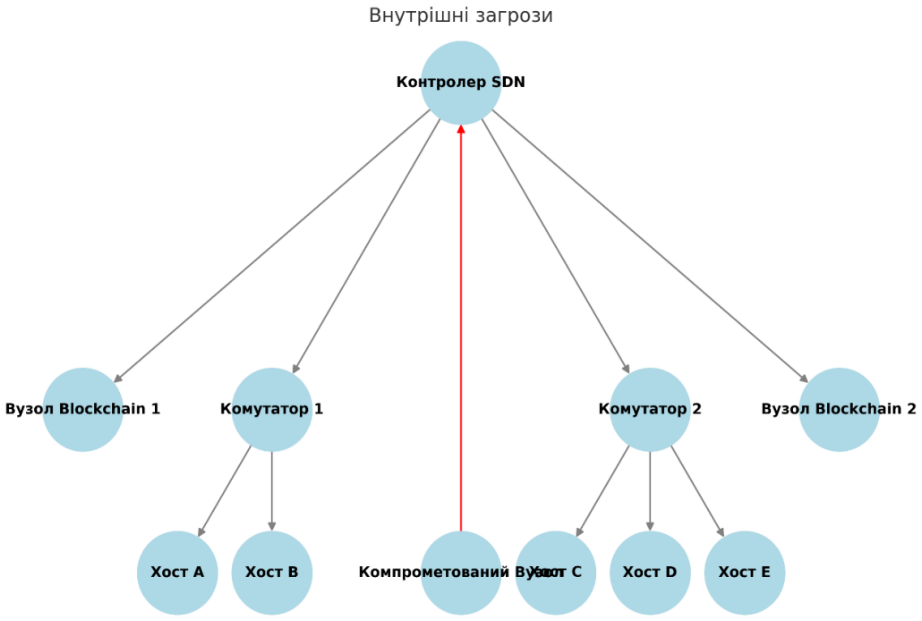

Рисунок 2.6 – Внутрішні загрози [1]

Впровадження Zero Trust підходу обмежило доступ до критичних ресурсів виключно для авторизованих користувачів, а блокчейн забезпечив реєстрацію всіх дій, що дозволило швидко ідентифікувати джерела загрози.

Результати тестування показали, що інтеграція Zero Trust підходу та Blockchain технологій значно підвищила рівень безпеки програмно-конфігурованих мереж. Було досягнуто високої стійкості до зовнішніх і внутрішніх загроз, забезпечено прозорість дій у мережі та зменшено час відповіді на атаки. Аналіз зібраних даних також продемонстрував, що система зберігала стабільність навіть за умов інтенсивного навантаження, обробляючи до 1000 транзакцій за секунду із затримкою до 2 секунд. Усі результати були документально зафіксовані та використані для подальшого вдосконалення механізмів захисту мереж.

Висновки до другого розділу

Аналіз кібервпливів в умовах гібридних воєн засвідчує їхню надзвичайну багатогранність, технологічну складність і зростаючу загрозу як на рівні окремих індивідів, так і для державних інституцій. Основні форми кібервпливів — інформаційно-психологічні, технічні, соціально-інженерні, політичні та фінансові — утворюють складну систему, що діє синергійно, підриваючи основи інформаційної безпеки та політичної стабільності. Ці методи демонструють як технологічну еволюцію зловмисників, так і їхнє глибоке розуміння людської психології, соціальних процесів і державного управління. У цьому контексті особливо небезпечним виявляється вплив на державні інститути, що проявляється у вигляді цілеспрямованих атак на урядові системи, виборчі процеси, критичну інфраструктуру, медичні установи та інформаційний простір. Приклади з атаками на енергетичну систему України, систему охорони здоров’я Ірландії, вибори у США та Франції яскраво демонструють, що кібервпливи здатні призводити не лише до втрати даних, а й до значних соціально-політичних наслідків.

Вплив на громадську думку, реалізований через соціальні мережі, фейкові новини, діпфейки та таргетовану дезінформацію, посилюється завдяки алгоритмам

персоналізації, які створюють ефект "інформаційної бульбашки". Це не лише ускладнює розпізнавання правдивої інформації, а й сприяє радикалізації суспільства, посилюючи соціальну та політичну поляризацію.

Ефективна протидія цим загрозам потребує багаторівневого підходу, що включає: розвиток цифрової та медіаграмотності населення, впровадження сучасних технологій захисту, зокрема штучного інтелекту та систем поведінкового аналізу, удосконалення державної кіберстратегії, розвиток міжнародного співробітництва у сфері кібербезпеки, а також правового регулювання кіберпростору. Усі ці компоненти повинні діяти скоординовано й інтегровано.

РОЗДІЛ 3
МЕТОДИ ТА ІНСТРУМЕНТИ ПРОТИДІЇ КІБЕРВПЛИВАМ

3.1 Технологічні засоби захисту кіберпростору

У сучасних умовах стрімкого зростання кіберзагроз, особливо в контексті гібридних воєн, технологічні засоби захисту кіберпростору відіграють ключову роль у забезпеченні інформаційної та національної безпеки держави. Захист інформаційних систем більше не обмежується традиційними антивірусами чи брандмауерами — сучасний підхід вимагає комплексного, багаторівневого і адаптивного захисту, який охоплює як апаратну, так і програмну інфраструктуру, а також поведінкову аналітику користувачів.

Особливу увагу також приділяють оновленню системного та прикладного програмного забезпечення, адже часто атаки відбуваються через відомі вразливості, які могли бути усунені шляхом своєчасного патчування. Успішна практика впровадження політик автоматичного оновлення, централізованого управління конфігурацією систем та регулярного сканування на наявність застарілого ПЗ є запорукою зменшення кількості технічних отворів, через які зловмисники можуть отримати доступ (табл. 3.1.).

Таблиця 3.1

Технологічні засоби захисту кіберпростору

№	Назва засобу	Призначення	Особливості реалізації	Приклади впровадження
1	Мережеві екрани нового покоління (NGFW)	Аналіз мережевого трафіку, виявлення та блокування загроз	Робота на рівні прикладного протоколу, контроль доступу, фільтрація трафіку	Cisco Firepower, Palo Alto Networks, Check Point

продовження таблиці 3.1

2	Системи виявлення та реагування (IDS/IPS, EDR/XDR)	Виявлення підозрілої активності та автоматичне реагування	Аналіз аномалій, поведінкова аналітика, вбудоване машинне навчання	CrowdStrike Falcon, Microsoft Defender for Endpoint
3	Honeypot-системи	Імітація вразливих систем для виявлення та вивчення поведінки зловмисника	Віртуальні «пастки», які приваблюють атакувальників, не впливаючи на продуктивне середовище	T-Pot, Honeyd, KFSensor
4	Системи захисту SCADA	Захист інфраструктурних об'єктів (енергетика, водопостачання тощо)	Сегментація мереж, контроль доступу, шифрування комунікацій, оновлення ПЗ	GE Digital iFIX, Siemens SINEC, Kaspersky Industrial CyberSecurity
5	Системи управління оновленнями ПЗ	Автоматизація оновлення безпеки та патчів	Централізоване управління, графіки оновлення, захист від відомих уразливостей	WSUS, Ivanti, ManageEngine Patch Manager
6	Інструменти stress testing / penetration testing	Виявлення вразливостей шляхом моделювання атак	Симуляція реальних загроз, аудит безпеки, тестування під навантаженням	Kali Linux, Metasploit, Burp Suite
7	AI-системи кіберзахисту	Автоматичний аналіз і адаптація до нових кіберзагроз	Самонавчання, виявлення аномалій, прогнозування дій зловмисників	Darktrace, Vectra AI, IBM QRadar

На практиці значна увага приділяється побудові багаторівневої архітектури кібербезпеки, де кожен рівень виконує свою функцію: від виявлення загроз до

нейтралізації наслідків інцидентів. Наприклад, система виявлення вторгнень (IDS) у поєднанні з системою запобігання вторгнень (IPS) дозволяє не лише фіксувати спроби злому, але й автоматично блокувати трафік, що викликає підозри. Це особливо актуально в умовах зростаючої активності кібершпигунства, коли вразливості експлуатуються впродовж лічених хвилин після їх появи в публічному просторі.

3.2 Освітні та інформаційні кампанії

Освітні та інформаційні кампанії є ключовим інструментом у системі протидії кібервпливам, оскільки забезпечують не лише технічну, а й соціальну стійкість суспільства до дезінформаційних загроз і цифрових атак. На відміну від технічних засобів, які мають переважно реактивний характер і функціонують у межах визначених протоколів, освітні кампанії виконують проактивну роль. Вони спрямовані на формування стійкого світогляду громадян, здатності критично сприймати інформацію, розпізнавати маніпулятивні меседжі та приймати обґрунтовані рішення в умовах інформаційного тиску.

Одним із головних завдань таких кампаній є формування цифрової гігієни - свідомого ставлення до користування інформаційними технологіями, захисту особистих даних, дотримання елементарних правил кібербезпеки, таких як регулярне оновлення програмного забезпечення, використання надійних паролів і двофакторної аутентифікації. Крім того, значна увага приділяється роз'ясненню принципів верифікації джерел інформації, розпізнаванню фейків, ботів, емоційно маніпулятивного контенту, що часто використовується під час гібридних атак.

Особливої актуальності такі заходи набувають в умовах, коли об’єктом кібервпливів стає широке коло населення — школярі, студенти, військовослужбовці, державні службовці, медіапрацівники. Для кожної з цих категорій розробляються специфічні навчальні модулі, тренінги, семінари та курси підвищення кваліфікації. В Україні вже реалізовано кілька національних ініціатив з кіберосвіти, зокрема проєкти під егідою Держспецзв'язку, Мінцифри та партнерств з міжнародними організаціями, які передбачають як онлайн-курси, так і очне навчання в освітніх закладах.

Ще одним важливим аспектом інформаційних кампаній є побудова довіри до офіційних джерел інформації. Це вимагає не лише технічного забезпечення безпеки урядових сайтів, а й регулярної комунікації з громадськістю у зрозумілій і доступній формі. Під час кризових ситуацій, коли країна стикається з кібератаками або хвилею дезінформації, своєчасне інформування громадян, спростування фейків і пояснення ризиків відіграють вирішальну роль у запобіганні паніці та збереженні стабільності.

Також варто відзначити роль медіаосвіти, яка є не менш важливою складовою освітніх кампаній. Йдеться про навчання аудиторії критичному мисленню в медіапросторі, розумінню механізмів пропаганди, використанню інструментів перевірки фактів і свідомому споживанню контенту. У країнах, що мають досвід гібридної агресії, медіаграмотність уже інтегрована в шкільні програми або впроваджується у вигляді факультативних курсів.

Практичні результати таких кампаній доводять, що обізнане суспільство менш схильне до впливу ворожих наративів, краще підготовлене до інформаційних викликів і демонструє вищий рівень згуртованості в умовах криз. Таким чином, інвестиції в кіберосвіту та інформаційне просвітництво є не лише доповненням до технічних заходів, а й базисом ефективної національної системи кіберзахисту.

Розробка стратегій інформаційної протидії є наступним етапом у побудові ефективної системи захисту від кібервпливів. Якщо технічні засоби забезпечують миттєве реагування на загрози, а освітні кампанії формують загальну стійкість суспільства, то стратегічні підходи до інформаційної протидії покликані забезпечити довготривалу й цілісну відповідь на гібридні загрози, що змінюються в часі. У цьому контексті держава виступає не лише як об’єкт, але і як активний суб’єкт, який формує власну інформаційну політику, засновану на принципах прозорості, системності та проактивності.

Стратегія інформаційної протидії повинна передбачати, перш за все, ідентифікацію основних векторів загроз: дезінформаційних кампаній, спроб маніпулювання свідомістю населення, провокативних наративів, спрямованих на розкол суспільства, підрив авторитету державних інститутів або дискредитацію міжнародної співпраці. З огляду на це, важливо налагодити систему постійного

моніторингу інформаційного простору, яка дозволить своєчасно виявляти підозрілу активність, координовано реагувати на спроби впливу ззовні та адаптувати захисні заходи до нових сценаріїв гібридної агресії.

Не менш важливою складовою стратегічної протидії є створення контрнаративів, які не лише спростовують фейки, а й пропонують позитивний, заснований на правді інформаційний порядок денний. Формування таких меседжів потребує участі не лише державних структур, а й журналістської спільноти, громадських організацій, академічного середовища та ІТ-сектору. Скоординована робота цих суб'єктів дозволяє не лише боротися з наслідками кібервпливів, але й запобігати їх виникненню через формування свідомого, інформаційно захищеного суспільства. Також слід враховувати необхідність адаптації стратегій до різних аудиторій. Підходи, що застосовуються до молодіжної аудиторії, можуть суттєво відрізнятися від тих, які доцільно реалізовувати серед пенсіонерів або мешканців сільської місцевості. Тому стратегія протидії має бути диференційованою, чутливою до соціальних, культурних і психологічних особливостей різних верств населення. Це дозволяє забезпечити ширше охоплення, підвищити ефективність кампаній і мінімізувати ризики нерівномірного захисту в межах однієї країни.

Інформаційна протидія також передбачає активну міжнародну співпрацю. В умовах глобального характеру кіберзагроз окрема країна не здатна самостійно протистояти транснаціональним кампаніям цифрового впливу. Обмін досвідом, координація дій, участь у міжнародних ініціативах та залучення до альянсів у сфері кібербезпеки дають змогу консолідувати зусилля та реалізовувати спільні стратегії на рівні всього демократичного світу. Багаторівнева, комплексна стратегія інформаційної протидії, яка інтегрує національні та міжнародні інструменти, є необхідною умовою для ефективного забезпечення безпеки в умовах сучасної гібридної війни.

Важливим чинником стратегічного підходу є постійний аналіз інформаційного середовища та пристосування заходів протидії до нових викликів. Саме ці елементи складають основу ефективної стратегії інформаційної протидії, що наведена в таблиці нижче.

Таблиця 3.2

Компоненти стратегії інформаційної протидії

Компонент	Зміст	Очікуваний результат
Моніторинг інформаційного простору	Безперервне спостереження за ЗМІ, соцмережами, інформаційними платформами з метою виявлення загроз.	Оперативне виявлення та аналіз дезінформації.
Аналітичні центри та фактчекінг	Створення незалежних аналітичних структур, що перевіряють достовірність даних.	Підвищення рівня довіри до перевіреної інформації.
Побудова наративів	Формування проактивних інформаційних повідомлень, що просувають позитивні цінності.	Зміцнення інформаційної стійкості громадськості.
Міжвідомча координація	Співпраця між державними структурами, медіа та IT-сектором.	Ефективне реагування на складні інформаційні загрози.

Після впровадження освітніх і інформаційних кампаній, зазначених у таблиці, важливим є забезпечення їх регулярності, адаптивності та охоплення широкої аудиторії. Кампанії повинні не лише передавати технічну інформацію, але й формувати критичне мислення, здатність розпізнавати маніпулятивні повідомлення, фейки та шкідливий вміст. У сучасному інформаційному середовищі, де соціальні мережі є головним джерелом новин для багатьох громадян, важливо працювати безпосередньо з платформами, навчати користувачів правилам безпечного споживання контенту, підвищувати рівень цифрової гігієни.

Крім загальних кампаній для населення, особливу увагу слід приділяти освітнім програмам для державних службовців, журналістів, працівників медіа, освітян, студентів та інших груп, які мають вплив на формування громадської думки. Їхня грамотність у питаннях інформаційної безпеки може стати вирішальним чинником у стримуванні впливу ворожих кібератак та психологічних операцій.

Ефективні освітні ініціативи мають включати як очне навчання, так і онлайн-курси, тренінги, вебінари, інтерактивні платформи для самоперевірки знань. Крім того, в умовах гібридної війни держава повинна постійно моніторити ефективність таких кампаній, адаптувати їх зміст відповідно до нових загроз, виявлених у кіберпросторі, та забезпечувати міжвідомчу координацію з міжнародними партнерами.

Розробка стратегій інформаційної протидії є одним із ключових напрямів у комплексній системі кіберзахисту держави в умовах гібридної війни. Успішна стратегія повинна враховувати як технічні, так і соціально-психологічні аспекти впливу, охоплювати короткострокові й довгострокові дії, а також включати механізми адаптації до нових викликів. Центральне місце в цій діяльності займає створення координаційних центрів при урядових структурах, які відповідають за моніторинг інформаційного простору, виявлення фейків, маніпуляцій і дезінформації, а також розробку відповідей на них.

Важливим елементом є взаємодія між державою, громадським сектором і приватними технологічними компаніями. Для цього на практиці створюються інформаційно-аналітичні хаби, де фахівці з кібербезпеки, соціології, психології, масових комунікацій та IT-технологій розробляють інтегровані підходи до стримування ворожих впливів. На їх основі формуються рекомендації для медіа, розробляються методики фактчекінгу, визначаються ключові наративи, якими ворог намагається маніпулювати громадською думкою.

Однією з ефективних практик у протидії інформаційним атакам є створення так званих центрів швидкого реагування на інформаційні інциденти. Їх функціонування передбачає виявлення загроз у режимі реального часу, оперативне поширення спростувань, контрнаративів, а також підтримку довіри до офіційних джерел. Такі центри можуть бути інтегровані в структуру національних CERT (команд реагування на комп’ютерні інциденти) або діяти при урядових прес-службах.

Крім того, важливим напрямом є моделювання сценаріїв інформаційних атак та тестування стійкості суспільства до них. У рамках таких симуляцій проводяться навчання для державних інституцій, журналістів і громадських активістів, де

відпрацьовуються алгоритми дій у разі поширення дезінформації, витоків даних або медійних кампаній, що підривають довіру до держави. Також застосовується аналіз великих масивів даних з використанням штучного інтелекту, що дозволяє ідентифікувати координацію бот-мереж, динаміку поширення фейкових повідомлень і формувати ефективну контрпропаганду.

Не менш важливою практикою є формування прозорих комунікаційних стратегій для офіційних інституцій. Це означає, що будь-яка реакція на інформаційну атаку має бути вчасною, чіткою, заснованою на фактах і спрямованою на збереження довіри до джерела інформації. Такий підхід передбачає не лише оборону, але й активну інформаційну ініціативу з боку держави, яка формує власний порядок денний, блокує наративи противника та забезпечує психологічну стійкість населення.

3.3 Розробка стратегій інформаційної протидії

Розробка стратегій інформаційної протидії є надзвичайно важливим елементом забезпечення кібербезпеки держави, особливо в умовах гібридних війн, коли інформаційний простір стає головним полем битви за уми, поведінку і стабільність суспільства. На відміну від суто технічних заходів захисту, стратегія інформаційної протидії передбачає системну, цілеспрямовану, комплексну діяльність, яка охоплює організаційні, комунікаційні, правові та гуманітарні аспекти. Її мета полягає не лише в нейтралізації ворожих інформаційних впливів, а й у формуванні власного стійкого, відкритого й достовірного інформаційного середовища, яке не піддається деструктивним кампаніям.

Перш за все, така стратегія має спиратися на глибоке розуміння механізмів поширення дезінформації, фейків, маніпуляцій та інших форм інформаційного впливу. Йдеться про ідентифікацію джерел загроз, визначення основних каналів поширення (зокрема соціальні мережі, месенджери, новинні сайти, блогосферу), а також типових патернів поведінки зловмисників. Успішна стратегія обов’язково включає постійний моніторинг інформаційного поля за допомогою спеціалізованих програмних засобів, машинного навчання та аналітичних центрів. Це дозволяє

виявляти аномалії, джерела фейкових повідомлень, скоординовані бот-мережі та кібератаки, які супроводжуються деструктивною інформаційною кампанією.

Невід'ємною частиною стратегії є формування дієздатної системи фактчекінгу, яка повинна мати відповідні кадрові, технологічні та ресурсні можливості для оперативної перевірки сумнівної інформації. Практика світових медіа показує, що наявність авторитетних незалежних платформ, які на постійній основі перевіряють новини, заяви політиків, пости в соціальних мережах, сприяє підвищенню медіаграмотності населення і зниженню довіри до фейкових джерел. Важливу роль у цьому відіграє і співпраця з міжнародними ініціативами, такими як EUvsDisinfo або First Draft News, що надають методичну підтримку та аналітику.

Інформаційна протидія не може обмежуватися лише реакцією. Вона повинна бути проактивною, тобто випереджувальною. Це означає створення та просування власних інформаційних наративів, які базуються на фактах, цінностях демократичного суспільства, прав людини, прозорості та відкритості. Стратегічно важливо, щоб держава і громадянське суспільство не лише захищалися від ворожих атак, а й формували позитивний образ країни на міжнародному рівні, просували об'єктивну інформацію про події в країні, будували довіру до державних інституцій. Особливу увагу у стратегії слід приділяти вразливим групам населення, зокрема молоді, людям похилого віку, жителям сільських територій, які через низький рівень медіаграмотності або обмежений доступ до якісної інформації є більш схильними до впливу пропаганди. Для цього розробляються таргетовані освітні кампанії, проводяться медіауроки в школах, організовуються публічні лекції, тренінги, створюється відповідний інформаційний контент.

Окремим напрямом є нормативно-правове забезпечення інформаційної безпеки. Стратегія протидії кібервпливам передбачає вдосконалення законодавства у сфері поширення інформації, відповідальності за дезінформацію, кіберзлочини, співпрацю між державними структурами, регуляторами, технологічними платформами і правоохоронними органами. При цьому важливо не порушити принципи свободи слова і права на доступ до інформації. У рамках розробки інформаційної стратегії важливо застосовувати міждисциплінарний підхід:

поєднувати знання з кібербезпеки, соціальної психології, масових комунікацій, юриспруденції, політичної науки, технологій. Такий підхід дозволяє створити комплексну систему протидії загрозам, яка охоплює як технологічну інфраструктуру, так і соціальні аспекти стійкості суспільства до впливу.

Успішна реалізація стратегії інформаційної протидії потребує політичної волі, достатнього фінансування, якісної координації між усіма суб'єктами інформаційного простору, а також постійного вдосконалення інструментів і механізмів реагування. Вона не є статичним документом, а повинна динамічно адаптуватися до нових умов, загроз і технологічних змін. Тільки за таких умов можна забезпечити ефективний захист держави, суспільства та кожного громадянина від руйнівного впливу гібридної інформаційної війни.

На практиці стратегія інформаційної протидії повинна реалізовуватись через конкретні дії, спрямовані на створення національної інфраструктури інформаційної безпеки. Прикладом такої практики є створення центрів стратегічних комунікацій, які діють при державних установах, зокрема при міністерствах оборони, внутрішніх справ, закордонних справ. Ці центри займаються не лише моніторингом інформаційного середовища, а й аналізом інформаційних загроз, розробкою комунікаційних меседжів у відповідь на деструктивні кампанії, координацією між державними відомствами у сфері інформаційної безпеки. Наприклад, в Україні Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики здійснює не лише аналітичну роботу, а й активну комунікаційну діяльність, включаючи розвінчання фейків, створення тематичних інформаційних кампаній, інфографіки, відео та просування контрнаративів.

Ще однією практичною реалізацією стратегії є впровадження системи інформаційної розвідки (OSINT), яка дозволяє на основі відкритих джерел виявляти потенційні інформаційні атаки, встановлювати їхнє походження, структуру поширення, цільові аудиторії. Ця технологія активно використовується в розвинених країнах НАТО для виявлення кампаній впливу з боку ворожих держав. В Україні OSINT-фахівці беруть участь у спільних ініціативах із цифровими активістами, кіберспільнотами та

волонтерськими об’єднаннями, що моніторять соцмережі, месенджери та форуми на предмет поширення фейкових новин або ворожої пропаганди.

Практичним інструментом також є створення спеціальних кризових інформаційних команд, які оперативно реагують на випадки масштабних фейків, що мають потенціал до дестабілізації. У разі поширення панічної дезінформації, наприклад про нібито обстріли, аварії, вбивства, ці команди забезпечують миттєве спростування з достовірних джерел, залучаючи представників ЗМІ, правоохоронців, місцеву владу.

Додатково важливо застосовувати так звані "наративні щеплення" — тобто заздалегідь поширювати інформацію про типові маніпуляції, якими користуються пропагандисти, із поясненням механізмів їх дії. Наприклад, у межах кампаній з медіаграмотності можуть пояснюватися приклади маніпулятивних заголовків, псевдоекспертних думок, підтасованої статистики тощо. Таким чином, населення отримує імунітет до поширених інформаційних атак.

Реальним прикладом застосування такої практики є кейс роботи британського Rapid Response Unit, який під час критичних подій (наприклад, виборів або терактів) взаємодіє з урядовими структурами та онлайн-платформами для виявлення і блокування шкідливого контенту. Подібний досвід був адаптований у багатьох країнах Європи, включно з Литвою, Естонією та Чехією, які стали лідерами у протидії дезінформації з боку зовнішніх гравців.

Ці приклади показують, що ефективна стратегія інформаційної протидії – це не декларація, а практично впроваджуваний комплекс дій, який передбачає координацію між різними рівнями влади, аналітичними структурами, громадським сектором і міжнародними партнерами. Така стратегія має базуватись на постійному аналізі актуальних загроз, адаптації до нових форм інформаційної агресії, а також активному залученні суспільства до побудови інформаційного імунітету нації.

У таблиці 3.3 наведені основні практики реалізації стратегій інформаційної протидії, які застосовуються на сучасному етапі для посилення інформаційної безпеки України.

Таблиця 3.3

Практики реалізації стратегій інформаційної протидії

Стратегія інформаційної протидії	Опис	Приклад реалізації
Моніторинг інформаційного простору	Постійний аналіз онлайн-контенту для виявлення фейкових новин, тролінгу, бот-мереж та кампаній впливу. Включає створення аналітичних центрів і груп швидкого реагування.	Центр протидії дезінформації при РНБО України; StopFake.org
Контрнаративи та спростування дезінформації	Оперативне створення контенту, що спростовує неправдиву інформацію. Важливо дотримуватись достовірності, відкритості джерел і професійної подачі.	Проєкт “По той бік новин”; ініціативи Центру стратегічних комунікацій
Побудова комунікації держави з громадянами	Публічне інформування про дії держави, її позиції, виклики і загрози через зрозумілі меседжі, регулярні брифінги, офіційні сторінки у соцмережах та сайти органів влади.	Сторінка Кабміну України у Telegram та Facebook; щотижневі звіти Міноборони
Співпраця з платформами соціальних мереж	Угода з Facebook, X (Twitter), YouTube, TikTok про видалення ворожого або фейкового контенту, позначення дезінформації, блокування фейкових акаунтів та ботів.	Позначки дезінформації Meta на сторінках; блокування російських бот-мереж
Міжнародне партнерство у сфері інформаційної безпеки	Спільні ініціативи з НАТО, ЄС, урядами інших країн, обмін аналітичними звітами, розробка стандартів інформаційної протидії та протоколів кібергігієни.	Кіберцентр НАТО у Таллінні; програма ЄС “Cyber4Dev”; українсько-естонські навчання

Після впровадження практик інформаційної протидії, описаних у таблиці, важливо акцентувати увагу на міжсекторальній координації, яка відіграє вирішальну роль у забезпеченні ефективності протидії кібервпливам. Успішна реалізація стратегій потребує чіткого розподілу відповідальності між державними органами, приватним сектором, громадськими організаціями та медіаспільнотою. Така взаємодія забезпечує оперативне виявлення та нейтралізацію інформаційних загроз, а також підвищує довіру суспільства до офіційних джерел інформації.

Особливу роль відіграють інформаційні аналітичні центри, які здійснюють моніторинг інформаційного простору, виявляють ворожі наративи та координують відповіді державних структур. Їхня робота тісно пов’язана з алгоритмічними інструментами штучного інтелекту, які використовуються для аналізу великих обсягів даних, виявлення фейкових новин, бот-активності та пропагандистських кампаній. Прогресивні держави інтегрують ці технології в національні центри кіберзахисту, що дозволяє не лише виявляти загрози, але й прогнозувати можливі інформаційні сценарії.

Крім того, необхідним є безперервне оновлення та вдосконалення стратегій відповідно до динаміки розвитку кіберпростору. Зміна підходів до інформаційної безпеки має відбуватися з урахуванням нових каналів впливу, технологій дистрибуції контенту, еволюції алгоритмів соціальних мереж та змін у поведінкових патернах аудиторії. Підхід до розробки інформаційної протидії повинен бути проактивним і базуватися не лише на аналізі минулих загроз, а й на випереджальному моделюванні майбутніх ризиків.

Висновки до третього розділу

Аналіз сучасних технологічних засобів захисту кіберпростору показав, що значення мають не лише технічні можливості запобігання атакам, але й адаптивність систем до нових форм загроз, здатність до самонавчання, вчасне оновлення інфраструктури кіберзахисту та наявність міжвідомчої координації. Виявлено, що

побудова ефективної кібероборони повинна спиратися на використання інтегрованих платформ кібермоніторингу, застосування механізмів машинного навчання, а також активну участь спеціалізованих центрів реагування.

Водночас, технологічні заходи не здатні самостійно нейтралізувати всі форми кіберзагроз, особливо ті, що мають інформаційно-психологічний характер. Саме тому освітні та інформаційні кампанії відіграють ключову роль у формуванні критичного мислення громадян, підвищенні обізнаності щодо сучасних методів дезінформації та культивуванні культури інформаційної безпеки. Доведено, що найефективнішими є ті інформаційні програми, які проводяться постійно, мають практичну спрямованість та враховують вікові, соціальні й професійні особливості цільової аудиторії. Практичні приклади, як-от кампанії Європейського Союзу або платформи кіберосвіти, засвідчують, що довгострокові інвестиції в людський капітал забезпечують більш тривалий захисний ефект, ніж суто технічні рішення.

Стратегії інформаційної протидії повинні розроблятися з урахуванням мінливості інформаційного середовища. Встановлено, що тільки проактивний і динамічний підхід до формування стратегій дозволяє ефективно виявляти й нейтралізовувати кібервпливи на ранніх етапах. На особливу увагу заслуговує залучення міжсекторальних акторів до розробки та реалізації таких стратегій, що дозволяє підвищити якість аналітики, забезпечити різнорівневу взаємодію і зміцнити довіру громадськості до офіційної інформації. Досвід провідних держав, зокрема США, Великої Британії та Естонії, свідчить про ефективність створення національних центрів протидії дезінформації, а також законодавчого закріплення механізмів боротьби з інформаційними загрозами.

Результати цього розділу підтвердили, що боротьба з кібервпливами повинна вестися не лише на рівні державної безпеки, а й через комплексні дії в освітньому, технологічному та стратегічному вимірах. Ключем до ефективної протидії є не тільки наявність засобів, а й здатність оперативно адаптуватися до нових загроз, що постійно еволюціонують у межах гібридних воєн. Суспільство, яке володіє знаннями, інфраструктурою й механізмами захисту, здатне не лише встояти перед

інформаційною агресією, а й перетворити кіберпростір на сферу стійкого розвитку та безпеки.

РОЗДІЛ 4
ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ВІД КІБЕРВПЛИВІВ

4.1 Розробка національних програм кіберзахисту

Розробка національних програм кіберзахисту є критично важливим елементом державної політики у сфері національної безпеки, особливо в умовах гібридних загроз, де кібератаки стають невід'ємною складовою збройного або політичного протистояння. Сучасний кіберпростір є ареною для широкого спектру агресивних дій – від шкідливого програмного забезпечення до інформаційно-психологічних операцій, які спрямовані на підрив державної стабільності, порушення функціонування критичної інфраструктури, деморалізацію населення та знищення довіри до інституцій. У цьому контексті формування комплексної, багаторівневої та скоординованої національної програми кіберзахисту є необхідною передумовою для гарантування суверенітету в цифровій сфері.

Національна програма кіберзахисту повинна бути стратегічним документом, що містить не лише окреслення потенційних кіберзагроз, але й чітко визначену структуру інституційної взаємодії між державними органами, приватним сектором, науковими установами та міжнародними партнерами. Основоположними принципами при розробці такої програми є безперервність дії, превентивність, адаптивність та прозорість процесів. Вона має охоплювати нормативно-правове поле, технічну інфраструктуру, механізми оперативного реагування на інциденти, стандарти інформаційної безпеки, а також програми підготовки кадрів у сфері кібербезпеки.

Одним із ключових викликів у процесі розробки національної програми кіберзахисту є необхідність міжвідомчої координації та уникнення дублювання функцій. Для цього доцільно створити центральний орган або координаційний центр, відповідальний за управління національною системою кіберзахисту. Такий орган

повинен мати повноваження не лише з моніторингу ситуації, а й з оперативного втручання, законодавчої ініціативи та стратегічного планування. Крім того, програма повинна передбачати створення регіональних підрозділів, здатних реагувати на локальні загрози та здійснювати взаємодію з громадськими структурами.

Досвід провідних країн, зокрема США (National Cybersecurity Strategy), Німеччини (Cyber-Sicherheitsstrategie), Франції та Ізраїлю, демонструє, що ефективна національна програма кіберзахисту повинна включати положення щодо обов'язкового аудиту інформаційних систем органів влади, критичної інфраструктури та суб'єктів стратегічного значення. Програма має створити правові підстави для взаємодії з приватними компаніями, які є власниками чи операторами інфраструктури, що потенційно може стати об'єктом атаки. Важливо також передбачити механізми обміну інформацією про інциденти, уразливості та способи реагування в реальному часі.

Суттєве місце в національній програмі кіберзахисту має посідати питання освіти та наукових досліджень. Програма має сприяти розвитку профільних освітніх програм, стимулювати створення центрів компетенцій у закладах вищої освіти, а також передбачати державну підтримку наукових досліджень у сфері кібербезпеки. Це дозволить сформувати стійке кадрове ядро фахівців, здатних як на оперативне реагування, так і на стратегічне планування.

Практична реалізація національної програми кіберзахисту має відбуватись поетапно – через прийняття супутніх підзаконних актів, створення інституційної інфраструктури, запуск пілотних проєктів та поступове розширення системи на нові галузі. При цьому необхідно забезпечити постійний моніторинг ефективності дій, гнучкість у коригуванні заходів у відповідь на зміну кіберзагроз та періодичну актуалізацію стратегії.

У підсумку, практична реалізація національних програм кіберзахисту охоплює комплекс дій – від інституційного будівництва та навчання кадрів до технічного зміцнення цифрової інфраструктури. Кожен етап реалізації програми має супроводжуватись моніторингом, коригуванням політик та адаптацією до нових

реалій загроз. Такий підхід дозволяє формувати не лише стійкий кіберпростір, а й підвищувати загальну національну безпеку у цифрову епоху (табл. 4.1.).

Таблиця 4.1

Практичні компоненти національних програм кіберзахисту

Компонент програми	Опис	Приклад реалізації
Централізована координація	Створення національного кіберцентру або агентства, яке координує всі заходи з кіберзахисту.	Державна служба спеціального зв'язку та захисту інформації України
Освітні ініціативи	Впровадження курсів, тренінгів та сертифікаційних програм з кібербезпеки на всіх рівнях освіти.	Національна програма «Кіберосвіта 2030»
Міжнародне співробітництво	Участь у міжнародних ініціативах, підписання угод про обмін інформацією про кіберзагрози.	Участь України в ініціативі EU CyberNet
Регулярний аудит безпеки	Періодичне тестування систем на вразливості та відповідність стандартам безпеки.	Аудити IT-інфраструктури державних органів
Реагування на інциденти	Створення CERT-структур, здатних оперативно реагувати на кіберінциденти та усувати наслідки.	Національний CERT-UA
Інформаційна підтримка населення	Ведення роз'яснювальної роботи серед громадян щодо кібергігієни та методів самооборони.	Платформа «Кібербезпека для кожного»

Велике значення має наявність централізованої інституції (наприклад, Національного центру кібербезпеки), що не лише координує міжвідомчу взаємодію, але й бере участь у міжнародних обмінах інформацією, сприяючи підвищенню рівня кіберстійкості. Практика показує, що країни з ефективними кіберстратегічними центрами значно швидше локалізують наслідки інцидентів та зменшують економічні й соціальні втрати.

Додаткову увагу слід приділити політиці відкритості та співпраці з громадськістю: формування культури кіберграмотності, прозоре інформування про загрози, залучення фахівців з ІТ до розробки інноваційних засобів захисту. Одним із прикладів такої взаємодії є платформи типу bug bounty, де держава заохочує фахівців з етичного хакінгу до виявлення вразливостей у державних системах. Також важливо реалізовувати проєкти на кшталт «кібернавчання у школах», що інтегрують основи безпечної поведінки у цифровому середовищі з раннього віку, формуючи відповідальну цифрову свідомість.

У підсумку, стратегія кіберзахисту має бути гнучкою, всеохопною та такою, що враховує інтереси різних секторів. Тільки за умов комплексного підходу та системної реалізації програми можуть забезпечити ефективну протидію сучасним цифровим загрозам та підвищити національну кіберстійкість у довгостроковій перспективі.

4.2 Підвищення кіберграмотності населення

Підвищення кіберграмотності населення є однією з ключових передумов ефективного забезпечення кібербезпеки держави в умовах гібридних загроз. У сучасному інформаційному суспільстві, де цифрові технології пронизують усі сфери життя – від особистого спілкування до державного управління – рівень обізнаності громадян про правила безпечної поведінки в кіберпросторі має прямий вплив на загальну стійкість країни до кібератак, дезінформації, фішингових схем та соціальної інженерії. Низький рівень цифрової культури часто стає причиною несанкціонованого витоку конфіденційних даних, поширення шкідливого програмного забезпечення та навіть втручання у критичні елементи інфраструктури через людський фактор.

Процес підвищення кіберграмотності передбачає не лише навчання користувачів базовим технічним навичкам (таким як створення надійних паролів, верифікація джерел інформації, уникнення підозрілих посилань або додатків), але й формування критичного мислення, що дозволяє людині усвідомлювати ризики й уникати маніпуляцій. Це вимагає впровадження систематичної освітньої політики,

яка б охоплювала всі вікові групи населення: від дітей до осіб похилого віку. У цьому контексті важливим стає включення курсів з основ кібербезпеки до навчальних програм закладів загальної середньої освіти, закладів професійної та вищої освіти, а також організація позашкільних тренінгів і просвітницьких кампаній на рівні громад. На практиці одним із найефективніших інструментів підвищення кіберграмотності є створення онлайн-платформ, які надають доступ до інтерактивних курсів, тренажерів, симуляторів кібератак, тестування знань користувачів, а також відеолекцій з прикладами актуальних кіберзагроз. Такі ресурси дозволяють людям не лише отримати знання, а й перевірити рівень їхнього засвоєння у практичних умовах. Крім того, важливою є роль медіа у поширенні достовірної інформації про кіберзагрози: спеціальні рубрики в новинах, інтерв'ю з фахівцями, соціальна реклама, що популяризує цифрову безпеку.

Практична діяльність у сфері підвищення кіберграмотності повинна мати безперервний характер і бути адаптованою до нових викликів. Тільки так можна створити ефективний щит не лише на рівні державних систем, але й на рівні кожного громадянина, що забезпечить стабільність, захищеність і довіру до цифрового середовища (табл. 4.2.).

Таблиця 4.2

Практики підвищення кіберграмотності населення

Практика	Опис реалізації
Симуляція фішингових атак	Імітація атак у державних установах з подальшим аналізом та навчанням персоналу
Кібертабори для молоді	Проведення навчальних заходів з кібербезпеки, змагань CTF, формування командних навичок
Мобільні додатки з елементами гейміфікації	Додатки з щоденними завданнями, навчальними блоками, оцінюванням і сертифікацією
Інтерактивні заняття у школах і вишах	Навчальні ігрові сценарії, модулі з інформаційної безпеки в освітньому процесі

продовження таблиці 4.2

Цифрові хаби для населення	Організація курсів у бібліотеках, ЦНАПах, для літніх людей з практичними прикладами

Значну роль у цьому процесі відіграє партнерство між державними структурами, освітніми закладами, бізнесом і громадянським суспільством. Завдяки такій взаємодії вдається розробляти інтегровані програми навчання, які поєднують теоретичні знання з практичними навичками реагування на кіберзагрози. Крім того, важливим аспектом є мотивація громадян до вивчення основ кібербезпеки через впровадження сертифікаційних програм, що можуть стати перевагою при працевлаштуванні або просуванні кар'єрою.

Успішним прикладом практичного впровадження ініціатив з кіберграмотності є досвід Естонії, де з початку 2000-х років цифрова освіта стала обов'язковою у школах, а також активно розвивається серед дорослого населення через державні та приватні проєкти. Завдяки цьому країна змогла сформувати суспільство з високим рівнем цифрової культури, що значно зменшило вразливість до інформаційних атак. Інший приклад – програма CyberAware у Великій Британії, яка охоплює широкий спектр навчальних ресурсів для домогосподарств і малого бізнесу.

4.3 Удосконалення законодавчої бази

Удосконалення законодавчої бази у сфері кібербезпеки є ключовим компонентом ефективної протидії кібервпливам, особливо в умовах гібридних воєн. Сучасні цифрові виклики вимагають від держав не лише технічної, але й нормативно-правової готовності до реагування на загрози в кіберпросторі. Відсутність або фрагментарність законодавчих актів, що регулюють правила захисту інформаційних систем, кіберрозслідувань, відповідальності за кіберзлочини, значно ускладнює боротьбу з кіберзагрозами, знижує ефективність реагування та координації між державними органами, а також унеможливлює участь країни в міжнародних ініціативах з кіберзахисту.

Один із найважливіших напрямів удосконалення - це адаптація законодавства до міжнародних стандартів та практик, зокрема рекомендацій ЄС, НАТО, Будапештської конвенції про кіберзлочинність та актів ENISA. Україна, яка є активним учасником партнерських програм з Європейським Союзом і США у сфері цифрової безпеки, має потребу не лише в гармонізації свого законодавства з цими нормами, але й у створенні національних механізмів контролю за їх реалізацією.

Особливу увагу слід приділяти формуванню чітких визначень понять «кібератака», «кібертероризм», «інформаційна зброя», «глобальна інформаційна операція», а також встановленню відповідальності за такі дії на законодавчому рівні. Також важливим є унормування правового статусу суб’єктів, які здійснюють кіберзахист: державні органи, підрозділи кіберполіції, приватні компанії, об’єкти критичної інфраструктури. У діючому законодавстві часто спостерігається дублювання функцій, розмитість відповідальності або суперечності між законами, що створює проблеми в координації дій під час інцидентів.

Крім того, необхідно впроваджувати правові механізми для обов’язкової сертифікації IT-продуктів, безпечного зберігання персональних даних, протидії фішингу, DDoS-атакам та іншим кіберінцидентам. Законодавство має передбачати вимоги до цифрової гігієни в органах державної влади, установах, що працюють з конфіденційною інформацією, а також у сфері оборони. Обов’язковим має бути аудит інформаційної безпеки та створення резервних копій критичних даних.

Надзвичайно важливим є розвиток нормативної бази щодо державного реагування на масштабні кіберінциденти. Потрібно мати чітко прописані протоколи взаємодії між Службою безпеки України, Міністерством оборони, Національним координаційним центром кібербезпеки, Національною поліцією, державними та приватними структурами, які володіють інфраструктурою, що може стати об'єктом кібератак.

Окремим блоком у правовому полі мають стати положення щодо інформаційно-психологічної безпеки: боротьба з фейками, дезінформацією, маніпулятивними кампаніями, що здійснюються через соціальні мережі, блоги, новинні сайти. Законодавство має регулювати механізми моніторингу інформаційного простору,

право держави на блокування джерел інформаційного впливу, а також взаємодію з платформами на кшталт Meta, Google, Telegram у рамках кіберграмотної модерації контенту.

Поряд із цим, удосконалення законодавчої бази має базуватись на принципах дотримання прав людини та інформаційної свободи. Усі зміни мають здійснюватися прозоро, з участю громадськості та експертного середовища. Саме поєднання правової жорсткості у сфері захисту держави та поваги до демократичних принципів робить законодавство дієвим і легітимним в очах громадян.

Висновки до четвертого розділу

У сучасних умовах гібридної війни, що супроводжується інтенсивними цифровими загрозами, роль держави у формуванні системного підходу до кіберзахисту значно зросла. У розділі було розглянуто ключові напрями реалізації практичних заходів, спрямованих на захист національного кіберпростору, серед яких важливе місце посідає розробка національних програм кіберзахисту, підвищення кіберграмотності населення та вдосконалення законодавчої бази. Ці напрями взаємопов’язані, оскільки створення ефективної програми кіберзахисту передбачає не лише впровадження технологічних рішень, але й забезпечення належної обізнаності громадян, стимулювання їх до критичного сприйняття інформації, а також закріплення відповідних норм у правовому полі.

Аналіз практичних аспектів показав, що комплексна національна стратегія кібербезпеки має охоплювати не тільки державний сектор, а й приватний бізнес, освітні установи та громадянське суспільство. Вона повинна передбачати як превентивні, так і реактивні механізми — від виявлення потенційних загроз до швидкої локалізації та відновлення після інцидентів. При цьому ключову роль відіграє міжвідомча координація, яка має бути підкріплена чіткими законодавчими механізмами. Запровадження міжсекторальної взаємодії у сфері кібербезпеки є не лише вимогою часу, а й обов’язковою умовою підвищення стійкості країни до зовнішнього цифрового тиску.

Підвищення рівня кіберграмотності є ще одним фундаментальним елементом, що визначає ефективність національного опору кібервпливам. Освітні ініціативи, орієнтовані як на молодь, так і на доросле населення, повинні стати частиною державної політики. Практика доводить, що навіть найсучасніші технічні засоби кіберзахисту втрачають ефективність, якщо користувачі залишаються вразливими до фішингу, соціальної інженерії або маніпуляцій у медіа. Саме тому розвиток цифрової свідомості, критичного мислення та навичок безпечної поведінки в мережі має стати стратегічним напрямом у межах національного безпекового дискурсу.

Водночас удосконалення законодавчої бази у сфері кібербезпеки вимагає не лише адаптації до новітніх загроз, але й випереджувального підходу. У результаті аналізу можна стверджувати, що правове регулювання кіберсфери має бути динамічним і передбачати механізми гнучкої реакції на появу нових форм кібервтручань. Законодавство має забезпечити прозору і водночас оперативну процедуру реагування на інциденти, передбачати міждержавну співпрацю, а також врегульовувати питання відповідальності у сфері кіберпростору як на рівні держав, так і приватних акторів.

ВИСНОВКИ

У ході виконання роботи було здійснено комплексне дослідження загроз кібервпливів у контексті гібридних воєн, що дозволило виявити ключові чинники, які визначають ефективність інформаційної та кібернетичної безпеки держави. Аналіз теоретичних засад кібервпливів продемонстрував, що вони становлять нову форму ведення конфліктів, яка поєднує технічні атаки на інформаційну інфраструктуру з інформаційно-психологічним впливом на громадську свідомість. Ця особливість перетворює кіберпростір на поле бою, де бойові дії замінюються цифровими маніпуляціями, шкідливими програмами, дезінформацією, фішингом, атакою на критичну інфраструктуру, фінансову систему та інститути влади.

Розглянуто особливості гібридних воєн у сучасному світі, зокрема з акцентом на випадок України, яка є одним із ключових об’єктів таких атак у контексті збройного протистояння з Російською Федерацією. Це дозволило глибше зрозуміти специфіку поєднання кібероперацій із військовими, політичними, економічними та пропагандистськими засобами, що використовуються синхронно задля досягнення стратегічного ефекту. Теоретичний і практичний аналіз сучасних кіберзагроз засвідчив, що основними векторами атак залишаються інформаційні системи державного управління, енергетична інфраструктура, фінансовий сектор, а також громадська свідомість через соціальні мережі та онлайн-медіа. Саме тому поняття кібербезпеки сьогодні потребує переосмислення як складової національної безпеки в її найширшому сенсі.

В результаті проведеного дослідження вдалося виокремити найбільш поширені форми реалізації кібервпливів, серед яких домінують атаки типу DDoS, впровадження шкідливого ПЗ, злам державних порталів, а також систематичні дезінформаційні кампанії. Вивчення реальних прикладів кібератак на Україну, США, країни ЄС та міжнародні інституції дало змогу класифікувати ці загрози за рівнем технічної складності, цільовою аудиторією, механізмами впливу та наслідками для функціонування суспільства.

Особливу увагу в роботі було приділено методам і засобам протидії кібервпливам. Дослідження засвідчило, що найефективніший результат дає не окремий технічний засіб, а цілісна система, яка поєднує цифрові технології захисту (фаєрволи, шифрування, виявлення аномалій тощо), інформаційні кампанії з підвищення обізнаності населення, розвиток кіберосвіти та постійне удосконалення законодавчої бази. Показано, що саме міжгалузева взаємодія між державними структурами, приватним сектором, освітніми установами та громадянським суспільством здатна забезпечити високий рівень стійкості до гібридних загроз. Важливою є також адаптивність законодавства до новітніх викликів — потреба у гнучких, але водночас чітких нормах, які регулюють і надають відповідальність за дії у кіберпросторі, є очевидною в умовах швидкої трансформації цифрових ризиків.

Окремо проаналізовано роль освітніх і просвітницьких кампаній, спрямованих на підвищення рівня цифрової культури населення. Доведено, що без належного рівня кіберграмотності навіть найкращі технічні засоби не можуть гарантувати повноцінного захисту від цифрових маніпуляцій. Практичні приклади доводять ефективність таких кампаній у країнах Балтії, Ізраїлі, а також в окремих проєктах в Україні, де завдяки комплексним освітнім програмам вдалося суттєво знизити вразливість населення до інформаційних атак.

У межах роботи також запропоновано рекомендації щодо формування національних програм кіберзахисту, які повинні мати системний характер, охоплюючи нормативне регулювання, технічну інфраструктуру, моніторинг загроз, реагування на інциденти, а також міжнародну співпрацю. Визначено доцільність створення єдиного координаційного центру кіберзахисту, який діятиме як головний аналітичний і виконавчий орган із реагування на загрози та координації міжвідомчої взаємодії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стратегія забезпечення кібербезпеки в гібридній війні // Збірник наукових праць. – 2022. – №3. – С. 45-60.

2. Петренко І., Сидоренко О. Російська гібридна війна: загрози і кібервиклики для європейської інформаційної безпеки // Науковий вісник міжнародних відносин. – 2021. – №1. – С. 78-92.

3. Гібридна війна і журналістика: проблеми інформаційної безпеки: навч. посіб. / За ред. В. Іванченко. – Київ: НПУ ім. М. П. Драгоманова, 2020. – 256 с.

4. Війни інформаційної епохи: міждисциплінарний дискурс / Під ред. С. Коваленка. – Харків: Право, 2021. – 312 с.

5. Савченко О., Марченко Л. Роль інформаційно-медійних технологій як інструменту гібридної війни // Журнал соціальних комунікацій. – 2020. – №4. – С. 112-130.

6. Климчук М. Гібридна війна та її інформаційна складова // Вісник політологічних досліджень. – 2022. – №2. – С. 54-69.

7. Мельник В. Гібридна війна та кібератаки Російської Федерації проти України // Журнал міжнародної безпеки. – 2021. – №5. – С. 85-98.

8. Шевченко П. Основні теоретичні і практичні аспекти ведення проксі-війн та гібридних воєн у сучасній світовій геополітичній та безпековій обстановці // Геополітичні студії. – 2020. – №3. – С. 102-118.

9. Бойко О. Удосконалення адміністративно-правового забезпечення кібербезпеки в умовах гібридних кіберзагроз // Вісник державного управління. – 2022. – №1. – С. 67-82.

10. Гончаренко І. Гібридна війна: сутність, складові та ключові поняття // Аналітичний огляд безпекових студій. – 2021. – №4. – С. 91-105.

11. Conflict Barometer: Число «войн» снизилось, «ограниченных войн» возросло. – 1 марта 2019 года [Електронний ресурс]. – Режим доступу: https://eadaily.com/ru/news/2019/03/01/conflictbarometer-chislo-voyn-snizilos-ogranichennyh-voyn-vozroslo

12. Country Reports on Terrorism. – 2019 [Електронний ресурс]. – Режим доступу: https://www.state.gov/wpcontent/uploads/2020/06/Country-Reports-on-Terrorism-2019-2.pdf

13. Присяжнюк М. М. Інформаційна складова сучасних гібридних воєн. -2017 [Електронний ресурс]. – Режим доступу: https://nuou.org.ua/assets/documents/zbirn-gibr-mizhn-konf.pdf/

14. Schwartz. A. Partners, Not Proxies: Capacity Building in Hybrid Warfare. – 2020 [Електронний ресурс]. – Режим доступу: https://www.csis.org/analysis/partners-not-proxies-capacity-buildinghybrid-warfare

15. Danyk Y., Maliarchuk T., Briggs C. Hybrid War: High-tech, Information and Cyber Conflicts. – 2017 [Електронний ресурс]. – Режим доступу: https://infosec-journal.com/article/hybrid-war-high-techinformation-and-cyber-conflicts

16. Raugh D. Is the Hybrid Threat a True Threat?. Current Issue: Volume 14, Number. [Електронний ресурс]. – Режим доступу: https://digitalcommons.usf.edu/cgi/viewcontent.cgi?referer=&httpsredi r=1&article=1507&context=jss

17. Кротюк В.А., Староконь Є.Г. Війни інформаційної епохи: міждисциплінарний дискурс : монографія. – 2021 [Електронний ресурс]. – Режим доступу: https://dspace.nlu.edu.ua/bitstream/123456789/19017/1/Dzeban_mono.pdf

18. Мартинюк В. Гібридні загрози Україні і суспільна безпека. досвід ЄС і східного партнерства. – 2018 [Електронний ресурс]. – Режим доступу: https://www.civic-synergy.org.ua/wpcontent/uploads/2018/04/blok_XXI-end_0202.pdf

19. Середа В.В., Серкевич І.Р. Тероризм: кримінологічна детермінація і кримінально-правова протидія: монографія. – 2016 [Електронний ресурс]. – Режим доступу: http://nbuviap.gov.ua/images/dorobku_partneriv/Teroryzm%20kryminolohichna%20determinatsiia%20i%20kryminalno-pravova%20protydiia.pdf

20. Стратегія розвитку Державної прикордонної служби України. Схвалено розпорядженням Кабінету Міністрів України від 23 листопада 2015 р. № 1189-р [Електронний ресурс]. – Режим доступу: https://dpsu.gov.ua/ua/strategiya rozvitku-

derzhavnoi-prikordonnoi-sluzhbiukraini-shvalenarozporyadzhennyam-kabinetu-ministriv-ukraini-vid-23-listopada2015-roku-1189-r/

21. Власюк В.В., Карман Я.В. Деякі основи поняття “гібридна війна” в міжнародному праві // Право і громадянське суспільство. – 2015 [Електронний ресурс]. – Режим доступу: http://lcslaw.knu.ua/index.php/item/207-deyaki-osnovy-ponyattya-hibrydna-viyna-vmizhnarodnomu-pravi-vlasiuk-v-v-karman-ya-v.

22. Мельник О., Пашков М., Поляков Л., Сунгуровський М. Партнерство Україна-ЄС у безпековій сфері: сучасний стан і перспективи. – Київ : Український центр економічних та політичних досліджень ім. О. Разумкова, 2021. – 71 с.

23. Проблеми суспільної безпеки в процесі розвитку соціальних мереж [Електронний ресурс]. – Режим доступу: buviap.gov.ua/index.php?option=com_content&view=article&id=1745:problemisuspilnoji-bezpeki-v-protsesi-rozvitku-sotsialnikh merezh&catid=78&Itemid=412

24. Малик Я. Інформаційна війна і Україна // Науковий вісник. – 2015. – Вип. 15. “Демократичне врядування” [Електронний ресурс]. – Режим доступу: http://www.lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Malyk.pdf

25. Стасюк В. Морально-психологічне забезпечення у Збройних силах України : підручник : у 2 ч. Ч. 1. – 2-е вид., перероб. зі змін. та допов. / Н. А. Агаєв, В. Г. Дикун, В. С. Чорний та ін. ; за заг. ред. В. В. Стасюка. – 2020. – 754 с. [Електронний ресурс]. – Режим доступу: https://dovidnykmpz.info/wp-content/uploads/2021/10/mpz-u-zsu-2020.pdf

26. Duggan M. Strategic Development of Special Warfare in Cyberspace [Електронний ресурс]. – Режим доступу: https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterl79/Article/621123/strategicdevelopment-of-special-warfare-in-cyberspace/

27. Telelim, Muzychenko, and Punda. Force Planning for the ‘Hybrid War’ Scenarios; Kofman M. Russian Hybrid Warfare and Other Dark Arts; Gerasimov V. The Value of Science in Prediction // Military Industrious Courier Journal. – 2013. – №8. – С. 1-3 (in Russian).

28. Gerasimov V. The Value of Science in Prediction // The ‘Gerasimov Doctrine’ and Russian Non-Linear War [Електронний ресурс]. – Режим доступу:

https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-andrussian-non-linear-war

29. This is a design of of the S.Korolov Zhytomyr Military Institute [Електронний ресурс]. – Режим доступу: https://uni-educationukraine.com/en/university/zhytomyr-military-institutenamed-after-s-p-korilov/

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

Тези наукових доповідей:

1. Рень Роман, Володимир Наконечний. Методи протидії кібервпливам в умовах ведення гібридної війни. VIII Міжнародної науково-практичної конференції “Проблеми кібербезпеки інформаційно-комунікаційних систем” (CPICS).