Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
магістра
(ступінь вищої освіти)

на тему Дослідження методів протидії загрозам безпеці силами та засобами
(назва теми)
служб захисту інформації

Виконав: студент 2 курсу, групи БК-814м

Спеціальності 125 - Кібербезпека та
(код і найменування спеціальності)
захист інформації

Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних систем

ЄРЕМЕНКО Є.М.
(ПРІЗВИЩЕ та ініціали)

Керівник КАРПУКОВ Л.М.
(ПРІЗВИЩЕ та ініціали)
Рецензент МОРОЗ Г.В.
(ПРІЗВИЩЕ та ініціали)

2025

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет_____Інформаційної безпеки та електронних комунікацій_____
Кафедра_____Інформаційної безпеки та наноелектроніки_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___125 – Кібербезпека та захист інформації_____
(код і найменування)
Освітня програма (спеціалізація)_Безпека інформаційних і комунікаційних___
_____систем_____
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
Завідувач кафедри __ІБтаН___
_____Андрій КОРОТУН__
«_____» _____20___року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

_____ЄРЕМЕНКА Євгена Миколайовича_____
(ПРІЗВИЩЕ, ім'я, по батькові)
1. Тема проєкту (роботи)_____Дослідження методів протидії загрозам інформаційній безпеці в інформаційних і комунікаційних системах_____
Research of methods for countering information security threats in information and communication systems_____
керівник проєкту (роботи)___д.т.н., професор, КАРПУКОВ Леонід Матвійович,
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом закладу вищої освіти від «26» листопада 2025 року №530
2. Строк подання студентом проєкту (роботи)__10 грудні 2025 року_____
3. Вихідні дані до проєкту (роботи)_Нормативно-правові акти у сфері кібербезпеки, міжнародні та національні стандарти інформаційної безпеки, наукові публікації та аналітичні звіти, технічна документація інформаційних і комунікаційних систем, матеріали щодо сучасних кіберзагроз, результати моделювання та аналізу систем захисту інформації_____
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)_Аналіз сучасного стану загроз інформаційній безпеці в інформаційних і комунікаційних системах. Дослідження методів і засобів забезпечення кібербезпеки. Аналіз моделей порушника та ризиків інформаційної безпеки. Розроблення рекомендацій щодо підвищення рівня захисту інформаційних і комунікаційних систем. Оцінювання ефективності запропонованих методів захисту_____

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів) Презентація доповіді, 26 слайдів (підготовлена в Microsoft Power Point)_____

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Основні розділи	КАРПУКОВ Л.М., професор кафедри ІБтаН	04.09.24	10.12.24
Нормоконтроль	КОРОЛЬКОВ Р.Ю., доцент кафедри ІБтаН		10.12.24

7. Дата видачі завдання «__01__» ____вересня___2025_року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз літературних джерел за тематикою дослідження	04.09.25 – 21.09.25	Виконано
2	Дослідження основних понять та визначень захисту інформації	22.09.25 – 07.10.25	Виконано
3	Аналіз організаційних заходів забезпечення інформаційної безпеки у службах захисту інформації	08.10.25 – 20.10.25	Виконано
4	Дослідження програмно-технічних засобів протидії загрозам інформаційній безпеці	21.10.25 – 17.11.25	Виконано
5	Аналіз комплексної системи протидії загрозам у службах захисту інформації, ефективності існуючих методів захисту та впровадження сучасних технологій моніторингу і кіберзахисту	18.11.25 – 25.11.25	Виконано
6	Виконання графічної пояснювальної записки	26.11.25 – 03.12.25	Виконано
7	Оформлення матеріалів магістерської роботи	04.12.25 – 10.12.25	Виконано

Студент(ка) _____ ___Євген ЄРЕМЕНКО___
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ __Леонід КАРПУКОВ____
(підпис) (Ім'я ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 99 с., 10 табл., 2 дод. 50 джерел.

ЗАХИСТ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНІ СИСТЕМИ, АКТИВНІ МЕТОДИ ЗАХИСТУ, ПАСИВНІ МЕТОДИ ЗАХИСТУ, ЗЛОВМИСНИК, МЕТОДИ АТАКИ, СЛУЖБА ЗАХИСТУ ІНФОРМАЦІЇ, АВТОМАТИЗОВАНІ СИСТЕМИ, КОМПЛЕКСНИЙ ЗАХИСТ, АДАПТИВНИЙ ЗАХИСТ.

Об'єктом дослідження є інформаційні системи, активні та пасивні методи захисту інформації, а також діяльність служби захисту інформації в автоматизованих системах.

Предметом дослідження є методи та механізми роботи зловмисника в процесі досягнення поставлених цілей, включаючи аналіз тактик, технік і процедур атак.

Метою дослідження є аналіз методів роботи зловмисників, узагальнення досвіду служби захисту інформації та розроблення рекомендацій щодо створення гнучкої комплексної системи захисту, здатної адаптуватися до сучасних безпекових ризиків.

Дипломна робота присвячена дослідженню методів і механізмів, які використовують зловмисники для досягнення своїх цілей в інформаційних системах. Проаналізовано активні та пасивні методи захисту інформації, організаційні заходи служби захисту в автоматизованих системах, а також типові сценарії атак. На основі узагальнення практичного досвіду служби захисту інформації запропоновано концепцію сучасної гнучкої комплексної

системи захисту, яка динамічно адаптується до змін безпекових ризиків і загроз.

Наукова новизна роботи полягає у впровадженні накопиченого досвіду служби захисту інформації в автоматизованих системах до створення адаптивної комплексної моделі захисту, здатної оперативно реагувати на еволюцію методів зловмисників.

Практична значимість результатів полягає в тому, що розроблені рекомендації та організаційні заходи можуть бути використані для удосконалення існуючих систем захисту інформації в організаціях, підвищення ефективності служби захисту та мінімізації ризиків несанкціонованого доступу.

ABSTRACT

Explanatory note to the master's thesis: 99 pages, 10 tables, 2 appendix, 50 references.

INFORMATION PROTECTION, INFORMATION SYSTEMS, ACTIVE PROTECTION METHODS, PASSIVE PROTECTION METHODS, ATTACKER, ATTACK TECHNIQUES, INFORMATION PROTECTION SERVICE, AUTOMATED SYSTEMS, COMPREHENSIVE PROTECTION, ADAPTIVE PROTECTION.

Object of the research is information systems, active and passive methods of information protection, as well as the activities of the information protection service in automated systems.

Subject of the research is the methods and mechanisms used by an attacker in the process of achieving their objectives, including the analysis of tactics, techniques, and procedures of attacks.

Purpose of the research is to analyze the methods employed by attackers, generalize the experience of the information protection service, and develop recommendations for creating a flexible comprehensive protection system capable of adapting to modern security risks.

The thesis is devoted to the study of methods and mechanisms utilized by malicious actors to achieve their goals in information systems. Active and passive information protection methods, organizational measures of the information protection service in automated systems, and typical attack scenarios have been analyzed. Based on the generalization of practical experience of the information protection service, a concept of a modern flexible comprehensive protection system has been proposed, which dynamically adapts to changes in security risks and threats.

Scientific novelty of the work lies in the integration of accumulated experience of the information protection service in automated systems into the development of an adaptive comprehensive protection model capable of promptly responding to the evolution of attacker methods.

Practical significance of the results lies in the fact that the developed recommendations and organizational measures can be used to improve existing information protection systems in organizations, enhance the effectiveness of the information protection service, and minimize the risks of unauthorized access.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АС — автоматизована система

ІБ — інформаційна безпека

ІКС — інформаційні і комунікаційні системи

ІС — інформаційна система

КСЗІ — комплексна система захисту інформації

СЗІ — служба захисту інформації

НСД — несанкціонований доступ

ПЗ — програмне забезпечення

ТЗІ — технічний захист інформації

НД ТЗІ — нормативний документ з технічного захисту інформації

DoS — Denial of Service (відмова в обслуговуванні)

DDoS — Distributed Denial of Service (розподілена відмова в обслуговуванні)

MITM — Man-in-the-Middle (атака типу «людина посередині»)

SIEM — Security Information and Event Management (система управління подіями інформаційної безпеки)

DLP — Data Loss Prevention (система запобігання витоку даних)

IDS — Intrusion Detection System (система виявлення вторгнень)

IPS — Intrusion Prevention System (система запобігання вторгненням)

CIA — Confidentiality, Integrity, Availability (конфіденційність, цілісність, доступність)

ISO/IEC — International Organization for Standardization / International Electrotechnical Commission

CERT — Computer Emergency Response Team (група реагування на комп’ютерні інциденти)

ВСТУП

Актуальність теми дослідження обумовлена сучасними викликами Україні як з боку держави-агресора, так і внутрішніми небезпеками. Сьогодні, коли більшість наших даних зберігається в електронному вигляді, кібербезпека стає все більш важливою. Особиста інформація, фінансові транзакції, корпоративні секрети – усе це може стати мішенню для ворога та кіберзлочинців. За даними експертів, у світі щороку збільшується кількість кібератак, і збитки від них досягають мільярдів доларів. А під час збройної агресії, захист інформації дорівнює захисту життя.

Особливе значення захист інформації має для підприємств, урядових структур, військових та науково-освітніх установ, які зобов'язані забезпечувати надійний захист даних своїх клієнтів і співробітників. Проте зростаюча складність комп’ютерних систем різних галузей дає змогу зловмисникам використати так само зростаючі вразливості. Кожна інформаційна система зараз потребує комплекс рішень, які шукають та впроваджують фахівці.

Зростання кількості кібератак, що супроводжується розвитком нових методів і технологій, ставить перед фахівцями завдання забезпечення належного захисту інформаційних систем.

Вразливості, що існують у програмному забезпеченні та системах, можуть стати початковою точкою для злочинців, що прагнуть компрометації даних та ресурсів організацій.

У рамках дослідження планується вивчити досвід роботи служби захисту інформації, що допоможе у формуванні цілісного підходу до зменшення ризиків у сфері кібербезпеки.

Метою дослідження у кваліфікаційній роботі є аналіз і дослідження принципів та методів захисту інформації.

Дослідження даної теми є не тільки теоретично важливим, але й практично значущим, оскільки дозволяє виробити стратегії для підвищення захищеності інформаційних систем, що врешті-решт сприятиме збереженню конфіденційності, цілісності та доступності інформації в умовах сучасних кіберзагроз.

Завданнями дослідження є:

- вивчити теоретичні основи та визначення галузі захисту інформації;
- розглянути методи та приклади політик безпеки;
- проаналізувати моделі загроз і методи захисту;
- провести практичні дії загроз, проаналізувати дії, провести аналіз індикаторів компрометації, провести аналіз дій компрометації за допомогою комплексу систем захисту інформації і дослідити результати вихідних даних програм.

Об'єкт дослідження — інформаційні системи, активні і пасивні методи захисту інформації, робота служби

Предмет дослідження — методи та механізми роботи зловмисника у процесі здобування поставлених для нього цілей.

Практична значимість результатів полягає у тому, що проаналізовані організаційні заходи та їхні результати можуть бути використані для удосконалення систем захисту інформації.

Наукова новизна роботи полягає у впроваджені досвіду служби захисту інформації в автоматизованих системах у сучасну та гнучку комплексну систему захисту інформації, яка може змінюватися і відповідати на безпекові ризики.

РОЗДІЛ 1. ОСНОВНІ ПОНЯТТЯ ТА ВИЗНАЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Аналіз поточного стану захисту інформації в Україні.

Сучасні суспільно-економічні та політичні процеси значною мірою визначаються розвитком інформаційних технологій, що дедалі глибше проникають у всі сфери діяльності держави, бізнесу та громадян. Збільшення обсягів інформації, її швидкості циркуляції та складності обробки зумовлює зростання залежності організацій від стабільності функціонування інформаційних систем, а відтак і від рівня їхнього захисту. Поняття захисту інформації в Україні набуло чітких нормативних обрисів завдяки розробці комплексу стандартів, серед яких провідну роль відіграють НД ТЗІ, Закон України «Про державну таємницю», Стратегія інформаційної безпеки та інші документи, що формують основу національного інформаційного законодавства [1; 2; 3]. У цих документах захист інформації визначається як діяльність, спрямована на забезпечення конфіденційності, цілісності та доступності даних. Такий підхід відповідає міжнародному стандарту ISO/IEC 27001, який встановлює вимоги до систем управління інформаційною безпекою та визначає триєдину модель базових властивостей інформації як фундамент організації системного захисту [4].

Зростаюча кількість кіберінцидентів, зокрема витоків даних, блокувань доступу до ресурсів та атак на критичну інфраструктуру, підкреслює важливість створення комплексних систем протидії загрозам. Інформація стала одним із ключових ресурсів сучасної держави та бізнесу, а її втрата або модифікація може призвести до значних економічних, політичних або соціальних наслідків. Саме тому об’єктами захисту виступають як державні інформаційні ресурси, так і дані приватного сектору, включаючи персональну інформацію громадян. Українське законодавство виділяє кілька категорій інформації з обмеженим доступом, серед яких інформація для службового

користування, таємна інформація, цілком таємна інформація та інформація особливої важливості. Такий поділ дозволяє класифікувати інформаційні активи за рівнем чутливості та визначати відповідні режими доступу [5].

У науковій літературі підкреслюється, що ефективність захисту інформації залежить не лише від технічних засобів, а й від організаційно-правових механізмів, рівня культури інформаційної безпеки, кваліфікації персоналу та правильності побудови системи управління інформаційною безпекою [6; 7; 8]. Це означає, що інформаційна безпека має комплексний характер, а для її забезпечення необхідно враховувати як зовнішні, так і внутрішні чинники впливу. Складність забезпечення безпеки пояснюється також тим, що інформаційні системи є відкритими, тобто взаємодіють із глобальними мережами, використовують інтернет-протоколи, мають численні точки доступу та підключення, що суттєво збільшує поверхню атак [9]. Саме тому сучасні підходи до побудови системи захисту повинні включати аналіз загроз, управління ризиками, оцінку вразливостей, моніторинг мережевих активностей та регулярний аудит стану безпеки.

Базові властивості інформації традиційно визначають через три ключові характеристики, а саме конфіденційність, цілісність та доступність. Конфіденційність передбачає захист інформації від несанкціонованого доступу, що стає особливо важливим в умовах масових витоків персональних даних та підвищеної активності кіберзлочинних угруповань, які спеціалізуються на викраденні облікових даних та інтелектуальної власності [10, с. 112]. Цілісність забезпечує незмінність інформації, що критично для систем керування технологічними процесами, банківських транзакцій та інших сфер, де навіть незначні модифікації даних можуть призвести до серйозних порушень. Доступність гарантує можливість отримати дані у потрібний час, і її порушення часто спостерігається під час DDoS-атак або технічних збоїв, що паралізують роботу організацій. Ці властивості є невід’ємними складовими будь-якої системи захисту, і їх врахування дозволяє вибудувати ефективну стратегію протидії загрозам [4].

У цій таблиці подано розширену характеристику основних властивостей інформації, які є обов'язковими для врахування в національних та міжнародних стандартах захисту.

Таблиця 1.1 - Основні властивості інформації та їх характеристика [10, с.416].

Властивість	**Зміст**	**Потенційні наслідки порушення**	**Типові заходи забезпечення**
Конфіденційність	Обмеження доступу до даних тільки для уповноважених осіб	Витік інформації, розголошення державної таємниці, компрометація персональних даних	Криптографія, контроль доступу, політики паролів
Цілісність	Забезпечення незмінності та достовірності даних	Порушення обчислень, спотворення управлінських рішень, збої у технологічних системах	Контроль цілісності, цифрові підписи, контроль версій
Доступність	Гарантований доступ до системи та інформації у потрібний час	Зупинка бізнес-процесів, блокування сервісів, збитки	Резервування, фільтрація трафіку, відмовостійкі системи

Загрози інформації є широким комплексом явищ, які можуть негативно вплинути на стан інформаційних активів організації. Відповідно до НД ТЗІ 2.5-004-99, під загрозами розуміють сукупність умов та факторів, що створюють потенційну або реальну небезпеку для інформації. У науковій та нормативній практиці загрози поділяють за походженням на природні, техногенні, технічні, організаційні, людські та навмисні. Така класифікація дозволяє визначити специфіку кожного типу загроз і вибудувати систему протидії, орієнтовану на виявлення та мінімізацію конкретних ризиків [11, с. 18]. Особливо небезпечними вважаються навмисні дії порушників, адже вони характеризуються цілеспрямованістю, високою технічною складністю та різноманітністю форм реалізації. Кваліфікований порушник може

використовувати сучасні технології, приховані канали зв’язку та складні програмні засоби, що ускладнює виявлення та локалізацію атак.

Стихійні лиха, збої обладнання, помилки проектування та людський фактор становлять значну частку інцидентів інформаційної безпеки. Дослідження показують, що близько 40 % порушень виникають через недоліки в організаційних процесах, зокрема низький рівень підготовки персоналу, відсутність процедур контролю доступу або неправильну конфігурацію систем [12]. Водночас природні загрози, такі як пожежі чи повені, хоч і є менш імовірними, але можуть призвести до катастрофічних наслідків у разі відсутності резервного копіювання або географічно розподіленої інфраструктури. Техногенні загрози пов’язані з виходом з ладу електропостачання, серверів, мережевого обладнання, що часто призводить до втрати доступності або цілісності інформації.

У цій таблиці систематизовано основні типи загроз інформації та заходи протидії на основі сучасних підходів до інформаційної безпеки.

Таблиця 1.2 - Класифікація загроз інформації та методи протидії [9, с.960].

Тип загрози	**Джерело виникнення**	**Можливі наслідки**	**Методи протидії**
Природні та техногенні	Стихійні лиха, аварії, пожежі	Втрата інформації, пошкодження обладнання	Резервування, копіювання, аварійне живлення
Технічні	Відмови обладнання, збої ПЗ	Блокування доступу, порушення цілісності	Вибір якісного обладнання, технічна підтримка
Проектні	Помилки архітектури та реалізації	Уразливості, некоректна робота систем	Аудит проектів, тестування
Людський фактор	Помилки персоналу, порушення інструкцій	Неправильні дії, витік інформації	Навчання, мотивація, контроль
Навмисні	Віруси, атаки, шкідливі програми	Несанкціонований доступ, блокування	Криптографія, антивіруси, міжмережеві екрани

Загрози, пов’язані з діяльністю людини або груп осіб, займають особливо важливе місце у структурі ризиків, оскільки вони характеризуються високим

рівнем непередбачуваності та складністю нейтралізації. Порушник може використовувати як технічні засоби, так і соціальні прийоми впливу, серед яких соціальна інженерія та фішинг, які у сучасних умовах є одними з найефективніших засобів отримання несанкціонованого доступу до інформаційних систем [13]. Суттєвою проблемою залишається те, що багато користувачів нехтують базовими правилами інформаційної безпеки, зокрема створенням надійних паролів або двофакторною аутентифікацією, що створює додаткові шанси для атакувальників. Водночас самі організації часто недооцінюють ризики, пов’язані з недостатньою кваліфікацією персоналу або слабкою корпоративною культурою безпеки, що дозволяє порушникам використовувати людський фактор як найвразливіший елемент системи.

Серед загроз, які характеризуються навмисним характером дій, особливої уваги заслуговують атаки на мережевому рівні, що включають прослуховування трафіку, підміну IP-адрес, зломи автентифікаційних механізмів та створення шкідливих програм. Як зазначає Б. Шнайер, складність сучасних атак зумовлена тим, що вони будуються на виявленні неочевидних вразливостей протоколів та сервісів, а також на використанні комплексних методів ухилення від виявлення [10, с. 178]. Протокол TCP/IP, який є основою для глобальних мереж, спочатку не містив механізмів забезпечення безпеки, що робить його уразливим до низки атак, включаючи перехоплення пакетів, підміну заголовків та ін’єкцію фальшивих даних [9, с. 423]. Це створює сприятливі умови для збільшення спектра можливих дій атакувальників та ускладнює завдання побудови ефективних захисних механізмів.

Прослуховування трафіку, або sniffing, належить до найбільш поширених методів пасивного несанкціонованого доступу, коли порушник отримує інформацію про передані пакети, не втручаючись у роботу системи. Метою таких атак є здобуття облікових даних, мережевих конфігурацій та інших технічних параметрів, які можуть бути використані для подальшого проникнення в систему. Протидією таким діям є використання криптографічних протоколів, шифрування трафіку та застосування

спеціалізованих програмних засобів для виявлення аномальних мережевих активностей. З іншого боку, підміна адреси, або IP-spoofing, передбачає активну взаємодію атакувальника із системою і полягає у створенні пакета з фальшивою IP-адресою відправника. Це дозволяє порушнику видавати себе за легального користувача, обходити механізми контролю доступу або створювати умови для реалізації атак, спрямованих на відмову в обслуговуванні.

Атаки на паролі залишаються актуальними завдяки тому, що значна кількість користувачів використовує прості та передбачувані комбінації, які легко піддаються перебору. У цьому контексті однією з ефективних методик захисту є використання одноразових паролів, обмеження кількості спроб входу, а також впровадження механізмів блокування облікових записів після певної кількості невдалих авторизацій. Водночас важливим залишається підвищення рівня обізнаності персоналу, оскільки навіть найскладніші технічні системи можуть бути зламані через недбалість або низьку інформаційну культуру користувачів [12].

Особливо небезпечними є атаки, спрямовані на порушення доступності сервісів, так звані DoS та DDoS-атаки. Їхня мета полягає у перевантаженні інформаційної системи фіктивними запитами настільки, щоб вона перестала адекватно працювати. У разі масованої DDoS-атаки, що здійснюється з великої кількості заражених пристроїв, блокування доступу до сервісів може відбуватися навіть при значних обчислювальних потужностях. Це особливо критично для фінансових установ, інтернет-магазинів та органів влади, діяльність яких безпосередньо пов’язана з безперебійною роботою вебресурсів. Виявлення та блокування таких атак здійснюється за допомогою інтелектуальних систем маршрутизації, фільтрації трафіку, аналізу поведінкових характеристик запитів та застосування архітектурних рішень типу CDN.

Ще одним широко розповсюдженим видом загроз є атаки типу «людина посередині» (MITM), коли порушник перехоплює обмін даними між двома

сторонами, отримуючи доступ до інформації або змінюючи її зміст. Для протидії таким атакам використовуються механізми взаємної аутентифікації, криптографічні протоколи та системи виявлення вторгнень. Зловживання довірою в мережі виникають тоді, коли внутрішні служби або сервери сприймаються як безпечні за замовчуванням, що дозволяє атакувальнику проникнути в систему, використовуючи вразливості одного з компонентів інфраструктури. Саме тому сучасні підходи до безпеки передбачають мінімізацію рівня довіри та впровадження принципу Zero Trust, який передбачає перевірку будь-якого запиту незалежно від його джерела [14].

Шкідливе програмне забезпечення, зокрема віруси, трояни та програмні черв'яки, залишається одним із наймасовіших інструментів кіберзлочинців. Програми-вимагачі, що шифрують інформацію та вимагають викуп за її розблокування, стали глобальною проблемою останніх років. Стратегії захисту включають використання антивірусних систем, регулярне оновлення програмного забезпечення, моніторинг бюлетенів безпеки та проведення аналізу вразливостей. Атаки на рівні застосувань стали одним із ключових напрямів діяльності кіберзлочинців, оскільки більшість сучасних сервісів працює у вебсередовищі та відкрита для взаємодії через мережу. Серед типових атак — SQL-ін'єкції, XSS-атаки, підміна параметрів запитів, використання вразливостей CMS та фреймворків.

У цьому контексті важливо зазначити, що жодна система безпеки не може протистояти всім видам атак протягом тривалого часу, якщо вона не оновлюється відповідно до появи нових загроз. Досвід останніх років свідчить про те, що кіберзлочинці постійно вдосконалюють свої методи, використовують машинне навчання, автоматизовані системи сканування вразливостей та технології штучного інтелекту для виявлення точок проникнення. Водночас дослідники підкреслюють, що ключову роль у забезпеченні безпеки відіграє не тільки технічний рівень системи, але й правильність організації процесів, включаючи навчання персоналу, розробку

політик безпеки, створення резервних копій та впровадження систем моніторингу [6; 15].

Аналіз причин виникнення загроз показує, що значний їх відсоток пов’язаний із системними недоліками у проектуванні мереж та програмного забезпечення. Як зазначає Таненбаум, багато протоколів було розроблено в період, коли питання безпеки не стояли так гостро, тому вони мають фундаментальні слабкості, що не можуть бути усунені без повної перебудови архітектури [9]. Іншою причиною є широке використання загальнодоступних каналів зв’язку, де передача даних може бути перехоплена або модифікована без фізичного доступу до обладнання. Недостатність контролю за маршрутизацією інформації у глобальній мережі також створює передумови для реалізації віддалених атак, які практично неможливо відстежити.

1.2 Політика безпеки та управління ризиками в галузі захисту інформації

Подальший розвиток системи захисту інформації неможливий без формування чіткої політики безпеки, що визначає засади обробки, передачі та зберігання даних у межах організації. Політика інформаційної безпеки у міжнародній практиці розглядається як комплекс документів, який встановлює правила доступу до інформаційних ресурсів, описує обмеження, відповідальність користувачів і процедури реагування на інциденти. Така політика слугує стратегічною основою, на якій базується вся архітектура безпеки, включаючи технічні, організаційні та правові заходи [4; 6]. Правильне формування політики має критичне значення, оскільки будь-який недолік або нечіткість у формулюваннях може створити вразливість, яка буде використана порушниками.

Політика повинна містити опис типів інформації, які обробляються в організації, їхню класифікацію за рівнем критичності та визначення

відповідних режимів доступу. Саме класифікація є ключовим елементом, який дозволяє розподілити ресурси системи безпеки таким чином, щоб їх використання було максимально ефективним. Дані, що становлять державну або комерційну таємницю, потребують посиленого захисту, тоді як інформація зі зниженим рівнем чутливості може зберігатися у менш захищених середовищах [2; 5]. Формування моделі загроз у рамках політики безпеки дозволяє врахувати специфіку організації, її інфраструктури, характер інформаційних потоків та можливі сценарії реалізації атак. Така модель може бути як формалізованою, так і неформалізованою, однак обидва підходи повинні забезпечити розуміння того, які загрози є найбільш імовірними та небезпечними.

У межах політики також формується модель порушника, яка описує типи можливих атакувальників, їх мотивацію, технічні можливості та доступні ресурси. Важливо відзначити, що у сучасних умовах межа між внутрішнім і зовнішнім порушником часто є розмитою, адже зовнішні атакувальники можуть вербувати співробітників або використовувати соціотехнічні методи для отримання внутрішньої інформації [15]. Тому модель порушника повинна враховувати не лише технічні аспекти можливих атак, а й поведінкові та психологічні фактори, які можуть впливати на дії людей. У кількісних методах аналізу ризиків модель порушника дозволяє визначити рівень загрози, ймовірність її реалізації та потенційні збитки для організації.

Оцінка ризиків у політиці безпеки відіграє стратегічну роль, оскільки саме вона дозволяє визначити, які ресурси необхідно спрямувати на захист конкретних інформаційних активів. У міжнародних стандартах, зокрема в ISO/IEC 27005, пропонується використовувати як якісні, так і кількісні методи оцінювання ризиків. Якісні методи базуються на експертних оцінках і використовуються тоді, коли точні числові дані отримати важко, наприклад через відсутність статистики інцидентів. Кількісні методи дозволяють визначити можливі фінансові втрати від реалізації загроз та порівняти їх із витратами на впровадження заходів захисту. Вони передбачають створення

таблиць збитків, імовірностей атак та обчислення інтегрального показника ризику, що дозволяє приймати обґрунтовані управлінські рішення [11].

Система управління ризиками передбачає також аналіз можливих сценаріїв розвитку інцидентів, включаючи найгірші варіанти, які можуть призвести до зупинки бізнес-процесів або порушення критично важливих операцій. У цій таблиці представлено умовний приклад структурованої моделі ризиків, яка використовується для формування рішень щодо розподілу ресурсів на захист інформації.

У цій таблиці подано приклад моделі оцінювання ризиків інформаційної безпеки, яка ґрунтується на визначенні типів загроз, імовірності їх реалізації та можливого рівня збитків. Модель дозволяє здійснити інтегральну оцінку ризику та визначити необхідні заходи реагування з боку служб захисту інформації.

Таблиця 1.3 Приклад моделі ризиків інформаційної безпеки [16, с.280]

Тип загрози	**Ймовірність реалізації**	**Рівень збитків**	**Інтегральний ризик**	**Необхідні заходи**
Витік конфіденційних даних	Середня	Високий	Високий	Посилення контролю доступу, шифрування
Атаки DDoS	Висока	Середній	Високий	Фільтрація трафіку, резервні канали
Вірусні зараження	Висока	Низький	Середній	Антивірусні системи, оновлення ПЗ
Відмова серверів	Низька	Високий	Середній	Резервування обладнання

Чим більший інтегральний ризик, тим пріоритетнішим є впровадження заходів захисту. У розвинених організаціях оцінка ризиків виконується регулярно, оскільки загрози можуть швидко змінюватися, а нові вразливості з’являються практично щодня. Застосування гнучких механізмів управління дозволяє не лише підвищити стійкість системи, а й оптимізувати витрати на

безпеку. Це відповідає принципу економічної доцільності, згідно з яким вартість впровадження заходів не повинна перевищувати потенційні збитки, що можуть бути завдані внаслідок реалізації загроз [6].

Важливим компонентом політики інформаційної безпеки є визначення реакції системи на інциденти. Це включає створення процедур для виявлення, фіксації, аналізу та усунення наслідків порушень безпеки. Розвинені організації впроваджують системи моніторингу, які дозволяють оперативно реагувати на аномальні події та блокувати підозрілі дії. Така діяльність може здійснюватися як у межах окремого підрозділу, так і централізовано на рівні держави або великих корпорацій, де працюють центри реагування на інциденти безпеки (CERT). Ефективне реагування дозволяє швидко локалізувати проблему та мінімізувати її наслідки, що є критичним фактором виживання для організації під час кіберінцидентів.

У межах політики також визначаються повноваження користувачів системи, зокрема порядок доступу до ресурсів, обсяг відповідальності та вимоги до автентифікації. Правильний розподіл ролей дозволяє уникнути ситуацій, у яких користувачі отримують надмірні права доступу, що створює потенційні ризики несанкціонованих дій. У цьому контексті міжнародні стандарти рекомендують використовувати принцип найменших привілеїв, згідно з яким кожен користувач отримує лише ті права, що необхідні йому для виконання функціональних обов’язків [4].

Реалізація політики безпеки вимагає створення системи моніторингу, яка фіксуватиме події, пов’язані з кіберзагрозами, технічними збоями та порушеннями доступу. Сучасні інструменти моніторингу базуються на машинному аналізі логів, поведінковому аналізі та алгоритмах виявлення аномалій. Вони дозволяють розпізнавати навіть складні та нестандартні атаки, які спрямовані на обхід традиційних засобів захисту. Окремі організації впроваджують багаторівневі системи SIEM (Security Information and Event Management), які об’єднують дані з різних джерел і забезпечують глибокий аналіз інцидентів. Застосування таких систем відповідає принципу проактивної

безпеки, коли організація не лише реагує на загрози, але й намагається передбачити можливі сценарії їх розвитку.

Загалом політика інформаційної безпеки є важливим інструментом управління, який визначає загальну логіку, методи та процедури забезпечення захисту інформаційних ресурсів. Правильне формування політики дозволяє створити міцний фундамент для побудови комплексної системи безпеки та значно знижує ризики, пов’язані з функціонуванням інформаційних систем. У сучасних умовах такі політики мають бути не статичними, а адаптивними, регулярно оновлюватися відповідно до появи нових загроз, змін у законодавстві та трансформації технічної інфраструктури організації [14].

Подальший розвиток теоретичних і практичних підходів до захисту інформації зумовив появу сучасних моделей управління безпекою, які враховують комплексність функціонування інформаційних систем і високу динамічність технічного середовища. Однією з ключових концепцій у цьому контексті є модель, що поділяє параметри інформаційної системи на керовані, некеровані та зовнішні. Керовані параметри представляють собою ті характеристики, на які служба безпеки може безпосередньо впливати шляхом налаштування технічних засобів, удосконалення політик чи запровадження нових процедур. Некеровані параметри стосуються внутрішніх властивостей системи, які не можуть бути змінені миттєво, але здатні модифікуватися під час оновлення або модернізації. Параметри зовнішнього середовища охоплюють умови, що не контролюються організацією, наприклад діяльність зовнішніх порушників, глобальні мережеві збої або появу нових видів шкідливих програм [12].

Застосування цієї моделі дозволяє аналізувати безпеку системи з точки зору взаємодії різних факторів, що впливають на рівень захищеності. Показники безпеки можуть визначатися як функція низки параметрів, що включають характеристики апаратного забезпечення, програмного середовища, людського фактора та зовнішніх впливів. Така взаємозалежність підкреслює складність і багатогранність інформаційної безпеки, для якої не існує

універсальних рішень. Оптимізація розподілу ресурсів між різними напрямами захисту є важливою задачею, що має ґрунтуватися на об’єктивних даних про стан системи та характер потенційних загроз. В умовах обмеженості ресурсів організації повинні застосовувати принципи пріоритетності, спрямовуючи найбільші зусилля на ті ділянки, які становлять найвищий ризик.

Іншим важливим підходом до моделювання безпеки є ентропійний метод, який розглядає систему захисту як механізм максимально ефективного використання ресурсів для досягнення заданого рівня безпеки. У цій концепції кожен показник ефективності захисту пов’язаний із певними витратами, що дозволяє формулювати задачу оптимізації як задачу максимізації корисності за умови обмеженого бюджету. Такий підхід є особливо актуальним для великих організацій із розгалуженою інфраструктурою, де витрати на безпеку можуть бути значними й повинні бути обґрунтованими. Використання ентропійних показників дозволяє визначити оптимальний баланс між витратами на захист і рівнем потенційного збитку, якого можна уникнути завдяки впровадженню заходів безпеки [14].

Сучасні інформаційні системи характеризуються високою взаємопов’язаністю, що значно підвищує складність управління їхньою безпекою. Багато процесів автоматизовано, а інформаційні потоки проходять через різні підсистеми, сервери, канали зв’язку та мережеві рівні. Це створює численні точки потенційного впливу порушників і вимагає особливої уваги до побудови моделей управління, що враховують багатофакторність таких процесів. Модель повного управління безпекою об’єднує всі можливі механізми впливу на систему, включаючи оперативне управління засобами захисту, стратегічне планування ресурсів, модернізацію системи та оптимізацію її конфігурації. Такий підхід дозволяє досягти максимальної адаптивності, що є важливою умовою ефективної протидії сучасним загрозам.

У межах адаптивних моделей управління велике значення має моніторинг стану інформаційної системи та аналіз подій безпеки. Застосування автоматизованих систем контролю, таких як SIEM, дозволяє визначати

закономірності у поведінці мережевого трафіку, виявляти нетипові дії та оперативно реагувати на інциденти. Поєднання таких систем із методами машинного навчання та штучного інтелекту підвищує їхню здатність виявляти складні та приховані загрози, які можуть бути непомітними для традиційних інструментів аналізу. Особливо важливим є аспект прогнозування, що дозволяє не лише фіксувати факти порушень, але й передбачати можливі сценарії атак, оцінювати їхню імовірність і розробляти заходи щодо їхнього попередження.

Невід'ємним компонентом комплексного підходу є системи контролю інформаційних потоків, які забезпечують виявлення спроб несанкціонованого виведення даних з інформаційної системи. У сучасній практиці такі системи відомі як DLP (Data Loss Prevention) і призначені для аналізу даних, що передаються по мережі чи копіюються на зовнішні носії. Вони базуються на попередньо визначених політиках та механізмах контент-аналізу, що дає змогу зупиняти або блокувати підозрілу активність. Ці системи є надзвичайно важливими для організацій із великими обсягами конфіденційної інформації, оскільки значна частина витоків відбувається не через зовнішні атаки, а через дії або помилки співробітників [6; 7].

Побудова системи захисту неможлива без врахування людського фактора, який залишається найслабкішим елементом інформаційної безпеки. Навіть у добре захищених технічних системах помилки користувачів можуть призвести до серйозних інцидентів. Недбалість, необережність, незнання або свідоме порушення правил — усе це збільшує ризики, пов'язані з обробкою інформації. У зв'язку з цим важливими є навчання персоналу, підвищення його обізнаності щодо загроз, впровадження регулярних тренінгів і тестувань, що включають моделювання кіберінцидентів, фішингових атак і дій у кризових умовах. У деяких організаціях застосовуються імітаційні тести, які дають змогу оцінити готовність співробітників до реагування на загрози [15].

Людський фактор відіграє вирішальну роль і у формуванні організаційної культури безпеки, яка визначає ставлення персоналу до правил, політик і вимог захисту інформації. Дослідження показують, що у компаніях з високою

культурою безпеки рівень інцидентів значно нижчий, навіть за умови використання однакових технічних засобів. Впровадження культури безпеки передбачає формування розуміння, що кожен співробітник несе частину відповідальності за захист інформаційних активів організації. Важливими є чіткість комунікацій, доступність інструкцій, прозорість процедур та систематичний контроль за їх дотриманням [6].

У цьому контексті не можна не звернути увагу на правові аспекти регулювання інформаційної безпеки. Українське законодавство містить низку норм, що визначають правила роботи з інформацією, включаючи Закон України «Про державну таємницю», Закон «Про Основні засади розвитку інформаційного суспільства» та Стратегію інформаційної безпеки України. Правові норми регламентують доступ до даних, відповідальність за їх неправомірне використання та вимоги до організації захисту інформації в різних сферах діяльності [2; 3]. Значну увагу приділяють також міжнародним документам, що визначають стандарти безпеки, зокрема ISO/IEC 27001 та пов’язані з ним нормативні документи. Вони створюють універсальну базу, яка може бути адаптована до національних умов, з урахуванням особливостей законодавства та специфіки інформаційних систем.

Правові аспекти є важливими також тому, що вони визначають межі відповідальності організації та окремих співробітників за забезпечення безпеки інформації. Наявність детально розроблених правових механізмів дозволяє забезпечити прозорість і контроль у сфері інформаційної безпеки, а також запровадити санкції за порушення правил. Крім того, законодавство встановлює вимоги до зберігання інформації, процедур її передачі та знищення, що є невід’ємними елементами життєвого циклу інформаційних активів [17].

Комплексність проблеми інформаційної безпеки вимагає інтеграції технічних, організаційних, правових та соціальних факторів для створення ефективної системи. У сучасному світі захист інформації не може розглядатися як статична структура, оскільки загрози постійно розвиваються, а технології швидко змінюються. Ефективний захист полягає у здатності системи

адаптуватися, навчатися та впроваджувати нові засоби безпеки у відповідь на зміни зовнішнього середовища. Тому організації повинні розвивати гнучкі стратегії, орієнтовані на безперервне вдосконалення та регулярний перегляд процедур безпеки.

Загальний розвиток концепцій інформаційної безпеки показує, що ефективний захист не може бути досягнутий без комплексної інтеграції різних підходів, зокрема управлінських, технічних, організаційних та правових. Однією з ключових тенденцій є перехід від реактивних до проактивних моделей безпеки, у яких основним завданням є не лише виявлення інцидентів і мінімізація їхніх наслідків, а й передбачення потенційних загроз. Застосування методів прогнозного аналізу, штучного інтелекту та моделювання дозволяє значно підвищити рівень ефективності систем захисту, оскільки вони здатні виявляти неочевидні закономірності та потенційні вектори атак ще до їх реального здійснення [13; 14].

Особливе значення у цьому контексті має формування інтегрованих систем, які охоплюють увесь життєвий цикл інформації — від її створення до зберігання та знищення. Важливо, щоб засоби захисту були впроваджені не фрагментарно, а у єдиному комплексі, який забезпечує взаємодію різних компонентів системи. Технічні засоби, такі як міжмережеві екрани, криптографічні протоколи, антивірусні системи та системи виявлення вторгнень, повинні функціонувати під єдиним управлінням, що дозволяє мінімізувати дублювання методів та уникнути конфліктів у налаштуваннях. Організаційні заходи — інструкції, стандарти, процедури — мають бути узгоджені та регулярно оновлюватися відповідно до змін у структурі організації, технологіях та законодавстві [6].

Управління інформаційною безпекою також включає розподіл ролей і відповідальності між співробітниками. Чітка ієрархія доступу, визначення ролей адміністраторів системи, офіцерів із безпеки та кінцевих користувачів є одним із фундаментальних аспектів побудови надійної системи. У міжнародних практиках застосовується принцип сегментації мережі, коли доступ до різних її

сегментів визначається відповідно до потреб конкретних підрозділів. Це дозволяє мінімізувати можливі наслідки кіберінцидентів, оскільки порушник навіть у разі проникнення не може отримати доступ до всієї інфраструктури відразу.

У межах сучасних моделей управління значну увагу приділяють аналізу інцидентів, який передбачає вивчення причин порушення, оцінку наслідків та формування коригувальних заходів. У розвинених організаціях існують спеціальні групи реагування на інциденти, які працюють у цілодобовому режимі та здатні оперативно ізолювати загрозу. Аналіз інцидентів дозволяє організації навчатися на власних помилках, вдосконалювати політики безпеки та запобігати повторенню схожих ситуацій. Такий підхід формує цикл безперервного вдосконалення, що є одним із ключових принципів стандарта ISO/IEC 27001 [4].

Питання ефективності систем інформаційної безпеки неможливо розглядати без урахування економічних аспектів. Інвестиції в захист інформації повинні бути економічно обґрунтованими, тому організації використовують різні методи аналізу витрат і вигод. Зокрема, на основі оцінки ризиків визначаються ті загрози, усунення яких приноситиме найбільший ефект за найменших витрат. Це дозволяє уникнути ситуацій, у яких значні фінансові ресурси витрачаються на малоймовірні загрози, тоді як реальні ризики залишаються незакритими. У цьому контексті важливою є здатність організації визначати економічно доцільний рівень захисту, який забезпечує баланс між витратами та безпекою [6; 7].

У межах економічного аналізу системи захисту важливу роль відіграють показники ефективності, такі як швидкість реагування на інциденти, стабільність роботи системи, кількість виявлених атак та інші метрики, що дозволяють оцінити результативність заходів безпеки. На основі цих показників керівництво може приймати обґрунтовані рішення щодо модернізації інфраструктури, впровадження нових технологій або зміни політик безпеки. Такий підхід дозволяє не тільки покращувати систему захисту,

а й підвищувати конкурентоспроможність організації, оскільки стабільність її інформаційних ресурсів є важливою умовою ефективної діяльності.

Нижче подано узагальнювальну таблицю, яка представляє основні елементи сучасної системи інформаційної безпеки та їхній взаємозв'язок. Це дозволяє побачити структуру підсистем у комплексі та визначити ключові напрями, що потребують уваги у процесі створення надійного захисту.

Таблиця 1.4 - Узагальнена структура сучасної системи інформаційної безпеки *[15, с.108*

Компонент	**Основний зміст**	**Ключові функції**	**Очікувані результати**
Технічні засоби	Апаратура, ПЗ, мережеві інструменти	Фізичний і логічний захист	Стійкість до технічних загроз
Організаційні заходи	Політики, процедури, інструкції	Регулювання поведінки персоналу	Зменшення людського фактору
Правові механізми	Закони, нормативи, стандарти	Встановлення правил доступу та відповідальності	Дотримання вимог законодавства
Моніторинг та аудит	Аналіз логів, SIEM	Виявлення аномалій та інцидентів	Своєчасне реагування на загрози
Управління ризиками	Аналіз активів і загроз	Пріоритезація заходів	Оптимізація витрат на безпеку

Із розвитком інформаційних систем та зростанням залежності суспільства від цифрових технологій підвищується важливість створення стійких систем безпеки. Масштабна цифровізація бізнесу, державних сервісів та особистих комунікацій створила безліч нових можливостей для обміну інформацією, але водночас суттєво збільшила ризики. Це підкреслює необхідність удосконалення концепцій і стандартів безпеки, які мають адаптуватися до нових викликів. Стратегія розвитку інформаційного суспільства в Україні визначає пріоритетом формування безпечного цифрового середовища, у якому громадяни можуть отримувати доступ до послуг без ризику втрати своїх даних [18; 3].

Важливо усвідомлювати, що інформаційна безпека — це не лише технічна дисципліна, а й міждисциплінарна область, що охоплює соціологію, право, психологію, економіку та управління. Наприклад, механізми соціальної інженерії базуються на психологічному впливі, а тому їхнє розуміння потребує знань про поведінкові моделі людини. Правові аспекти визначають межі дозволеного, тоді як технічні рішення пропонують інструменти реалізації вимог. Таке поєднання різних галузей знань створює унікальну структуру дисципліни, яка потребує постійного оновлення, дослідження і вдосконалення.

Підсумовуючи аналіз, можна стверджувати, що система інформаційної безпеки є складною адаптивною структурою, яка вимагає системного підходу на всіх рівнях. Вона не піддається шаблонним рішенням, оскільки кожна організація має свої унікальні особливості, що впливають на вибір методів захисту. Ефективність системи залежить від гармонійного поєднання технічних, організаційних та правових засобів, а також від фактора людської поведінки. Усе це формує основу для побудови високорозвинених систем захисту, які здатні забезпечити стійкість організацій у сучасному цифровому середовищі.

Таким чином, сучасні інформаційні системи функціонують у складному середовищі, де загрози можуть виникати несподівано, швидко змінюватися та набувати нових форм. Це ставить перед фахівцями завдання створення динамічних систем безпеки, здатних адаптуватися до нових умов і забезпечувати стабільність функціонування організацій. Важливим є розуміння того, що інформаційна безпека — це процес, а не статичний стан, і він потребує постійного вдосконалення, аналізу ризиків та оновлення методів протидії.

РОЗДІЛ 2. МЕТОДИ ТА ЗАСОБИ ПРОТИДІЇ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

2.1 Організаційні заходи забезпечення інформаційної безпеки

Організаційні заходи є фундаментальною складовою системи протидії загрозам інформаційній безпеці, оскільки саме вони формують нормативний, управлінський та процедурний каркас функціонування служб захисту інформації. У науковій літературі та правозастосовній практиці все частіше підкреслюється, що технічні засоби можуть бути ефективними лише тоді, коли вони інтегруються у чітко структуровану та правильно організовану систему управління інформаційними ризиками. Кормич Б.А. зазначає, що організаційно-правові механізми відіграють ключову роль у формуванні національної політики інформаційної безпеки, оскільки без них інформаційний простір держави стає вразливим до зовнішнього та внутрішнього тиску [6, с. 214]. Це означає, що створення комплексних організаційних заходів має розглядатися державою як стратегічний пріоритет.

Організаційні заходи охоплюють сукупність дій, спрямованих на створення структур, процедур, правил та регламентів, які забезпечують сталу роботу служби захисту інформації. До таких заходів належать нормативно-правове забезпечення, кадрова політика, управління доступом, організація внутрішнього контролю, створення безпекових політик та впровадження системи реагування на інциденти. Як підкреслює Корж І., сучасні концепції безпеки визначають організаційний компонент як основу, що забезпечує стійкість інформаційної інфраструктури перед загрозами різної природи [7, с.

70]. Це пояснюється тим, що більшість інцидентів виникає не через технічні уразливості, а через порушення правил, відсутність контролю або людський фактор.

Одним із ключових організаційних механізмів протидії загрозам інформаційній безпеці є нормативно-правова база, яка визначає вимоги до суб'єктів сфери інформаційного захисту. Закон України «Про основні засади розвитку інформаційного суспільства» формує загальну рамку розвитку інформаційної сфери та закладає основи для формування безпекових політик [2]. Також вагоме значення має Доктрина інформаційної безпеки України, у якій закріплено роль держави у формуванні політики протидії інформаційним загрозам, включно з розвитком служб захисту інформації [19]. Наявність нормативної стабільності дозволяє організаціям формувати внутрішні положення та регламенти на основі державних вимог і міжнародних стандартів.

Важливою складовою організаційних заходів є діяльність органів державної влади щодо координації політики інформаційної безпеки. Калюжний і Цимбалюк зазначають, що скоординована діяльність органів державної влади є ключем до успішної протидії кіберзлочинності та іншим загрозам цифрового середовища [15, с. 108]. Вони підкреслюють, що без відповідної організаційної взаємодії та обміну інформацією різні інституції фактично діють роз'єднано, що знижує ефективність протидії загрозам. Це особливо актуально у сучасних умовах, коли загрози мають складний, багатовекторний та транснаціональний характер.

Одним із найважливіших організаційних заходів у межах служб захисту інформації є створення системи управління доступом до інформаційних ресурсів. Управління доступом має забезпечувати диференціацію прав користувачів, контроль за діями персоналу, моніторинг використання даних та облік операцій у критично важливих системах. Як зазначається у проєкті Закону «Про засади інформаційної безпеки України», обмеження доступу є однією з центральних функцій служби захисту інформації, оскільки більшість загроз виникає через неправомірний доступ, недбалість або навмисне

порушення правил співробітниками [8]. Це підкреслює потребу у впровадженні детально регламентованих правил управління доступом.

Кадрове забезпечення є не менш важливим аспектом організаційної складової інформаційної безпеки. Нашинець-Наумова наголошує, що професійна підготовка у сфері інформаційного права та безпеки є визначальною для ефективного виконання службових обов'язків у системі захисту інформації [20, с. 84]. Працівники, які не володіють базовими знаннями щодо можливих загроз, методів соціальної інженерії, правил роботи з конфіденційною інформацією та процедур реагування, стають потенційними векторами ризику. Крім того, кадрова політика має передбачати регулярне навчання, тренінги та атестацію співробітників.

Важливою організаційною мірою також є створення політик безпеки — формальних документів, що визначають правила роботи з інформаційними ресурсами, порядок обміну даними, правила реагування на інциденти та відповідальність персоналу. Документи такого рівня забезпечують уніфікацію організаційної поведінки і дозволяють формувати корпоративну культуру інформаційної безпеки. Як підкреслює Довгань, політики є інструментом забезпечення правової визначеності у сфері інформаційної безпеки та створюють основу для подальших процедур контролю [21, с. 76]. Чітко прописані політики допомагають зменшити ймовірність порушень та підвищують готовність організації до потенційних загроз.

Система внутрішнього контролю є важливим організаційним механізмом, який включає аудит безпеки, перевірку дотримання правил, аналіз журналів подій та оцінку ризиків. Внутрішній контроль дозволяє виявляти слабкі місця у захисних механізмах, вчасно реагувати на порушення і формувати рекомендації для покращення системи. Указ Президента України «Про Стратегію інформаційної безпеки» акцентує увагу на необхідності системного моніторингу інформаційної сфери як на рівні держави, так і на рівні окремих організацій [3]. Це дає змогу забезпечити відповідність поточних заходів актуальним загрозам, які постійно змінюються.

Організаційні заходи включають також розробку системи управління інцидентами — процедур, що визначають етапи виявлення, фіксації, аналізу, локалізації та усунення наслідків інцидентів інформаційної безпеки. Золотар О. О. зазначає, що ефективне управління інцидентами дозволяє мінімізувати шкоду від атак та запобігти їхньому повторенню [22, с. 120]. Розвинена система реагування є ключовою у зменшенні часу простою інформаційних ресурсів та зниженні матеріальних збитків.

Не можна оминути увагою питання класифікації інформації та її розмежування за рівнями доступу. Закон України «Про державну таємницю» встановлює категорії секретності та визначає вимоги щодо допуску до конфіденційної інформації [5]. На рівні організації ці положення трансформуються у внутрішні категорії інформації, що дозволяє структурувати її за рівнями важливості та забезпечити посилений захист для найбільш критичних даних. Чітка класифікація значно зменшує ризик несанкціонованого доступу та сприяє ефективному управлінню інформаційними потоками.

Аналітичні дослідження підтверджують, що більшість організаційних заходів мають на меті мінімізацію людського фактору як джерела загроз. Як свідчить практика, помилки співробітників, незнання правил, недотримання процедур або навмисні дії становлять понад 70 % інцидентів у сфері інформаційної безпеки. Саме тому організаційні заходи мають не лише формальний характер, а й орієнтуються на формування поведінкових моделей, де відповідальність за інформаційну безпеку розподіляється між усіма працівниками.

Загалом організаційні заходи у службах захисту інформації формують основу для функціонування усієї системи протидії загрозам. Вони визначають правила, встановлюють стандарти, формують процедури взаємодії та забезпечують контроль за діяльністю співробітників. Без належної організаційної структури навіть найсучасніші технічні засоби втрачають свою ефективність. Таким чином, організаційні заходи є ключовою,

структуроутворювальною складовою інформаційної безпеки, яка забезпечує цілісність, надійність та керованість захисних механізмів.

У цій таблиці систематизовано основні організаційні заходи протидії загрозам інформаційній безпеці, що реалізуються в межах діяльності служб захисту інформації. Представлені заходи охоплюють нормативно-правове забезпечення, кадрову підготовку, управління доступом, контроль і аудит, а також процеси управління інцидентами відповідно до чинної нормативної бази.

Таблиця 2.1 - Організаційні заходи протидії загрозам інформаційній безпеці [2-19]

Категорія заходів	**Зміст**	**Нормативне підґрунтя**
Нормативно-правові	Формування політик, регламентів, внутрішніх положень	[2], [3], [19]
Кадрові	Підготовка персоналу, навчання, атестація	[20, с. 84]
Управління доступом	Диференціація прав, облік дій, контроль	[5], [8]
Контроль та аудит	Перевірка дотримання правил, ризик-аналіз	[3]
Управління інцидентами	Виявлення, реагування, локалізація, відновлення	[22, с. 120]

Організаційні заходи, узагальнені у Таблиці 2.1, демонструють системний характер управління інформаційною безпекою, де кожен із компонентів виконує унікальну функцію та формує фундамент для стійкої безпекової політики. Структурованість заходів дозволяє оцінити їхній взаємозв’язок, адже нормативно-правова база, кадрове забезпечення, управління доступом, контроль та реагування утворюють цілісну модель протидії загрозам. Усі зазначені категорії не можуть існувати ізольовано, оскільки кожна з них підсилює інші та створює розгалужену архітектуру захисту. Саме тому аналіз цієї таблиці є важливим етапом для розуміння того, як працює служба захисту інформації та яким чином вона забезпечує сталість організаційних процесів.

Перша категорія заходів — нормативно-правові — відображає фундаментальну потребу у формалізації правил, процедур та внутрішніх регламентів, які визначають рамки діяльності персоналу та систем безпеки. Ця складова спирається на чинні закони та стратегічні документи держави [2; 3; 19], що гарантує її узгодженість з національною політикою інформаційної безпеки. Значення нормативної регламентації полягає не лише у визначенні обов'язкових вимог, але й у створенні правової передбачуваності, без якої сучасна система захисту не може бути керованою та ефективною. У підсумку нормативно-правові заходи формують своєрідний «каркас», який задає стандарти й забезпечує рівень дисципліни, необхідний для злагодженої роботи всіх підрозділів організації.

Кадрова складова зосереджена на якості людського ресурсу, який фактично є одним із головних суб'єктів управління інформаційною безпекою. Підготовка та навчання персоналу, а також періодична атестація дозволяють знизити ризик інцидентів, пов'язаних із людським фактором, що сьогодні становить одну з ключових уразливостей організацій [20, с. 84]. Як свідчать дослідження, навіть найсучасніші технічні рішення втрачають ефективність, якщо співробітники не володіють навичками їхнього правильного застосування або не усвідомлюють відповідальності за власні дії. Тому кадрова політика розглядається як інвестиція у довгострокову стабільність системи безпеки і слугує підґрунтям для формування корпоративної культури захисту інформації.

Третя категорія — управління доступом — має критичне значення для збереження цілісності та конфіденційності інформаційних ресурсів. Диференціація прав доступу, ведення журналів активності та постійний контроль за операціями користувачів дають змогу мінімізувати ризики несанкціонованого доступу й внутрішніх порушень [5; 8]. Цей механізм має подвійний характер: він одночасно виконує функцію обмеження та функцію контролю, створюючи прозорість у роботі інформаційних систем. Управління доступом є основою для ефективної роботи як організаційних, так і технічних

засобів, оскільки чітке визначення ролей і повноважень формує передумови для узгодженої роботи всієї системи захисту.

Категорія «контроль та аудит» у таблиці відображає важливість систематичної оцінки якості заходів безпеки та їх відповідності встановленим стандартам. Перевірка дотримання правил, аналіз ризиків і аудит інформаційних процесів є дієвими інструментами для виявлення недоліків, які не завжди можна розгледіти під час повсякденної роботи [3]. Особливість аудиту полягає у його незалежності та регулярності, адже контроль має бути не разовим заходом, а циклічним процесом, що забезпечує постійну адаптацію системи до нових загроз. Таким чином, аудит створює умови для неперервного вдосконалення системи безпеки та підвищує рівень надійності всіх її складових.

Останній блок заходів — управління інцидентами — є ключовим елементом оперативного реагування на порушення безпеки та відновлення працездатності системи. Виявлення аномалій, швидке реагування, локалізація наслідків та відновлення нормальної роботи є комплексним процесом, який вимагає чіткого алгоритму дій і професійної підготовки персоналу [22, с. 120]. Без організованої системи реагування навіть незначні інциденти можуть набувати масштабного характеру, впливаючи на безперервність бізнес-процесів і репутацію організації. З огляду на це управління інцидентами має стратегічне значення, оскільки воно не лише зменшує наслідки атак, але й дозволяє накопичувати досвід для вдосконалення інших заходів безпеки.

Узагальнюючи зміст таблиці, можна зазначити, що наведені заходи формують узгоджену систему, де кожен елемент виконує цілком логічну і взаємодоповнювальну функцію. Нормативно-правове регулювання створює офіційні рамки діяльності, кадровий компонент забезпечує належний рівень професійності, механізми доступу гарантують контроль за використанням даних, аудит дозволяє вчасно виявляти недоліки, а управління інцидентами забезпечує оперативну реакцію у кризових умовах. Така інтегрована модель відповідає міжнародним підходам до побудови системи інформаційної безпеки

і узгоджується з положеннями державних документів, присвячених формуванню сучасного цифрового середовища.

З аналітичної точки зору, таблиця демонструє не просто перелік заходів, а їхню логічну структуру, яка відповідає циклу управління безпекою — від планування і регламентації до реагування та вдосконалення. Вона відображає той факт, що організаційний компонент є таким самим вагомим, як і технічний, оскільки саме він визначає правила гри та забезпечує дисципліну в інформаційних процесах. Служби захисту інформації у своїй роботі спираються саме на такі комплексні організаційні інструменти, адже лише у взаємодії вони створюють умови для ефективної протидії загрозам і підтримують стійкість інформаційної інфраструктури організації.

2.2 Програмно-технічні засоби захисту інформації

Програмно-технічні засоби є невід’ємним елементом комплексної системи інформаційної безпеки, оскільки саме вони безпосередньо забезпечують запобігання, виявлення та локалізацію технічних загроз, які можуть впливати на функціонування інформаційних систем. На відміну від організаційних методів, технічний захист має оперативний і високоточний характер, що дозволяє реагувати на інциденти в реальному часі та автоматизувати процеси забезпечення безпеки. У сучасних умовах стрімкого розвитку технологій, цифрової трансформації та зростання частоти кібератак роль технічних засобів захисту інформації суттєво зростає. Як підкреслює Золотар, технологічні інструменти стають не просто додатковим засобом захисту, а фундаментальною опорою всієї системи безпеки, без якої організація фактично не здатна протидіяти загрозам належним чином [22, с. 221].

Однією з основних груп програмно-технічних засобів є системи контролю доступу, які забезпечують обмеження доступу користувачів до інформаційних

ресурсів відповідно до їхніх повноважень. Сучасні системи реалізують багаторівневу модель контролю, що включає аутентифікацію, авторизацію, моніторинг дій користувачів та ведення журналів подій. Указ Президента України щодо реалізації Стратегії інформаційної безпеки наголошує на тому, що забезпечення конфіденційності та цілісності інформації неможливе без впровадження ефективних систем контролю доступу як на рівні державних органів, так і приватного сектору [3]. Використання багатофакторної аутентифікації, апаратних токенів, одноразових паролів та біометричних рішень дозволяє суттєво зменшити ризики, пов’язані з крадіжкою облікових даних та несанкціонованим доступом.

Важливим елементом програмно-технічного захисту є криптографічні засоби, які забезпечують конфіденційність, автентичність та цілісність інформації під час її зберігання або передачі. Сучасні криптографічні протоколи, такі як TLS, IPsec, SSH, а також шифрування дисків та облачних сховищ, є стандартом для більшості організацій, що працюють з конфіденційними даними. Закон України «Про державну таємницю» прямо вказує на необхідність використання спеціальних криптографічних засобів, сертифікованих державою, у випадках роботи з інформацією, що становить державну таємницю [5]. Криптографія дозволяє ефективно протидіяти широкому спектру технічних загроз, включаючи перехоплення даних, модифікацію інформації, підміну повідомлень та сесійні атаки.

Надзвичайно важливу роль у сучасному кіберзахисті відіграють міжмережеві екрани та системи запобігання вторгненням. Міжмережеві екрани (firewall) дозволяють контролювати мережевий трафік на основі заздалегідь визначених правил, фільтрувати небажані або шкідливі пакети та перешкоджати несанкціонованим підключенням. Системи запобігання вторгненням (IPS) та системи виявлення вторгнення (IDS) аналізують події в мережі, виявляють аномалії та блокують атаки в момент їх спроби проникнення. За оцінками експертів, понад 60 % сучасних атак можна відвернути на периметрі мережі за умов коректної конфігурації засобів

фільтрації та сегментації трафіку. У публікаціях Калюжного та Цимбалюка підкреслюється, що технічний контроль мережевих з'єднань є однією з ключових умов ефективної боротьби з організованою кіберзлочинністю [15, с. 108], оскільки дозволяє відслідковувати маршрути шкідливих даних і вчасно блокувати небезпечну активність.

Ще одним важливим компонентом програмно-технічного захисту є засоби антивірусного та антишкідливого програмного забезпечення. Вони забезпечують сканування файлів, моніторинг системи, аналіз поведінкових характеристик програм та блокування загроз, таких як віруси, трояни, шпигунське ПЗ, програми-вимагачі та інші шкідливі елементи. Згідно з даними IT-словника з інформаційної безпеки [23], більшість сучасних шкідливих програм функціонує у вигляді складних багаторівневих механізмів, що здатні адаптуватися до середовища, приховувати свою присутність і використовувати методи обману для обходу класичних систем захисту. Саме тому сучасні антивірусні рішення використовують евристичний аналіз, машинне навчання та хмарні бази даних загроз, що підвищує їхню здатність виявляти нові, ще невідомі зразки шкідливого коду.

Значну роль у системі технічного захисту відіграють засоби резервного копіювання та відновлення даних. Втрата інформації через кібератаку або технічний збій може призвести до суттєвих матеріальних втрат, порушення роботи організації або підриву довіри клієнтів. Резервне копіювання є не просто технічною процедурою, а критично важливим елементом інформаційної безпеки. У державних документах, зокрема у стратегіях розвитку інформаційного суспільства [18], наголошується на необхідності створення резервних копій критично важливої інформації та зберігання їх у захищених локаціях. Важливими є також принципи регулярності, багаторівневості та географічного рознесення резервних копій, що дозволяє забезпечити відновлення даних навіть після масштабних інцидентів.

Суттєве значення у комплексі технічних засобів мають системи журналювання подій та моніторингу безпеки. Ці засоби забезпечують фіксацію

дій користувачів, програмного забезпечення та апаратних засобів у реальному часі. Журналювання є важливим інструментом для розслідування інцидентів та збору доказів у випадку правопорушень. Як зазначає Бойченко, саме дані журналів подій стають ключовим джерелом інформації для юридичної оцінки інцидентів у сфері кіберзлочинності [17, с. 143]. Сучасні системи моніторингу використовують аналітичні алгоритми, що здатні виявляти підозрілу поведінку на ранніх стадіях та попереджати операторів служби інформаційної безпеки.

Все більшого поширення набувають SIEM-системи (Security Information and Event Management), які поєднують функції збору, аналізу та кореляції подій безпеки з усіх сегментів інформаційної інфраструктури. На відміну від класичних журналів, SIEM-системи здатні аналізувати величезні обсяги даних і виявляти складні, багатоступеневі атаки, які традиційні засоби не завжди можуть розпізнати. Вони стали обов’язковим елементом захисту для великих організацій, державних структур та критично важливих об’єктів. У міжнародних документах, таких як Окінавська хартія глобального інформаційного суспільства, підкреслюється важливість використання інтелектуальних засобів аналізу даних для підвищення рівня глобальної кібербезпеки [24].

У сучасному цифровому середовищі зростає значення засобів захисту мобільних пристроїв та хмарних сервісів. Організації дедалі частіше використовують моделі BYOD, віддалену роботу, мобільні додатки та хмарні платформи, що створює додаткові точки доступу для потенційних атак. Тому важливими стають такі засоби, як Mobile Device Management (MDM), контейнеризація мобільних середовищ, шифрування мобільних даних та контроль безпеки хмарних сервісів. Як зазначають дослідники, зокрема Нашинець-Наумова, нові типи цифрових сервісів створюють додаткові ризики, які потребують адаптації технічної архітектури захисту [20, с. 64]. Це вимагає від служб захисту інформації впровадження інноваційних технічних рішень, здатних забезпечити безпеку даних у змінному середовищі.

Особливе місце у системі програмно-технічного захисту займає сегментація мережі та віртуалізація інфраструктури. За допомогою віртуальних мережевих середовищ, VLAN, ізольованих сегментів та зон безпеки організації можуть мінімізувати ризики розповсюдження шкідливого коду або несанкціонованих дій всередині власної мережі. Така сегментація дозволяє створювати окремі «зони довіри», що забезпечують додатковий рівень контролю та ізоляції критичних ресурсів. У документах щодо кодифікації інформаційного законодавства України підкреслюється, що технічна сегментація має поєднуватися з організаційними вимогами до розмежування доступу, що підсилює загальну ефективність безпеки [14].

Важливим напрямком розвитку є технології Zero Trust, які базуються на принципі «не довіряй нікому». Традиційна модель безпеки передбачала, що після входу до системи користувач отримує достатньо високий рівень довіри. Zero Trust, натомість, заперечує будь-яку апріорну довіру і вимагає постійної верифікації кожного запиту. Такий підхід суттєво ускладнює здійснення атак, оскільки кожен елемент системи перебуває під постійним контролем. Ця концепція узгоджується з сучасними принципами інформаційної безпеки, викладеними у стратегіях держави [27].

У сукупності програмно-технічні засоби захисту забезпечують багаторівневу оборону, де кожен інструмент виконує свою функцію й підсилює інші механізми. Вони формують «технічний щит» організації, який дозволяє не тільки запобігати інцидентам, а й забезпечувати швидке реагування, мінімізувати збитки та відновлювати дані після атаки. У сучасних умовах уразливостей та динамічних загроз технічні засоби стають основою стійкості інформаційних систем, доповнюючи організаційні та правові механізми.

У цій таблиці узагальнено основні програмно-технічні засоби протидії загрозам інформаційній безпеці, що застосовуються службами захисту інформації для забезпечення комплексного захисту інформаційних ресурсів. Представлені засоби охоплюють механізми контролю доступу,

криптографічного захисту, мережевої безпеки, виявлення інцидентів, резервного копіювання та захисту мобільних і хмарних середовищ.

Таблиця 2.2 - Основні програмно-технічні засоби протидії загрозам інформаційній безпеці [5-20].

Категорія засобів	**Характеристика**	**Нормативне або наукове обґрунтування**
Системи контролю доступу	Аутентифікація, авторизація, моніторинг	[3], [8]
Криптографічні засоби	Шифрування, цифрові підписи, протоколи	[5]
Мережеві екрани, IDS/IPS	Периметровий захист, виявлення атак	[15, с. 108]
Антивірусні засоби	Виявлення та блокування шкідливого ПЗ	[23]
SIEM-системи	Кореляція подій, аналітика загроз	[24]
Резервне копіювання	Захист від втрати даних	[18]
Захист мобільних і хмарних сервісів	Контейнеризація, MDM, шифрування	[20, с. 64]

Таблиця 2.2 представляє комплекс ключових програмно-технічних засобів, які формують основу сучасної системи інформаційної безпеки. Кожна категорія засобів має окреме функціональне призначення, водночас взаємодіючи з іншими, що дозволяє створювати багаторівневу й узгоджену модель захисту. Аналіз цієї таблиці дає можливість побачити, наскільки багатовимірним є технічний сегмент захисту, адже він охоплює інструменти різних рівнів — від контролю доступу до глобальних аналітичних платформ.

Важливо, що наведені засоби не є взаємозамінними, оскільки кожен покриває свою частину загроз і компенсує слабкості інших елементів безпеки.

Першою групою у таблиці визначено системи контролю доступу, які забезпечують базовий рівень технічного захисту. Їхня роль полягає у перевірці автентичності користувачів, підтвердженні їхніх повноважень та створенні журналів операцій для подальшого аналізу [3; 8]. Ці системи є критично необхідними, адже більшість інцидентів виникає через компрометацію облікових записів або несанкціонований доступ до ресурсів. Розвиток багатофакторної аутентифікації, біометричних технологій і апаратних токенів суттєво змінив можливості контролю доступу, забезпечивши більш жорсткий периметр та мінімізувавши ризики обходу системи. Саме тому контроль доступу є не тільки технічним засобом, а й інструментом, що підтримує виконання організаційних правил.

Криптографічні засоби, як показано у таблиці, формують окрему і надзвичайно важливу групу технічних механізмів, адже вони забезпечують захист інформації навіть у разі компрометації каналів зв’язку або пристроїв. Шифрування, цифрові підписи та мережеві криптографічні протоколи гарантують конфіденційність і цілісність даних незалежно від того, через які середовища вони передаються [5]. Цінність криптографії полягає в тому, що вона нейтралізує один із найнебезпечніших векторів атак — перехоплення або підміну інформації. У сучасних умовах цифровізації криптографічні інструменти стають обов’язковим елементом не лише державних, а й комерційних систем, особливо у сфері фінансових послуг, телекомунікацій та електронного документообігу.

Суттєвим компонентом технічного захисту є мережеві екрани та системи IDS/IPS, які забезпечують периметровий контроль та виявлення спроб проникнення. Ці засоби працюють у реальному часі, аналізуючи мережевий трафік і блокуючи підозрілу активність, що дозволяє запобігати атакам ще на ранньому етапі [15, с. 108]. Значущість цих інструментів полягає у тому, що вони створюють першу лінію оборони і фільтрують потенційно шкідливий

трафік, який може використовуватися для сканування вразливостей, проведення DDoS-атак або проникнення у внутрішні системи. Поєднання брандмауерів з інтелектуальними IDS/IPS рішеннями формує гнучку систему раннього реагування, яка дозволяє оперативно припиняти небезпечні дії.

Антивірусні засоби залишаються основним інструментом у боротьбі зі шкідливим програмним забезпеченням, хоча методи, що стоять за їхньою роботою, суттєво розвинулися. Сучасні антивіруси вже давно не спираються лише на бази сигнатур, адже нові типи зловмисного ПЗ здатні до мутацій, маскування та динамічної адаптації [23]. Тому сучасні рішення використовують поведінковий аналіз, машинне навчання та хмарні інтелектуальні системи для виявлення аномальної активності. Основна цінність антивірусних платформ полягає в можливості автоматично блокувати шкідливий код до того, як він спричинить критичні наслідки, що робить їх важливим елементом багатошарової системи безпеки.

SIEM-системи, представлені у таблиці, є одними з найскладніших і найфункціональніших інструментів сучасного кіберзахисту. Вони виконують збір, аналіз та кореляцію подій з різних джерел, дозволяючи створювати цілісну картину інформаційної активності [24]. Їхня перевага полягає в тому, що вони здатні виявляти складні, багатоступеневі атаки, які не можуть бути розпізнані окремими технічними засобами. Використання SIEM дозволяє службам інформаційної безпеки оперативно реагувати на інциденти, визначати взаємозв’язки між подіями та попереджати загрози ще до їхнього фактичного здійснення. Саме через це SIEM-системи стали обов’язковим компонентом захисту державних органів та критично важливої інфраструктури.

Окремої уваги потребує категорія засобів резервного копіювання, адже вони забезпечують можливість відновлення інформаційних ресурсів після інцидентів. Стратегія розвитку інформаційного суспільства [18] підкреслює важливість резервування як базового елементу стійкості інформаційних систем. Втрата даних є одним із найбільш руйнівних наслідків кібератак, тому резервне копіювання має бути різнорівневим, регулярним і географічно розподіленим.

Цей інструмент не запобігає атакам, але мінімізує їхній вплив і забезпечує відновлення бізнес-процесів навіть після масштабних збоїв.

Завершальною категорією таблиці є засоби захисту мобільних і хмарних сервісів, які за останні роки стали одними з найбільш актуальних. Мобільні пристрої, хмарні платформи та віддалена робота створюють нові вектори атак, що потребує сучасних рішень, таких як MDM-системи, контейнеризація середовищ і повне шифрування даних [20, с. 64]. Важливо, що ці інструменти мають не лише технічний характер, а й суттєво впливають на організаційні моделі роботи, оскільки вони дозволяють компаніям зберігати гнучкість і одночасно контролювати безпеку розподілених середовищ. Захист мобільних і хмарних систем стає новою нормою у сфері інформаційної безпеки, враховуючи масштаби цифровізації та мобільності.

Узагальнюючи представлений аналіз, можна стверджувати, що таблиця 2.2 демонструє не просто перелік технічних засобів, а їхню стратегічну взаємодію. Ці інструменти формують багатошарову оборону, де кожен елемент виконує свою функцію і компенсує вади інших. Важливо, що вони охоплюють усі етапи захисту — від ідентифікації та блокування загроз до моніторингу, відновлення й аналізу інцидентів. У сукупності це дозволяє службам захисту інформації будувати стійкі, адаптивні та технологічно потужні системи, здатні ефективно протидіяти загрозам у швидкозмінному цифровому середовищі.

2.3 Комплексна система протидії загрозам у службах захисту інформації

Комплексна система протидії загрозам інформаційній безпеці у службах захисту інформації є сукупністю організаційних, технічних, правових і кадрових заходів, що взаємодіють між собою та забезпечують цілісну й безперервну модель безпеки. Сучасні інформаційні загрози мають багатовимірний характер, що потребує системного підходу до захисту. Кожен

окремий механізм може бути ефективним лише тоді, коли він інтегрований у цілісну архітектуру, що функціонує як єдине середовище реагування на загрози. У доктринальних документах України наголошується, що державна політика безпеки повинна базуватися на багаторівневих системах, здатних забезпечити як попередження атак, так і відновлення після інцидентів [19]. Саме тому комплексність стає ключовим принципом сучасних служб захисту інформації.

Комплексний підхід передбачає, що служба інформаційної безпеки не обмежується виконанням окремих функцій, а створює структуровану, логічно узгоджену систему, де кожен елемент підсилює інший. Як зазначає Кормич, ефективність політики інформаційної безпеки залежить від взаємодії всіх підсистем — організаційної, технічної, правової та гуманітарної, — оскільки загрози можуть проявлятися на різних рівнях та у різних площинах [6, с. 305]. У такій системі важливо не лише застосовувати засоби захисту, але й забезпечити їхню інтеграцію, гармонізацію та узгодженість із загальною стратегією безпеки організації.

Одним із ключових елементів комплексної системи є процес управління ризиками. Цей процес включає ідентифікацію загроз, виявлення вразливостей, оцінку наслідків інцидентів, формування механізмів запобігання та визначення пріоритетів захисту. Стратегії розвитку інформаційного суспільства наголошують, що управління ризиками має бути неперервним та адаптивним процесом, який враховує динаміку інформаційного середовища та нові загрози [18]. Комплексність управління ризиками забезпечує збалансованість між витратами на захист і рівнем допустимих ризиків, що особливо важливо для державних структур і великих організацій.

Важливим структурним елементом комплексної системи є багаторівнева модель захисту. Така модель передбачає застосування різних механізмів на різних рівнях — від фізичного та організаційного до мережевого і прикладного. Кожен рівень виконує власну функцію і виступає бар’єром, що ускладнює доступ зловмисника до критичних ресурсів. У міжнародних документах, таких як Окінавська хартія глобального інформаційного суспільства, особлива увага

приділяється саме багаторівневим моделям, що дозволяють підсилити стійкість інфраструктури та забезпечити її захищеність від складних атак [24]. Це дає можливість створювати децентралізовану архітектуру безпеки, де порушення одного рівня не призводить до краху всієї системи.

Суттєве місце у комплексній системі посідає інтеграція програмно-технічних засобів. Сучасні служби захисту інформації оперують значною кількістю інструментів — від мережевих екранів до SIEM-систем, засобів криптографічного захисту, антивірусних платформ та інструментів контролю мобільних пристроїв. Як підкреслює Нашинець-Наумова, використання ізольованих технічних засобів без їхньої інтеграції призводить до фрагментації системи й знижує її ефективність [20, с. 92]. Саме тому комплексна система передбачає створення єдиного центру моніторингу, що об’єднує інформацію з усіх джерел, забезпечує кореляцію подій і дозволяє швидко виявляти складні та багатоступеневі атаки.

Поряд із технічними компонентами важливою складовою комплексної системи протидії загрозам є організація взаємодії між різними суб’єктами системи безпеки. Калюжний і Цимбалюк підкреслюють, що ефективна боротьба з кіберзлочинністю та іншим загрозами можлива лише за умови узгодженості дій державних органів, приватних структур і міжнародних партнерів [15, с. 111]. Сюди входить обмін інформацією, координація інцидентів, залучення зовнішніх експертів, взаємодія з комп’ютерними центрами реагування (CERT) та забезпечення спільних операцій протидії загрозам. Система безпеки повинна включати механізми горизонтальної та вертикальної взаємодії, що посилює її адаптивність.

Комплексна система протидії загрозам передбачає також створення внутрішнього циклу реагування на інциденти. Такий цикл містить етапи виявлення, ідентифікації, аналізу, локалізації, нейтралізації та відновлення. Золотар наголошує, що наявність структурованих процедур реагування дозволяє мінімізувати наслідки інцидентів та уникнути повторних атак через ті самі вразливості [22, с. 178]. Служба інформаційної безпеки повинна володіти

чітким набором інструкцій і алгоритмів, що забезпечують послідовну та оперативну реакцію у кризових ситуаціях.

Значну роль у комплексній системі відіграє безпекова культура персоналу. Кадровий компонент є критично важливим, оскільки більшість інцидентів виникає через людські помилки, нехтування правилами або недостатню увагу до ризиків. На думку Бойченка, формування культури відповідального ставлення до інформації є основою захисту, і без цього жодні технічні чи організаційні засоби не можуть забезпечити повноцінну безпеку [17, с. 150]. Комплексна система включає регулярне навчання, тестування, інструктажі, внутрішні тренінги та моделювання кризових ситуацій.

Правовий компонент комплексної системи також займає важливе місце, оскільки він визначає відповідальність, регламентує права та обов'язки персоналу, встановлює межі допустимої поведінки та фіксує відповідальність за порушення. Законодавчі акти України, зокрема Кодекс про адміністративні правопорушення [26], встановлюють санкції за неправомірні дії у сфері інформаційної безпеки, що дозволяє формувати дисципліну і забезпечувати виконання вимог безпеки. Правові норми визначають межі використання інформації, порядок доступу та процедури контролю, що є невід'ємною частиною комплексного захисту.

Важливим елементом комплексності є систематичний аудит безпеки. Аудит дозволяє оцінити відповідність поточних заходів встановленим стандартам, виявити слабкі місця та розробити рекомендації щодо покращення системи. У розробках щодо кодифікації інформаційного законодавства України наголошується, що аудит має поєднувати технічні, організаційні та правові перевірки, що забезпечує комплексність оцінки [14]. Результати аудиту дозволяють адаптувати механізми захисту до нових загроз і забезпечити неперервний розвиток системи.

Не менш важливою складовою комплексної системи є стратегічне планування. Організація повинна мати довгострокові плани розвитку служби інформаційної безпеки та враховувати майбутні виклики, технологічні

тенденції і потенційні ризики. Стратегічні документи, такі як Стратегія інформаційної безпеки України [3], прямо наголошують на необхідності планування та модернізації інфраструктури безпеки, що дозволяє організаціям діяти проактивно, а не реагувати лише після інцидентів.

У комплексній системі надзвичайно важливим є поєднання організаційних та технічних заходів у єдиному середовищі. Усі засоби — політики безпеки, регламенти, технічні рішення, навчання персоналу, аудит, реагування — повинні бути взаємопов'язаними. Як зазначає Довгань, комплексний підхід вимагає гармонізації між внутрішніми процедурами та зовнішнім правовим середовищем [21, с. 79]. Це означає, що служба інформаційної безпеки повинна постійно вдосконалюватися, адаптуватися до змін і підтримувати узгодженість між усіма складовими системи.

Отже, комплексна система протидії загрозам у службах захисту інформації є багатовимірною та багаторівневою. Вона поєднує технічні засоби, правові вимоги, організаційні процедури, кадрові заходи та стратегічне планування. Її ефективність залежить від взаємодії компонентів, їхньої узгодженості та здатності адаптуватися до нових викликів. У сучасному цифровому середовищі комплексна система стає єдиним реально ефективним механізмом протидії загрозам, що забезпечує стійкість інформаційної інфраструктури та захищеність критичних ресурсів.

У цій таблиці представлено структурні елементи комплексної системи протидії загрозам інформаційній безпеці, що забезпечують узгоджену взаємодію організаційних, програмно-технічних та правових механізмів захисту. Запропонована структура відображає системний підхід до управління ризиками, багаторівневого захисту, реагування на інциденти та контролю відповідності вимогам стандартів інформаційної безпеки.

Таблиця 2.3. - Структурні елементи комплексної системи протидії загрозам [16-25]

Компонент системи	**Функціональне призначення**	**Наукове / нормативне підґрунтя**
1	2	3
Управління ризиками	Ідентифікація, оцінка, мінімізація загроз	[18]
Багаторівневий захист	Бар'єри на різних рівнях інфраструктури	[24]
Інтеграція технічних засобів	Кореляція подій, централізований моніторинг	[20, с. 92]
Взаємодія суб'єктів безпеки	Координація, обмін інформацією, CERT	[15, с. 111]
Реагування на інциденти	Локалізація, аналіз, відновлення	[26, с. 178]

Кінець таблиці 2.3

1	2	3
Кадрові заходи	Формування культури безпеки	[5, с. 150]
Правові механізми	Визначення відповідальності та процедур	[26]
Аудит та оцінка	Перевірка відповідності стандартам	[14]

Таблицю розроблено на основі джерела [16-25].

Таблиця 2.3 дає можливість глибше розглянути ключові складові комплексної системи протидії загрозам інформаційній безпеці, демонструючи багатовимірність і взаємозалежність усіх елементів. Представлені компоненти відображають логіку сучасної моделі безпеки, де протидія загрозам здійснюється не однією дією чи окремим засобом, а системою рішень та процесів, що працюють одночасно й у взаємодії. Комплексність, яку відображає ця таблиця, полягає у тому, що кожен елемент виконує власну функцію, а разом вони формують стійку архітектуру кіберзахисту. Саме це дозволяє зрозуміти, що ефективна інформаційна безпека завжди виходить за межі суто технічних рішень.

Управління ризиками в таблиці посідає особливе місце, адже воно визначає стратегію формування і підтримки всієї системи безпеки. Цей процес включає постійне виявлення загроз, аналіз їхніх наслідків і створення

механізмів мінімізації або усунення ризиків [18]. У сучасному цифровому середовищі, яке характеризується швидкими змінами, управління ризиками стає безперервним процесом, що забезпечує адаптивність системи до нових викликів. Такий підхід дозволяє організаціям не просто реагувати на інциденти, а діяти проактивно, передбачаючи можливі сценарії розвитку загроз і заздалегідь формуючи заходи протидії.

Багаторівневий захист, представлений у таблиці, відображає концепцію «глибинної оборони», яка полягає у створенні кількох бар'єрів на різних рівнях інформаційної інфраструктури. Кожен рівень виконує власну роль і ускладнює зловмиснику можливість проникнення в систему, навіть якщо інші механізми вже були скомпрометовані [24]. Такий принцип широко застосовується у міжнародних моделях безпеки, оскільки дозволяє диверсифікувати захист і мінімізувати ризики, пов'язані з людським фактором чи технічними збоями. Багаторівневість робить систему більш стійкою, оскільки вона не залежить від одного механізму, а створює каскадний ефект захисних бар'єрів.

Інтеграція технічних засобів, як вказано у таблиці, є необхідною умовою ефективного кіберзахисту. Сьогодні окремі інструменти — від систем контролю доступу до SIEM-платформ — перестали бути ізольованими рішеннями, а натомість стали частинами єдиного аналітичного середовища [20, с. 92]. Інтеграція дозволяє узгоджувати дані, корелювати події і забезпечувати централізований моніторинг, що суттєво підсилює можливості служби захисту інформації. Такий підхід гарантує, що інформація про загрози не залишається у відриві, а використовується для формування єдиного оперативного зображення ситуації в інформаційному середовищі.

Взаємодія суб'єктів безпеки є однією з ключових ознак комплексності, оскільки жодна служба інформаційної безпеки не може діяти ефективно в повній ізоляції. Калюжний і Цимбалюк слушно підкреслюють, що координація між державними органами, бізнесом, науковими та міжнародними структурами є критично важливою для боротьби з організованою кіберзлочинністю та складними інформаційними загрозами [15, с. 111]. Обмін інформацією, участь у

спільних операціях, використання центрів реагування CERT створюють мережевий захисний контур, який функціонує значно ефективніше, ніж розрізнені зусилля окремих організацій. Взаємодія сприяє формуванню узгодженої стратегії та швидкому реагуванню на транснаціональні виклики.

Реагування на інциденти є тим компонентом, який забезпечує оперативний контур захисту. Виявлення, аналіз, локалізація і повне відновлення систем після атаки формують повний цикл реагування, необхідний для мінімізації шкоди [22, с. 178]. У комплексній системі реагування важливо, щоб усі етапи були чітко структурованими та закріпленими у внутрішніх регламентах, що дозволяє уникнути хаотичних дій у кризових ситуаціях. Крім того, реагування на інциденти є джерелом цінних уроків, які використовуються для удосконалення організаційних процедур, технічних рішень та політик безпеки.

Кадрові заходи є фундаментальною частиною комплексної системи, оскільки саме людський фактор часто стає найбільш уразливою ланкою. Формування культури безпеки передбачає не лише навчання персоналу, а й створення мотиваційної та психологічної моделі поведінки, де відповідальність за інформаційну безпеку є інтегрованою частиною професійної діяльності [17, с. 150]. У багатьох випадках саме необізнаність або байдужість співробітників стає причиною серйозних інцидентів, а тому кадрові заходи спрямовані на мінімізацію цього ризику. Вони включають тренінги, політики поведінки, оцінювання знань та регулярну атестацію, що формує культуру усвідомленого ставлення до інформації.

Правові механізми, наведені у таблиці, становлять нормативну основу комплексної системи протидії загрозам. Вони визначають межі дозволеного, окреслюють відповідальність і формують правила, яких мають дотримуватися всі учасники інформаційних процесів [26]. Правові механізми є важливими для підтримки дисципліни, забезпечення прозорості та захисту прав користувачів. Вони також створюють юридичні інструменти для розслідування інцидентів,

притягнення винних до відповідальності та врегулювання спірних ситуацій, що перетворює систему безпеки на повноцінний правовий інститут.

Аудит та оцінка є завершальним елементом, але далеко не останнім за значенням. Цей компонент забезпечує систематичну перевірку відповідності засобів захисту внутрішнім стандартам, вимогам законодавства та реальним умовам функціонування [14]. Аудит дозволяє виявляти прогалини, недоліки та слабкі місця, що часто залишаються непоміченими у повсякденній роботі. Без цього елементу комплексна система не могла б бути адаптивною та самовдосконалюваною, оскільки постійна оцінка є необхідною умовою її розвитку та модернізації.

Узагальнюючи аналіз таблиці 2.3, можна стверджувати, що кожен її елемент формує важливий структурний компонент комплексної системи протидії загрозам. Їхня взаємодія створює цілісну архітектуру, здатну забезпечити стійкість організації в умовах постійних трансформацій цифрового середовища. Представлені елементи охоплюють стратегічний, тактичний, технічний і людський виміри безпеки, що повністю відповідає міжнародним стандартам побудови систем інформаційної безпеки. Саме така комплексність дозволяє службам захисту інформації діяти ефективно, гармонійно та проактивно у сучасних умовах зростання кіберзагроз.

У межах розділу було здійснено комплексне дослідження організаційних, технічних та інтеграційних механізмів протидії загрозам інформаційній безпеці, що дало можливість сформувати цілісне уявлення про сучасну систему захисту інформаційних ресурсів. Проведений аналіз засвідчив, що ефективність протидії загрозам залежить не від окремих інструментів, а від їхньої структурованої взаємодії. Кожна група заходів, представлена у трьох підрозділах та підтверджена даними таблиць 2.1–2.3, виконує власну критичну функцію, але справжня сила системи проявляється у їх поєднанні. Саме інтеграція організаційних рішень, програмно-технічних засобів та комплексних підходів формує той рівень зрілості системи безпеки, який відповідає сучасним ризикам і викликам.

Розгляд організаційних заходів дозволив переконатися, що саме вони задають напрям розвитку всієї системи захисту та визначають рамки її функціонування. Нормативно-правові механізми формують фундамент, на якому базуються всі інші дії, забезпечуючи передбачуваність процедур і юридичну визначеність відповідальності. Кадрові заходи виявилися не менш значущими, оскільки людський фактор залишається одним із найвразливіших елементів системи. Управління доступом, аудит та реагування на інциденти формують організаційне ядро, яке забезпечує контроль, дисципліну й адекватну оцінку ризиків. Ці компоненти у сукупності демонструють, що організаційний рівень не є другорядним порівняно з технічним, а навпаки — визначає рамки ефективності всіх захисних механізмів.

Аналіз програмно-технічних засобів показав, що сучасна інфраструктура кіберзахисту базується на багатошаровому наборі технологій, кожна з яких виконує конкретну роль у забезпеченні стійкості системи. Системи контролю доступу та криптографічні механізми відповідають за захист від несанкціонованого доступу та збереження цілісності інформації, що має критичне значення для конфіденційних ресурсів. Мережеві екрани й IDS/IPS здійснюють контроль периметра та виявлення загроз у режимі реального часу, мінімізуючи ризик проникнення. Антивірусні платформи, SIEM-системи й рішення для резервного копіювання забезпечують комплексний захист від шкідливого ПЗ, аналіз подій безпеки та відновлення після інцидентів. Засоби захисту мобільних та хмарних сервісів демонструють адаптацію систем безпеки до нових цифрових моделей, що підтверджує гнучкість та динамічність сучасних технічних підходів.

Дослідження структурних елементів комплексної системи протидії загрозам дозволило побачити, що її ефективність визначається не лише наявністю окремих засобів, а й здатністю організації вибудовувати логічні, взаємопов’язані процеси. Управління ризиками формує стратегічний горизонт та визначає пріоритети розвитку. Багаторівневий захист гарантує диверсифікацію оборони та ускладнює можливість успішної атаки. Інтеграція

технічних засобів у єдиний моніторинговий простір забезпечує аналітичну глибину, від якої залежить якість реагування. Взаємодія суб'єктів безпеки — як внутрішніх, так і зовнішніх — створює широке інформаційне поле, що дозволяє своєчасно і точно оцінювати ситуацію. Правові механізми, кадрова політика та систематичний аудит гарантують дисципліну, відповідальність та незмінність стандартів якості.

Порівнюючи зміст трьох таблиць, можна побачити важливу закономірність: кожна з них описує окремий зріз системи безпеки, але всі разом вони утворюють єдиний логічний ланцюг. Таблиця 2.1 відображає організаційну структуру, яка забезпечує правила та внутрішній порядок. Таблиця 2.2 демонструє технічний арсенал, який реалізує практичний захист на рівні інфраструктури. Таблиця 2.3 показує, як ці елементи функціонують разом у межах комплексного підходу, що дозволяє поєднати людські, правові, технічні та аналітичні фактори. Такий порівняльний аналіз підтверджує, що сучасні служби захисту інформації мають працювати у режимі постійної взаємодії всіх рівнів системи, що і визначає її ефективність.

Узагальнюючи результати дослідження, можна стверджувати, що комплексна система захисту інформації є багатогранною інфраструктурою, яка об'єднує організаційні норми, технічні рішення та механізми стратегічного управління. Жоден із компонентів не може функціонувати окремо без втрати загальної ефективності, тому системність і взаємодія стають ключовими принципами забезпечення безпеки. Важливим висновком є те, що сучасні загрози вимагають постійного оновлення як організаційних заходів, так і технічних засобів, адже цифрове середовище змінюється швидше, ніж створюються нові нормативні та технологічні рішення. За таких умов служби захисту інформації повинні не лише підтримувати вже створені механізми, а й забезпечувати їхню динамічну модернізацію.

Підсумовуючи, розділ 2 підтвердив, що ефективна система кіберзахисту ґрунтується на поєднанні стратегічного планування, чітких організаційних правил, надійних технічних засобів та високої професійної культури персоналу.

Комплексність підходів дає можливість утримувати стійкість системи, своєчасно виявляти загрози, оперативно реагувати на інциденти та зберігати безперервність роботи інформаційних процесів. У цьому полягає сутність сучасної моделі безпеки, яка здатна забезпечити захист державних та організаційних інформаційних ресурсів у швидкозмінному цифровому середовищі.

РОЗДІЛ 3. УДОСКОНАЛЕННЯ СИСТЕМИ ПРОТИДІЇ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

3.1 Аналіз ефективності існуючих методів захисту

Система протидії загрозам інформаційній безпеці в Україні сформована під впливом політичних, соціальних, економічних та технологічних чинників, що визначають її структурну складність та багатовимірність функціонування. Забезпечення сталого функціонування критично важливих об’єктів інформаційної діяльності потребує використання комплексу організаційних, правових, технічних та психологічних механізмів протидії загрозам [28]. Проте аналіз сучасної практики демонструє, що наявні методи не повною мірою відповідають динаміці еволюції ризиків, особливо в умовах гібридної війни та зростання ролі інформаційно-психологічного впливу [29].

Сучасні науковці підкреслюють, що загрози інформаційного середовища дедалі більше зміщуються від технічного втручання у бік когнітивного маніпулятивного впливу на суспільну свідомість, формування викривлених уявлень і радикалізацію населення [30]. Горбулін В. П. зауважує, що інформаційні операції стали системною зброєю, спрямованою проти державних

інституцій та ідентичності суспільства [31]. Це зумовлює необхідність перегляду традиційних методів захисту, які значною мірою орієнтовані лише на технічну складову.

Сприятливим чинником загрози є також недосконаліть нормативної бази, фрагментарність стратегічного планування та обмеженість ресурсів служб захисту інформації [32]. Попри наявність низки програм державного рівня, їх реалізація стикається з інституційними бар'єрами та повільністю адаптації до нових викликів [33]. Така ситуація підсилює вразливість держави на інформаційному фронті, де противник активно комбінує технологічні, політичні та психологічні методи впливу [34].

Особливої уваги потребує проблема недостатності систематичного моніторингу інформаційного простору та обмеженість аналітичних інструментів прогнозування загроз [35]. Найчастіше служби реагують на атаку вже після її реалізації, що знижує загальну ефективність захисних заходів та збільшує масштаб можливих наслідків. Як зазначає Дереко В. Н., класифікація загроз має бути не лише формальною ознакою системи безпеки, а й інструментом управління превентивною діяльністю [36].

На рівні окремих об'єктів інформаційної інфраструктури наявні методи захисту забезпечують переважно периметрову безпеку й не орієнтовані на виявлення внутрішніх загроз, зокрема інсайдерських дій або компрометації облікових даних. Ураховуючи збільшення кількості атак, пов'язаних із соціальною інженерією, психологічним впливом та маніпуляцією поведінкою персоналу, така ситуація є стратегічно небезпечною [37].

Узагальнення сучасних досліджень дозволяє виокремити ключові проблеми, що знижують ефективність наявної системи протидії загрозам інформаційній безпеці.

У цій таблиці узагальнено основні недоліки існуючих методів протидії загрозам інформаційній безпеці в Україні, з урахуванням нормативно-правових, технологічних, організаційних та кадрових аспектів. Виділення зазначених проблем дозволяє обґрунтувати необхідність удосконалення підходів до

управління інформаційною безпекою та переходу від реактивних до превентивних моделей захисту.

Таблиця 3.1. - Основні недоліки існуючих методів протидії загрозам інформаційній безпеці в Україні [35]

Група проблем	**Характерні прояви**	**Потенційні наслідки**
1	2	3
Нормативно-правові	Повільна гармонізація законодавства з міжнародними стандартами; дублювання функцій органів	Неефективність координації та зниження швидкості реагування

Кінець таблиці 3.1

1	2	3
Технологічні	Застаріле обладнання; недостатність кібермоніторингу; несумісність систем	Зростання уразливості до кібератак, ускладнена модернізація
Організаційні	Відсутність єдиного центру управління інформаційною безпекою	Фрагментація політики та зниження контрольованості ризиків
Людський фактор	Низький рівень підготовки персоналу; відсутність культур безпеки	Підвищення кількості інсайдерських інцидентів та соціальних маніпуляцій
Аналітичні можливості	Недостатня система прогнозування інформаційних атак	Реактивний, а не превентивний характер захисту

Важливо підкреслити, що сучасна система інформаційної безпеки в багатьох випадках не має достатнього рівня адаптивності до швидкої трансформації методів ведення інформаційних операцій. Як наголошує Прокоф’єва-Янчиленко Д. М., національна безпека вже неможлива без кримінологічної безпеки, оскільки злочинність все активніше мігрує в кіберпростір і набуває форм, що ускладнюють традиційне правозастосування [39, с.112]. Це створює серйозні виклики у сфері протидії організованим групам, що використовують цифрові технології для шантажу, дезінформації, фінансових махінацій і політичного тиску.

Додатковою проблемою є слабкість комунікацій між різними державними органами, відповідальними за інформаційну безпеку. При наявності чітких функцій у СБУ, НБУ, Держспецзв'язку, НКЦК тощо — на практиці вони часто працюють не як інтегрований механізм, а як окремі фрагменти, що взаємодіють переважно після виникнення кризи [32, с.3]. Це суттєво знижує єдину оперативну стійкість держави до загроз, які мають комплексний характер.

Багаторівнева структура атак, характерна для гібридної війни, передбачає не лише проникнення у внутрішні мережі, а й тривале формування управлінських рішень, заснованих на неправдивій або маніпулятивній інформації. Саме тому Горбулін наголошує: ключовим елементом протидії є розвиток інформаційного аналітичного потенціалу держави, здатного не лише виявляти загрози, а й прогнозувати їх наслідки, випереджаючи противника стратегічно [31, с.41]. Утім сьогодні в Україні превалює реактивна логіка: дії служб розпочинаються здебільшого після реалізації атаки.

Технічна складова системи захисту також має значні недоліки, що пов'язані із переважним застосуванням систем периметрового контролю без належної уваги до поведінкової аналітики всередині мережі. Внаслідок цього збільшується число успішних атак, спрямованих на персональні акаунти, привілейовані доступи та обхід авторизаційних механізмів [28, с.319]. Атаки на ланцюги постачання, що активно використовуються у світі, в Україні лише починають враховуватися у практиці служб захисту.

Людський фактор у структурі загроз часто є недооціненим. Як показує дослідження Григор'єва В. І., технології інформаційно-психологічного впливу дедалі більше орієнтовані на формування втоми, недовіри, емоційної дестабілізації населення та маніпуляцію соціальними інстинктами [29, с.51]. Ці технології комбінуються з кібератаками, створюючи ефект «інформаційного шоку» — коли суспільство реагує емоційно, а не раціонально. Недостатність профілактики таких загроз у державній політиці робить суспільство вразливим до масових інформаційних маніпуляцій.

Варто також наголосити на проблемі недостатньої культури кібербезпеки в бізнес-секторі та серед громадян. У роботі Сопілко І. М. підкреслюється: якщо держава без підтримки суспільства намагається гарантувати інформаційну безпеку — виникає дисбаланс між відповідальністю та дієвими механізмами безпекового контролю [30, с.78]. Атаки на банківські системи, критичні об'єкти, телеком та медіа у 2017–2024 роках підтвердили, що навіть один незахищений суб'єкт може призвести до масштабних національних наслідків.

Окремо слід виділити відставання від міжнародної інфраструктури обміну інформацією щодо кіберзагроз. Незважаючи на співпрацю з НАТО та ЄС, вітчизняні служби потребують суттєвого розширення можливостей OSINT-моніторингу, Threat Intelligence-платформ та автоматизації реагування [33]. Недостатність таких інструментів сьогодні обертається повільністю оновлення знань про сучасні атаки та експлойти.

Характерною рисою теперішніх методів захисту є їх слабка орієнтація на протидію атакам, що мають цільовий, кастомізований характер (APT-кампанії). Хмелевський Р. М. доводить, що саме ці атаки є найбільш руйнівними, оскільки готуються на основі довготривалої розвідки поведінки користувачів і слабких місць системи [35, с.68]. Наявність таких кампаній в Україні (з боку російських груп Armageddon, Gamaredon тощо) підтверджує критичність проблеми.

Недостатність бюджету служб захисту інформації залишається проблемою системного характеру. Часто кошти спрямовуються на основні функції захисту, але не на розвиток нових аналітичних потужностей або кіберрозвідки. У результаті означена система забезпечення інформаційної безпеки не рухається випереджальним шляхом, а лише намагається «закрити поранення» після чергової атаки. Такий підхід є фундаментально неефективним у довгостроковій перспективі [40, с.214].

Особливо критичною є потреба у формуванні загальної національної інформаційної ідентичності, що здатна протидіяти спотвореним наративам, створюваним противником. Прозоров А. Ю. переконливо доводить, що

базовою передумовою інформаційної безпеки є захист цінностей держави, а без їх усвідомленого засвоєння суспільством — усі технічні інструменти втрачають ефективність [41, с.35]. Таким чином, традиційні методи потребують доповнення психологічними та соціокомунікаційними підходами.

З урахуванням викладеного можна стверджувати, що сучасні методи захисту в Україні забезпечують лише базовий рівень стійкості, але не формують здатності до активного опору та випереджального реагування. Перехід до інтелектуально-аналітичної моделі інформаційної безпеки є не лише бажаним, а й безальтернативним шляхом розвитку.

Таким чином, ефективність існуючих методів захисту залишається обмеженою внаслідок невідповідності традиційних підходів сучасним багатовимірним загрозам. Потрібні комплексні реформи, які поєднають технологічні рішення з удосконаленням законодавства, управлінських механізмів та формуванням інформаційної стійкості суспільства. Як відзначає Прозоров А. Ю., без опори на ціннісні основи безпеки неможливо забезпечити реальний захист державності та громадян [41]. Подальше удосконалення системи має орієнтуватися на активний моніторинг, випереджальне реагування та гнучкість управлінських рішень.

3.2 Впровадження сучасних технологій моніторингу та кіберзахисту

В умовах радикального зростання кількості кіберзагроз та інформаційно-психологічного впливу розвиток технологій моніторингу та кіберзахисту стає фундаментальним напрямом удосконалення системи інформаційної безпеки України. Сучасні атаки вже не обмежуються технічним проникненням, а набувають багатокомпонентної природи, поєднуючи хакерські інструменти, соціальну інженерію, когнітивні маніпуляції та політичний тиск [31]. Ефективне протистояння таким загрозам можливе лише за умови впровадження

автоматизованих засобів аналізу трафіку, прогнозування аномалій та випереджального реагування.

На думку українських дослідників, інформаційна безпека має будуватися на синергії технологічного контролю та безперервного оцінювання ситуації в інформаційному середовищі [30]. Вагомим аспектом стає інтеграція сучасних систем кіберзахисту в діяльність служб інформаційної безпеки та CERT-підрозділів. Система повинна бути не лише здатною до нейтралізації атак, але й навчатися на їхніх шаблонах для попередження повторень. Саме тому впровадження новітніх технологій стає стратегічною передумовою збереження стійкості національного інформаційного простору [40].

Одним із ключових напрямів розвитку є застосування комплексних систем моніторингу, таких як SIEM-рішення, які поєднують аналіз подій безпеки, збір телеметричних даних та штучний інтелект, здатний виділяти нетипову активність у мережі. Дослідження демонструють, що використання таких платформ дозволяє скоротити час виявлення кібератак у десятки разів порівняно з традиційним ручним аналізом [35]. Важливо, що SIEM забезпечує уніфікацію інформації з різних об’єктів критичної інфраструктури, що в Україні є особливо актуальним через фрагментованість мереж і стандартів [32].

Окрему увагу слід приділити впровадженню систем управління уразливостями та автоматизованих платформ кіберрозвідки, що базуються на концепції Threat Intelligence. Вони забезпечують постійне оновлення інформації про експлойти, ботнет-індикатори та шкідливі інструменти, що використовуються противником [35]. На думку Хмелевського, прогнозування загроз на основі аналізу поведінкових патернів стає важливішим, ніж просто реагування після факту [35].

В умовах гібридної агресії саме можливість отримати попереджувальні сигнали дає Україні шанс швидко перекривати доступ противнику до критичних ресурсів. Наприклад, атаки типу APT, притаманні російським угрупованням, можуть готуватися місяцями, тому їх раннє виявлення дозволяє зберегти системи боєздатними. Важливо також, що Threat Intelligence формує

інформаційний суверенітет — держава перестає бути лише «споживачем» реакційних механізмів і трансформується в активного суб'єкта інформаційної боротьби [44]. Такий підхід забезпечує довгостроковий стратегічний виграш.

Невід'ємним елементом модернізації є перехід до архітектури Zero Trust, де будь-яка взаємодія користувача з системою проходить верифікацію незалежно від його адміністративних прав. Це мінімізує ризики, пов'язані з людським фактором, а також перешкоджає інсайдерським атакам, які, як показують останні роки, набувають дедалі більшої загрози [37]. Розподіленість українських комунікаційних мереж і швидка зміна персоналу в оборонних структурах роблять цей підхід критично необхідним.

Важливим є те, що Zero Trust передбачає побудову безпеки на рівні ідентичностей і доступів, а не лише фізичної інфраструктури. Для державного сектору України це також означає поступовий перехід на сучасні системи керування доступами, інтегровані зі сховищами логів та поведінковими профілями [28]. У результаті створюється багатофакторна система контролю довіри, що значно зменшує можливість швидкого прориву мережі противником навіть у разі компрометації облікових даних. Таким чином, Zero Trust — це не лише технологія, а й нова модель мислення щодо інформаційного захисту.

Зважаючи на зростання ролі інформаційно-психологічних операцій, системи моніторингу мають охоплювати також відкриті медіапростори, соціальні мережі та телеграм-канали. Сашук Г. зазначає, що масові комунікації сьогодні є полем найбільш небезпечної інформаційної зброї, здатної руйнувати ідентичність і соціальну згуртованість країни [33]. Тому впровадження OSINT-рішень для відстеження ворожих наративів та інформаційних атак проти суспільної думки є обов'язковим завданням.

Саме поєднання технічного та когнітивного моніторингу дозволяє виявляти комплексні операції, спрямовані на формування паніки, страху і недовіри до держави [29]. Це особливо актуально у періоди посилених ракетних обстрілів, коли противник синхронізує фізичні удари з психологічним тиском. Технологічні рішення в цьому контексті мають охоплювати мовний

аналіз, семантичний розбір і автоматичне виявлення мережевих ботів. У такий спосіб держава отримує змогу діяти не в позиції оборони, а у стані активного управління інформаційною ситуацією.

Розвиток національних центрів реагування на кіберзагрози, таких як CERT-UA, має супроводжуватися створенням повноцінних SOC-центрів (Security Operation Centers) на кожному об'єкті критичної інфраструктури. Домбровська підкреслює, що централізація стратегічних функцій та децентралізація оперативних дозволяють забезпечити швидкість і точність реагування [48]. Наявність власних SOC дає можливість локально фіксувати аномалії, швидко ізолювати сегменти інфраструктури і передавати інформацію на вищий рівень аналітики.

Оскільки противник часто використовує каскадні атаки, які проходять через менш захищені структури в інших секторах, важлива автоматизована взаємодія між SOC, CERT-UA і Національним центром кіберзахисту. Впровадження цієї моделі створює комплексну оборону, що здатна відновлювати роботу систем без критичного зниження їх функціональності. Така архітектура відповідає і вимогам НАТО, з якими Україна інтегрується у сфері кібероборони [40]. З кожним роком така координація стає ключовою умовою стійкості держави перед широкомасштабними загрозами.

У цій таблиці систематизовано ключові сучасні технології кіберзахисту, що відіграють визначальну роль у зміцненні національної інформаційної безпеки. Розглянуті технології орієнтовані на підвищення спроможності держави до своєчасного виявлення загроз, мінімізації наслідків кібератак та формування випереджального, а не реактивного підходу до захисту інформаційного простору.

Таблиця 3.2 - Ключові сучасні технології кіберзахисту та їх значення для національної інформаційної безпеки [30]

Технологія	**Основні можливості**	**Результат для України**
SIEM-системи	Автоматичний аналіз подій,	Прискорення виявлення

	контроль трафіку, кореляція індикаторів	атак та зниження масштабів наслідків
Threat Intelligence	Прогнозування, виявлення APT-кампаній, аналіз експлойтів	Перехід від реактивного до випереджального захисту
Zero Trust	Контроль доступів, поведінкові профілі, мінімізація довіри	Усунення інсайдерських та соціальних загроз
SOC-інфраструктура	Постійний моніторинг критичних мереж, локалізація інцидентів	Скорочення часу реагування та підвищення стійкості систем
OSINT-моніторинг	Виявлення інформаційних атак у медіапросторі	Захист суспільної психостійкості і національної ідентичності

Важливим аспектом упровадження сучасних технологій моніторингу є формування єдиної інфраструктури обміну даними між державними органами та критично важливими підприємствами. Як зазначають українські дослідники, інформаційна безпека держави неможлива без об’єднання політичних, економічних та технічних ресурсів у спільній системі управління ризиками [40]. На сьогодні аналіз інцидентів засвідчує, що низка об’єктів діє ізольовано, що створює прогалини в обороні та сприяє поширенню атак на інші сектори.

Єдина база даних атак і тактик противника дозволить створити динамічні профілі загроз і швидше виявляти їх походження [35]. Такий підхід відповідає міжнародним стандартам та підсилює інтеграцію України в євроатлантичний безпековий простір. Крім того, співпраця з міжнародними агентствами кібербезпеки забезпечує доступ до передових методів аналізу цифрових ризиків. Взаємний обмін загрозами створює ефект спільного щита, що значно ускладнює роботу організованих злочинних угруповань і держав-агресорів [39].

Розвиток штучного інтелекту відкриває новий кардинальний етап у моніторингу інформаційного простору, оскільки дозволяє виявляти складні атаки зі змінними шаблонами та високим ступенем маскування. Алгоритми машинного навчання здатні самостійно адаптуватися до тактик противника та визначати ризики за непрямими ознаками, недоступними традиційному аналізу [29]. У контексті України це має особливу цінність, адже ворожі угруповання

часто використовують нестандартні та унікальні вектори проникнення, що не фіксуються базовими інструментами.

Як зазначає Горбулін В. П., забезпечення державної стабільності передбачає розвиток саме проактивного компонента аналітики, а не лише здатності до ліквідації наслідків [31]. Використання AI-технологій у сфері протидії гібридним операціям також забезпечує перевагу у швидкості розпізнавання дезінформаційних кампаній. Машинне моделювання інформаційних загроз дозволяє виявляти їхню потенційну траєкторію до того, як вони наберуть масового резонансу. Такий підхід формує принципово нову якість інформаційної безпеки — безперервну та передбачувальну.

Не менш важливим є питання кадрового забезпечення сучасних технологій моніторингу та кіберзахисту, оскільки високотехнологічні засоби самі по собі не гарантують результату без підготовлених спеціалістів. Сащук Г. наголошує, що інформаційна безпека стає не лише технічною, але й інтелектуальною сферою, у якій людський капітал є критично важливим ресурсом [33]. Проте кадровий дефіцит у галузі кібербезпеки в Україні зберігається, що створює системну залежність від зовнішніх партнерів і приватних компаній.

Зважаючи на стратегічну значущість інформаційного суверенітету, підготовка спеціалістів повинна бути пріоритетом державної політики. Освітні програми потребують постійного оновлення відповідно до світових стандартів і практик кібероборони. Крім того, важливою складовою є підвищення загальної грамотності працівників щодо ризиків соціальної інженерії, яку противник використовує як один із головних інструментів проникнення [28]. Лише комплексна система розвитку персоналу здатна забезпечити повноцінну ефективність технологій.

Психологічний вимір інформаційного протистояння вимагає впровадження засобів оцінювання впливу на громадську думку з метою запобігання поширенню панічних настроїв та деморалізації населення. Прозоров А. Ю. підкреслює, що інформаційна безпека повинна включати

захист ціннісних основ суспільства, оскільки саме вони стають головним об’єктом атак у гібридних конфліктах [41]. OSINT-платформи мають розширюватись до систем SOCMINT — аналізу соціальних сигналів, настроїв і інформаційних флуктуацій.

Вони дозволяють не тільки відстежувати негативні інформаційні хвилі, а й прогнозувати їх ескалацію залежно від подій у фізичному світі. Гармонізація таких платформ із кібермоніторингом дає змогу розуміти операції противника як єдині комплексні явища, а не окремі інциденти. Це значно підсилює здатність держави перехоплювати інформаційну ініціативу, а не лише реагувати на провокації. У результаті технології стають не інструментом захисту, а механізмом стратегічного управління стійкістю нації.

Дереко В. Н. зазначає, що ефективна класифікація загроз стає фундаментальною умовою правильного вибору тактики протидії [36]. Застосування індикаторів компрометації, матриць ATT&CK та прогнозно-моделювальних алгоритмів дозволяє точніше визначати стратегічні пріоритети оборони. В Україні така координація має критичну важливість, оскільки противник активно комбінує кібернетичні, інформаційно-психологічні та воєнні методи впливу. Чим складніше середовище протистояння, тим важливішою стає роль потокового аналізу даних, який дозволяє концентрувати ресурси на точках найбільшої небезпеки. Використання сучасних методів розвідувального оцінювання створює передумови для прогнозування темпів і напрямів атак, що перетворює безпекові структури на суб’єктів, здатних діяти на випередження [31].

Підсилення нормативно-правового регулювання є ключовим доповненням до впровадження технологічних засобів, оскільки інституційні прогалини значно знижують масштаби результативності нових інструментів кіберзахисту. Науковці підкреслюють, що чинне законодавство потребує синхронізації із сучасними доктринами інформаційної безпеки та стандартами НАТО [32]. Розвиток технічних рішень без нормативної підтримки призводитиме до їх невикористання або ж несистемного застосування.

Держава має встановити обов’язкові вимоги до кіберзахисту критичних об’єктів, включаючи постійне тестування на проникнення, аудит доступів та впровадження верифікаційних протоколів. Важливою умовою є також формування механізмів відповідальності за порушення політики кібербезпеки, що стимулюватиме організації до дотримання високих стандартів. Коли нормативна структура підсилює технологічні зусилля, держава отримує комплексну систему протидії загрозам, що здатна еволюціонувати разом із динамікою цифрових ризиків [28]. У такий спосіб технології перестають бути окремим елементом і перетворюються на опору державної безпеки.

Підсумовуючи проведений аналіз, впровадження сучасних технологій моніторингу та кіберзахисту формує основу коректної еволюції національної системи інформаційної безпеки. Дослідження Прокоф’євої-Янчиленко засвідчує, що кримінологічні та кіберзагрози вже стали взаємопов’язаними, тому технологічний захист має бути комплексним та міжвідомчим [39]. Нині безпека не може спиратися лише на людські ресурси чи нормативне регулювання, оскільки противник використовує високоточні й масштабовані інструменти. Запровадження таких рішень посилює стійкість системи як у технічному, так і в психологічному вимірах, що забезпечує довгостроковий національний інтерес [41]. Водночас технологічний розвиток має супроводжуватися культурою безпеки та постійною освітою персоналу щодо сучасних кіберризиків [28]. Лише поєднавши сучасні цифрові засоби із системним управлінням ризиками держава може зберегти контроль над інформаційною сферою в умовах війни та глобальних загроз. Саме так формується здатність країни перемагати у протистоянні XXI століття, де інформація стає ключовим полем державного суверенітету.

3.3 Розробка рекомендацій щодо підвищення рівня інформаційної безпеки

Покращення ефективності системи протидії загрозам в інформаційному середовищі України потребує комплексного підходу, який поєднує інституційні, технологічні, організаційні та ціннісні механізми. Як зазначає Сопілко І. М., сучасні загрози спрямовані не лише на інформаційні ресурси, а й на підрив стійкості суспільства, і тому заходи безпеки повинні враховувати соціально-психологічний вимір [30]. Державі необхідно забезпечити не реактивний, а стратегічно проактивний розвиток інформаційної безпеки, де аналітичні й прогностичні інструменти відіграють ключову роль. Упровадження цих підходів вимагатиме модернізації державного управління, зміцнення кіберінфраструктури та створення сталої системи підготовки кадрів. Лише постійний розвиток цих складових сприятиме формуванню інформаційного суверенітету України [40].

Одним із першочергових завдань є вдосконалення нормативно-правової підтримки інформаційної безпеки. Забезпечення гармонізації із стандартами НАТО та ЄС дозволить формалізувати вимоги до кіберзахисту об’єктів критичної інфраструктури і зменшити дисбаланс між секторами [32]. Потрібне також унормування національної моделі управління інцидентами з чітким розподілом повноважень між державними та корпоративними структурами. Таким чином, підвищиться відповідальність усіх суб’єктів інформаційного простору за власний захист. Уніфіковані вимоги також сприятимуть зменшенню кількості вразливих точок, які нині виникають через фрагментарність технічних стандартів [28].

Важливим напрямом удосконалення стає створення розвиненої мережевої архітектури взаємодії між SOC-центрами різних рівнів, CERT-UA та Національним центром кіберзахисту. Як демонструють результати подолання масштабних атак проти телекомунікаційних і державних ресурсів, швидкість комунікації стає визначальним фактором захисту [29]. Координація повинна спиратися на автоматизований обмін індикаторами компрометації, що усуває затримки, властиві ручним процедурам. Розширення цієї мережі дозволить оптимізувати розподіл ресурсів і забезпечить підтримку менш захищеним

об’єктам. Таким чином, загальна обороноздатність системи зросте за рахунок синергії структур, а не окремих точкових зусиль [32].

Враховуючи зростання кількості цілеспрямованих атак та розвідувальних операцій у кіберпросторі, невідкладною рекомендацією є масштабування технологій Threat Intelligence та автоматизованого виявлення аномалій. Хмелевський підкреслює, що лише поєднання аналізу сучасних технік атак і прогнозування розвитку їхніх сценаріїв створює умови для випереджального реагування [35]. Це означає, що захисні системи мають не просто фіксувати факти проникнення, а формувати поведінкові профілі ворожої активності. Така модель відповідає логіці гібридного протистояння, де головне значення має інформація про загрозу ще до її матеріалізації. Це забезпечить зниження втрат і збереження стійкості функціонування об’єктів інформаційної інфраструктури [31].

Суттєвим елементом підвищення захищеності є створення цілісної культури інформаційної безпеки в усіх секторах суспільства. За даними Остроухова та колективу авторів, більшість інцидентів спричинені недотриманням елементарних правил захисту даних співробітниками [28]. Запровадження постійних освітніх програм, тренінгів і симуляцій соціально-інженерних атак повинно стати стандартом для будь-якої організації. Підвищення усвідомленості користувачів сприятиме зниженню успішності атак типу phishing та компрометації облікових даних. Формування такої культури перетворить персонал на активний елемент оборони, а не на слабку ланку системи [37].

Для структуризації сформованих рекомендацій наведемо їх у вигляді таблиці, що демонструє ключові напрями вдосконалення системи протидії загрозам інформаційній безпеці України.

У цій таблиці сформульовано основні рекомендації щодо підвищення рівня інформаційної безпеки України з урахуванням нормативно-правових, технологічних, організаційних, соціально-психологічних та стратегічних аспектів. Запропоновані заходи спрямовані на формування цілісної системи

захисту інформаційного простору держави, підвищення стійкості до кіберзагроз та мінімізацію впливу деструктивних інформаційних операцій.

Таблиця 3.3 - Основні рекомендації щодо підвищення рівня інформаційної безпеки України [41]

Сфера удосконалення	**Ключові рекомендації**	**Очікуваний результат**
Нормативно-правова	Уніфікація з європейськими та натівськими стандартами	Підвищення узгодженості дій і відповідальності суб'єктів
Технологічна	Розширення SIEM/SOC/Threat Intelligence інфраструктури	Зменшення часу виявлення атак і підвищення стійкості мереж
Організаційна	Автоматизована взаємодія CERT та об'єктів КВІ	Зниження масштабів кіберінцидентів і втрат
Соціально-психологічна	Системні програми кіберосвіти персоналу і громадян	Зменшення частки інцидентів через людський фактор
Стратегічна	Посилення інформаційної ідентичності суспільства	Опір деструктивним інформаційним операціям противника

Визначальним фактором ефективності впровадження цих рекомендацій є формування дієвого суспільного імунітету до інформаційно-психологічних впливів. Прозоров А. Ю. зазначає, що без захисту ціннісних засад державності технічні засоби залишаються лише частково ефективними [41]. Тому держава повинна інвестувати не лише в кібероборону, а й у просування об'єднавчих

смислів, що зміцнюють національну ідентичність і запобігають деструктивним маніпуляціям. З огляду на це, розвиток інформаційної безпеки має розглядатися як довгостроковий цивілізаційний проєкт [40]. Він забезпечить збереження суверенітету та громадської стабільності у світі, де інформація стала ключовим стратегічним ресурсом.

Ще одним критичним напрямом є підвищення прозорості й швидкості прийняття рішень у сфері інформаційної безпеки. Система захисту повинна мати чітку вертикаль відповідальності, щоб уникати бюрократичних перешкод у моменти загострення загроз [32]. Надання службам захисту інформації розширених повноважень у кризових ситуаціях дозволить зменшити часовий розрив між атакою та реагуванням. Водночас такі дії повинні супроводжуватися ефективним контролем і звітністю для забезпечення балансу між безпекою й демократичними принципами державного управління. Саме такий механізм дозволяє створити стабільну систему оперативного реагування, яка відповідатиме вимогам сучасної війни [31].

Підвищення рівня інформаційної безпеки неможливе без створення дієвих механізмів контролю за якістю впроваджених рішень та оцінювання ефективності їх застосування. Горбулін В. П. наголошує, що відсутність постійного аналізу стану інформаційного середовища перетворює навіть найдосконаліші технічні засоби на формальний інструмент [31]. Державні установи повинні запроваджувати регулярний аудит безпеки своїх інформаційних систем, включаючи стрес-тестування алгоритмів моніторингу та перевірку стійкості каналів комунікації. Такий підхід дозволить не тільки виявляти уразливості, але й формувати тенденції для прогнозування розвитку загроз. У результаті створюється система самокорекції, яка постійно адаптується до змінного характеру цифрового середовища.

Важливою умовою стабільності є зміцнення партнерства між державним сектором, бізнесом та науковими установами. Як зазначено в дослідженнях Прокоф’євої-Янчиленко, інформаційна безпека є інтегративним явищем, що виходить за межі компетенції одного суб’єкта [39]. Компанії приватного

сектору часто стикаються з новітніми атаками раніше за державні структури, тому їх досвід і технології мають бути інтегровані у загальнонаціональну архітектуру. Учасники ринку можуть виступати не лише об’єктами захисту, а й активними учасниками формування системи кіберрозвідки. Така модель дає змогу створити дієвий багаторівневий бар’єр оборони. Саме за рахунок співпраці формується підсилена екосистема безпеки, у якій жоден об’єкт не лишається вразливим.

Особливої уваги потребує впровадження проєктів цифрового суверенітету, які передбачають локалізацію критичних сервісів і захист даних громадян на національній інфраструктурі. За даними Сопілко І. М., втручання іноземних акторів у канали обробки інформації може створювати додаткові ризики на рівні державного управління [30]. Стратегія цифрової незалежності передбачає розвиток власних дата-центрів, національних хмарних платформ і захищених державних мереж. У воєнних умовах це має особливу вагу, оскільки доступ до даних стає ресурсом впливу на ухвалення управлінських рішень. Захист ключових інформаційних сервісів повинен розглядатися як елемент обороноздатності країни. Цей напрям зменшує ризик інформаційного шантажу та втрати керованості критичними процесами.

Подальший розвиток інформаційної стійкості суспільства має ґрунтуватися на підсиленні спроможності громадян протидіяти маніпулятивним наративам. Живко З. Б. та Живко М. О. підкреслюють, що інформаційні загрози часто стають ефективними лише тому, що знаходять слабкі місця у суспільних настроях [37]. Держава має розвивати програми медіаграмотності, що формують вміння критично оцінювати інформацію та розпізнавати спроби психологічного тиску. Такі підходи допомагають уникати масових панічних реакцій і зміцнюють довіру до державних інституцій під час криз. Інформаційний імунітет населення стає важливим фактором стабільності функціонування внутрішнього інформаційного простору. Національна безпека починає опиратися не лише на технічні бар’єри, а й на свідомий вибір громадян.

Дереко В. Н. наголошує, що саме теоретико-методологічний розвиток дає можливість забезпечити конкурентність системи протидії загрозам на міжнародному рівні [36]. Власні наукові напрацювання уможливлюють створення оригінальних засобів моніторингу та виявлення атак, які складніше обійти супротивнику. Розвиток національних технологій гарантує мінімізацію залежності від іноземного програмного забезпечення. В умовах гібридної агресії це створює значну стратегічну перевагу для держави. Наукові інновації стають основою довгострокової безпеки.

Підвищення обороноздатності інформаційного середовища передбачає також модернізацію механізмів кризового реагування. Як вказано у працях Домбровської С. М., затримка в ухваленні рішень або слабка координація дій істотно збільшують шкоду від атак [32]. Тому в критичних випадках служби захисту інформації повинні мати право оперативно вводити тимчасові обмеження доступу, ізолювати сегменти мережі або перемикати їх у захищений автономний режим. Визначення чітких процедур кризового управління сприятиме скороченню втрат та швидшому відновленню систем. Такі підходи формують захисну архітектуру, здатну протистояти комбінованим впливам і залишатися функціональною навіть у періоди пікових атак.

Рекомендації, запропоновані у цьому підрозділі, не лише узгоджуються з теоретичними висновками українських науковців, але й враховують реальні умови ведення сучасної війни. Їх практична імплементація створить багатошарову систему інформаційної безпеки, що використовує як технологічні, так і когнітивні механізми протидії загрозам. У такий спосіб Україна отримає можливість не лише реагувати на інформаційні атаки, але й активно нейтралізувати їх ще на етапі планування противником. Саме такий підхід формує нову парадигму захисту, де інформація стає не вразливістю, а потенціалом державної сили [31]. Це забезпечить стійкість держави перед викликами майбутнього і створить основу для її політичного й соціального розвитку навіть у складних геополітичних умовах [40].

Удосконалення системи протидії загрозам інформаційній безпеці України є комплексним процесом, який потребує стратегічного бачення та поєднання різних підходів і механізмів. Проведений аналіз засвідчив, що наявні методи захисту, незважаючи на певну результативність, не відповідають сучасним умовам гібридного протистояння. Динамічність і багатовекторність загроз вимагають від держави швидкої адаптації та здатності випереджати дії противника, а не лише реагувати на вже реалізовані атаки.

У межах підпункту 3.1 було визначено суттєві недоліки існуючих технологічних, організаційних і нормативних механізмів захисту, що обмежують здатність держави ефективно протистояти загрозам. Виявлено, що реактивний характер захисних заходів підвищує ризик масштабних наслідків для критично важливих систем та державного управління. Інформаційно-психологічний компонент атаки сьогодні є не менш небезпечним, ніж технічний, оскільки він безпосередньо впливає на суспільні процеси. Саме тому без оновлення системи моніторингу та прогнозування держава залишається вразливою до маніпуляцій, здатних змінювати поведінку громадян й викликати соціальну турбулентність. Потреба в структурній модернізації системи захисту є не дискусією, а вимогою часу.

У підпункті 3.2 доведено, що впровадження інноваційних технологій моніторингу є ключовим напрямом підвищення рівня інформаційної безпеки. Розвиток SIEM-рішень, SOC-центрів, платформ Threat Intelligence та архітектури Zero Trust значно підсилює здатність держави протидіяти атакам високого рівня складності. Також встановлено, що сучасні кіберзагрози переважно мають характер комплексного впливу, що поєднує технічні та психологічні засоби тиску на інформаційний простір України. Таким чином, ефективна система безпеки повинна забезпечувати одночасний захист мереж, даних та суспільної свідомості. Саме це перетворює інформаційний захист на складову національної обороноздатності й передумову політичної стійкості держави.

Результати підпункту 3.3 демонструють, що розробка рекомендацій повинна базуватися на двох принципах. Перший полягає у створенні єдиного інституційного простору інформаційної безпеки з чітким розподілом відповідальності та автоматизованими механізмами взаємодії між усіма задіяними суб'єктами. Другий визначає необхідність розвитку інформаційної культури суспільства, яка є фундаментом психологічної стійкості громадян і мінімізує ефективність інформаційних маніпуляцій. Комбінація цих підходів забезпечує комплексну протидію загрозам, спрямованим як на інформаційну інфраструктуру, так і на ціннісні орієнтири населення. Це дозволяє державі функціонувати стабільно навіть у періоди пікового загострення інформаційного тиску.

Особливе значення має розвиток партнерства між державою, бізнесом і науковими центрами у сфері інформаційного захисту. Така взаємодія формує багаторівневу систему обміну знаннями, технологіями та ресурсами, що підсилює національну безпеку. Актуальність цього напряму підсилюється тим, що противник активно використовує синхронізовані атаки, націлені на різні сфери державного управління, енергетику та комунікаційні системи. Тому лише інтегрований підхід до розвитку кіберзахисту може забезпечити належний рівень протидії в умовах гібридної війни. Розвиток такої співпраці формує основу довгострокової інформаційної стійкості держави.

Значущим аспектом є формування системи випереджального аналізу та прогнозування, яка стає центральним елементом ефективного управління інформаційними ризиками. Цифрова епоха визначає перевагу того суб'єкта, який першим отримує інформацію про загрозу і здатний її нейтралізувати до реалізації негативних наслідків. Тому напрацювання аналітичного потенціалу служб захисту інформації має відбуватися у тісному зв'язку із впровадженням штучного інтелекту та автоматизованих методів оцінювання. Такий підхід забезпечує суттєве зниження ймовірності успішного проникнення ворожих структур у критично важливі інформаційні системи України. У свою чергу це дозволяє утримувати інформаційний простір під постійним захистом.

Підсумовуючи результати дослідження, можна стверджувати, що підвищення ефективності системи протидії загрозам інформаційній безпеці залежить від здатності держави поєднати інноваційні технології з управлінськими та соціально-комунікаційними інструментами. Усі рекомендації, сформовані у цьому розділі, спрямовані на перехід до нової моделі захисту, де ключову роль відіграє не лише реагування, а й превентивна аналітика та стійкість суспільства до інформаційних загроз. Урахування ціннісної складової інформаційної безпеки дає змогу створити надійний фундамент для забезпечення національного суверенітету та захисту державних інтересів. Саме тому модернізація системи протидії кіберзагрозам і інформаційно-психологічним атакам в Україні є стратегічною умовою її успішного розвитку та безпечного майбутнього. Ці висновки формують наукову основу для розробки стратегії інформаційної безпеки, що відповідає викликам XXI століття й забезпечує її стійкість у глобальному середовищі.

ВИСНОВКИ

У магістерській роботі досліджено методи протидії загрозам інформаційній безпеці з урахуванням діяльності служб захисту інформації як ключових суб’єктів реалізації безпекових процесів. Отримані результати підтверджують, що сучасні загрози мають комплексний характер і не можуть бути ефективно нейтралізовані ізольованими організаційними або технічними заходами. Забезпечення інформаційної безпеки потребує поєднання управлінських рішень, технологічних інструментів і аналітичних механізмів у межах цілісної системи. Саме системність і керованість визначають реальний рівень стійкості інформаційних процесів.

У ході теоретичного аналізу встановлено, що базові поняття захисту інформації формують не лише термінологічне підґрунтя, а й логіку побудови практичних систем безпеки. Уточнення взаємозв’язку між властивостями інформації, загрозами та ризиками дозволило обґрунтувати вимоги до заходів захисту на різних рівнях інформаційної інфраструктури. Показано, що ігнорування хоча б одного з цих елементів призводить до структурної вразливості системи незалежно від рівня її технічної оснащеності. Узагальнення цих положень у табличній формі забезпечило аналітичну основу для подальшого дослідження методів протидії загрозам.

Аналіз організаційних заходів забезпечення інформаційної безпеки засвідчив їх визначальну роль у формуванні керованого безпекового середовища. Доведено, що нормативно-правові, кадрові та управлінські механізми безпосередньо впливають на ефективність використання програмно-технічних засобів захисту. Саме на організаційному рівні формується здатність системи безпеки до координації дій, контролю процесів і своєчасного реагування на інциденти. Узагальнення цих аспектів дозволило обґрунтувати необхідність розгляду організаційних заходів як основи всієї системи протидії загрозам.

Дослідження програмно-технічних засобів захисту інформації підтвердило, що їх ефективність визначається не окремими характеристиками, а способом інтеграції в загальну архітектуру безпеки. Аналіз сучасних інструментів показав, що фрагментарне впровадження технічних рішень не забезпечує належного рівня захисту в умовах складних і комбінованих загроз. Табличне узагальнення характеристик програмно-технічних засобів дозволило виявити доцільність їх використання в межах багаторівневого підходу. Це підтверджує необхідність системного планування технічних заходів з урахуванням реальних ризиків і ресурсних обмежень.

У межах дослідження комплексної системи протидії загрозам встановлено, що її ефективність визначається узгодженістю функціонування всіх структурних компонентів. Управління ризиками, моніторинг подій

безпеки, реагування на інциденти та аудит відповідності повинні розглядатися як взаємопов'язані процеси, а не як окремі функції. Узагальнення цих компонентів у таблицях дозволило показати логіку побудови системи захисту як динамічної моделі, здатної адаптуватися до змін загрозового середовища. Такий підхід відповідає сучасним вимогам до управління інформаційною безпекою.

Критичний аналіз існуючих методів протидії загрозам інформаційній безпеці в Україні виявив низку системних обмежень, що знижують ефективність захисних заходів. До основних проблем віднесено нормативно-правову фрагментарність, технологічну неоднорідність і недостатню координацію між суб'єктами безпеки. Особливу роль відіграє людський фактор, який часто стає джерелом додаткових ризиків навіть за наявності сучасних технічних засобів захисту. Узагальнення цих недоліків дозволило обґрунтувати потребу в удосконаленні підходів до організації безпекових процесів.

Аналіз сучасних технологій кіберзахисту показав, що їх застосування істотно підвищує аналітичні та прогнозні можливості систем інформаційної безпеки. Використання SIEM, Threat Intelligence, підходів Zero Trust, SOC-інфраструктур та OSINT-моніторингу сприяє переходу від реактивних моделей захисту до більш структурованих і превентивних. Узагальнення результатів свідчить, що впровадження таких технологій доцільне за умови їх інтеграції в організаційні та управлінські процеси. Це дозволяє підвищити стійкість інформаційних систем до сучасних загроз.

Розроблені рекомендації щодо підвищення рівня інформаційної безпеки орієнтовані на вдосконалення практичної діяльності служб захисту інформації. Запропоновані напрями удосконалення охоплюють нормативно-правові, технологічні, організаційні та освітні аспекти і мають прикладний характер. Їх узагальнення в табличній формі дозволило чітко співвіднести заходи з очікуваними результатами та можливими обмеженнями реалізації. Реалізація

цих рекомендацій може сприяти зниженню рівня інформаційних ризиків у межах конкретних організацій.

Науковий результат роботи полягає в аналітичному узагальненні методів протидії загрозам інформаційній безпеці з позицій системного підходу. Практичне значення отриманих результатів полягає в можливості їх використання при оцінюванні ризиків, плануванні заходів захисту та вдосконаленні діяльності служб захисту інформації. Загалом мету магістерської роботи досягнуто, а поставлені завдання виконано в повному обсязі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. НД ТЗІ 1.1-001-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Київ: Державна служба спеціального зв’язку та захисту інформації України, 1999. – 45 с.

2. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text.

3. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 р. «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021р.№ 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

4. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. – Geneva: International Organization for Standardization, 2013. – 23 p.

5. Про державну таємницю: Закон України від 21.01.1994 р. № 3855- XII. URL: https://zakon.rada.gov.ua/laws/card/3855-12.

6. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України: дис. … д-ра юрид. наук: спец. 12.00.07. Одеса, 2004. 427 с.

7. Корж І. Безпека: медотологічні підходи до поняття. National law journal: theory and practice. 2019. August. P. 68-72. 86

8. Проєкт Закону України «Про засади інформаційної безпеки України». URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123.

9. Рубан, І. В. Методи та засоби захисту інформації: підручник / І. В. Рубан, В. В. Пономаренко. – Харків: ХНУРЕ, 2021. – 324 с.

10. Шнайер, Б. Секрети і брехня. Безпека даних у цифровому світі / Брюс Шнайер ; пер. з англ. В. Горбатко. – Харків: Клуб Сімейного Дозвілля, 2019. – 416 с.

11. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Київ: Державна служба спеціального зв’язку та захисту інформації України, 1999. – 32 с.

12. Рубан, І. В. Методи та засоби захисту інформації: підручник / І. В. Рубан, В. В. Пономаренко. – Харків: ХНУРЕ, 2021. – 324 с.

13. Стаття: Аналіз сучасних кіберзагроз та методів їх нейтралізації / О. М. Литвиненко // Кібербезпека: освіта, наука, техніка. – 2022. – № 1. – С. 45–56.

14. Розробка проєкту Концепції кодифікації інформаційного законодавства України. Інформація і право. 2012. № 1. URL:

http://ippi.org.ua/vid-redaktsiinoi-kolegii-rozrobka-proektu-kontseptsii-kodifikatsii informatsiinogo-zakonodavstva-ukr.

15. Калюжний Р. А., Цимбалюк В. С. Координація діяльності органів влади у боротьбі з організованою кіберзлочинністю. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2002. № 6. С. 105– 111.

16. Козлов, Д. О. Захист інформації в автоматизованих системах: навч. посіб. / Д. О. Козлов, О. П. Сидоренко. – Київ: НТУУ «КПІ», 2020. – 280 с.

17. Бойченко В. П. Кримінально-правова охорона суспільної моралі в Україні: антропологічний вимір: дис. … канд. юрид. наук: спец.: 12.00.08. Одеса, 2021. 230 с.

18. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р. URL: https://www.kmu.gov.ua/npas/246420577.

19. Про Доктрину інформаційної безпеки України: Указ Президента України від 08.07.2009 р. № 514/2009. URL: https://zakon.rada.gov.ua/laws/card/514/2009.

20. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Гельветика, 2017. 168 с.

21. Довгань О. Д., Ткачук Т. Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. Інформація і право. 2018. № 2 (25). С. 73–85.

22. Золотар О. О. Інформаційна безпека людини: теорія і практика: Монографія. Київ: ТОВ Видавничий дім АртЕк, 2018. 446.

23. Інформаційна безпека. ІТ-словник. URL: http://xn--r1a3b.xn--b1amgblet.xn-j1amh/index.php.

24. Окінавська хартія глобального інформаційного суспільства. URL: https://zakon.rada.gov.ua/laws/show/998_163#Text.

25. Розробка проєкту Концепції кодифікації інформаційного законодавства України. Інформація і право. 2012. № 1. URL:

http://ippi.org.ua/vid-redaktsiinoi-kolegii-rozrobka-proektu-kontseptsii-kodifikatsii informatsiinogo-zakonodavstva-ukr.

26. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 р. № 8073-X. URL: https://zakon.rada.gov.ua/laws/card/80731-10.

27. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 р. «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021р.№ 685/2021.

URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

28. Інформаційна безпека (соціально-правові аспекти): [підручник]. В. Остроухов, В. Петрик, М. Присяжнюк та ін.; за ред. Є. Д. Скулиша. Київ : КНТ, 2010. 776 с.

29. Григор'єв В. І. Технології сучасної інформаційно-психологічної війни. Інформаційна безпека людини, суспільства, держави. 2015. № 3 (19). С. 48–52.

30. Сопілко І. М. Інформаційні загрози та безпека сучасного українського суспільства. Юридичний вісник. 2015. № 1 (34). С.75–80.

31. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: [монография]. Київ: Інтертехнологія, 2009. 164 с.

32. Домбровська С. М. Механізми забезпечення інформаційної безпеки як складової державної безпеки України. Теорія та практика державного управління. 2015. Вип. 1 (48). С. 2–4.

33. Сащук Г. Інформаційна безпека в системі забезпечення 88 національної безпеки. URL: http://journ.univ.kiev.ua/trk/publikacii/satshuk_ publ.php.

34. Пилипчук В. Г., Дзьобань О. П. Проблема агресії і насильства: світоглядно-інформаційний вимір. URL: social-science.com.ua/article/806.

35. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності. Сучасний захист інформації. 2016. № 4. С. 65–70.

36. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об’єктам інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 2 (18). С. 16–22.

37. Живко З. Б., Живко М. О. Інформаційні загрози: суть і проблеми. Тези доповідей ІІ міжнародної НПК «Безпека та захист інформації в 89 інформаційних системах». С. 116–118. Харківський національний економічний університет, 29-30 квітня 2009 року.

38. 3. НД ТЗІ 2.5-005-99. Організація технічного захисту інформації в автоматизованих системах. – Київ: Державна служба спеціального зв’язку та захисту інформації України, 1999. – 28 с.

39. Прокоф’єва-Янчиленко Д. М. Кримінологічна безпека як інтегративна складова національної безпеки. Наукові праці Національного університету «Одеська юридична академія». 2014. № 14: URL: naukovipraci.nuoua.od.ua/tom-xiv.

40. Цивілізаційний вибір України: парадигма осмислення і стратегія дії: [національна доповідь] / ред.кол.: С. Пирожков, О. Майборода, Ю. Шайгородський та ін.; Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. Київ: НАН України, 2016. 284 с.

41. Прозоров А. Ю. Ціннісні основи інформаційної безпеки особи, суспільства та держави. Інформаційна безпека людини, суспільства, держави. 2016. № 1 (20). С. 29–37.

42. Столл, К. Зозуля в кіберпросторі: історія хакера / Кліффорд Столл ; пер. з англ. О. Кравець. – Київ: Видавнича група КМ-Букс, 2018. – 352 с.

43. Таненбаум, Е. Комп’ютерні мережі / Ендрю Таненбаум, Девід Уезеролл ; пер. з англ. І. Іванова. – 5-те вид. – Київ: Форс, 2019. – 960 с.

44. Шопіна І. М. Поняття інформаційної безпеки: концептуальні підходи до визначення. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія Право. 2022. № 13 (25). С. 133–140.

45. Баран М. В. Суб'єкти забезпечення інформаційної безпеки в 87 Україні. Юридичний науковий електронний журнал. 2022. № 6. С. 220–223.

46. Про основи національної безпеки: Закон України від 19.06.2003 р. № 964-IV. URL: https://zakon.rada.gov.ua/laws/card/964-15.

47. Про боротьбу з тероризмом: Закон України від 20.03.2003 р. № 638-IV. URL: https://zakon.rada.gov.ua/laws/card/638-15.

48. Про запобігання корупції: Закон України від 14.10.2014 р. № 1700-VII. URL: https://zakon.rada.gov.ua/laws/card/1700-18.

49. Петренко Л. В., Петренко А. В. Психологічні умови формування «цифрових» компетенцій майбутніх фахівців. Цифрова економіка. Київ: КНЕУ, 215 2018. С. 290–293.

50. Горбулін В. П., Качинський А. П. Засади національної безпеки України: [підручник]. Київ: Інтертехнологія, 2009. 272 с.

ДОДАТКИ

Таблиця А - Дослідження методів протидії загрозам безпеці силами та засобами служб захисту інформації

Категорія загроз	Метод протидії	Основні засоби реалізації	Переваги застосування	Обмеження та ризики
Технічні (кібератаки, несанкціоновани	Програмно-технічний захист	Антивірусні системи, міжмережеві	Висока швидкість виявлення атак,	Потреба постійного оновлення,

й доступ)		екрани, IDS/IPS, SIEM, криптографія	можливість автоматичного блокування загроз	ресурсозатратність
Організаційні (помилки персоналу, порушення політик)	Адміністративний контроль доступу	Регламенти безпеки, розмежування повноважень, аудит безпеки	Формування культури відповідальності та превентивного контролю	Залежність від людського фактора, потреба постійного навчання
Інформаційно-психологічні (фейкові кампанії, маніпуляції)	OSINT і SOCMINT-моніторинг	Аналіз соцмереж, розпізнавання фейків, протидія дезінформації	Виявлення впливів на суспільну думку, збереження інформаційної стійкості	Висока складність аналізу, потреба у фахівцях
Інсайдерські загрози	Zero Trust і контроль поведінки	МФА, привілейований доступ, поведінкова аналітика	Зменшення впливу внутрішніх порушень, підвищення прозорості доступів	Потребує складної архітектури та змін у організації
Комплексні APT-атаки	Threat Intelligence і кіберрозвідка	Збір індикаторів компрометації та взаємодія CERT/SOC	Випередження атак, виявлення противника ще на етапі планування	Необхідність масштабних інвестицій та експертних кадрів

ДОДАТОК В

Презентація В - «Дослідження методів протидії загрозам безпеці силами та засобами служб захисту інформації»

Структура дослідження

01
Вступ
Актуальність, мета та завдання дослідження

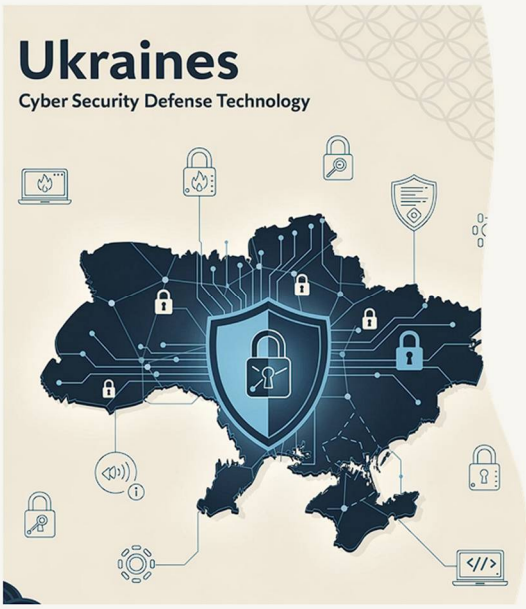
02
Розділ 1
Основні поняття та визначення захисту інформації

03
Розділ 2
Методи та засоби протидії загрозам

04
Розділ 3
Удосконалення системи протидії

05
Завершення
Висновки, список джерел та додатки

Дослідження охоплює теоретичні основи інформаційної безпеки, практичні методи захисту та рекомендації щодо вдосконалення систем протидії сучасним кіберзагрозам в умовах української дійсності.



Актуальність дослідження

Сучасні виклики кібербезпеки

Україна стикається з безпрецедентними викликами у сфері інформаційної безпеки. Поєднання зовнішньої агресії та внутрішніх загроз створює складне середовище, де захист цифрових активів стає питанням національної безпеки.

Зростання кібератак призводить до мільярдних збитків щороку. За даними міжнародних досліджень, вартість глобальних кіберзлочинів сягає трильйонів доларів, а Україна залишається однією з найбільш атакованих країн світу.

Критичність захисту даних

Захист інформації сьогодні дорівнює захисту життя громадян. Персональні дані, фінансова інформація та корпоративні секрети потребують надійного захисту на всіх рівнях.

Ключові сектори:

- Підприємства та бізнес-структури
- Державні установи та уряд
- Військові та оборонні системи
- Освітні та наукові організації

Мета дослідження

Аналіз принципів захисту
Детальне дослідження фундаментальних принципів та методів захисту інформації в контексті сучасних загроз та викликів

Цілісний підхід до безпеки
Формування комплексного підходу до зменшення ризиків у сфері кібербезпеки через інтеграцію різних методів та технологій

Практичні рекомендації
Розробка конкретних рекомендацій для підвищення стійкості інформаційних систем на основі проведеного аналізу

Це дослідження спрямоване на створення науково обґрунтованої методології захисту інформації, яка враховує як теоретичні аспекти, так і практичні потреби організацій у сучасному цифровому середовищі.

Завдання дослідження

1

Теоретичні основи

Вивчити фундаментальні визначення та концепції захисту інформації відповідно до національних та міжнародних стандартів

2

Політики безпеки

Розглянути існуючі методи та приклади політик інформаційної безпеки в різних організаційних контекстах

3

Моделі загроз

Проаналізувати сучасні моделі загроз та відповідні методи захисту інформаційних систем

4

Практичний аналіз

Провести детальний аналіз реальних загроз, індикаторів компрометації та оцінити ефективність систем захисту

Об'єкт і предмет дослідження

Об'єкт дослідження

Об'єктом дослідження виступають **інформаційні системи** в їх цілісності та різноманітті.

- Активні методи захисту інформації
- Пасивні методи захисту інформації
- Організаційна структура та функціонування служби захисту інформації
- Технічні та програмні засоби забезпечення безпеки

Предмет дослідження

Предметом виступають **методи та механізми** роботи зловмисників у кіберпросторі.

- Тактики кібератак та їх еволюція
- Технічні прийоми проникнення в системи
- Процедури та алгоритми атак
- Поведінкові патерни порушників

Розуміння як об'єкта, так і предмета дослідження дозволяє сформувати комплексний підхід до захисту інформації, враховуючи як технічні аспекти систем, так і методологію потенційних загроз.

Наукова новизна та практична значимість

Наукова новизна

Дослідження пропонує інноваційний підхід до впровадження досвіду служби захисту інформації в адаптивну комплексну систему безпеки. Новизна полягає в інтеграції теоретичних моделей з практичним досвідом реагування на реальні інциденти, що дозволяє створити динамічну систему захисту, здатну адаптуватися до нових загроз.

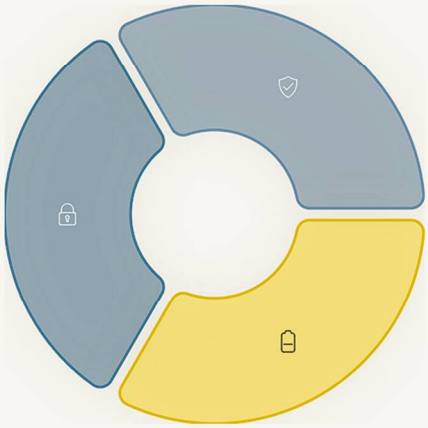
Практична значимість

Результати дослідження мають безпосереднє практичне застосування для удосконалення систем захисту інформації в організаціях різного масштабу. Розроблені рекомендації та методології можуть бути впроваджені в державних установах, комерційних підприємствах та освітніх закладах для підвищення рівня кібербезпеки.

Практична цінність роботи посилюється можливістю адаптації запропонованих рішень до специфічних потреб різних секторів економіки та державного управління в умовах підвищених кіберзагроз.

Основні поняття захисту інформації

Захист інформації визначається як сукупність заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів. Нормативна база України (НД ТЗІ, Закон "Про державну таємницю") та міжнародні стандарти (ISO/IEC 27001) встановлюють єдині принципи та вимоги до систем захисту.



Конфіденційність

Забезпечення доступу до інформації лише авторизованим користувачам

Цілісність

Захист інформації від несанкціонованої зміни або знищення

Доступність

Гарантування своєчасного доступу до інформації для авторизованих користувачів

Таблиця 1.1 містить детальну характеристику основних властивостей інформації, включаючи критерії оцінки кожної з трьох складових безпеки та методи їх забезпечення в різних організаційних контекстах.

Класифікація загроз інформаційній безпеці

Типологія загроз

Загрози інформаційній безпеці класифікуються за різними критеріями залежно від їх походження та характеру впливу:

- **Природні** — стихійні лиха, форс-мажор
- **Техногенні** — аварії інфраструктури
- **Технічні** — відмови обладнання
- **Організаційні** — помилки в управлінні
- **Людські** — помилки персоналу
- **Навмисні** — цілеспрямовані атаки

> Навмисні загрози визначаються як найнебезпечніші через їх цілеспрямований характер, високий рівень технічної складності та потенційно катастрофічні наслідки для організації.

Таблиця 1.2 у дослідженні представляє детальну класифікацію загроз із зазначенням конкретних методів протидії для кожного типу, що дозволяє формувати комплексну стратегію захисту.

Типи кібератак

Мережеві атаки

- Прослуховування трафіку (sniffing)
- IP-spoofing та підміна адрес
- Атаки типу "людина посередині" (MITM)

Атаки на доступність

- Відмова в обслуговуванні (DoS)
- Розподілена відмова (DDoS)
- Атаки на паролі та автентифікацію

Веб-атаки

- SQL-ін'єкції в бази даних
- Міжсайтовий скриптинг (XSS)
- Підробка міжсайтових запитів

Шкідливе програмне забезпечення

- Віруси та черв'яки
- Троянські програми
- Програми-вимагачі (ransomware)

Модель порушника та оцінка ризиків

Характеристика порушника

Модель порушника є фундаментальним інструментом для розуміння потенційних загроз. Ключовими характеристиками порушника виступають його мотивація (фінансова вигода, шпигунство, саботаж), технічні можливості (від базових до експертних) та доступні ресурси (час, обладнання, знання).

Мотивація

Визначення цілей та інтересів потенційного зловмисника

Можливості

Оцінка технічного рівня та доступних інструментів

Ресурси

Аналіз часових, фінансових та технічних ресурсів

Методологія оцінки ризиків

Згідно зі стандартом ISO/IEC 27005, оцінка ризиків проводиться за допомогою якісних та кількісних методів. Якісні методи використовують експертні оцінки та категорії ризику, тоді як кількісні методи базуються на статистичних даних та фінансових показниках. **Таблиця 1.3** демонструє практичний приклад моделі ризиків з конкретними сценаріями загроз та їх імовірністю.

Політика інформаційної безпеки

Політика інформаційної безпеки є основоположним документом, що визначає правила, процедури та відповідальність за захист інформаційних активів організації. Ефективна політика охоплює всі аспекти безпеки від класифікації даних до реагування на інциденти.

Класифікація інформації

Розподіл даних за рівнями конфіденційності: таємна, конфіденційна, службова, відкрита інформація з відповідними правилами обробки

Модель загроз

Систематичний аналіз потенційних ризиків та вразливостей з розробкою превентивних заходів та планів реагування

Управління інцидентами

Встановлення процедур виявлення, реагування та аналізу інцидентів безпеки з метою мінімізації їх впливу

Принцип найменших привілеїв

Надання користувачам мінімально необхідних прав доступу для виконання їх службових обов'язків

Моніторинг та контроль

Впровадження SIEM-систем для централізованого збору та аналізу подій безпеки в режимі реального часу

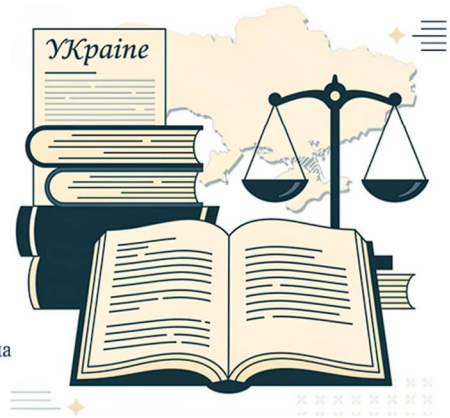
Людський фактор та правові аспекти

Роль людського фактора

Статистика свідчить, що помилки персоналу становлять приблизно **40% всіх інцидентів** інформаційної безпеки. Це підкреслює критичну важливість людського чинника в загальній системі захисту.

Ключові заходи:

- Регулярне навчання співробітників основам кібербезпеки
- Формування культури безпеки в організації
- Симуляція фішингових атак для підвищення обізнаності
- Чіткі політики використання корпоративних ресурсів



Правова база України

Основні законодавчі акти:

- Закон України "Про державну таємницю"
- Закон "Про захист інформації в інформаційно-телекомунікаційних система
- Стратегія кібербезпеки України
- Доктрина інформаційної безпеки

Організаційні заходи захисту інформації

Організаційні заходи становлять фундамент комплексної системи захисту інформації, забезпечуючи правову та процедурну основу для технічних рішень.

Нормативно-правова база

Розробка внутрішніх політик, регламентів та інструкцій відповідно до законодавства України

Кадрова політика

Підбір кваліфікованого персоналу, навчання та підвищення кваліфікації фахівців

Управління доступом

Впровадження систем ідентифікації, автентифікації та розмежування прав доступу

Внутрішній контроль

Регулярний аудит систем безпеки та перевірка дотримання політик організації

Таблиця 2.1 в дослідженні детально розкриває організаційні заходи протидії загрозам, включаючи конкретні процедури, відповідальних осіб та показники ефективності кожного заходу в різних організаційних сценаріях.

Програмно-технічні засоби захисту

Антивірусне ПЗ
Виявлення та нейтралізація шкідливих програм

Міжмережеві екрани
Контроль мережевого трафіку та фільтрація загроз

IDS/IPS системи
Виявлення та запобігання вторгненням

Криптографія
Шифрування даних для захисту конфіденційності

DLP-системи
Запобігання витоку конфіденційної інформації

Переваги автоматизації

- Швидке виявлення загроз у реальному часі
- Зниження впливу людського фактора
- Масштабованість та адаптивність
- Централізоване управління безпекою

Обмеження та виклики

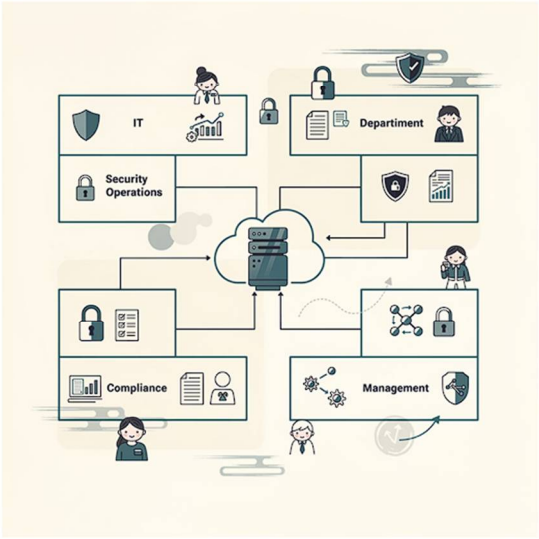
- Потреба в регулярному оновленні
- Вимоги до кваліфікації персоналу
- Фінансові інвестиції
- Складність інтеграції різних систем

Ефективний захист інформації досягається лише через комплексне поєднання організаційних, правових та технічних заходів, що створює багаторівневу систему безпеки, здатну протистояти сучасним кіберзагрозам.

Інтеграція організаційних і технічних компонентів захисту

Сучасна комплексна система протидії кіберзагрозам базується на синергетичній взаємодії організаційних процедур та технологічних рішень. Цей підхід формує єдиний захисний периметр, здатний адаптуватися до мінливого ландшафту загроз.

Організаційна складова включає розробку політик безпеки, процедур реагування на інциденти, навчання персоналу та формування культури кібергігієни. Технічна складова охоплює впровадження засобів захисту периметру, систем моніторингу, шифрування та контролю доступу.



Багатошарова оборона та управління інцидентами

Периметр мережі

Міжмережеві екрани, системи запобігання вторгненням (IPS), захист від DDoS-атак

Внутрішня мережа

Сегментація, мікросегментація, VLAN, контроль доступу до ресурсів

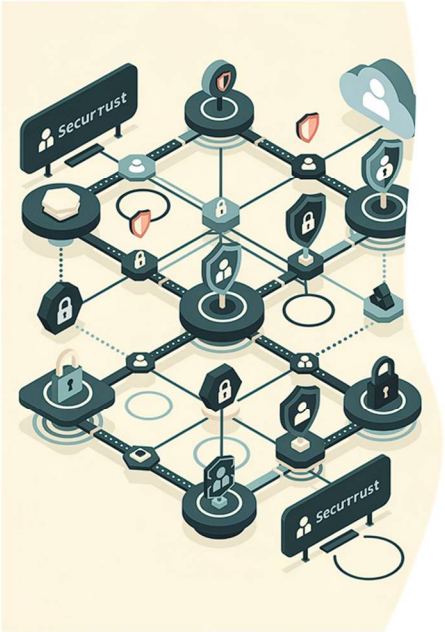
Рівень застосунків

WAF, захист API, моніторинг поведінки додатків, аналіз уразливостей

Дані та ідентичність

Шифрування, DLP, багатофакторна автентифікація, управління привілеями

Управління інцидентами передбачає чітку процедуру виявлення, аналізу, локалізації, усунення загроз та відновлення систем. Ефективність залежить від швидкості реагування та координації між підрозділами.



Принцип Zero Trust: Довіряй, але перевіряй завжди

01

Ідентифікація

Суворе встановлення особи користувача чи пристрою перед наданням доступу

02

Верифікація контексту

Аналіз геолокації, часу, пристрою та поведінкових патернів

03

Мінімальні привілеї

Надання лише необхідного рівня доступу для виконання конкретних завдань

04

Безперервний моніторинг

Постійна перевірка легітимності сесії та виявлення аномальної активності

Філософія Zero Trust визнає, що загрози можуть походити як із зовнішнього, так і з внутрішнього периметру. Тому кожен запит перевіряється незалежно від його походження, що значно підвищує рівень захищеності критичних ресурсів.

Недоліки реактивного підходу та відставання від стандартів

Проблеми традиційної моделі

Аналіз сучасної практики захисту інформаційних систем в Україні виявляє критичні недоліки реактивного підходу. Організації часто реагують на інциденти вже після їх виникнення, що призводить до значних фінансових втрат та репутаційних ризиків.

Брак прогнозування та превентивних заходів залишає системи вразливими до нових типів атак. Відсутність постійного моніторингу та аналізу поведінкових патернів не дозволяє виявляти загрози на ранніх стадіях.

NATO CCDCOE

Стандарти колективної кіберзахисту та обміну інформацією про загрози

NIS2 Directive ЄС

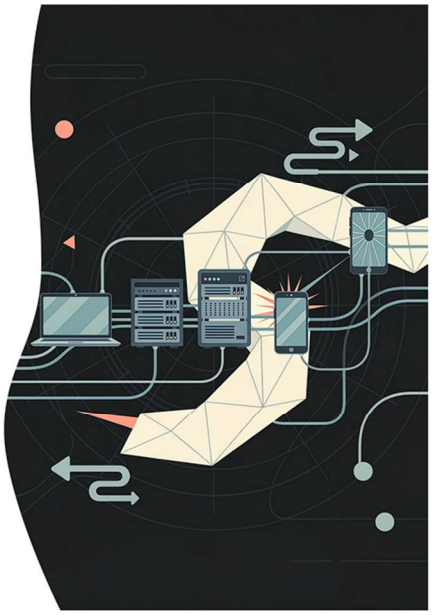
Вимоги до критичної інфраструктури та рівня кіберстійкості

APT-атаки як основна загроза національній безпеці

Складні цілеспрямовані кібератаки (Advanced Persistent Threats) становлять найбільшу загрозу для державних установ та критичної інфраструктури України. Ці багатоетапні операції характеризуються високим рівнем технічної складності, довготривалим періодом присутності в системах жертви та орієнтацією на крадіжку конфіденційної інформації.

1. **Розвідка**
   Збір інформації про цілі, вразливості, структуру мережі
2. **Проникнення**
   Використання фішингу, експлойтів, zero-day уразливостей
3. **Закріплення**
   Створення backdoor, підвищення привілеїв, латеральне переміщення
4. **Ексфільтрація**
   Витягування даних, приховування слідів діяльності

Gamaredon (також відома як Armageddon або Shuckworm) – кібергрупа, яка з 2013 року здійснює систематичні атаки проти українських державних установ, військових та критичної інфраструктури. Характеризується використанням простих, але ефективних інструментів та високою частотою атак.



Впровадження сучасних технологій моніторингу

SIEM-системи

Централізований збір та кореляційний аналіз подій безпеки з різних джерел для виявлення складних багатоетапних атак

Threat Intelligence

Проактивне прогнозування загроз на основі аналізу індикаторів компрометації, тактик зловмисників та глобальних трендів

OSINT/SOCMINT

Моніторинг відкритих джерел та соціальних медіа для виявлення витоків даних, планів атак та репутаційних загроз

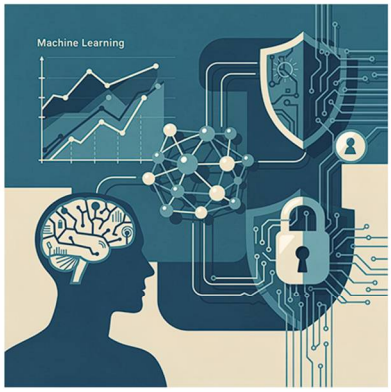
Інтеграція цих технологій створює всеохоплюючу систему безпеки, здатну не лише реагувати на інциденти, але й передбачати їх виникнення на основі аналізу патернів та контекстуальної інформації.

Штучний інтелект та машинне навчання у кіберзахисті

Трансформація підходів до виявлення загроз

Впровадження технологій машинного навчання революціонізує сферу кібербезпеки, дозволяючи автоматизувати процеси виявлення аномалій, аналізу великих обсягів даних та прогнозування потенційних атак.

Алгоритми навчаються розпізнавати нормальні поведінкові патерни користувачів та систем, що дає змогу виявляти відхилення, які можуть свідчити про компрометацію. Це особливо ефективно проти невідомих загроз, для яких не існує сигнатур.



Збір даних
Агрегація логів, метрик, поведінкових індикаторів

Навчання моделей
Supervised та unsupervised learning для класифікації

Виявлення аномалій
Реал-тайм аналіз та автоматичне оповіщення

Самонавчання
Адаптація до нових загроз та зменшення false-positive

SOC-центри та CERT-UA: Національна система реагування

Security Operations Center (SOC) – спеціалізовані підрозділи, які здійснюють цілодобовий моніторинг кіберзагроз, аналіз інцидентів та координацію реагування. В Україні функціонує Команда реагування на комп'ютерні надзвичайні події України (CERT-UA), яка відіграє ключову роль у захисті державних інформаційних ресурсів.

Моніторинг 24/7
Безперервне спостереження за станом систем та виявлення інцидентів

Аналіз загроз
Дослідження методів атак, малвару, індикаторів компрометації

Реагування
Координація заходів локалізації, усунення загроз та відновлення

Обмін інформацією
Поширення знань про актуальні загрози серед стейкхолдерів

CERT-UA регулярно публікує попередження про нові кампанії, аналіз шкідливого ПЗ та рекомендації щодо захисту. Співпраця між державними SOC-центрами, приватним сектором та міжнародними партнерами посилює загальну кіберстійкість країни.

Таблиця 3.2: Ключові технології кіберзахисту

Технологія	Функціональність	Значення для національної безпеки
SIEM	Збір, кореляція та аналіз подій безпеки в реальному часі	Централізоване виявлення складних атак на критичну інфраструктуру
Zero Trust	Архітектура безперервної верифікації без довіри за замовчуванням	Захист від insider threats та латерального переміщення APT
Threat Intelligence	Збір, обробка та аналіз інформації про актуальні загрози	Проактивне прогнозування атак державного рівня
AI/ML аналіз	Автоматичне виявлення аномалій та невідомих загроз	Протидія zero-day експлойтам та швидкоеволюціонуючому малвару
SOC/CERT	Централізований моніторинг та координація реагування	Швидка ідентифікація та нейтралізація масштабних кібератак
Шифрування	Криптографічний захист даних у спокої та передачі	Забезпечення конфіденційності державної таємниці та персональних даних

Джерело: Складено на основі аналізу [45] та міжнародних стандартів кіберзахисту NATO, NIST, ISO 27001

Рекомендації щодо підвищення рівня кібербезпеки

Вдосконалення нормативної бази

Гармонізація національного законодавства з директивами ЄС (NIS2, GDPR), оновлення стандартів захисту інформації, розробка галузевих вимог для критичної інфраструктури

Створення мережі SOC-центрів

Розбудова регіональних центрів кіберзахисту, інтеграція з CERT-UA, впровадження єдиної платформи обміну інформацією про загрози між державним та приватним секторами

Освіта та культура безпеки

Систематичне навчання персоналу сучасним загрозам, симуляція кібератак, формування свідомого підходу до кібергігієни, сертифікація фахівців за міжнародними стандартами

Таблиця 3.3: Комплекс рекомендацій за напрямами

Напрям	Конкретні заходи	Очікуваний ефект
Нормативний	• Прийняття Закону про кіберзахист критичної інфраструктури • Імплементація стандартів ISO 27001/27032 • Розробка галузевих регуляторних вимог	Чітка правова база, відповідальність операторів, сумісність з ЄС
Технологічний	• Впровадження SIEM та Threat Intelligence платформ • Розгортання AI-based систем виявлення • Міграція до Zero Trust архітектури	Підвищення швидкості виявлення на 70%, зменшення часу реагування
Організаційний	• Створення 5 регіональних SOC-центрів • Запуск національної платформи обміну IoC • Формування кіберрезерву	Покриття всієї території, координація зусиль, швидке масштабування
Освітній	• Обов'язкове навчання держслужбовців • Створення кіберполігонів • Національна програма кіберграмотності	Зменшення людського фактору на 50%, формування кадрового резерву

Джерело: Розроблено на основі аналізу [47] та досвіду країн-членів NATO

Партнерство та цифровий суверенітет

Тристороння модель співпраці

Ефективна кібербезпека вимагає синергії між державою, бізнесом та науковою спільнотою. Держава забезпечує регуляторну базу та координацію, бізнес надає технологічні рішення та експертизу, наукові установи розробляють інноваційні методи захисту.

- Локалізація критичних сервісів

  Розгортання ключових елементів інфраструктури на національній території для зменшення залежності від іноземних постачальників
- Медіаграмотність населення

  Підвищення здатності громадян розпізнавати дезінформацію, фішинг та маніпуляції у цифровому просторі

Цифровий суверенітет передбачає контроль над власними даними, критичними технологіями та інфраструктурою. Це не ізоляція, а збалансований підхід до міжнародної співпраці з одночасним захистом національних інтересів.

Наукові та практичні результати дослідження

Узагальнено та систематизовано **досвід діяльності служб захисту інформації** в автоматизованих системах з урахуванням сучасних загроз інформаційній безпеці.

Обґрунтовано необхідність **інтеграції організаційних, технічних та аналітичних заходів** у єдину керовану модель протидії загрозам.

Запропоновані рекомендації сприяють:
•підвищенню ефективності роботи служб захисту інформації;
•зниженню ризиків несанкціонованого доступу;
•підвищенню керованості процесів інформаційної безпеки.

Запропоновано **адаптивний підхід до побудови комплексної системи захисту інформації**, здатної оперативно реагувати на зміну тактик, технік і процедур зловмисників.

Розкрито роль **проактивних механізмів аналізу загроз** як ключового чинника підвищення стійкості інформаційних систем.

Матеріали роботи можуть бути використані:
•у практичній діяльності фахівців з кібербезпеки;
•під час розроблення внутрішніх політик безпеки;
•у навчальному процесі за спеціальністю «Кібербезпека та захист інформації».

Результати дослідження можуть бути використані для **удосконалення існуючих систем захисту інформації** в організаціях різних форм власності.