УДК 004.056:004.7
DOI https://doi.org/10.32782/tnv-tech.2024.4.3

РОЗРОБКА ТА ВПРОВАДЖЕННЯ ІННОВАЦІЙНИХ МЕТОДІВ КІБЕРБЕЗПЕКИ У КОМП'ЮТЕРНИХ СИСТЕМАХ

Бондарчук О. І. *– магістр комп'ютерних наук*
Університету WSB Домброва Гурнича, фахівець з обробки даних Akademia WSB
ORCID ID: 0009-0003-9626-1124

Науменко Т. С. *– старший викладач кафедри вищої математики*
Навчально-наукового інституту «Український державний хіміко-технологічний університет» Українського державного університету науки і технологій
ORCID ID: 0000-0003-0835-7074

Товт Б. М. *– кандидат технічних наук, доцент кафедри вищої математики, фізики та загальноінженерних дисциплін*
Дніпровського державного аграрно-економічного університету
ORCID ID: 0009-0000-7670-8898

Швидкі темпи розвитку цифрових технологій призвели до суттєвого збільшення складності та кількості кіберзагроз, що робить кібербезпеку одним з найважливіших питань для сучасних комп'ютерних систем. У міру того, як кібератаки стають все більш складними, традиційні заходи безпеки стають недостатніми для захисту конфіденційних даних і забезпечення цілісності інформаційних систем. Це зумовлює необхідність розробки та впровадження інноваційних методів кібербезпеки, здатних ефективно протистояти таким новим загрозам. Актуальність цього дослідження полягає в необхідності підвищення стійкості комп'ютерних систем до кіберзагроз, зокрема в секторах, де захист даних має вирішальне значення, таких як фінанси, охорона здоров'я та національна безпека.

Метою цієї статті є дослідження розвитку та практичного застосування інноваційних методів кібербезпеки, адаптованих до сучасних комп'ютерних систем. Основна увага приділяється інтеграції передових технологій, таких як штучний інтелект, машинне навчання та криптографічні методи, для створення багаторівневої стратегії захисту, здатної виявляти, запобігати та пом'якшувати кіберзагрози в режимі реального часу.

Отримані результати дослідження показують, що інтеграція інноваційних технологій значно покращує виявлення та запобігання кібер-загроз. Наприклад, алгоритми машинного навчання можуть виявляти аномалії в структурі мережевого трафіку, що дозволяє на ранніх стадіях виявляти потенційні атаки. Криптографічні технології посилюють захист даних, забезпечуючи безпеку комунікації та зберігання інформації. Дослідження також показало, що поєднання декількох рівнів захисту створює більш надійну інфраструктуру безпеки, здатну адаптуватися до еволюції кіберзагроз.

Отже, розробка та впровадження інноваційних методів кібербезпеки є необхідною умовою для подолання викликів, пов'язаних із сучасними кіберзагрозами. Дослідження наголошує на важливості постійних інновацій у сфері кібербезпеки для попередження зловмисників і захисту критично важливих інформаційних систем. Висновки висвітлюють потенціал сучасних технологій для революційних змін у практиці кібербезпеки, відкриваючи багатообіцяючий шлях до посилення безпеки та стійкості комп'ютерних систем.

Ключові слова: *захист даних, інформаційна безпека, кіберзагрози, криптографічні технології, мережеві атаки.*

Bondarchuk O. I., Naumenko T. S., Tovt B. M. Development and implementation of innovative cybersecurity methods in computer systems

The rapid pace of digital technology development has led to a significant increase in the complexity and frequency of cyber threats, making cybersecurity one of the most critical issues for modern computer systems. As cyber-attacks become increasingly sophisticated, traditional

security measures are becoming insufficient to protect sensitive data and ensure the integrity of information systems. This necessitates the development and implementation of innovative cybersecurity methods capable of effectively countering such emerging threats. The relevance of this research lies in the need to enhance the resilience of computer systems against cyber threats, particularly in sectors where data protection is crucial, such as finance, healthcare, and national security.

The purpose of this article is to explore the development and practical application of innovative cybersecurity methods adapted to modern computer systems. The main focus is on integrating advanced technologies, such as artificial intelligence, machine learning, and cryptographic methods, to create a multi-layered defense strategy capable of detecting, preventing, and mitigating cyber threats in real-time.

The research results demonstrate that the integration of innovative technologies significantly improves the detection and prevention of cyber threats. For instance, machine learning algorithms can detect anomalies in network traffic patterns, enabling early detection of potential attacks. Cryptographic technologies enhance data protection by ensuring secure communication and information storage. The study also revealed that combining multiple layers of defense creates a more robust security infrastructure capable of adapting to the evolution of cyber threats.

Therefore, the development and implementation of innovative cybersecurity methods are essential for addressing the challenges posed by modern cyber threats. The research emphasizes the importance of continuous innovation in cybersecurity to stay ahead of malicious actors and protect critical information systems. The findings highlight the potential of advanced technologies to bring about revolutionary changes in cybersecurity practices, paving the way for enhanced security and resilience of computer systems.

Key words: *data protection, information security, cyber threats, cryptographic technologies, network attacks.*

Постановка проблеми. Швидка еволюція цифрових технологій значно трансформувала простір інформаційних систем, що призвело до зростання складності та частоти кіберзагроз, а також до появи нових, досі невідомих, типів загроз. Організації різних секторів все більше залежать від комп'ютерних систем при виконанні критично важливих операцій, тому безпека цих систем стала однією з першочергових проблем. Традиційні заходи кібербезпеки, які роками були основою захисту даних, все частіше виявляються неефективними перед складними кібератаками. Ці атаки не лише зростають у кількості, але й удосконалюються у своїх методах, використовуючи такі передові технології, як штучний інтелект, машинне навчання та соціальна інженерія, для подолання захисних систем [1].

Проблема ускладнюється взаємопов'язаністю сучасних комп'ютерних мереж, де одна вразливість може мати каскадний ефект, компрометуючи цілі системи і відкриваючи зловмисникам доступ до конфіденційних даних. Наслідки таких порушень можуть бути просто катастрофічними – від фінансових втрат і перебоїв у роботі до репутаційних збитків і юридичної відповідальності.

Розробка і впровадження інноваційних методів кібербезпеки в комп'ютерних системах стали актуальною проблемою для протидії загрозам, що постійно еволюціонують. Такі методи мають виходити за межі звичайних захисних стратегій і включати передові технології, такі як штучний інтелект, машинне навчання та криптографія, для проактивного виявлення, запобігання та пом'якшення кіберзагроз. Динамічний характер кіберзагроз вимагає, щоб ці методи були адаптивними, здатними розвиватися у відповідь на нові виклики і вразливості [2].

Ефективність таких інноваційних методів слід оцінити в реальних умовах, щоб упевнитися в їх здатності протистояти викликам і складнощам сучасного кіберпростору. Це передбачає не лише технічну розробку нових інструментів і стратегій, але й їх інтеграцію в існуючі системи кібербезпеки та узгодження з політикою та практикою організації.

Мета дослідження – аналіз розвитку та практичного застосування інноваційних методів кібербезпеки, адаптованих до сучасних комп'ютерних систем.

Аналіз останніх досліджень і публікацій. Одним з основних напрямків сучасних досліджень є створення новітніх криптографічних технологій. Такі науковці, як Герасимчук О. [3, с. 290] та Педяш В. [4, с. 391], які розглядали засади сучасної криптографії, стали передумовою для нового покоління науковців до вивчення інноваційних методів шифрування. Такі методи спрямовані на створення ефективніших механізмів захисту даних від нових кіберзагроз. Наприклад, гомоморфне шифрування, яке дозволяє проводити обчислення над зашифрованими даними без необхідності їх попереднього розшифрування, стало значним досягненням. Втім, його реалізація в системах реального часу залишається проблемою через обчислювальні затрати та проблеми з ефективністю. Такі науковці, як Гевко І. [5, с. 64] та Гуржій С. [6, с. 211], досягли значних успіхів у дослідженні ефективності гомоморфного шифрування, але для того, щоб зробити його придатним для масового використання, необхідна подальша оптимізація.

Ще однією важливою темою досліджень є розробка систем виявлення вторгнень (IDS) та систем запобігання вторгненням (IPS), які використовують штучний інтелект (ШІ) та машинне навчання (ML). Такі науковці, як Грицишен Д. [7, с. 26] та Нестеров Ф. [8, с. 64] стали новаторами у дослідженні використання алгоритмів ML для виявлення та пом'якшення кіберзагроз у режимі реального часу. Ці системи розроблені для виявлення незвичайних моделей поведінки, які можуть свідчити про кібератаку. Однак, незважаючи на прогрес, ці системи все ще вразливі до ворожих атак, коли зловмисники маніпулюють вхідними даними, щоб уникнути виявлення.

Виклад основного матеріалу дослідження. Криптографічні технології є основою сучасного захисту даних, оскільки вони забезпечують конфіденційність, цілісність та автентичність інформації у світі, який постійно переходить у цифрову реальність. В умовах, коли кіберзагрози стають надзвичайно складними та масштабними, криптографія відіграє важливу роль у захисті конфіденційних даних від несанкціонованого доступу та зловмисного втручання.

З ростом складності кіберзагроз криптографічні технології розвиваються, щоб відповідати на ці проблеми. Однією з найважливіших інновацій останніх років є гомоморфне шифрування, яке дозволяє виконувати обчислення над зашифрованими даними без необхідності їх попереднього розшифрування. Це зберігає конфіденційність даних і водночас забезпечує їх безпечну обробку, що робить його особливо актуальним у хмарних обчисленнях та аналітиці даних [9, с. 13].

Квантова криптографія – ще один інноваційний підхід, який використовує принципи квантової механіки для створення захищених каналів зв'язку. Квантовий розподіл ключів («КРК») дозволяє обом сторонам генерувати спільний секретний ключ, безпека якого забезпечується законами фізики. Будь-яка спроба перехоплення квантового каналу зв'язку призведе до порушення квантового стану, що сповістить сторони про наявність стороннього втручання.

Пост-квантова криптографія також набирає популярності як відповідна реакція на потенційні загрози з боку нових квантових комп'ютерних технологій, які можуть призвести до зламу більшості криптографічних систем, що наразі використовуються. Науковці розробляють нові алгоритми, стійкі до квантових атак, що забезпечують довготривалу безпеку шифрування даних.

На основі цих інноваційних методів, технологія блокчейн запровадила інноваційні криптографічні практики. Блокчейн ґрунтується на системі розподіленого реєстру, де кожен блок пов'язаний з іншими за допомогою криптографічних хешів. Така структура дозволяє забезпечити, щоб після запису дані не могли бути

змінені без зміни всіх наступних блоків, що забезпечує міцний механізм цілісності та прозорості даних.

Криптографія є невід'ємним інструментом захисту від багатьох кіберзагроз. Її роль виходить за межі захисту даних у стані зберігання або передачі; вона є невід'ємною частиною перевірки особистості, безпечного зв'язку та захисту критичної інфраструктури.

Одне з головних застосувань криптографії – захист комунікацій в інтернеті. Такі протоколи, як SSL/TLS (Secure Sockets Layer/Transport Layer Security) використовують криптографічні методи для встановлення зашифрованих з'єднань між веб-браузерами і серверами, забезпечуючи безпечну передачу конфіденційної інформації, наприклад, облікових даних для входу в систему або фінансових даних [10, с. 134].

Криптографія відіграє важливу роль у запобіганні неавторизованому доступу до даних, що зберігаються в базах даних або на пристроях. Шифрування даних у стані очікування означає, що навіть якщо зловмисник отримає фізичний доступ до носія інформації, дані залишаться захищеними. Для захисту конфіденційної інформації від зламу зазвичай використовують шифрування всього диска, шифрування на рівні файлів і рішення для зашифрованого резервного копіювання.

У процесі верифікації ідентичності криптографічні методи використовуються для створення та перевірки цифрових ідентифікаторів. Інфраструктура відкритих ключів («ІВК») активно використовується для управління цифровими сертифікатами та ключами шифрування, що дозволяє забезпечити безпечну автентифікацію користувачів і пристроїв. Це дуже важливо для захисту доступу до онлайн-сервісів, фінансових транзакцій та конфіденційних корпоративних ресурсів [11].

Криптографія відіграє ключову роль у захисті від кібератак критично важливих об'єктів інфраструктури, таких як електромережі, системи водопостачання та транспортні мережі. Ці системи стають дедалі більше взаємопов'язаними та залежними від цифрових технологій, що робить їх вразливими до кіберзагроз. Для забезпечення цілісності та автентичності даних, якими обмінюються системи управління, а також для захисту від зловмисних втручань або збоїв у роботі використовуються криптографічні протоколи.

У таблиці 1, нами узагальнено зв'язок між різними типами кіберзагроз і відповідними криптографічними рішеннями (табл. 1).

Таблиця 1

Загальна характеристика криптографічних рішень для різних типів кіберзагроз

Кіберзагроза	Криптографічне рішення
Витік даних	Шифрування даних, повне шифрування диска
Man-In-The-Middle attack	SSL/TLS, цифрові підписи
Викрадення ідентифікаційних даних	Інфраструктура відкритих ключів, цифрові сертифікати
Програми-вимагачі	Зашифровані резервні копії, безпечне керування ключами
Неавторизований доступ	Двофакторна автентифікація, шифрування
Квантові обчислювальні загрози	Пост-квантова криптографія, квантовий розподіл ключів

Джерело: власна розробка авторів

Технології виявлення порушень є першою лінією захисту при виявленні несанкціонованого доступу або аномальних дій в мережі. Традиційні системи виявлення вторгнень (IDS) можна розділити на два типи: на основі сигнатур і на основі аномалій. IDS на основі сигнатур використовують для виявлення вторгнень заздалегідь визначені шаблони або сигнатури для відомих загроз. Вони ефективні проти відомих загроз, але недостатньо ефективні проти атак «нульового дня» – тих, що використовують раніше невідомі вразливості. З іншого боку, IDS на основі аномалій виявляють відхилення від нормальної поведінки в мережі. Ці системи ефективніше виявляють нові загрози, але часто дають хибні спрацьовування, що робить їх менш надійними без належного налаштування [12, с. 24].

Розвиток новітніх технологій призвів до створення більш складних систем виявлення вторгнень. Машинне навчання та штучний інтелект (ШІ) все більше інтегруються в IDS для розширення їхніх можливостей. IDS на основі ШІ можуть з часом вивчати шаблони мережевого трафіку, покращуючи свою здатність виявляти аномалії та зменшуючи кількість помилкових спрацьовувань. Такі системи можуть адаптуватися до змін у характері мережевого трафіку та загроз, що робить їх більш стійкими до нових векторів атак.

А ще для аналізу величезних обсягів даних і виявлення складних закономірностей, які можуть свідчити про вторгнення, використовується метод глибинного навчання – підмножина машинного навчання. Такі системи можуть обробляти дані в режимі реального часу, забезпечуючи швидке виявлення потенційних загроз. Використання ШІ та глибинного навчання в IDS є значним кроком на шляху до виявлення вторгнень, що дозволяє точніше і своєчасно виявляти мережеві атаки.

Попередження мережевих атак вимагає багаторівневого підходу, який поєднує різні технології та стратегії для захисту мережі з різних сторін. Брандмауери залишаються основним компонентом мережевої безпеки, контролюючи потік трафіку між надійними і ненадійними мережами. Сучасні брандмауери все частіше інтегруються з розширеними функціями, такими як глибока перевірка пакетів (DPI) і фільтрація на рівні додатків, що дозволяє здійснювати детальніший контроль над мережевим трафіком [13].

На доповнення до брандмауерів, системи запобігання вторгненням (IPS) відіграють важливу роль в активному блокуванні шкідливих дій. На відміну від IDS, які лише виявляють вторгнення, IPS можуть автоматично вживати заходів, щоб запобігти успіху атаки. Це може бути блокування трафіку, відправка уражених систем на карантин або реконфігурація мережевих пристроїв для зменшення загрози. IPS можуть бути розгорнуті як окремі пристрої або інтегровані з IDS в так звану уніфіковану систему управління загрозами (UTM).

Ще одним важливим методом запобігання мережевим атакам є сегментація мережі. Розділивши мережу на менші ізольовані сегменти, можна зменшити розповсюдження атаки, якщо один з них буде скомпрометований. Цей підхід дуже ефективний для захисту конфіденційних даних та критично важливої інфраструктури від латерального переміщення зловмисників.

Рішення для захисту кінцевих точок розвиваються і включають в себе розширені можливості запобігання загрозам. Вони здатні виявляти і блокувати шкідливе програмне забезпечення, програми-вимагачі та інші шкідливі програми ще до того, як вони встигнуть завдати збитків. Вони часто використовують комбінацію виявлення на основі сигнатур, поведінкового аналізу та машинного навчання для виявлення та нейтралізації загроз.

Ефективність нових підходів до виявлення та запобігання мережевим атакам потребує постійної оцінки, щоб переконатися, що вони забезпечують бажаний рівень безпеки. Однією з основних метрик, що використовуються для оцінки ефективності цих підходів, є рівень виявлення – відсоток фактичних атак, правильно ідентифікованих системою. Високий показник виявлення вказує на те, що система ефективно ідентифікує загрози, але він повинен бути збалансований з показником помилкових спрацьовувань, який вимірює частоту нешкідливих дій, помилково позначених як зловмисні [14, с. 31].

Іншим важливим показником є час реакції, який відображає швидкість, з якою система може виявити атаку і відреагувати на неї. У контексті мережевої безпеки навіть кілька секунд затримки можуть мати значні наслідки, що робить швидке виявлення та реагування вкрай важливим. Інтеграція штучного інтелекту та машинного навчання в IDS та IPS показала високу ефективність у покращенні показників виявлення та часу реагування, що робить ці системи ефективнішими у запобіганні атакам в режимі реального часу.

Для комплексної оцінки ефективності різних методів у таблиці 2 нами наведено ключові показники традиційних та інноваційних технологій виявлення та запобігання вторгненням (табл. 2).

Таблиця 2

Показники інноваційних та традиційних технологій виявлення та запобігання кіберзагрозам [14–15]

Технологія	Рівень виявлення	Рівень помилкових спрацювань	Час реагування	Адаптивність до нових загроз
IDS на основі сигнатур	Високий для відомих загроз	Низький для відомих загроз	Середній	Швидка
IDS на основі аномалій	Середній	Високий	Середній	Висока
IDS на основі штучного інтелекту	Високий	Низький	Швидкий	Висока
Традиційна IPS	Високий для відомих загроз	Низький для відомих загроз	Середній	Низька
ШІ-інтегровані IPS	Високий	Низький	Швидкий	Висока

Джерело: власна розробка авторів

Розробка та впровадження інноваційних методів кібербезпеки має важливе значення для того, щоб випередити складні кіберзагрози, які стають все більш і більш складними.

Однією з найперспективніших розробок у цій сфері є використання платформ аналізу загроз, які агрегують та аналізують дані з різних джерел для виявлення нових загроз. Такі платформи використовують штучний інтелект і машинне навчання для кореляції даних, виявлення закономірностей і прогнозування потенційних атак. Завдяки обміну даними про загрози між організаціями та галузями, ці

технології допомагають створити надійніший та проактивніший захист від мережевих атак.

Концепція архітектури нульової довіри набула популярності як метод посилення мережевої безпеки. Нульова довіра передбачає, що весь мережевий трафік, як внутрішній, так і зовнішній, розглядається як потенційно зловмисний. Такий підхід вимагає постійної перевірки ідентифікаційних даних користувачів і жорсткого контролю доступу, що гарантує, що тільки авторизовані користувачі і пристрої можуть отримати доступ до мережевих ресурсів. Архітектура нульової довіри найбільш ефективна для запобігання латеральному руху в мережі, що знижує ризик масштабних порушень [16].

Впровадження інноваційних методів кібербезпеки поширюється і на використання технології блокчейн для захисту мережевих транзакцій. Децентралізована природа блокчейну та криптографічний захист роблять його важливим інструментом для захисту цілісності та автентичності даних. Записуючи транзакції в незмінний реєстр, блокчейн може запобігти фальсифікаціям і забезпечити прозорий запис мережевої діяльності, який можна перевірити.

Такі системи використовують штучний інтелект для автоматизованого реагування, що дозволяє автоматично виявляти загрози і запобігати їхньому впливу на мережу. Ці системи використовують штучний інтелект для автоматичного виявлення загроз і реагування на них, мінімізуючи необхідність втручання людини і скорочуючи час між виявленням і усуненням загрози. Автоматизовані системи реагування можуть виконувати заздалегідь визначені дії, такі як ізоляція уражених систем або блокування зловмисного трафіку, з мінімальною затримкою, тим самим підвищуючи загальну стійкість мережі.

Висновки. Криптографічні технології є необхідним інструментом у сучасну цифрову епоху, оскільки вони забезпечують основні інструменти для захисту даних та кіберзахисту. З розвитком кіберзагроз розвиваються і криптографічні методи, що застосовуються для захисту конфіденційної інформації.

Система мережевої безпеки постійно розвивається, що зумовлено необхідністю протистояти складним кіберзагрозам, які стають дедалі досконалішими. Технології виявлення вторгнень, методи запобігання мережевим атакам і розробка інноваційних методів кібербезпеки є важливими компонентами комплексної стратегії захисту. Інтеграція штучного інтелекту, машинного навчання і передових аналітичних технологій в ці системи дає змогу значно підвищити точність виявлення, швидкість реагування і адаптивність до нових загроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Фролов І., Колодінська Я. Менеджмент кібкрбезпеки ІТ-продуктів. *Кібербезпека: освіта, наука, техніка.* 2024. № 3(23). С. 310-317. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/618 (дата звернення: 24.09.2024).

2. Ревак І. О., Грень Р. Т. Особливості формування безпечного кіберпростору в умовах розвитку цифрової економіки. *Інноваційна економіка*. 2021. № 3 – 4. С. 164 – 169. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4099/3/%d1%80%d0%b5%d0%b2%d0%b0%d0%ba%20%d0%b7%d0%b0%d0%bc%d1%96%d0%bd%d0%b0.pdf (дата звернення: 24.09.2024).

3. Гарасимчук О., Партика А., Нємкова О., Совин Я. Інтегрований підхід та дослідження кіберзлочинів критичної інфраструктури за допомогою системи моніторингу інцидентів вірусів-вимагачів. *Кібербезпека: освіта, наука, техніка.* 2023. № 1 (21). С. 286-296. URL: https://doi.org/10.28925/2663-4023.2023.21.286296 (дата звернення: 24.09.2024).

4. Педяш В., Ледовський Є., Ткач В. Сучасні методи виявлення шкідливого програмного забезпечення. *Вісник Хмельницького національного університету. Серія: Технічні науки.* 2024. № 333(2). С. 389-392. URL: https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/164 (дата звернення: 24.09.2024).

5. Гевко І., Ящик О., Савчин Т., Гільтай Л. Кібербезпека в децентралізованій інтернет екосистемі WEB 3.0. *Наукові записки Тернопільського національного педагогічного університету імені Володимира Гнатюка. Серія: Педагогіка.* 2023. № 1(1). С. 61–68. URL: http://dspace.tnpu.edu.ua/bitstream/123456789/29580/1/8_HEVKO_YASHCHYK_SAVCHYN_HILTAI.pdf (дата звернення: 24.09.2024).

6. Гуржій С. Особливості використання штучного інтелекту у питаннях забезпечення кібербезпеки. *Інформація і право*. 2023. № 4 (47). С. 207-216. URL: http://il.ippi.org.ua/article/view/291669 (дата звернення: 24.09.2024).

7. Грицишен Д., Малишев К., Нонік В., Молотай В. Механізм забезпечення кібербезпеки правоохоронної системи. *Social Development and Security.* 2023. № 13 (4). С. 18-34. URL: https://ouci.dntb.gov.ua/en/works/ldwnApo4/ (дата звернення: 24.09.2024).

8. Нестеров В. Ф. Визначення впливу методів візуалізації даних на процеси прийняття бізнес-рішень. *Таврійський науковий вісник. Серія: Технічні науки.* 2024. № 1. С. 60-70. URL: https://journals.ksauniv.ks.ua/index.php/tech/article/view/540 (дата звернення: 24.09.2024).

9. Скіцько О., Складанний П., Ширшов Р., Гуменюк М., Ворохоб М. Загрози та ризики використання штучного інтелекту. *Кібербезпека: освіта, наука, техніка.* 2023. № 2(22). С. 6-18. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/520 (дата звернення: 24.09.2024).

10. Маруняк С. Виявлення та пом'якшення вразливостей безпеки в протоколах динамічної маршрутизації: поточні виклики та рішення. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво.* 2024. № 55. С. 130-136. URL: http://cit-journal.com.ua/index.php/cit/article/view/567 (дата звернення: 24.09.2024).

11. Hasan M. K., Habib A. A., Shukur Z., Ibrahim F., Islam S., Razzaque M. A. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of network and computer applications.* 2023. № 209. URL: https://dl.acm.org/doi/10.1016/j.jnca.2022.103540 (date of access: 24.09.2024).

12. Васищев В., Денисенко Є. Теоретико-методологічний аналіз інноваційних форм і методів ведення інформаційної боротьби: виклики та загрози кібербезпеці. *Безпека держави.* 2023. № 1(1). С. 21-26. URL: http://sts.nangu.edu.ua/article/view/288258 (дата звернення: 24.09.2024).

13. Sarker I. H., Abushark Y. B., Alsolami F., Khan A. I. Intrudtree: a machine learning based cyber security intrusion detection model. *Symmetry*. 2020. № 12 (5). URL: https://www.mdpi.com/2073-8994/12/5/754 (date of access: 24.09.2024).

14. Вовк А. Сучасні проблеми публічного управління забезпеченням кібербезпеки в Україні. *Публічне управління: концепції, парадигма, розвиток, удосконалення.* 2024. № 8. С. 28-35. URL: https://pa.journal.in.ua/index.php/pa/article/view/136 (дата звернення: 24.09.2024).

15. Пантюшенко Р., Чайка Ю. Штучний інтелект у сфері кібербезпеки: інновації, виклики та перспективи розвитку. *Міжнародний науковий журнал «Military Science»*. 2024. № 2(1). С. 200-206. URL: https://themilitaryscience.com/index.php/journal/article/view/46 (дата звернення: 24.09.2024).

16. Aslan Ö., Aktuğ S. S., Ozkan-Okay M., Yilmaz A. A., Akin E. A. comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics.* 2023. № 12(6). URL: https://www.mdpi.com/2079-9292/12/6/1333 (date of access: 24.09.2024).

REFERENCES:

1. Frolov, I., & Kolodinska, Ya. (2024). Menedzhment kibebezpeky IT-produktiv [Cybersecurity management of IT products]. *Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: education, science, technology*, 3(23), 310-317. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/618 [in Ukrainian].

2. Revak, I.O., & Hren, R.T. (2021). Osoblyvosti formuvannya bezpechnoho kiberprostoru v umovakh rozvytku tsyfrovoi ekonomiky [Features of creating a secure cyberspace in the context of the digital economy development]. *Innovatsiyna ekonomika – Innovative economy*, 3-4, 164-169. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4099/3/%d1%80%d0%b5%d0%b2%d0%b0%d0%ba%20%d0%b7%d0%b0%d0%bc%d1%96%d0%bd%d0%b0.pdf [in Ukrainian].

3. Harasymchuk, O., Partyka, A., Niemkova, O., & Sovin, Ya. (2023). Intehrovanyi pidkhid ta doslidzhennya kiberzlochyniv krytychnoi infrastruktury za dopomohoiu systemy monitorynhu inkydentiv virusiv-vymahachiv [Integrated approach and research of cybercrimes in critical infrastructure using ransomware incident monitoring systems]. *Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: education, science, technology*, 1(21), 286-296. URL: https://doi.org/10.28925/2663-4023.2023.21.286296 [in Ukrainian].

4. Pedyash, V., Ledovskyi, Ye., & Tkach, V. (2024). Suchasni metody vyiavlennya shkidlyvoho prohramnoho zabezpechennya [Modern methods for detecting malware]. *Visnyk Khmelnytskoho natsionalnoho universytetu. Seriya: Tekhnichni nauky – Bulletin of Khmelnytskyi National University. Series: Technical Sciences*, 333(2), 389-392. URL: https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/164 [in Ukrainian].

5. Hevko, I., Yashchyk, O., Savchyn, T., & Hiltai, L. (2023). Kiberbezpeka v detsentralizovanii internet-ekosystemi WEB 3.0 [Cybersecurity in decentralized Internet ecosystem WEB 3.0]. *Naukovi zapysky Ternopilskoho natsionalnoho pedahohichnoho universytetu imeni Volodymyra Hnatyuka. Seriya: Pedahohika – Scientific notes of Ternopil National Pedagogical University named after Volodymyr Hnatyuk. Series: Pedagogy*, 1(1), 61-68. URL: http://dspace.tnpu.edu.ua/bitstream/123456789/29580/1/8_HEVKO_YASHCHYK_SAVCHYN_HILTAI.pdf [in Ukrainian].

6. Hurzhii, S. (2023). Osoblyvosti vykorystannya shtuchnoho intelektu u pytannyakh zabezpechennya kiberbezpeky [Features of using artificial intelligence in cybersecurity]. *Informatsiya i pravo – Information and Law*, 4(47), 207-216. URL: http://il.ippi.org.ua/article/view/291669 [in Ukrainian].

7. Hrytsyshen, D., Malyshev, K., Nonik, V., & Molotai, V. (2023). Mekhanizm zabezpechennya kiberbezpeky pravookhoronnoi systemy [Mechanism of ensuring cybersecurity of the law enforcement system]. *Social Development and Security*, 13(4), 18-34. URL: https://ouci.dntb.gov.ua/en/works/ldwnApo4/ [in Ukrainian].

8. Nesterov, V.F. (2024). Vyznachennya vplyvu metodiv vizualizatsii danykh na protsesy pryiniattya biznes-rishen [Determining the impact of data visualization methods on business decision-making processes]. *Tavriiskyi naukovyi visnyk. Seriya: Tekhnichni nauky – Tavriian Scientific Bulletin. Series: Technical Sciences*, 1, 60-70. URL: https://journals.ksauniv.ks.ua/index.php/tech/article/view/540 [in Ukrainian].

9. Skitsko, O., Skladannyi, P., Shirshov, R., Humeniuk, M., & Vorokhob, M. (2023). Zahrozy ta ryzyky vykorystannya shtuchnoho intelektu [Threats and risks of artificial intelligence use]. *Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: education, science, technology*, 2(22), 6-18. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/520 [in Ukrainian].

10. Marunyiak, S. (2024). Vyiavlennia ta pomiakshennia vrazlyvostei bezpeky v protokolakh dynamichnoi marshrutyzatsii [Detection and mitigation of security vulnerabilities in dynamic routing protocols: Current challenges and solutions]. *Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo – Computer-*

integrated technologies: education, science, production, 55, 130-136. URL: http://cit-journal.com.ua/index.php/cit/article/view/567 [in Ukrainian].

11. Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of network and computer applications*, 209. URL: https://dl.acm.org/doi/10.1016/j.jnca.2022.103540

12. Vasyshchev, V., & Denysenko, Ye. (2023). Teoretyko-metodolohichnyi analiz innovatsiinykh form i metodiv vedennia informatsiinoi borotby: vyklyky ta zahrozy kiberbezpetsi [Theoretical-methodological analysis of innovative forms and methods of conducting information warfare: Challenges and threats to cybersecurity]. *Bezpeka derzhavy – State security*, 1(1), 21-26. URL: http://sts.nangu.edu.ua/article/view/288258 [in Ukrainian].

13. Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. *Symmetry*, 12(5). URL: https://www.mdpi.com/2073-8994/12/5/754

14. Vovk, A. (2024). Suchasni problemy publichnoho upravlinnya zabezpechenniam kiberbezpeky v Ukraini [Current problems of public administration in ensuring cybersecurity in Ukraine]. *Publichne upravlinnya: kontseptsii, paradyhma, rozvytok, udoskonalennia – Public administration: concepts, paradigm, development, improvement*, 8, 28-35. URL: https://pa.journal.in.ua/index.php/pa/article/view/136 [in Ukrainian].

15. Pantiushenko, R. & Chaika, Yu. (2024). Artificial intelligence in the sphere of cybersecurity: innovations, challenges, and development prospects. *Military Science*, 2(1), 200-206. URL: https://themilitaryscience.com/index.php/journal/article/view/46 [in Ukrainian].

16. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6). URL: https://www.mdpi.com/2079-9292/12/6/1333