НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНІЧНІ ІНСТРУМЕНТИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Балагула Борис Борисович

Керівник: к.ф.-м.н., доцент,
Черевко Євген Володимирович

Рецензент: к.т.н., доцент
Кухаренко Сергій Вікторович

Одеса – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Балагула Борису Борисовичу

1. Тема роботи: «Технічні інструменти протидії кіберзлочинності»
Керівник роботи: к.ф.-м.н., доцент Черевко Євген Володимирович
затверджені наказом НУ ОЮА від 18 березня 2025 року № 548-6
2. Строк подання здобувачем роботи 19 травня 2025 рік
3. Дата видачі завдання 16 вересня 2024 рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Аналіз предметної області та пошук науково-технічної інформації за темою роботи	Вересень-жовтень 2024	
2	Узгодження теми з науковим керівником, формулювання мети завдань дослідження	Листопад 2024	
3	Робота над першим розділом	Листопад-грудень 2024	
4	Робота над другим розділом	Січень-лютий 2025	
5	Робота над третім розділом	Лютий-березень 2025	
6	Уточнення подальшого обсягу роботи та його коригування	Березень-травень 2025	
7	Оформлення звітної частини	Травень 2025	
8	Захист роботи	12.06.2025	

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Технічні інструменти протидії кіберзлочинності» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 2 рисунка, 4 таблиці та 20 літературних джерела за переліком посилань. Робота виконана на 45 сторінках загального тексту, з яких 37 сторінки основного тексту.

Метою роботи є аналіз кіберзлочинності, її наслідків, нормативно-правової бази та технічних інструментів протидії, а також розробка рекомендацій щодо їх вдосконалення. У дослідженні систематизовано класифікацію кіберзлочинів, проаналізовано їхні економічні, соціальні та безпекові наслідки, розглянуто міжнародні та національні нормативно-правові акти. У практичній частині оцінено ефективність антивірусних комплексів, систем виявлення та запобігання вторгненням (IDS/IPS), систем управління інформацією та подіями безпеки (SIEM), технологій шифрування та багатофакторної аутентифікації. Проведено аналіз кейсів успішного та невдалого застосування цих інструментів, а також досліджено перспективи їх розвитку на основі штучного інтелекту та машинного навчання.

Результати роботи можуть бути використані для підвищення безпеки інформаційних систем організацій, оптимізації реагування на кіберзагрози та розробки програм підвищення кіберграмотності. Вони також мають цінність для IT-фахівців, менеджерів з кібербезпеки та розробників систем захисту.

Можливими напрямами подальших досліджень є розробка адаптивних систем захисту на основі штучного інтелекту, створення постквантових криптографічних алгоритмів та вдосконалення нормативно-правової бази для протидії новим видам кіберзлочинів.

КІБЕРЗЛОЧИННІСТЬ, КІБЕРБЕЗПЕКА, АНТИВІРУСНІ КОМПЛЕКСИ, IDS/IPS, SIEM, ШИФРУВАННЯ, БАГАТОФАКТОРНА АУТЕНТИФІКАЦІЯ, ШТУЧНИЙ ІНТЕЛЕКТ, МАШИННЕ НАВЧАННЯ.

ABSTRACT

The bachelor's thesis on the topic "Technical Tools for Countering Cybercrime" for obtaining the first (bachelor's) level of higher education in specialty 125 Cybersecurity, educational program: Cybersecurity, includes 2 figures, 4 tables and 20 literary sources listed in the references. The work comprises 45 pages of total text, with 37 pages of main content.

The purpose of the thesis is to analyze cybercrime, its consequences, legal framework, and technical tools for countering it, as well as to develop recommendations for their improvement. The study systematizes the classification of cybercrimes, examines their economic, social, and security implications, and reviews international and national legal regulations. The practical part evaluates the effectiveness of antivirus complexes, intrusion detection and prevention systems (IDS/IPS), security information and event management systems (SIEM), encryption technologies, and multi-factor authentication. An analysis of successful and unsuccessful case studies of these tools' application is conducted, alongside an exploration of their development prospects based on artificial intelligence and machine learning.

The results of the work can be used to enhance the security of organizations' information systems, optimize responses to cyber threats, and develop cybersecurity awareness programs. They are also valuable for IT specialists, cybersecurity managers, and developers of security systems.

Potential directions for future research include the development of adaptive security systems based on artificial intelligence, the creation of post-quantum cryptographic algorithms, and the improvement of the legal framework to address new types of cybercrimes.

CYBERCRIME, CYBERSECURITY, ANTIVIRUS COMPLEXES, IDS/IPS, SIEM, ENCRYPTION, MULTI-FACTOR AUTHENTICATION, ARTIFICIAL INTELLIGENCE, MACHINE LEARNING.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному цифровому середовищі кіберзлочинність становить одну з найсерйозніших загроз для організацій, державних установ і окремих користувачів. Зростання кількості кібератак, таких як фішинг, зловмисне програмне забезпечення, атаки на відмову в обслуговуванні (DDoS) та соціальна інженерія, спричинене швидким розвитком інформаційних технологій і глобалізацією цифрового простору. Традиційні методи захисту, такі як базові антивіруси чи фізичні фаєрволи, часто виявляються недостатньо ефективними проти складних і багатокомпонентних кіберзагроз. Технічні інструменти протидії кіберзлочинності, включаючи системи виявлення вторгнень, аналітику поведінки користувачів і шифрування, відіграють ключову роль у забезпеченні безпеки інформаційних систем. Актуальність теми зумовлена необхідністю розробки та вдосконалення таких інструментів для протистояння постійно еволюціонуючим загрозам, а також зростанням вимог до кібербезпеки в умовах цифрової трансформації економіки та суспільства. Дослідження технічних інструментів протидії кіберзлочинності є важливим для створення стійких і адаптивних систем захисту, які здатні ефективно реагувати на сучасні виклики.

Мета дослідження – розробка теоретичних основ і практичних рекомендацій щодо використання технічних інструментів для протидії кіберзлочинності в інформаційних системах організацій, з метою підвищення їхньої безпеки, ефективності реагування на загрози та зниження ризиків кібератак. Для досягнення мети поставлено такі завдання:

- розробити класифікацію кіберзлочинів за типами, методами здійснення та цілями, навівши приклади для кожної категорії;
- проаналізувати соціально-економічні та технологічні наслідки кіберзлочинності для окремих користувачів, організацій та держави;
- систематизувати основні міжнародні та національні нормативно-правові акти, що регулюють протидію кіберзлочинності, та оцінити їх актуальність;

− провести порівняльний аналіз трьох популярних антивірусних комплексів, оцінивши їх ефективність у виявленні та нейтралізації шкідливого програмного забезпечення;

− описати принципи роботи систем виявлення та запобігання вторгнень (IDS/IPS) і оцінити їх роль у забезпеченні безпеки інформаційних систем;

− дослідити сучасні технології шифрування та багатофакторної аутентифікації, визначивши їх переваги та обмеження в захисті даних;

− розробити методику оцінки ефективності технічних засобів протидії кіберзлочинності на основі критеріїв швидкості реагування, точності виявлення та рівня автоматизації;

− проаналізувати два кейси (один успішний і один невдалий) застосування технічних інструментів протидії кіберзлочинності, визначивши ключові фактори успіху чи провалу;

− спрогнозувати перспективи розвитку технічних інструментів протидії кіберзлочинності на основі штучного інтелекту та машинного навчання, оцінивши їх потенційний вплив на безпеку.

Об’єкт дослідження – процеси забезпечення інформаційної безпеки в умовах кіберзлочинності, що включають виявлення, запобігання та реагування на кібератаки в інформаційних системах.

Предмет дослідження – технічні інструменти протидії кіберзлочинності, включаючи антивірусні системи, системи виявлення та запобігання вторгненням, моніторинг безпеки, а також технології шифрування та аутентифікації, що застосовуються для захисту даних і систем.

Практичне значення отриманих результатів. Результати дослідження мають практичну цінність для організацій, які прагнуть підвищити рівень захисту своїх інформаційних систем від кіберзлочинності. Запропоновані рекомендації щодо використання технічних інструментів, таких як IDS/IPS, SIEM, шифрування та багатофакторна аутентифікація, дозволяють оптимізувати процеси виявлення та реагування на кіберзагрози, а також знизити ризики витоків даних і фінансових втрат. Результати можуть бути використані ІТ-фахівцями, менеджерами з

кібербезпеки та розробниками систем безпеки для впровадження ефективних рішень у корпоративних і державних структурах. Крім того, рекомендації щодо інтеграції перспективних технологій, таких як штучний інтелект, сприятимуть створенню адаптивних систем захисту, здатних протистояти новим видам кібератак.

1 ТЕОРЕТИЧНІ ОСНОВИ КІБЕРЗЛОЧИННОСТІ ТА НЕОБХІДНІСТЬ ЇЇ ПРОТИДІЇ

1.1 Поняття та класифікація кіберзлочинності

Кіберзлочинність є складним і багатогранним явищем, що охоплює протиправні дії, вчинені з використанням інформаційно-комунікаційних технологій або спрямовані проти них. Цей вид злочинності характеризується високим рівнем технічної складності, що вимагає від зловмисників спеціальних знань і навичок. Крім того, кіберзлочини часто мають транскордонний характер, оскільки цифрове середовище не обмежується географічними кордонами, що значно ускладнює їх виявлення, розслідування та притягнення винних до відповідальності. Анонімність, яку забезпечують сучасні технології, також сприяє зростанню кіберзлочинності, дозволяючи зловмисникам приховувати свою особу та місце перебування.

Сутність кіберзлочинності полягає в тому, що цифрове середовище виступає як інструмент для вчинення злочину, так і об’єкт посягання. Наприклад, зловмисники можуть використовувати комп’ютерні системи для викрадення конфіденційної інформації, здійснення фінансових махінацій або порушення роботи критичної інфраструктури. Водночас інформаційні системи та дані стають мішенню атак, що спрямовані на їх знищення, модифікацію чи блокування. Такі дії можуть мати серйозні економічні, соціальні та навіть політичні наслідки, що підкреслює необхідність комплексної протидії цьому явищу [1].

Кіберзлочинність охоплює широкий спектр правопорушень, які постійно еволюціонують разом із розвитком технологій. Це явище не обмежується лише технічними аспектами, оскільки часто включає психологічні та соціальні методи впливу, такі як соціальна інженерія, спрямована на маніпулювання поведінкою людей для отримання доступу до їхніх даних або ресурсів. Зростання популярності інтернету речей, хмарних технологій і штучного інтелекту відкриває нові можливості для зловмисників, що робить кіберзлочинність однією з ключових загроз сучасного світу.

Для систематизації кіберзлочинів їх класифікують за кількома критеріями, що дозволяє краще зрозуміти їхню природу та розробити ефективні заходи протидії. Основні категорії кіберзлочинів включають:

1. Злочини проти конфіденційності, цілісності та доступності даних: це, зокрема, несанкціонований доступ до інформації, викрадення особистих даних або зміна інформації в базах даних.

2. Злочини проти комп'ютерних систем і мереж: сюди входять хакерські атаки, спрямовані на порушення роботи серверів, мереж або пристроїв.

3. Фінансові злочини: включають онлайн-шахрайство, фішинг, крадіжку банківських даних і незаконні транзакції.

4. Поширення шкідливого програмного забезпечення: створення та розповсюдження вірусів, троянів, програм-вимагачів тощо.

5. Злочини, пов'язані з контентом: розповсюдження незаконного контенту, такого як матеріали, що пропагують насильство чи дискримінацію.

6. Кібертероризм і кібершпигунство: дії, спрямовані на дестабілізацію державних чи корпоративних структур, викрадення секретної інформації або вплив на політичні процеси [2].

Кожен із цих типів злочинів має свої особливості, що впливають на методи їх вчинення та наслідки. Наприклад, фішинг часто базується на психологічній маніпуляції, тоді як атаки програм-вимагачів вимагають високого рівня технічної підготовки. Крім того, кіберзлочини можуть мати різні мотиви: від фінансової вигоди до політичного чи ідеологічного впливу. Наприклад, хакерські угруповання можуть атакувати урядові сайти для висловлення протесту, тоді як кібершахраї зосереджуються на викраденні грошей через фальшиві платіжні системи.

Розуміння природи кіберзлочинності є основою для формування ефективних стратегій її протидії. Оскільки технології постійно розвиваються, зловмисники адаптують свої методи, створюючи нові види загроз, такі як атаки на автономні транспортні системи чи розумні міста. Це вимагає не лише вдосконалення технічних засобів захисту, але й розвитку правової бази, яка б відповідала сучасним викликам. Міжнародна співпраця також відіграє важливу роль, адже кіберзлочини

часто мають глобальний масштаб, і їх розслідування потребує координації між правоохоронними органами різних країн.

Ефективна протидія кіберзлочинності передбачає комплексний підхід, що включає превентивні заходи, такі як підвищення кіберграмотності населення, розробку безпечного програмного забезпечення та впровадження сучасних систем захисту даних. Крім того, важливим є вдосконалення законодавства, яке б чітко визначало відповідальність за кіберзлочини та забезпечувало механізми їхнього розслідування. Нарешті, протидія кіберзлочинності неможлива без активної участі приватного сектору, який розробляє технології та сервіси, що стають об’єктами атак.

Кіберзлочинність є динамічним і багатогранним явищем, яке потребує постійного аналізу та адаптації стратегій протидії. Її класифікація допомагає систематизувати знання про це явище, тоді як глибоке розуміння її природи дозволяє розробляти ефективні інструменти для захисту цифрового простору.

1.2 Наслідки кіберзлочинності

Кіберзлочинність становить значну загрозу для сучасного суспільства, впливаючи на економіку, безпеку, соціальну стабільність і навіть психологічний стан людей. Її наслідки є багатогранними, охоплюючи індивідуальний, корпоративний і державний рівні. Зі стрімким розвитком цифрових технологій масштаби та складність цих наслідків лише зростають, що робить проблему кіберзлочинності однією з найактуальніших у світі.

Економічні наслідки кіберзлочинності є одними з найбільш відчутних. Компанії зазнають прямих фінансових втрат через крадіжку коштів, шахрайство або атаки програм-вимагачів, які блокують доступ до систем і вимагають викуп. Наприклад, атаки на банківські установи чи платіжні платформи можуть призвести до втрати мільйонів гривень, що впливає не лише на організації, але й на їхніх клієнтів. Окрім прямих збитків, бізнес стикається з непрямими витратами, такими як витрати на відновлення систем, посилення кібербезпеки та втрата клієнтської

довіри. Для окремих осіб кіберзлочини, як-от фішинг або крадіжка даних кредитних карток, можуть спричинити втрату особистих заощаджень і тривалі фінансові труднощі [3].

Безпека даних є ще однією сферою, що страждає від кіберзлочинності. Витік конфіденційної інформації, такої як персональні дані, комерційні таємниці чи державні секрети, може мати довгострокові наслідки. На індивідуальному рівні це загрожує шантажем або крадіжкою особи. Для компаній втрата інтелектуальної власності чи клієнтських даних підриває їхню конкурентоспроможність на ринку. На державному рівні кібершпигунство, спрямоване на викрадення інформації про критичну інфраструктуру чи військові розробки, створює загрозу національній безпеці.

Поширення дезінформації, маніпулятивного контенту чи пропаганди через кібератаки може дестабілізувати суспільство. Наприклад, втручання в інформаційні системи під час виборів здатне маніпулювати громадською думкою та підірвати довіру до демократичних процесів. Крім того, кіберзлочини, пов’язані з незаконним контентом, таким як матеріали, що пропагують насильство чи дискримінацію, сприяють деградації моральних і етичних норм.

Порушення роботи енергетичних мереж, транспортних систем, медичних закладів чи систем водопостачання може мати катастрофічні наслідки, включно із загрозою життю людей. Наприклад, атаки програм-вимагачів на лікарні можуть зупинити роботу життєво важливого обладнання, створюючи пряму небезпеку для пацієнтів. Такі інциденти також мають психологічний ефект, викликаючи паніку та знижуючи довіру до державних інститутів.

Психологічний вплив кіберзлочинності проявляється у стресі, тривозі та втраті довіри до цифрових технологій серед жертв атак. Особи, які зазнали крадіжки даних чи кібербулінгу, часто відчувають емоційну нестабільність і страх повторних інцидентів. Для організацій кібератаки можуть викликати напругу серед працівників, які відчувають провину за порушення безпеки або бояться нових загроз [4].

Міжнародна безпека також страждає через транскордонний характер кіберзлочинів. Розслідування таких злочинів ускладнене через різницю в законодавстві та юрисдикціях країн, що сприяє безкарності зловмисників. Політичні чи терористичні кібератаки, спрямовані на дестабілізацію економіки чи інфраструктури, можуть загострювати міждержавні конфлікти, створюючи додаткові виклики для глобальної безпеки.

Для систематизації наслідків кіберзлочинності наведено таблицю 1.1, яка відображає їхній вплив на різні сфери життя.

Таблиця 1.1 – Основні наслідки кіберзлочинності за сферами впливу

№	Сфера впливу	Наслідки
1.	Економічна	Фінансові втрати, витрати на відновлення, втрата репутації, зниження конкурентоспроможності
2.	Безпека даних	Витік конфіденційної інформації, крадіжка інтелектуальної власності, загроза національній безпеці
3.	Соціальна	Поширення дезінформації, дестабілізація суспільства, підрив довіри до інститутів
4.	Критична інфраструктура	Порушення роботи енергосистем, транспорту, медичних закладів, загроза життю
5.	Психологічна	Стрес, тривога, втрата довіри до технологій, внутрішня напруга в організаціях
6.	Міжнародна безпека	Ускладнення розслідувань, загострення міждержавних конфліктів, зростання кібертероризму

Ця таблиця підкреслює комплексний характер наслідків кіберзлочинності, що вимагає багатостороннього підходу до їхнього подолання. Протидія

кіберзлочинності передбачає впровадження сучасних технічних рішень, підвищення рівня кіберграмотності, вдосконалення правової бази та активізацію міжнародної співпраці. Лише скоординовані зусилля можуть зменшити шкоду від кіберзлочинів і забезпечити безпеку цифрового середовища.

1.3 Нормативно-правова база протидії кіберзлочинності

Нормативно-правова база протидії кіберзлочинності є ключовим елементом у забезпеченні безпеки цифрового простору. Вона охоплює сукупність міжнародних, регіональних і національних законодавчих актів, спрямованих на регулювання діяльності в інформаційно-комунікаційному середовищі, визначення відповідальності за кіберзлочини та створення механізмів їхнього запобігання й розслідування. Через транскордонний характер кіберзлочинності та швидкий розвиток технологій ця база постійно вдосконалюється, щоб відповідати сучасним викликам.

На міжнародному рівні основою для протидії кіберзлочинності є Конвенція Ради Європи про кіберзлочинність 2001 року. Цей документ є першим і найвпливовішим міжнародним договором, що встановлює стандарти для криміналізації кіберзлочинів, таких як незаконний доступ до комп’ютерних систем, перехоплення даних, шахрайство та злочини, пов’язані з контентом. Конвенція також визначає процедури міжнародної співпраці, зокрема обмін інформацією та екстрадицію, що є критично важливим для розслідування транскордонних злочинів. Багато країн, включаючи Україну, приєдналися до цього документа, адаптуючи своє законодавство до його вимог [5].

Окрім Будапештської конвенції, міжнародна нормативна база включає інші ініціативи. Наприклад, ООН активно працює над створенням глобальних стандартів боротьби з кіберзлочинністю через резолюції Генеральної Асамблеї та діяльність спеціалізованих груп, таких як Міжурядова експертна група з кіберзлочинності. Регіональні організації, як-от Європейський Союз, також відіграють важливу роль. Директиви ЄС, зокрема Директива про безпеку мереж та

інформації (NIS Directive) та Загальний регламент захисту даних (GDPR), встановлюють вимоги до кібербезпеки та захисту персональних даних, які є обов'язковими для країн-членів і впливають на глобальні стандарти.

На національному рівні в Україні нормативно-правова база протидії кіберзлочинності базується на Конституції України, Кримінальному кодексі України (ККУ) та низці спеціалізованих законів. ККУ містить розділ XVI, присвячений злочинам у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж, де визначено відповідальність за такі діяння, як несанкціонований доступ, створення шкідливого програмного забезпечення та комп'ютерне шахрайство. Закони України «Про основи національної безпеки України» [6], «Про захист інформації в інформаційно-телекомунікаційних системах» [7] встановлює принципи захисту критичної інфраструктури, регулюють діяльність у сфері кібербезпеки та визначають повноваження державних органів.

Важливу роль відіграють підзаконні нормативні акти, такі як Стратегія кібербезпеки України, затверджена у 2021 році, яка окреслює пріоритети держави в цій сфері, включаючи розвиток кіберзахисту, підготовку фахівців і міжнародну співпрацю [8]. Крім того, діяльність спеціалізованих установ, як-от Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) і кіберполіція, регулюється відповідними положеннями, що забезпечують оперативне реагування на кіберзагрози [9].

Для наочності основні нормативно-правові акти, що регулюють протидію кіберзлочинності, представлено в таблиці 1.2.

Таблиця 1.2 – Основні нормативно-правові акти протидії кіберзлочинності

Рівень	Нормативний акт	Основні положення
Міжнародний	Конвенція Ради Європи про кіберзлочинність (2001)	Криміналізація кіберзлочинів, міжнародна співпраця, процедури розслідування

Продовження таблиці

Рівень	Нормативний акт	Основні положення
Регіональний (ЄС)	Директива про безпеку мереж та інформації (NIS)	Вимоги до кібербезпеки критичної інфраструктури
Регіональний (ЄС)	Загальний регламент захисту даних (GDPR)	Захист персональних даних, штрафи за порушення
Національний (Україна)	Кримінальний кодекс України (Розділ XVI)	Кримінальна відповідальність за кіберзлочини
Національний (Україна)	Закон України «Про кібербезпеку»	Регулювання захисту критичної інфраструктури та координація кіберзахисту
Національний (Україна)	Стратегія кібербезпеки України (2021)	Пріоритети розвитку кібербезпеки, підготовка кадрів, міжнародна співпраця

Незважаючи на значний прогрес у формуванні нормативно-правової бази, протидія кіберзлочинності стикається з низкою викликів. По-перше, швидкий розвиток технологій випереджає оновлення законодавства, що створює прогалини в регулюванні нових видів кіберзлочинів, таких як атаки на штучний інтелект чи інтернет речей. По-друге, транскордонний характер кіберзлочинів ускладнює координацію між країнами, особливо якщо деякі держави не є учасниками міжнародних угод. По-третє, недостатній рівень гармонізації законодавства між країнами призводить до різного трактування кіберзлочинів і санкцій за них.

Для подолання цих викликів необхідне постійне вдосконалення нормативно-правової бази. Це включає адаптацію національного законодавства до міжнародних стандартів, посилення механізмів міжнародної співпраці та підвищення

кваліфікації правоохоронних органів. Крім того, важливим є залучення приватного сектору до розробки нормативних актів, оскільки технологічні компанії часто є першими, хто стикається з новими видами кіберзагроз.

Кіберзлочинність є складним і динамічним явищем, що становить серйозну загрозу для економічної, соціальної та національної безпеки в умовах стрімкого розвитку цифрових технологій. Її багатогранність, транскордонний характер і постійна еволюція методів зловмисників вимагають комплексного підходу до протидії. Класифікація кіберзлочинів за такими категоріями, як злочини проти даних, комп'ютерних систем, фінансові шахрайства, поширення шкідливого програмного забезпечення, незаконного контенту та кібертероризм, дозволяє систематизувати знання про це явище та розробляти цільові заходи захисту.

Наслідки кіберзлочинності мають широкий спектр впливу, включаючи фінансові втрати, порушення безпеки даних, дестабілізацію суспільства, загрози критичній інфраструктурі, психологічний дискомфорт і ускладнення міжнародної безпеки. Ці наслідки підкреслюють необхідність скоординованих дій на індивідуальному, корпоративному та державному рівнях.

Нормативно-правова база протидії кіберзлочинності, що включає міжнародні акти, такі як Конвенція Ради Європи про кіберзлочинність, регіональні директиви ЄС і національне законодавство України, створює основу для регулювання та розслідування кіберзлочинів. Проте швидкий розвиток технологій і транскордонний характер злочинів створюють виклики, які вимагають постійного вдосконалення законодавства, посилення міжнародної співпраці та підвищення кіберграмотності.

Ефективна протидія кіберзлочинності можлива лише за умови комплексного підходу, що поєднує технічні, правові, освітні та міжнародні заходи. Це дозволить мінімізувати шкоду від кіберзагроз і забезпечити безпеку цифрового середовища для суспільства.

2 ТЕХНІЧНІ ІНСТРУМЕНТИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

2.1 Антивірусні комплекси та системи захисту від шкідливого програмного забезпечення

Антивірусні комплекси та системи захисту від шкідливого програмного забезпечення (ПЗ) відіграють ключову роль у протидії кіберзлочинності. Вони призначені для виявлення, блокування та нейтралізації загроз, таких як віруси, трояни, програми-вимагачі чи шпигунське ПЗ, які зловмисники використовують для викрадення даних, порушення роботи систем або отримання фінансової вигоди. Ці системи забезпечують захист як індивідуальних користувачів, так і організацій, допомагаючи протистояти зростаючій кількості кібератак.

Антивірусні комплекси функціонують шляхом аналізу файлів, процесів і мережевого трафіку в реальному часі. Вони застосовують комбінацію методів, включаючи порівняння даних із базою відомих сигнатур шкідливих програм, аналіз поведінки програм для виявлення підозрілих дій і хмарні технології для швидкого реагування на нові загрози. Сучасні рішення також охоплюють захист від фішингу, аналіз зашифрованого трафіку та пошук системних вразливостей, що робить їх універсальними інструментами кібербезпеки [10].

Шкідливе ПЗ, з яким борються антивірусні комплекси, включає програми, що інфікують файли, маскуються під легітимне ПЗ, блокують доступ до даних або приховано збирають інформацію. Такі загрози поширюються через електронну пошту, ненадійні вебсайти, знімні носії або шляхом маніпуляцій із користувачами. Антивірусні системи нейтралізують ці загрози, використовуючи передові технології, такі як штучний інтелект і машинне навчання, які дозволяють виявляти навіть нові або модифіковані форми шкідливого коду.

Сучасні виклики, такі як поліморфні віруси, що змінюють свій код, або безфайлові атаки, які діють у пам’яті пристрою, вимагають від антивірусних комплексів постійного вдосконалення. Для цього вони використовують ізольовані середовища для тестування підозрілого коду, моніторинг мережевого трафіку та

аналіз великих обсягів даних у хмарі. Ці технології забезпечують швидке реагування на загрози та адаптацію до нових методів атак.

Антивірусні комплекси мають низку переваг, зокрема автоматичне виявлення загроз, захист від широкого спектра кібератак і простоту використання завдяки автоматичним оновленням. Проте вони не є універсальним рішенням. Нові загрози, що використовують невідомі вразливості, можуть обходити захист, а деякі антивірусні програми споживають значні системні ресурси, впливаючи на продуктивність пристроїв. Ефективність залежить від регулярного оновлення баз даних і правильного налаштування.

Антивірусні комплекси є частиною комплексної системи кібербезпеки, працюючи разом із міжмережевими екранами, шифруванням даних і механізмами автентифікації. Важливу роль відіграє кіберграмотність користувачів, оскільки багато атак, як-от фішинг, базуються на людських помилках, наприклад, переході за шахрайськими посиланнями.

Для ілюстрації основних функцій антивірусних комплексів наведено рисунку 2.1.

Рисунок 2.1 – Основні функції антивірусних комплексів

Антивірусні комплекси залишаються незамінним елементом захисту в умовах зростання кіберзагроз. Їхня здатність адаптуватися до нових викликів, таких як атаки на хмарні сервіси чи інтернет речей, визначає їхню ефективність у майбутньому. Розвиток технологій, зокрема штучного інтелекту, дозволяє

антивірусним системам не лише реагувати на відомі загрози, але й прогнозувати потенційні атаки, аналізуючи великі обсяги даних і виявляючи патерни, які можуть свідчити про зловмисну активність.

Одним із важливих напрямів розвитку є інтеграція антивірусних комплексів із системами управління безпекою (SIEM) [11] та платформами автоматизованого реагування на інциденти (SOAR) [12]. Це дозволяє організаціям не лише виявляти загрози, але й швидко координувати дії для їхньої нейтралізації, мінімізуючи потенційну шкоду. Крім того, зростає значення хмарних рішень, які забезпечують гнучкість і масштабованість, особливо для великих організацій із розподіленими мережами.

Іншим перспективним напрямом є створення антивірусних комплексів, орієнтованих на захист специфічних середовищ, таких як промислові системи управління (SCADA) [13], медичні пристрої чи автономні транспортні засоби. Ці галузі стають дедалі вразливішими до кібератак, оскільки їхня цифрова інфраструктура розширюється. Антивірусні системи для таких середовищ потребують спеціалізованих алгоритмів, які враховують унікальні особливості обладнання та протоколів.

Водночас антивірусні комплекси стикаються з новими викликами, пов’язаними з етикою та конфіденційністю. Наприклад, аналіз поведінки користувачів або моніторинг мережевого трафіку може викликати занепокоєння щодо порушення приватності. Виробники антивірусного ПЗ змушені балансувати між забезпеченням безпеки та дотриманням прав користувачів, що вимагає прозорості в обробці даних і чітких політик конфіденційності.

Для підвищення ефективності антивірусних комплексів також необхідна співпраця між розробниками, урядами та міжнародними організаціями. Обмін інформацією про нові загрози, створення глобальних баз сигнатур і координація зусиль у боротьбі з кіберзлочинністю дозволяють швидше реагувати на атаки та зменшувати їхні наслідки. Наприклад, міжнародні ініціативи, такі як Cyber Threat Alliance, сприяють обміну даними між виробниками антивірусного ПЗ, що підвищує загальний рівень безпеки [14].

У контексті України антивірусні комплекси набувають особливого значення через зростання кібератак, спрямованих на критичну інфраструктуру та державні установи. Впровадження сучасних антивірусних рішень, адаптованих до місцевих потреб, а також навчання населення основам кібергігієни можуть значно знизити вразливість до кіберзагроз. Крім того, підтримка локальних розробників антивірусного ПЗ сприяє розвитку національної індустрії кібербезпеки.

2.2 Системи виявлення та запобігання вторгнень і моніторингу безпеки

Системи виявлення вторгнень, запобігання вторгнень та управління інформацією і подіями безпеки є важливими інструментами кібербезпеки, що забезпечують захист інформаційних систем від несанкціонованого доступу, кібератак і зловмисної активності. Ці системи дозволяють організаціям моніторити, аналізувати та реагувати на загрози в реальному часі, що робить їх незамінними в протидії кіберзлочинності.

Системи виявлення вторгнень (IDS) призначені для моніторингу мережевого трафіку та системної активності з метою виявлення підозрілих подій, які можуть вказувати на кібератаку. Вони аналізують дані, порівнюючи їх із базами відомих сигнатур атак або виявляючи аномалії в поведінці мережі чи систем. IDS працює в пасивному режимі, сповіщаючи адміністраторів про потенційні загрози без втручання в роботу системи.

Системи запобігання вторгнень (IPS) розширюють функціонал IDS, оскільки не лише виявляють загрози, але й активно їх блокують. IPS може автоматично припиняти підозрілі з’єднання, блокувати IP-адреси або змінювати конфігурацію мережі для нейтралізації атаки. Часто ці системи інтегруються з міжмережевими екранами, створюючи додатковий рівень захисту.

Системи управління інформацією та подіями безпеки (SIEM) забезпечують централізований збір, аналіз і кореляцію даних із різних джерел, таких як сервери, мережеві пристрої, антивірусні програми та журнали подій. SIEM дозволяє

виявляти складні атаки, які можуть залишатися непомітними для окремих систем, шляхом аналізу великих обсягів даних і створення цілісної картини безпеки.

Основні завдання SIEM включають моніторинг у реальному часі, генерацію звітів, автоматизацію реагування на інциденти та підтримку відповідності нормативним вимогам.

Для наочності основні функції IDS, IPS і SIEM представлено в таблиці 2.1.

Таблиця 2.1 – Основні функції систем IDS, IPS і SIEM

Система	Основні функції	Режим роботи	Приклади
IDS	Виявлення підозрілої активності, аналіз сигнатур і аномалій, генерація сповіщень	Пасивний (тільки моніторинг)	Snort, Suricata
IPS	Виявлення та блокування загроз, активне втручання, захист у реальному часі	Активний (блокування)	Cisco Secure IPS, Palo Alto Networks
SIEM	Збір і кореляція даних, аналіз подій, автоматизація реагування, створення звітів	Централізований аналіз і моніторинг	Splunk, IBM QRadar

Нижче наведено приклад конфігураційного файлу для Snort (IDS), який виявляє спроби несанкціонованого доступу до мережі через SSH.

```
# Конфігурація правила для Snort
alert tcp any any -> 192.168.1.0/24 22 (msg:"SSH brute force attempt detected"; flow:to_server,established; content:"SSH"; threshold:type threshold, track by_src, count 5, seconds 60; sid:1000001; rev:1;)
```

Цей код налаштовує Snort для виявлення п’яти або більше спроб підключення до SSH-порту (22) з однієї IP-адреси протягом 60 секунд, що може свідчити про

атаку методом грубої сили.

IDS і IPS ефективно захищають від відомих типів атак, таких як DDoS, SQL-ін’єкції чи експлойти, завдяки аналізу сигнатур і аномалій. Сучасні системи використовують машинне навчання для виявлення нових загроз, включаючи нульові атаки (zero-day exploits). Проте їхня ефективність залежить від регулярного оновлення баз сигнатур і правильного налаштування. Помилкові спрацьовування (false positives) можуть перевантажувати адміністраторів, ускладнюючи реагування на реальні загрози.

SIEM-системи є особливо цінними для великих організацій, оскільки дозволяють виявляти складні атаки, такі як цілеспрямовані тривалі загрози (APT), шляхом кореляції подій із різних джерел. Вони також допомагають відповідати нормативним вимогам, таким як GDPR чи ISO 27001, завдяки генерації детальних звітів. Однак впровадження SIEM вимагає значних ресурсів, включаючи потужну інфраструктуру та кваліфікований персонал. Обробка великих обсягів даних може створювати затримки, якщо система не оптимізована.

Інтеграція IDS/IPS із SIEM створює потужний механізм захисту. Наприклад, IDS виявляє підозрілу активність, IPS блокує атаку, а SIEM аналізує інцидент у контексті всіх подій, зберігаючи журнали для розслідування. Такий підхід дозволяє організаціям не лише реагувати на загрози, але й прогнозувати їх, використовуючи історичні дані.

Розвиток IDS/IPS і SIEM пов’язаний із застосуванням нових технологій. Штучний інтелект і машинне навчання підвищують точність виявлення загроз і зменшують кількість помилкових спрацьовувань. Хмарні рішення, такі як AWS Security Hub або Azure Sentinel, забезпечують гнучкість і масштабованість, що важливо для організацій із розподіленими мережами. Автоматизація реагування через платформи SOAR (Security Orchestration, Automation, and Response) дозволяє скоротити час реагування, мінімізуючи шкоду від атак.

В Україні IDS/IPS і SIEM набувають особливого значення через зростання кібератак на критичну інфраструктуру, державні установи та приватний сектор. Впровадження цих систем у рамках Стратегії кібербезпеки України сприяє

підвищенню стійкості до загроз. Проте обмежені ресурси, брак фахівців і необхідність локалізації рішень залишаються викликами, які потребують комплексного підходу, включаючи підготовку кадрів і співпрацю з міжнародними партнерами.

Окремим напрямом розвитку є адаптація IDS/IPS і SIEM до захисту нових технологій, таких як інтернет речей (IoT), хмарні сервіси та промислові системи управління. Ці середовища стають дедалі вразливішими до атак, що вимагає спеціалізованих алгоритмів і підходів. Наприклад, захист IoT-пристроїв потребує легких IDS-систем, які не перевантажують обмежені ресурси пристроїв, тоді як хмарні SIEM-системи мають забезпечувати аналіз даних у розподілених середовищах.

Ще одним важливим аспектом є підвищення прозорості та етичності використання цих систем. Моніторинг мережевого трафіку та аналіз поведінки користувачів можуть викликати занепокоєння щодо конфіденційності. Розробники систем повинні чітко визначати політики обробки даних і забезпечувати їх відповідність міжнародним стандартам захисту приватності.

Співпраця між виробниками IDS/IPS і SIEM, урядами та міжнародними організаціями відіграє ключову роль у підвищенні ефективності цих систем. Обмін інформацією про нові загрози, створення глобальних баз сигнатур і координація зусиль у боротьбі з кіберзлочинністю дозволяють швидше реагувати на атаки. Наприклад, ініціативи на кшталт Cyber Threat Alliance сприяють обміну даними між розробниками, що зміцнює глобальну кібербезпеку.

Системи IDS, IPS і SIEM є основою сучасної кібербезпеки, забезпечуючи виявлення, блокування та аналіз кіберзагроз. Їхня інтеграція дозволяє організаціям створювати комплексний захист, який охоплює моніторинг, реагування та прогнозування атак. У поєднанні з новими технологіями, такими як штучний інтелект і хмарні рішення, ці системи стають більш адаптивними та ефективними. В Україні їхнє впровадження є важливим кроком до зміцнення кіберстійкості, але вимагає подолання ресурсних і кадрових обмежень. Комплексний підхід, що

включає технічні, освітні та міжнародні заходи, є ключем до успішної протидії кіберзлочинності.

2.3 Технології шифрування та багатофакторної аутентифікації

Технології шифрування та багатофакторної аутентифікації (MFA) є фундаментальними інструментами кібербезпеки, що забезпечують захист даних і систем від несанкціонованого доступу. Вони допомагають гарантувати конфіденційність, цілісність і автентичність інформації, що робить їх незамінними в боротьбі з кіберзлочинністю. Ці технології мінімізують ризики викрадення даних, шахрайства та інших кібератак, які стають дедалі складнішими в умовах цифровізації.

Шифрування перетворює дані в нечитабельний формат, який можна розшифрувати лише за допомогою спеціального ключа. Це забезпечує захист інформації як під час її передачі через мережі, так і під час зберігання на пристроях чи серверах. Наприклад, шифрування використовується для захисту банківських транзакцій, електронної пошти, медичних даних і державних секретів. Воно ефективно протидіє перехопленню інформації, атакам типу "людина посередині" та витокам даних. Однак успіх шифрування залежить від стійкості алгоритмів, якості ключів і безпеки їхнього зберігання. Слабкі ключі або їхня компрометація можуть зробити навіть найнадійніші системи вразливими.

Багатофакторна аутентифікація підвищує безпеку, вимагаючи від користувача підтвердження особи за допомогою кількох незалежних факторів. Це значно ускладнює зловмисникам доступ до систем, навіть якщо вони отримали пароль. MFA застосовується в банківських сервісах, хмарних платформах, соціальних мережах і корпоративних мережах, знижуючи ризики атак, таких як фішинг чи брутфорс. Наприклад, для входу в обліковий запис може знадобитися пароль і одноразовий код, надісланий на смартфон. Незважаючи на ефективність, MFA може бути незручною для користувачів через додаткові кроки, а біометричні дані, які іноді використовуються, вразливі до фальсифікації чи витоку [15].

Основні різновиди технологій шифрування та MFA:

1. Симетричне шифрування (наприклад, AES) для швидкого захисту даних.

2. Асиметричне шифрування (наприклад, RSA) для безпечного обміну даними.

3. Протоколи шифрування (наприклад, TLS) для захисту передачі даних.

4. Шифрування пристроїв (наприклад, BitLocker) для захисту даних на дисках.

5. Квантове шифрування для майбутньої безпеки.

6. Фактор знання (пароль, PIN-код) для базової аутентифікації.

7. Фактор володіння (смартфон, апаратний токен) для додаткового захисту.

8. Фактор притаманності (біометрія, як відбитки пальців) для унікальної ідентифікації.

9. Фактор поведінки (аналіз стилю набору тексту) для адаптивної безпеки.

10. Фактор місцезнаходження для перевірки географії входу [16].

У контексті кіберзлочинності ці технології є критично важливими. Шифрування захищає дані від викрадення, що особливо актуально для організацій, які працюють із конфіденційною інформацією, наприклад, фінансовими чи медичними даними. MFA запобігає несанкціонованому доступу, що є ключовим у протидії атакам, спрямованим на викрадення облікових даних. В Україні, де зростає кількість кібератак на критичну інфраструктуру та державні установи, ці технології стають основою національної кібербезпеки.

Впровадження шифрування та MFA стикається з низкою викликів. Шифрування може ускладнювати аналіз даних правоохоронними органами, що викликає дискусії про баланс між безпекою та державним наглядом. Крім того, ненадійне зберігання ключів або використання застарілих алгоритмів знижує ефективність захисту. Для MFA проблемами є незручність для користувачів, особливо в системах із кількома факторами, і технічні обмеження, такі як брак інфраструктури для біометричної аутентифікації в невеликих організаціях. Соціальна інженерія також залишається загрозою, оскільки зловмисники можуть маніпулювати користувачами для обходу MFA.

Перспективи розвитку цих технологій пов’язані з інноваціями. Постквантова криптографія розробляється для захисту від майбутніх квантових комп’ютерів, які можуть зламати сучасні алгоритми шифрування. У сфері MFA зростає популярність безпарольної аутентифікації, наприклад, стандарту FIDO2, який використовує апаратні ключі чи біометрію для спрощення доступу без втрати безпеки. Штучний інтелект вдосконалює адаптивну аутентифікацію, аналізуючи поведінку користувачів і автоматично підвищуючи вимоги до безпеки в разі підозрілої активності. Хмарні рішення для шифрування та MFA забезпечують гнучкість і масштабованість, що важливо для організацій із розподіленими мережами.

В Україні впровадження цих технологій підтримується державними ініціативами, такими як Стратегія кібербезпеки, але потребує значних інвестицій у інфраструктуру та підготовку фахівців. Підвищення кіберграмотності населення є невід’ємною частиною успіху, оскільки багато атак базуються на людських помилках, наприклад, використанні слабких паролів чи ігноруванні MFA. Освітні програми, які навчають безпечному використанню цих технологій, можуть суттєво знизити вразливість до кіберзагроз.

Співпраця між приватним сектором, урядом і міжнародними організаціями відіграє важливу роль у розвитку шифрування та MFA. Обмін інформацією про нові загрози та стандарти безпеки допомагає створювати надійніші системи. Наприклад, міжнародні ініціативи з розвитку постквантової криптографії сприяють глобальній стійкості до майбутніх кіберзагроз.

Технічні інструменти протидії кіберзлочинності, зокрема антивірусні комплекси, системи виявлення та запобігання вторгненням, системи управління інформацією та подіями безпеки, а також технології шифрування та багатофакторної аутентифікації, є ключовими елементами забезпечення кібербезпеки. Антивірусні комплекси ефективно виявляють і нейтралізують шкідливе програмне забезпечення, використовуючи сучасні технології, такі як штучний інтелект і хмарні рішення, однак потребують регулярного оновлення та інтеграції з іншими системами для подолання нових загроз. Системи IDS/IPS і

SIEM забезпечують моніторинг, блокування та аналіз кібератак, дозволяючи організаціям оперативно реагувати на інциденти та прогнозувати загрози, хоча їхнє впровадження ускладнене високими вимогами до ресурсів і кваліфікації персоналу. Технології шифрування та MFA створюють надійний захист даних і доступу до систем, мінімізуючи ризики викрадення інформації та несанкціонованого доступу, але стикаються з викликами, пов’язаними з етичними питаннями, складністю впровадження та соціальною інженерією.

В Україні ці інструменти набувають особливого значення через зростання кібератак на критичну інфраструктуру та державні установи. Їхнє ефективне використання вимагає комплексного підходу, що включає розвиток інноваційних технологій, таких як постквантова криптографія та безпарольна аутентифікація, вдосконалення нормативної бази, підвищення кіберграмотності населення та міжнародну співпрацю. Інтеграція цих інструментів із сучасними технологіями, такими як штучний інтелект і хмарні рішення, а також подолання ресурсних і кадрових обмежень є ключем до створення стійкого цифрового середовища, здатного протистояти сучасним і майбутнім кіберзагрозам.

3 АНАЛІЗ ЕФЕКТИВНОСТІ ТЕХНІЧНИХ ІНСТРУМЕНТІВ ТА ПЕРСПЕКТИВИ ЇХ РОЗВИТКУ

3.1 Оцінка ефективності сучасних технічних засобів протидії кіберзлочинності

Ефективність технічних засобів оцінюється за кількома критеріями. Першим є швидкість і точність виявлення загроз. Наприклад, антивірусні комплекси з сигнатурним і поведінковим аналізом успішно ідентифікують відомі віруси та програми-вимагачі, але можуть пропускати нульові атаки (zero-day exploits). IDS/IPS ефективно протидіють мережевим атакам, таким як DDoS чи SQL-ін’єкції, але їхня точність залежить від актуальності баз сигнатур і мінімізації помилкових спрацьовувань (false positives). SIEM-системи забезпечують комплексний аналіз, виявляючи складні атаки, такі як APT (Advanced Persistent Threats), завдяки кореляції даних із різних джерел [17].

Другим критерієм є здатність до активного реагування. IPS і MFA мають перевагу, оскільки можуть автоматично блокувати загрози чи несанкціонований доступ. Наприклад, IPS припиняє підозрілі з’єднання, а MFA запобігає входу навіть за наявності скомпрометованого пароля. Антивірусні комплекси та SIEM, навпаки, частіше виконують пасивну роль, надаючи сповіщення для подальшого реагування адміністраторами.

Третій критерій – масштабованість і гнучкість. Хмарні рішення, такі як Azure Sentinel (SIEM) чи хмарні антивіруси, демонструють високу адаптивність до розподілених мереж, що важливо для великих організацій. Шифрування, зокрема TLS і AES, є універсальним і масштабованим, але потребує правильного управління ключами. IDS/IPS можуть бути менш гнучкими в малих організаціях через складність налаштування та високі вимоги до ресурсів.

Четвертим критерієм є відповідність нормативним вимогам. SIEM-системи допомагають організаціям генерувати звіти для аудиту, тоді як шифрування та MFA забезпечують захист даних відповідно до вимог конфіденційності. Однак

складність впровадження цих систем може створювати бар’єри для малих організацій.

Антивірусні комплекси ефективно захищають від широкого спектра шкідливого ПЗ, включаючи віруси, трояни та програми-вимагачі, завдяки комбінації сигнатурного, евристичного та поведінкового аналізу. IDS/IPS забезпечують захист мережевих периметрів, виявляючи та блокуючи атаки в реальному часі. SIEM-системи створюють цілісну картину безпеки, що дозволяє виявляти складні загрози. Технології шифрування гарантують конфіденційність даних, а MFA значно знижує ризики несанкціонованого доступу. Хмарні технології та штучний інтелект підвищують адаптивність цих засобів, дозволяючи швидше реагувати на нові загрози.

Незважаючи на переваги, технічні засоби мають обмеження. Антивірусні комплекси можуть бути неефективними проти нових загроз через затримки в оновленні сигнатур. IDS/IPS страждають від помилкових спрацьовувань, що перевантажують адміністраторів. SIEM-системи потребують значних ресурсів і кваліфікованого персоналу, що ускладнює їхнє впровадження в малих організаціях. Шифрування вразливе до слабких ключів або квантових атак у перспективі, а MFA може бути незручною для користувачів і вразливою до соціальної інженерії. Транскордонний характер кіберзлочинів ускладнює реагування, оскільки зловмисники часто діють із юрисдикцій, недоступних для правоохоронних органів.

Ефективність залежить від кількох факторів. Технічна інтеграція забезпечує синергію між системами: наприклад, поєднання IDS/IPS із SIEM дозволяє не лише виявляти, але й аналізувати атаки [18]. Людський фактор відіграє важливу роль, оскільки помилки користувачів, такі як слабкі паролі чи ігнорування MFA, знижують захист. Регулярне оновлення ПЗ і баз сигнатур є критично важливим, адже застарілі системи стають легкою мішенню. Кіберграмотність персоналу та навчання зменшують ризики атак, заснованих на соціальній інженерії.

Для ілюстрації основних аспектів оцінки ефективності технічних засобів наведено рисунок 3.1.

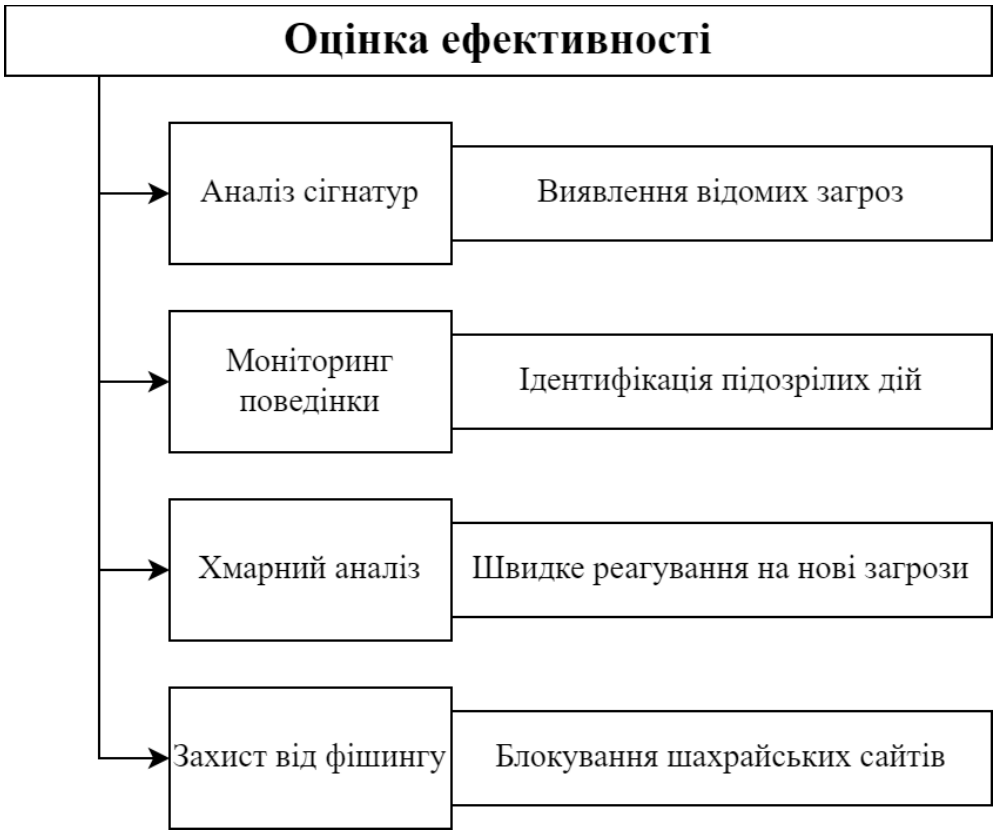

Рисунок 3.1 – Оцінка ефективності технічних засобів

В Україні технічні засоби протидії кіберзлочинності набувають особливого значення через зростання атак на критичну інфраструктуру, державні установи та приватний сектор. Антивірусні комплекси та MFA широко застосовуються в банківській сфері, тоді як IDS/IPS і SIEM використовуються в енергетичних і телекомунікаційних компаніях. Однак обмежені ресурси, брак фахівців і недостатня кіберграмотність населення знижують їхню ефективність. Наприклад, атаки програм-вимагачів, спрямовані на українські організації, часто успішні через застаріле ПЗ або ігнорування базових заходів безпеки.

Державні ініціативи, такі як Стратегія кібербезпеки України, сприяють впровадженню сучасних засобів, але потребують посилення фінансування та підготовки кадрів. Міжнародна співпраця, зокрема через обмін даними про загрози в рамках Cyber Threat Alliance, допомагає підвищувати ефективність систем, таких як SIEM і IDS/IPS. Локальні розробники, які створюють адаптовані рішення, також відіграють важливу роль у зміцненні кіберзахисту.

Сучасні технічні засоби протидії кіберзлочинності демонструють високу ефективність у виявленні та нейтралізації загроз, але їхня результативність залежить від інтеграції, оновлення та людського фактора. Антивірусні комплекси, IDS/IPS, SIEM, шифрування та MFA створюють комплексний захист, але мають обмеження, такі як вразливість до нових атак чи складність впровадження. В Україні ці засоби є основою кібербезпеки, але потребують вдосконалення інфраструктури, освіти та міжнародної співпраці для підвищення їхньої ефективності в умовах зростаючих кіберзагроз.

3.2 Кейси успішного та невдалого застосування технічних інструментів

Технічні інструменти протидії кіберзлочинності, такі як антивірусні комплекси, системи виявлення та запобігання вторгнень, системи управління інформацією та подіями безпеки, технології шифрування та багатофакторна аутентифікація, відіграють ключову роль у захисті інформаційних систем. Аналіз кейсів їхнього успішного та невдалого застосування дозволяє оцінити сильні сторони, обмеження та фактори, що впливають на ефективність. Нижче розглянуто приклади з реального світу, що ілюструють ці аспекти, а також надано код для аналізу логів безпеки як приклад практичного використання інструментів.

У 2017 році програма-вимагач WannaCry атакувала тисячі організацій у 150 країнах, шифруючи дані та вимагаючи викуп [19]. Однак компанії, які використовували оновлені антивірусні комплекси (наприклад, Kaspersky, Bitdefender) та MFA, змогли мінімізувати шкоду. Антивірусні системи виявили експлойт EternalBlue, що використовувався WannaCry, завдяки актуальним базам сигнатур і поведінковому аналізу. MFA, застосована для доступу до критичних систем, запобігла несанкціонованому входу, навіть коли зловмисники отримували паролі через фішинг. Наприклад, медична установа у Великобританії, яка використовувала оновлений Windows Defender і MFA, уникла зараження, тоді як інші лікарні, із застарілим ПЗ, зазнали значних втрат. Цей кейс підкреслює

важливість регулярного оновлення систем і комбінування інструментів для комплексного захисту.

Також щодо кейсу SolarWinds, атака на ланцюг постачання SolarWinds стала однією з наймасштабніших операцій кібершпигунства, скомпрометувавши десятки організацій, включно з урядовими установами США. Проте компанії, які використовували SIEM (наприклад, Splunk) у поєднанні з IDS/IPS (Palo Alto Networks), змогли швидко виявити та ізолювати загрозу. SIEM виявила аномальну активність у мережевому трафіку, пов’язану з командно-контрольними серверами зловмисників, а IPS заблокувала підозрілі з’єднання. Наприклад, технологічна компанія, що застосовувала ці системи, виявила компрометацію за лічені години та запобігла витоку даних. Цей кейс демонструє ефективність інтеграції SIEM і IDS/IPS для виявлення складних атак типу APT.

Витік даних у компанії Equifax, що зачепив 147 мільйонів осіб, став прикладом невдалого застосування технічних інструментів. Зловмисники скористалися вразливістю в Apache Struts, яка не була виправлена через затримку в оновленні ПЗ. Критичні дані, такі як номери соціального страхування, зберігалися без належного шифрування, що дозволило зловмисникам легко їх викрасти. Крім того, відсутність MFA для доступу до внутрішніх систем дала змогу хакерам використати скомпрометовані облікові дані адміністратора. Цей інцидент підкреслює, що навіть потужні інструменти стають неефективними без своєчасного оновлення, правильного налаштування та впровадження базових заходів безпеки.

Атака програми-вимагача на Colonial Pipeline, одного з найбільших операторів трубопроводів у США, призвела до зупинки постачання палива. Хоча компанія використовувала IDS/IPS, системи не змогли ефективно виявити атаку через недостатнє налаштування та брак інтеграції з SIEM. Зловмисники проникли через скомпрометований VPN-акаунт, який не мав MFA, і розгорнули програму-вимагач DarkSide. IDS виявила підозрілу активність, але через велику кількість помилкових спрацьовувань (false positives) адміністратори не встигли відреагувати.

Цей кейс ілюструє важливість правильного налаштування систем, інтеграції інструментів і використання MFA для захисту точок входу.

Нижче наведено приклад Python-скрипта для базового аналізу логів безпеки, який може використовуватися в SIEM-подібних системах для виявлення підозрілих подій, таких як множинні невдалі спроби входу.

```
    import pandas as pd
    import re
from datetime import datetime, timedelta
    # Зчитування лог-файлу (приклад: логи аутентифікації)
log_file = "auth_logs.txt"
    # Функція для парсингу логів
    def parse_logs(file_path):
        logs = []
    log_pattern = r'(\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2})
(\S+) (\S+) (\S+)'
       with open(file_path, 'r') as file:
            for line in file:
                match = re.match(log_pattern, line)
                if match:
                    timestamp, user, action, status =
match.groups()
                    logs.append({
                        'timestamp':
datetime.strptime(timestamp, '%Y-%m-%d %H:%M:%S'),
                        'user': user,
                        'action': action,
                        'status': status
                    })
    return pd.DataFrame(logs)
    # Виявлення множинних невдалих спроб входу
    def detect_bruteforce(df, time_window_minutes=5,
threshold=5):
        time_window =
timedelta(minutes=time_window_minutes)
    suspicious_activity = []
       for user in df['user'].unique():
            user_logs = df[(df['user'] == user) &
(df['status'] == 'failed')]
            for i, log in user_logs.iterrows():
                window_end = log['timestamp'] + time_window
                attempts =
user_logs[(user_logs['timestamp'] >= log['timestamp']) &
```

```
                                        (user_logs['timestamp']
<= window_end)]
                if len(attempts) >= threshold:
                    suspicious_activity.append({
                        'user': user,
                        'time': log['timestamp'],
                        'attempts': len(attempts)
                    })
    return suspicious_activity
    # Основна програма
    logs_df = parse_logs(log_file)
bruteforce_attempts = detect_bruteforce(logs_df)
    # Виведення результатів
    for attempt in bruteforce_attempts:
    print(f"Підозріла        активність:        Користувач
{attempt['user']} здійснив {attempt['attempts']} невдалих
спроб входу о {attempt['time']}")
```

Цей скрипт аналізує логи аутентифікації, виявляючи потенційні атаки грубої сили (bruteforce). Він може бути інтегрований у SIEM-систему для автоматизації моніторингу. Для роботи потрібен файл auth_logs.txt із логами у форматі: 2025-06-02 12:00:00 user1 login failed.

Успішні кейси, такі як WannaCry і SolarWinds, демонструють, що ефективність технічних інструментів залежить від їхньої інтеграції, своєчасного оновлення та комбінування. Антивірусні комплекси, SIEM і MFA створюють синергію, дозволяючи виявляти, блокувати та аналізувати загрози. Наприклад, у кейсі SolarWinds кореляція подій у SIEM допомогла ідентифікувати аномалії, які пропустили окремі системи.

Невдалі кейси, як Equifax і Colonial Pipeline, підкреслюють критичні помилки: застаріле ПЗ, відсутність MFA, неправильне налаштування IDS/IPS і слабке шифрування. Ці інциденти показують, що навіть найсучасніші інструменти стають неефективними без належного управління та кіберграмотності персоналу. Соціальна інженерія, використана в Colonial Pipeline, також вказує на необхідність навчання користувачів.

В Україні подібні кейси мають особливе значення. Наприклад, атаки на енергетичну мережу в 2015-2016 роках (BlackEnergy) показали вразливість через

брак шифрування та MFA, тоді як успішне використання SIEM державними установами під час атак 2022 року допомогло швидко ізолювати загрози [20]. Ці приклади підкреслюють потребу в локалізованих рішеннях і підвищенні кіберграмотності.

Аналіз кейсів показує, що технічні інструменти є ефективними за умови правильного впровадження, інтеграції та оновлення. Успішні приклади демонструють переваги комбінування антивірусів, SIEM, IDS/IPS і MFA, тоді як невдалі випадки вказують на ризики, пов’язані з людським фактором і технічними прогалинами. Код для аналізу логів ілюструє, як SIEM може автоматизувати виявлення загроз. Для підвищення ефективності в Україні необхідні інвестиції в інфраструктуру, освіту та міжнародну співпрацю, щоб адаптувати інструменти до локальних викликів.

3.3 Перспективи розвитку технічних інструментів на основі штучного інтелекту та машинного навчання

Штучний інтелект і машинне навчання відкривають нові горизонти для розвитку технічних інструментів протидії кіберзлочинності, таких як антивірусні комплекси, системи виявлення та запобігання вторгнень, системи управління інформацією та подіями безпеки, технології шифрування та багатофакторна аутентифікація. Ці технології дозволяють інструментам адаптуватися до нових загроз, підвищувати точність виявлення атак і автоматизувати реагування, що є критично важливим у динамічному середовищі кіберзлочинності.

ШІ та МН уже активно застосовуються в кібербезпеці. Антивірусні комплекси використовують МН для поведінкового аналізу, що дозволяє виявляти невідомі загрози, такі як поліморфні віруси чи безфайлові атаки. IDS/IPS застосовують алгоритми МН для аналізу аномалій у мережевому трафіку, зменшуючи кількість помилкових спрацьовувань (false positives). SIEM-системи використовують ШІ для кореляції великих обсягів даних і виявлення складних атак, таких як APT (Advanced Persistent Threats). У сфері MFA ШІ вдосконалює

адаптивну аутентифікацію, аналізуючи поведінку користувачів, наприклад, стиль набору тексту чи географічне розташування. Шифрування, хоча менш залежне від ШІ, отримує переваги від алгоритмів МН для управління ключами та виявлення спроб їх компрометації.

Перспективи розвитку:

1. Автоматизація та прогнозування загроз. ШІ та МН дозволяють автоматизувати реагування на кіберінциденти, що скорочує час між виявленням і нейтралізацією загрози. Платформи SOAR (Security Orchestration, Automation, and Response), інтегровані з ШІ, можуть автоматично ізолювати скомпрометовані пристрої, блокувати IP-адреси чи застосовувати патчі. МН також сприяє прогнозуванню атак шляхом аналізу історичних даних і трендів. Наприклад, ШІ може передбачити потенційні фішингові кампанії, аналізуючи патерни в електронних листах чи поведінці зловмисників.

2. Виявлення нульових атак. Нульові атаки (zero-day exploits) залишаються однією з найбільших проблем кібербезпеки. Алгоритми МН, такі як нейронні мережі, здатні виявляти аномалії, які не відповідають відомим сигнатурам, шляхом аналізу поведінки програм чи мережевого трафіку. Наприклад, системи на основі ШІ, як CrowdStrike Falcon, успішно ідентифікують невідомі загрози, аналізуючи відхилення від нормальної активності. У майбутньому такі системи стануть ще точнішими завдяки глибокому навчанню (deep learning).

3. Адаптивна кібербезпека. ШІ дозволяє створювати адаптивні системи, які динамічно змінюють стратегії захисту залежно від контексту. Наприклад, адаптивна MFA може вимагати додаткових факторів аутентифікації, якщо користувач входить із незнайомого місця чи пристрою. SIEM-системи, такі як IBM QRadar, використовують ШІ для автоматичного налаштування правил кореляції, що підвищує ефективність виявлення загроз у реальному часі.

4. Захист нових технологій. Зростання популярності інтернету речей (IoT), хмарних сервісів і автономних систем створює нові вразливості. ШІ та МН дозволяють розробляти спеціалізовані інструменти для захисту цих середовищ. Наприклад, алгоритми МН можуть аналізувати трафік IoT-пристроїв, виявляючи

аномалії, як-от спроби DDoS-атак. У хмарних системах ШІ, як у AWS GuardDuty, забезпечує моніторинг і захист від загроз у розподілених мережах.

5. Постквантова криптографія та ШІ. Розвиток квантових комп'ютерів загрожує сучасним алгоритмам шифрування, таким як RSA чи AES. ШІ та МН допомагають розробляти постквантові криптографічні алгоритми, стійкі до квантових атак. Наприклад, алгоритми на основі ґрат (lattice-based cryptography) тестуються з використанням МН для оцінки їхньої безпеки. Крім того, ШІ може оптимізувати управління ключами, зменшуючи ризик їх компрометації.

6. Протидія ШІ-заснованим атакам. Зловмисники також використовують ШІ для створення складних атак, таких як глибокі підробки (deepfakes) для фішингу чи автоматизовані атаки на основі МН. Для протидії цим загрозам розробляються ШІ-системи, які аналізують підозрілий контент або поведінку. Наприклад, алгоритми МН можуть виявляти deepfakes, аналізуючи мікроаномалії в аудіо чи відео.

Незважаючи на перспективи, впровадження ШІ та МН у кібербезпеці стикається з труднощами. По-перше, навчання моделей МН потребує великих обсягів якісних даних, які можуть бути обмеженими через конфіденційність. По-друге, ШІ-системи вразливі до атак типу "отруєння даних" (data poisoning), коли зловмисники маніпулюють даними для навчання, щоб обійти захист. По-третє, складність ШІ-систем вимагає висококваліфікованих фахівців, яких бракує, зокрема в Україні. Нарешті, етичні питання, пов'язані з моніторингом поведінки користувачів, викликають занепокоєння щодо приватності, що потребує чіткого нормативного регулювання.

В Україні ШІ та МН у кібербезпеці мають значний потенціал, особливо з огляду на зростання кібератак на критичну інфраструктуру та державні установи. Локальні розробники, такі як компанії, що створюють SIEM-подібні рішення, можуть адаптувати ШІ-системи до специфічних загроз, наприклад, атак на енергетичні мережі. Державні ініціативи, як Стратегія кібербезпеки України, підтримують розвиток ШІ-технологій, але потребують інвестицій у підготовку кадрів і інфраструктуру. Міжнародна співпраця, зокрема через обмін даними про

загрози в рамках ініціатив на кшталт Cyber Threat Alliance, може прискорити впровадження ШІ в Україні.

Для систематизації основних перспектив розвитку технічних інструментів на основі ШІ та МН наведено таблицю 3.1.

Таблиця 3.1 – Перспективи розвитку технічних інструментів на основі ШІ та МН

Напрям розвитку	Опис	Приклади застосування
Автоматизація реагування	Автоматичне блокування та ізоляція загроз	Платформи SOAR, Splunk Phantom
Виявлення нульових атак	Аналіз аномалій для ідентифікації невідомих загроз	CrowdStrike Falcon, Darktrace
Адаптивна кібербезпека	Динамічне налаштування захисту залежно від контексту	IBM QRadar, адаптивна MFA
Захист IoT і хмарних систем	Моніторинг і захист розподілених середовищ	AWS GuardDuty, Azure Sentinel
Постквантова криптографія	Розробка стійких алгоритмів шифрування	Алгоритми на основі ґрат
Протидія ШІ-атакам	Виявлення deepfakes і автоматизованих атак	Аналіз контенту з МН

ШІ та МН трансформують технічні інструменти протидії кіберзлочинності, забезпечуючи автоматизацію, прогнозування та адаптивність. Вони дозволяють ефективно виявляти нульові атаки, захищати нові технології та протидіяти ШІ-заснованим загрозам. Однак виклики, такі як брак даних, вразливості моделей і етичні питання, потребують уваги. В Україні ШІ та МН мають значний потенціал, але їхній розвиток залежить від інвестицій, підготовки фахівців і міжнародної співпраці. Комплексний підхід, що поєднує технологічні інновації, освіту та нормативне регулювання, є ключем до створення стійкого кіберзахисту.

ВИСНОВКИ

Проведене дослідження присвячене аналізу кіберзлочинності, її наслідків, нормативно-правової бази, технічних інструментів протидії та перспектив їхнього розвитку на основі сучасних технологій. Кіберзлочинність є однією з найсерйозніших загроз сучасного світу, що впливає на економіку, безпеку даних, соціальну стабільність, критичну інфраструктуру, психологічний стан людей і міжнародну безпеку. Її транскордонний характер, анонімність і швидкий розвиток технологій ускладнюють боротьбу із цим явищем, що вимагає комплексного підходу, який поєднує правові, технічні, організаційні та освітні заходи.

У першому розділі розглянуто теоретичні основи кіберзлочинності. Кіберзлочини охоплюють широкий спектр протиправних дій, від викрадення даних і шахрайства до атак на критичну інфраструктуру та кібертероризму. Їх класифікують за об’єктом посягання, способом вчинення та мотивами, що дозволяє систематизувати підходи до протидії. Наслідки кіберзлочинності є багатогранними: економічні збитки, витік конфіденційної інформації, дестабілізація суспільства та загрози національній безпеці підкреслюють необхідність ефективних заходів захисту. Нормативно-правова база, що включає міжнародні договори, як Будапештська конвенція, та національне законодавство України, зокрема Кримінальний кодекс і Закон «Про кібербезпеку», створює основу для боротьби з кіберзлочинністю, але потребує адаптації до нових викликів, таких як атаки на штучний інтелект чи інтернет речей.

Другий розділ присвячений технічним інструментам протидії кіберзлочинності. Антивірусні комплекси ефективно захищають від шкідливого програмного забезпечення завдяки сигнатурному, евристичному та поведінковому аналізу, але їхня результативність залежить від регулярного оновлення та інтеграції з іншими системами. Системи виявлення та запобігання вторгнень і моніторингу безпеки забезпечують захист мереж і аналіз складних атак, хоча потребують значних ресурсів і кваліфікованого персоналу. Технології шифрування та багатофакторної аутентифікації гарантують конфіденційність даних і безпечний

доступ, але стикаються з проблемами слабких ключів, незручності для користувачів і вразливостей до соціальної інженерії. Ці інструменти формують комплексний захист, але їхня ефективність залежить від правильного впровадження та людського фактора.

Третій розділ аналізує ефективність і перспективи розвитку технічних інструментів. Оцінка показує, що сучасні засоби, такі як антивірусні комплекси, IDS/IPS, SIEM, шифрування та MFA, ефективно протидіють відомим загрозам, але мають обмеження, зокрема вразливість до нульових атак і залежність від кіберграмотності користувачів. Кейси WannaCry і SolarWinds демонструють успіхи завдяки інтеграції та оновленню систем, тоді як інциденти Equifax і Colonial Pipeline вказують на ризики через застаріле ПЗ і брак MFA. Штучний інтелект і машинне навчання відкривають нові перспективи, забезпечуючи автоматизацію реагування, виявлення невідомих загроз і захист нових технологій, таких як IoT і хмарні сервіси. Однак виклики, як-от брак даних для навчання моделей, вразливість до атак на ШІ та етичні питання, потребують уваги.

В Україні кіберзлочинність становить особливу загрозу через атаки на критичну інфраструктуру та державні установи. Технічні інструменти, підтримані Стратегією кібербезпеки, відіграють важливу роль, але їхня ефективність обмежена недостатнім фінансуванням, браком фахівців і низькою кіберграмотністю населення. Міжнародна співпраця, локальні розробки та освітні програми є ключовими для подолання цих проблем.

Загальний висновок: протидія кіберзлочинності вимагає комплексного підходу, що поєднує вдосконалення нормативно-правової бази, впровадження сучасних технічних інструментів, розвиток ШІ та МН, підвищення кіберграмотності та міжнародну співпрацю. Успішне застосування антивірусних комплексів, IDS/IPS, SIEM, шифрування та MFA залежить від їхньої інтеграції, своєчасного оновлення та врахування людського фактора. Перспективи ШІ та МН обіцяють революційні зміни в кібербезпеці, але потребують інвестицій у інфраструктуру, підготовку кадрів і вирішення етичних питань. В Україні зміцнення кіберзахисту можливе через адаптацію глобальних стандартів, розвиток

локальних рішень і освіту, що забезпечить стійкість до сучасних і майбутніх кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Любавіна В. Сутність кіберзлочинності та способи боротьби. *Молодий вчений*, 2022. №8 (108). С. 22-25.
2. Лупай А. С., Павлюх О. А., Павлюх А. І. Актуальність питання боротьби з кіберзлочинністю як складова загальнокримінальної злочинності. *Ірпінський юридичний часопис*, 2023. №3 (12). С. 211-218.
3. Дзяд О. В., Стародуб Д. С. Економічні втрати та механізми протидії кіберзлочинності у світовому господарстві. Ефективна кономіка, 2022. №1. DOI: 10.32702/2307-2105-2022.1.91
4. Ковальчук А. Ю., Гавловський В. Д. Інформаційно-психологічні впливи як засіб маніпуляції свідомістю, що застосовується організованими злочинними угрупуваннями. *Інформація і право*, 2022. №2 (41). С. 94-98.
5. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 21.09.2010 № 2824-IV. *Відомості Верховної Ради України*, 2006, N 5-6, ст.7.
6. Про основи національної безпеки України : Закон України від 15.12.2005 № 3200-IV. *Відомості Верховної Ради України*, 2003, № 39, ст.351.
7. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 16.12.2020 № 1089-IX. *Відомості Верховної Ради України*, 1994, № 31, ст.286.
8. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Закон України від 26 серпня 2021 року № 447/2021. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 15.03.2024).
9. Державна служба спеціального зв’язку та захисту інформації України. Офіційний сайт. URL: https://cip.gov.ua/ua (дата звернення: 15.03.2024).
10. Аль-Аммурі А., Дехтяр М., Іщенко Р., Клочан Є. Методи та засоби захисту інформації. *Системи управління, навігації та зв’язку*: зб. наук. праць. 2024. №1(75). С. 38-44.

11. Гундер А. М., Мужанова Т. М. Моніторинг і управління безпекою на основі використання SIEM системи IBM QRadar. *Сучасний захист інформації*, 2022. №2. 6-14.
12. Гаврилов М. Захист інформаційних систем підприємства від кіберзагроз: підходи та інструменти в умовах цифрової трансформації бізнесу / Микола Гаврилов // Колективна *монографія*. Тернопіль : :ФОП Паляниця В.А, 2024. С. 287–305.
13. Михалюк А. П., Міркевич Р. М. Су-часний стан та аналіз кі-бербезпеки автоматизова-них систем керування тех-нологічними процесами та автоматизованих систем управління виробницт-вом. Наукові праці НУХТ, 2024. 30(4). С. 7-30. DOI: 10.24263/2225-2924- 2024-30-4-3
14. Zaman G. K., Hossain Z., Urmi S. S., Taher, K. A. Cyber-Partnership and Cyber-Alliance - Options for Developing Nations. *2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD)*, Dhaka, Bangladesh, 2021. pp. 486-490, doi: 10.1109/ICICT4SD50815.2021.9396966.
15. Дудикевич В. Б., Партика О. О., Наконечний Т. І. Впровадження систем одноразового входу (SSO) для підвищення кібербезпеки. *Сучасний захист інформації*, 2025. №1. 60-73.
16. Ткач В. О., Гаврилюк О. Г., Штонда Р. М., Білий О. А. Модель перспективної гібридної системи захисту інформації в інформаційно-комунікаційних системах організацій різних сфер діяльності. The research process in science and the implementation of results : proceedings of the XVII International Scientific and Practical Conference. Slovenia, April 24 – 25, 2023. С. 88-91.
17. Sharma A., Gupta B. B., Singh A. K., Saraswat V. K. Advanced persistent threats (apt): evolution, anatomy, attribution and countermeasures. *Journal of Ambient Intelligence and Humanized Computing*, 2023. №14(7). С. 9355-9381.
18. Котляров О. Ю., Бортнік Л. Л. Порівняльний аналіз сучасних систем захисту віртуальних мереж та їх методології. *Науковий журнал «Сучасний захист інформації».* 2024. №4. DOI: 10.31673/2409-7292.2024.040007

19. What was the WannaCry ransomware attack? Cloudfare. *Офіційний сайт.* URL: https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/ (дата звернення: 20.04.2024).
20. Зінченко О. І. Вплив політичної ситуації в Україні на проблеми кібербезпеки Європейського Регіону / О. І. Зінченко // *Політикус* : наук. журнал. 2024. № 5. С. 154-158.