ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

DOI: 10.18372/2225-5036.30.19238

ВПЛИВ НЕЙРОННИХ МЕРЕЖ НА РОЗВИТОК КІБЕРБЕЗПЕКИ В УМОВАХ РЕГУЛЯТОРНИХ ЗМІН

Олександр Кушнерьов[1], Ірина Позовна[1], Владислав Сокол[2]

[1]Сумський державний університет, Україна
[2]Національний технічний університет «Харківський політехнічний інститут», Україна

КУШНЕРЬОВ Олександр Сергійович, PhD
Дата та місце народження: 22.10.1991 р., с. Дуболугівка, Чернігівська область, Україна
Освіта: Сумський державний педагогічний університет ім. А.С. Макаренка, 2015; Сумський державний університет, 2017; Національний технічний університет "Харківський політехнічний інститут", 2023.
Посада: старший викладач кафедри економічної кібернетики, Сумський державний університет, Україна
Наукові інтереси: кібербезпека, штучний інтелект, програмування, інформаційні технології.
Публікації: більше 30 наукових публікацій, включаючи монографії, підручники, статті та патенти.
E-mail: o.kushnerov@biem.sumdu.edu.ua.
Orcid ID: 0000-0001-8253-5698.

ПОЗОВНА Ірина Вікторівна, к.е.н.
Дата та місце народження: 15.10.1991 р., м. Суми, Україна.
Освіта: ДВНЗ «Українська академія банківської справи», 2013.
Посада: старша викладачка кафедри економічної кібернетики, Сумський державний університет, Україна, Україна.
Наукові інтереси: поведінкова економіка, вплив пандемій на економічний та соціальний розвиток, фінансова залученість та грамотність, аналіз та візуалізація даних, великі дані.
Публікації: понад 50 наукових публікацій, серед яких монографії, навчальні посібники, статті та патенти.
E-mail: i.pozovna@biem.sumdu.edu.ua.
Orcid ID: 0000-0003-1934-7031.

СОКОЛ Владислав, к.е.н.
Освіта: Національний технічний університет «Харківський політехнічний інститут».
Посада: кандидат технічних наук, докторант за спеціальністю 125 «Кібербезпека та захист інформації».
Наукові інтереси: кібербезпека, системи управління знаннями, підготовка і перепідготовка персоналу ІТ-компаній, якість процесу розробки програмного забезпечення.
Публікації: понад 20 наукових публікацій. серед яких монографії, навчальні посібники та статті.
E-mail: Vladyslav.sokol@gmail.com.
Orcid ID: 0009-0009-9446-2049.

Анотація*. У статті досліджено вплив нейронних мереж на розвиток кібербезпеки в умовах постійних змін у регуляторному полі. У сучасному цифровому світі, де складність та частота кібератак стрімко зростають, традиційні методи безпеки стають недостатніми. Нейронні мережі, як одна з ключових технологій штучного інтелекту, відкривають нові можливості для підвищення ефективності систем кіберзахисту шляхом автоматизації виявлення загроз, аналізу аномалій та запобігання атакам. Інтеграція нейронних мереж з іншими новітніми технологіями, такими як блокчейн та квантові обчислення, відкриває нові горизонти для створення стійкіших систем. Однак такі виклики, як атаки типу adversarial, непрозорість алгоритмів (проблема «чорної скриньки») та дотримання регуляторних вимог, зокрема GDPR та ISO 27001, потребують особливої уваги. У дослідженні також розглянуто етичні та правові аспекти використання нейронних мереж у кібербезпеці, підкреслюючи важливість розвитку пояснювального штучного інтелекту (XAI) та збереження людського контролю для безпечного та етичного впровадження. Стаття робить висновок, що нейронні мережі є перспективним інструментом у боротьбі з кіберзагрозами, проте їх ефективність залежатиме від здатності організацій і держав вирішувати проблеми конфіденційності, етичні питання та технічні вразливості.*

Ключові слова: *нейронні мережі, кібербезпека, штучний інтелект, кібератаки, вразливості систем, регуляторні стандарти.*

Постановка проблеми

У сучасному цифровому світі, де кількість підключених до інтернету пристроїв збільшується з кожним роком, кіберзагрози стають критичним викликом для держав, організацій та приватних користувачів. Активний розвиток технологій, таких як Інтернет речей (IoT) та хмарні інфраструктури, хоча й створює значні можливості для бізнесу, водночас розширює вектори для кібератак. Зростання обсягу даних та швидка еволюція нових технологій потребують інтеграції комплексних підходів до кібербезпеки. Це підштовхує організації до використання штучного інтелекту в своїх захисних системах, що підвищує ефективність моніторингу та попередження загроз [[10]]. За даними Cybersecurity Ventures, до 2025 року глобальні втрати від кіберзлочинів можуть сягнути $10,5 трлн на рік [[5]]. Це перетворює кіберзлочинність на один із найшвидше зростаючих економічних ризиків у світі [[10]]. Як видно з графіку (Рис. 1), витрати на кіберзлочинність стрімко зростають: з $3 трлн у 2015 році до прогнозованих $10,5 трлн у 2025 році [[5]]. Оцінені збитки включають руйнування даних, фінансові крадіжки, втрати продуктивності, викрадення інтелектуальної власності та дестабілізацію бізнес-процесів. Хмарні платформи та Інтернет речей (IoT) є особливо вразливими до кіберзагроз, оскільки вони відіграють критичну роль у сучасній інфраструктурі й обробляють величезні обсяги даних.

Враховуючи ключову важливість цих технологій, вони стали основними цілями для кіберзлочинців. Поява нових типів атак, зокрема атак на мережеву інфраструктуру та IoT-пристрої, підкреслює необхідність застосування глибших методів моніторингу даних та виявлення загроз.

Використання штучного інтелекту, зокрема технологій для аналізу великих даних у реальному часі, є критично важливим кроком для підвищення рівня захисту [[1]].

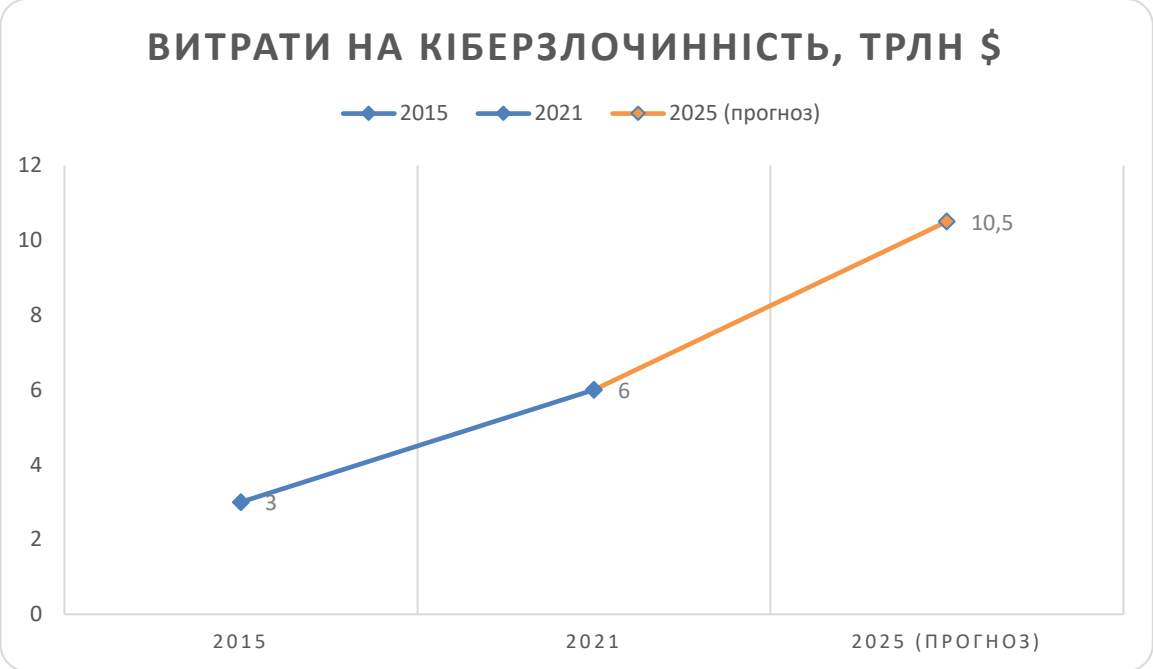

Рис. 1. Прогнозовані витрати на кіберзлочинність (2015-2025).
Джерело: складено авторами на основі [[5]]

Враховуючи ці виклики, з'являється гостра необхідність у впровадженні інноваційних підходів до виявлення та запобігання кіберзагрозам. Традиційні методи захисту, такі як фаєрволи та антивірусне програмне забезпечення, часто виявляються недостатньо ефективними в умовах динамічно змінюваного ландшафту загроз. Стрімкий розвиток технологій вимагає впровадження штучного інтелекту, зокрема нейронних мереж, які здатні самостійно навчатися та адаптуватися до нових загроз. Завдяки здатності автоматизувати процеси виявлення аномалій, нейронні мережі стали центральним елементом сучасних систем кіберзахисту [[4]]. Їхнє використання дозволяє не лише виявляти підозрілу активність у поведінці користувачів та мереж, але й ефективно прогнозувати нові кібератаки, що значно підвищує загальну ефективність захисних систем [[12]]. Окрім цього, генеративні нейронні мережі надають можливість моделювати ймовірні сценарії атак, що дозволяє системам безпеки бути проактивнішими та ефективніше реагувати на потенційні загрози у реальному часі [[13]].

Аналіз останніх досліджень і публікацій

Важливо відзначити, що нейронні мережі здатні обробляти великі обсяги даних у реальному часі, що є вирішальним для забезпечення швидкої реакції на потенційні загрози. Це дозволяє системам безпеки швидко адаптуватися до нових типів загроз і підвищувати точність виявлення шкідливих дій, особливо в умовах зростання складності атак на Інтернет речей (IoT) та хмарні платформи [[19]]. Особливу роль у цьому відіграють національні інфраструктури, які потребують надійного захисту від кіберзагроз. У таких системах нейронні мережі використовуються для виявлення аномалій та шкідливих дій, а також для моніторингу критичних процесів. Це дозволяє забезпечити безперервність та безпеку функціонування

національних інфраструктур, таких як енергетичні та транспортні системи [[1]].

Однак розвиток нейронних мереж у сфері кібербезпеки не є однозначним. Поряд із технічними викликами постають питання, пов'язані з регуляторними вимогами та етикою використання штучного інтелекту. Зокрема, нормативні акти, такі як Загальний регламент захисту даних (GDPR) [[6]; [11]] та ISO 27001 [[8]], запроваджують нові стандарти для захисту даних, які можуть як стимулювати, так і обмежувати впровадження нейронних мереж. Вивчення взаємодії між нейронними мережами та регуляторними вимогами є критично важливим для майбутнього розвитку кібербезпеки.

Мета та постановка завдання

Метою цієї статті є дослідження впливу нейронних мереж на розвиток кібербезпеки в умовах постійних змін регуляторного середовища. Поряд із технічними досягненнями у сфері штучного інтелекту, розвиток законодавчих та нормативних вимог відіграє ключову роль у впровадженні новітніх технологій у сфері кіберзахисту. Важливим аспектом є також вплив нормативних вимог, таких як GDPR (Загальний регламент захисту даних), NIS Directive (Директива про безпеку мережевих та інформаційних систем) та ISO 27001 [[8]], на використання нейронних мереж у кібербезпеці [[6]; [9]; [11]]. Ці стандарти встановлюють нові вимоги до захисту даних, що стимулює або обмежує впровадження технологій штучного інтелекту у різних секторах.

Виклад основного матеріалу дослідження

Нейронні мережі є однією з ключових складових сучасних технологій штучного інтелекту (ШІ) та машинного навчання, які вирізняються своєю здатністю обробляти великі обсяги даних і навчатися на основі прикладів. Нейронні мережі імітують роботу людського мозку через взаємодію численних штучних нейронів, які передають інформацію між собою та ухвалюють рішення на основі отриманих даних. Ця властивість робить нейронні мережі надзвичайно потужним інструментом у різних сферах, зокрема в кібербезпеці, де головною загрозою є не лише існуючі кібератаки, а й здатність зловмисників розробляти нові види атак. Завдяки здатності до самонавчання, нейронні мережі не лише здатні виявляти нові типи загроз, але й адаптувати свої стратегії для ефективної боротьби з ними, що робить їх надзвичайно цінними в умовах постійно змінюваних викликів у кіберпросторі.

Серед досягнень у галузі нейронних мереж особливу увагу привертає механізм уваги (Attention Mechanism). Ця технологія дозволяє нейронним мережам фокусуватися на найбільш релевантних аспектах даних, відсікаючи другорядну інформацію, що є критично важливим при роботі з великими масивами даних, як, наприклад, мережевий трафік чи поведінкові патерни користувачів [[16]].

Механізм уваги дозволяє нейронним мережам аналізувати трафік у реальному часі, виділяючи підозрілу активність, яка може вказувати на потенційну загрозу. Така здатність є особливо важливою для захисту хмарних сервісів та інфраструктур Інтернету речей (IoT), де обсяги інформації величезні, а ризик кібератак зростає щороку [[17]; [15]].

Трансформери, як одна з різновидів нейронних мереж, вже продемонстрували свою ефективність у сфері обробки послідовних даних та виявлення аномалій. Вони забезпечують високий рівень точності під час аналізу мережевого трафіку та можуть виявляти загрози в реальному часі, що робить їх надзвичайно корисними для систем кіберзахисту. Здатність трансформерів до навчання на основі попередніх загроз дозволяє їм не тільки виявляти нові атаки, але й прогнозувати їх розвиток, що є вирішальним фактором для запобігання кіберзлочинів. Наприклад, нейронні мережі з механізмом уваги можуть аналізувати тисячі одночасних сесій мережевого трафіку та виявляти відхилення від нормальної поведінки, сигналізуючи про спроби несанкціонованого доступу [[17]].

Серед різних типів нейронних мереж кожна має свої специфічні переваги у вирішенні певних завдань кібербезпеки. Згорткові нейронні мережі (CNN) здебільшого використовуються для аналізу графічних даних та обробки відео. У контексті кібербезпеки ці мережі можуть застосовуватись для аналізу мережевих топологій або візуалізації кіберзагроз, зокрема у системах відеоспостереження. CNN також можуть бути використані для моніторингу активності у фізичних об'єктах, таких як серверні кімнати або центри обробки даних, де візуальні сигнали можуть свідчити про спроби фізичного втручання або несанкціонованого доступу до обладнання. Такий підхід дозволяє ідентифікувати загрози в реальному часі та оперативно на них реагувати, що підвищує загальний рівень безпеки [[14]; [15]].

Рекурентні нейронні мережі (RNN), особливо їх вдосконалені версії, такі як LSTM (довготривала короткочасна пам'ять), є ідеальними для аналізу часових рядів даних. Вони дозволяють виявляти поведінкові патерни, які можуть сигналізувати про поступове зростання загроз, наприклад, атаки типу «відмова в обслуговуванні» (DDoS). RNN використовуються для аналізу мережевого трафіку впродовж тривалих періодів часу, що дозволяє виявляти відхилення від нормальної поведінки та прогнозувати потенційні загрози на основі змін у трафіку. Це надає можливість системам безпеки оперативно ідентифікувати загрози та вживати необхідних заходів для їхньої нейтралізації [[15]].

Ще одним ключовим інструментом у сфері кібербезпеки є автокодувальники (Autoencoders). Ці нейронні мережі використовуються для виявлення аномалій у даних через відновлення вхідної інформації. Якщо вихідні дані суттєво відрізняються від вхідних, це може вказувати на наявність аномалій або шкідливого коду в системі. Автокодувальники активно застосовуються для виявлення шкідливих файлів, шкідливих активностей у мережі або інших порушень, які не можуть бути виявлені за допомогою традиційних методів на основі сигнатур. Вони стають ефективним інструментом у боротьбі зі складними загрозами, такими як нові версії шкідливих програм, що постійно модифікуються зловмисниками [[14]; [15]].

У сучасних системах кібербезпеки нейронні мережі стали невід'ємною частиною автоматизованих рішень для моніторингу та захисту інформаційних систем. Здатність нейронних мереж обробляти великі обсяги даних у реальному часі є критично важливою

для інфраструктур, таких як хмарні сервіси та IoT. Хмарні сервіси потребують постійного моніторингу активності для запобігання загрозам, адже вони обробляють величезні масиви даних. Нейронні мережі забезпечують ефективне виявлення підозрілої активності, аналіз трафіку в реальному часі та виявлення аномальної поведінки, яка може свідчити про кібер-загрози.

Завдяки здатності навчатися на основі попередніх атак, нейронні мережі можуть прогнозувати нові типи загроз і швидко реагувати на них, що значно підвищує безпеку хмарних систем [[14]; [15]].

Таблиця 1

Оглядова таблиця типів нейронних мереж

Тип нейронної мережі	Особливості	Застосування в кібербезпеці
CNN	Здатність аналізувати графічні дані, наприклад, зображення і відео.	Аналіз мережевих топологій та відеоспостереження для виявлення фізичних втручань або загроз.
RNN	Орієнтовані на обробку послідовних даних і аналіз часових рядів.	Виявлення патернів, які можуть сигналізувати про DDoS атаки та інші тривалі загрози.
LSTM	Вдосконалена версія RNN, здатна зберігати важливу інформацію на тривалий період.	Виявлення поступових загроз у часових рядах, таких як зростання аномалій у трафіку.
Autoencoders	Моделі для виявлення аномалій через відновлення вхідних даних.	Виявлення шкідливих файлів та активностей через аномальне відновлення даних.
Transformers	Здатність обробляти послідовні дані та ефективно виявляти аномалії.	Аналіз мережевого трафіку для виявлення загроз в реальному часі і прогнозування їх розвитку.

Існує багато успішних прикладів використання нейронних мереж для захисту інформаційних систем, одним із найвідоміших є їхнє впровадження в антивірусні системи. Завдяки машинному навчанню, антивірусні програми можуть виявляти не тільки вже відомі шкідливі програми, але й нові загрози, які ще не зареєстровані в базах даних. Це надає нейронним мережам можливість швидко реагувати на нові загрози та захищати користувачів від потенційно небезпечних атак, навіть якщо ці загрози раніше не були відомі. Крім того, нейронні мережі активно застосовуються для аналізу мережевого трафіку. Вони можуть ідентифікувати аномальні патерни у поведінці користувачів чи пристроїв, що свідчить про спроби несанкціонованого доступу до мережі або інших загроз. Таке використання нейронних мереж стає важливою складовою сучасних рішень для забезпечення безпеки підприємств та організацій [[14]; [15]].

У контексті IoT нейронні мережі сприяють підвищенню безпеки підключених пристроїв, які є особливо вразливими до кібератак через недостатність захисних механізмів. Нейронні мережі дозволяють аналізувати поведінкові патерни цих пристроїв, виявляти підозрілу активність і швидко реагувати на потенційні загрози. В умовах критичних інфраструктур, таких як системи охорони здоров'я чи енергетики, де безпека є пріоритетом, нейронні мережі дозволяють автоматично моніторити стан підключених пристроїв, забезпечуючи їхню безперебійну роботу та захист від зовнішніх загроз [[14]; [15]].

У контексті швидкого розвитку цифрових технологій та широкого впровадження штучного інтелекту (ШІ) питання регулювання та створення нормативних рамок для цієї технології набувають особливого значення на міжнародному рівні. Впровадження ШІ в різні сфери суспільного життя піднімає низку етичних, правових і технічних питань, що потребують ретельного аналізу з боку урядів, приватного сектора та наукової спільноти. ШІ створює нові можливості, але водночас приносить нові виклики, пов'язані з конфіденційністю даних, прозорістю алгоритмів, можливими зловживаннями та іншими ризиками. У цьому контексті виникає потреба у створенні чітких регуляторних рамок, які забезпечать етичне, безпечне та законне використання ШІ [[18]].

Однією з найважливіших ініціатив у цій сфері є EU AI Act, що представляє собою всеосяжну нормативну базу для регулювання штучного інтелекту на території Європейського Союзу [[3]]. Основна мета цього акта — забезпечити розробку та використання систем ШІ таким чином, щоб вони відповідали етичним стандартам, поважали права людини та гарантували безпеку у використанні. Основна концепція акта базується на класифікації систем ШІ за рівнем ризику – від мінімального до неприпустимого. Особливу увагу приділено високоризиковим системам, які застосовуються в таких сферах, як критична інфраструктура, охорона здоров'я, зайнятість і надання основних приватних послуг. До таких систем висуваються підвищені вимоги щодо прозорості алгоритмів, якості даних та забезпечення людського нагляду. Регламент спрямований на попередження порушень прав людини, а також на захист громадян від можливих зловживань технологіями ШІ [[18]].

Ще одним важливим документом є NIST AI Risk Management Framework, розроблений Національним інститутом стандартів і технологій (NIST) у США [[2]]. Ця рамка створена для того, щоб допомогти організаціям оцінювати та управляти ризиками, пов'язаними з впровадженням ШІ. Вона пропонує соціотехнічний підхід, враховуючи як технічні, так і етичні аспекти ризиків, що виникають у процесі впровадження ШІ. Основні компоненти цього підходу включають управління контекстом ризиків, оцінку продуктивності систем ШІ та управління ризиками протягом усього життєвого циклу.

З огляду на широке застосування ШІ в різних галузях, ця рамка допомагає забезпечити відповідальне

використання ШІ, мінімізуючи ризики як для організацій, так і для суспільства загалом [[18]].

Прикладом високих стандартів у галузі безпеки ШІ з боку приватного сектора є Google Secure AI Framework (SAIF) [[7]]. Цей фреймворк розроблений для вирішення унікальних викликів, пов'язаних з впровадженням ШІ, зокрема ворожими атаками на моделі, питаннями конфіденційності даних та надійністю алгоритмів. Google розробила SAIF для запровадження найкращих практик з безпеки та цілісності систем ШІ, приділяючи особливу увагу захисту конфіденційних даних і забезпеченню безпеки протягом усього життєвого циклу моделей. Це включає безпечні джерела даних, надійні практики навчання моделей та постійний моніторинг систем на предмет потенційних вразливостей [[18]]. Ця ініціатива демонструє, як приватні компанії можуть зробити вагомий внесок у розвиток етичних стандартів безпеки ШІ та сприяти відповідальному впровадженню цих технологій.

Міжнародний стандарт ISO 42001, який визначає систему управління штучним інтелектом, є важливим інструментом для організацій, що прагнуть інтегрувати ШІ відповідно до етичних норм і міжнародних стандартів. Цей стандарт спрямований на підвищення довіри до технологій ШІ через забезпечення їх прозорого та справедливого використання, зокрема шляхом дотримання принципів відповідальності, безпеки та поваги до прав людини. ISO 42001 охоплює всі етапи управління проєктами ШІ, від їх розробки до впровадження, і спрямований на забезпечення етичної відповідальності та підвищення громадської довіри до технологій ШІ [[18]].

Для організацій, які бажають відповідати найвищим стандартам у сфері інформаційної безпеки, стандарти ISO 27001 та ISO 27701 залишаються основними орієнтирами. Стандарт ISO 27001 пропонує інструкції щодо управління інформаційною безпекою, включаючи застосування технологій ШІ для моніторингу кіберзагроз та захисту інформаційних активів. У той же час, стандарт ISO 27701 доповнює ці вимоги, охоплюючи питання захисту персональних даних, що є особливо актуальним при використанні великих обсягів даних для навчання моделей ШІ [[18]].

Таблиця 2

Порівняльна таблиця регуляторних актів надає детальний огляд вимог і впливу нормативних актів на впровадження нейронних мереж у різних сферах

Назва нормативного акту	Сфера дії	Ключові вимоги	Вплив на впровадження нейронних мереж
U AI Act	Європейський Союз	Класифікація систем ШІ за рівнем ризику; вимоги до прозорості, якості даних та людського нагляду	Впровадження прозорих і безпечних ШІ систем, що поважають права людини
NIST AI Risk Management Framework	Сполучені Штати Америки	Соціотехнічний підхід; управління ризиками; оцінка продуктивності та ризиків	Оцінка та зменшення ризиків, пов'язаних з використанням нейронних мереж
Google Secure AI Framework (SAIF)	Приватний сектор (Google)	Безпечні джерела даних; надійні практики навчання моделей; моніторинг вразливостей	Забезпечення безпеки та захисту даних у нейронних мережах
ISO/IEC 42001 AI Management System	Міжнародний стандарт	Відповідальність, прозорість, справедливість, безпека, оцінювання впливів систем ШІ	Підтримка етичного та безпечного впровадження нейронних мереж

Важливим регуляторним актом є Загальний регламент захисту даних (GDPR), ухвалений Європейським Союзом у 2018 році. GDPR регулює обробку персональних даних і вимагає від організацій впровадження сучасних технологій, таких як нейронні мережі, для забезпечення надійного захисту конфіденційної інформації. Використання ШІ для виявлення витоків даних і прогнозування загроз дозволяє організаціям відповідати вимогам GDPR та підвищує їхню здатність забезпечувати захист даних [[6]; [11]].

Регуляторні акти, такі як Директива про безпеку мережевих та інформаційних систем (NIS Directive), відіграють важливу роль у забезпеченні кібербезпеки, особливо для критичної інфраструктури. Використання нейронних мереж у цих системах дає змогу автоматично виявляти аномалії в мережевій поведінці та прогнозувати потенційні загрози, що значно підвищує рівень безпеки інфраструктури [[9]].

Інтеграція таких стандартів, як ISO 42001, ISO 27001 і GDPR, створює міцну основу для безпечного, етичного та законного використання штучного інтелекту. Дотримуючись цих стандартів, організації не лише забезпечують відповідність юридичним вимогам, але й підвищують довіру до своїх продуктів та послуг. Це сприяє сталому розвитку технологій штучного інтелекту на глобальному рівні.

Нейронні мережі, як один із основних інструментів штучного інтелекту, значно вплинули на розвиток кібербезпеки. Їхня здатність проводити глибокий аналіз великих обсягів даних і самонавчатися відкриває нові можливості для захисту цифрових систем. Головна перевага нейронних мереж полягає в їхній здатності автоматично виявляти аномалії, аналізувати складні поведінкові патерни та розпізнавати нові типи атак, які можуть залишитися непоміченими традиційними системами захисту, що базуються на сигнатурах. Завдяки своїй адаптивності та здатності до постійного вдосконалення, нейронні мережі стають ключовим елементом сучасних систем кіберзахисту.

У сучасному світі кібербезпека є однією з провідних сфер технологічного розвитку, особливо з огляду на зростання складності та частоти кібератак. Нейронні мережі демонструють значний потенціал у забезпеченні безпеки інформаційних систем у різних галузях економіки. Вони не тільки ефективно виявляють загрози, але й прогнозують можливі вразливості

в системах, що дозволяє здійснювати превентивні заходи для захисту критичної інфраструктури.

Одним із ключових секторів, де нейронні мережі вже демонструють свою ефективність, є хмарні сервіси. Завдяки здатності обробляти великі обсяги даних у реальному часі, ці системи дозволяють виявляти аномалії в поведінці користувачів та пристроїв, запобігаючи потенційним загрозам несанкціонованого доступу до даних або атакам на віртуальні машини. Наприклад, нейронні мережі використовуються для аналізу змін у поведінці пристроїв у хмарній інфраструктурі, що дозволяє зменшити ризики втрати даних або компрометації систем [[14]].

У фінансовому секторі нейронні мережі допомагають виявляти шахрайські операції в реальному часі, що значно зменшує кількість шахрайських транзакцій і запобігає витоку фінансових даних клієнтів. Це має особливе значення в умовах зростання кількості атак на банківські системи. Використання таких технологій дозволяє знизити ризик шахрайства на 18% та підвищити точність виявлення аномалій до 23%, як зазначено в дослідженнях Сумана Тапалії [[15]]. Ефективність нейронних мереж у фінансовому секторі підтверджується їхньою здатністю прогнозувати загрози, аналізуючи поведінкові патерни клієнтів та операції, що значно підвищує рівень захисту.

Важливу роль нейронні мережі відіграють також у сфері Інтернету речей (IoT). Системи IoT є особливо вразливими до кібератак через брак належних засобів захисту. Проте, завдяки використанню нейронних мереж можна автоматично виявляти підозрілі поведінкові патерни пристроїв, запобігаючи потенційним загрозам у критичних інфраструктурах, таких як розумні будинки або автомобілі. Наприклад, автокодувальники використовуються для виявлення аномалій у поведінці пристроїв IoT, що дозволяє швидко реагувати на підозрілу активність [[17]].

Незважаючи на очевидні переваги нейронних мереж, їхнє використання супроводжується низкою викликів. Однією з головних проблем є вразливість до атак типу «adversarial attacks», які спрямовані на введення системи в оману через спеціально модифіковані вхідні дані. Це може призвести до неправильного тлумачення даних системою безпеки, що в критичних умовах може дозволити зловмисникам проникнути в систему або залишити без уваги реальні загрози [[15]]. Вразливість до таких атак особливо актуальна для систем машинного навчання, що використовуються для виявлення кіберзагроз, оскільки кожне неправильне розпізнавання може спричинити серйозні наслідки. Такі атаки становлять серйозну загрозу для критичних систем, таких як системи виявлення шкідливого ПЗ або фінансові системи, оскільки модифіковані дані можуть залишатися непоміченими, що дозволяє зловмисникам здійснювати атаки або викрадати дані [[13]].

Крім того, велика кількість хибних спрацьовувань (false positives) також становить значну проблему для використання нейронних мереж у кібербезпеці. Це питання є особливо важливим для систем, що працюють із великими обсягами даних у режимі реального часу. Якщо система помилково визначає нешкідливі дії як загрозу, ресурси компаній можуть бути витрачені на обробку хибних тривог, що знижує загальну ефективність захисних заходів. У фінансових установах такі хибні спрацьовування можуть блокувати важливі транзакції або затримувати обслуговування клієнтів, що призводить до серйозних наслідків для бізнесу, зокрема фінансових втрат та зниження рівня довіри клієнтів [[14]; [17]].

Враховуючи ці проблеми, дослідники активно працюють над розробкою нових методів захисту від атак, зокрема шляхом створення більш стійких до adversarial attacks алгоритмів. До таких рішень належить застосування методів захисту на основі глибокого навчання, які здатні адаптуватися до нових видів загроз і зменшувати кількість хибних спрацьовувань [[13]; [15]].

Використання нейронних мереж у кібербезпеці також відкриває нові перспективи для інтеграції з іншими технологіями, такими як блокчейн і квантові обчислення. Блокчейн забезпечує децентралізований і надійний захист даних, тоді як квантові обчислення підвищують обчислювальну потужність, що дозволить нейронним мережам більш ефективно виявляти загрози. Інтеграція цих технологій здатна забезпечити новий рівень захисту від кіберзагроз, зокрема квантових атак, які можуть зламати сучасні криптографічні методи [[14]].

Таким чином, нейронні мережі вже сьогодні займають ключове місце у системах кібербезпеки та мають значний потенціал для подальшого розвитку в умовах постійно змінюваного кіберландшафту. Однак, для забезпечення їхньої ефективності слід враховувати вразливість до атак, проблеми з точністю, а також інтеграцію з новітніми технологіями, такими як блокчейн і квантові обчислення.

Використання нейронних мереж у кібербезпеці створює нові виклики в контексті конфіденційності даних, особливо з огляду на обсяги персональної інформації, що використовується для навчання моделей. Нейронні мережі, що потребують великих масивів даних для точного прогнозування кіберзагроз, можуть становити ризики порушення конфіденційності, якщо дані містять чутливу інформацію про користувачів або бізнеси. Регуляторні акти, такі як GDPR та CCPA, вимагають, щоб будь-яка обробка персональних даних відповідала суворим правилам конфіденційності. Це стосується також випадків, коли нейронні мережі аналізують мережевий трафік або поведінкові дані користувачів. Наприклад, якщо для навчання моделі ШІ використовуються дані про поведінку користувачів в інтернеті, компанії повинні отримати явну згоду на обробку таких даних і гарантувати, що конфіденційна інформація не буде передана третім сторонам без згоди користувачів [[15]].

Щоб запобігти порушенню конфіденційності, багато компаній почали впроваджувати методи федеративного навчання, які дозволяють навчати нейронні мережі без централізації даних. Це означає, що дані залишаються на локальних пристроях користувачів, а модель ШІ оновлюється за допомогою узагальнених параметрів, що значно знижує ризик витоку даних. Подібні підходи не тільки сприяють захисту конфіденційності, але й відповідають вимогам регуляторних органів щодо захисту персональних даних [[17]]. Оскільки нейронні мережі часто застосовуються для автоматизації процесів у кібербезпеці,

виникають питання управління та підзвітності таких систем. Одним із ключових викликів є непрозорість рішень, що ухвалюються нейронними мережами. Цей феномен, відомий як «чорна скринька» (black box), полягає в тому, що навіть розробники не завжди можуть пояснити, чому система ШІ прийняла те чи інше рішення. У сфері кібербезпеки це може мати серйозні наслідки, адже компанії повинні бути впевненими в надійності та обґрунтованості рішень, ухвалених алгоритмами. Наприклад, якщо нейронна мережа визначає певну активність у мережі як загрозу, компанія повинна мати можливість пояснити, чому така активність була класифікована як загроза. Це є особливо важливим у контексті дотримання регуляторних вимог, оскільки неправильне визначення загроз або порушення даних може спричинити серйозні юридичні наслідки [[14]].

Для вирішення цих проблем дослідники активно працюють над розвитком концепції пояснювального штучного інтелекту (Explainable AI, XAI), яка покликана зробити алгоритми ШІ більш прозорими і зрозумілими для користувачів. Пояснювальний ШІ не лише дає змогу зрозуміти, як і чому система ухвалює певні рішення, але й допомагає виявити можливі упередження або помилки, що можуть вплинути на результати аналізу. Це є особливо важливим для складних галузей, таких як медицина, фінанси або кібербезпека, де неправильні рішення можуть мати критичні наслідки [[14]; [15]].

Важливим аспектом є також вимога до компаній здійснювати регулярні аудити своїх систем ШІ, щоб забезпечити їхню відповідність встановленим стандартам і дотримання етичних та правових норм. Наприклад, такі аудити дозволяють забезпечити відповідність вимогам щодо захисту даних, прозорості прийняття рішень, а також дотримання етичних принципів, зокрема уникнення дискримінаційних моделей або використання ШІ в незаконних цілях [[13]]. За результатами досліджень, регулярні перевірки та моніторинг систем ШІ допомагають знизити ризики кіберзагроз і підвищити довіру користувачів до технологій, особливо у фінансовій сфері, де ці системи дедалі частіше використовуються для запобігання шахрайству та забезпечення безпеки транзакцій [[15]].

Таким чином, впровадження концепції XAI та регулярні аудити сприяють ефективнішому й безпечнішому використанню штучного інтелекту в різних сферах, що забезпечує не лише технологічний прогрес, а й дотримання етичних і правових стандартів на глобальному рівні.

Окрім питань конфіденційності та прозорості, автоматизація кібербезпеки за допомогою нейронних мереж викликає занепокоєння через можливе виключення людського фактора. Автоматизовані системи безпеки, здатні самостійно ухвалювати рішення, можуть мати серйозні наслідки, якщо ці рішення виявляться неправильними або недостатньо обґрунтованими.

Однією з основних загроз автоматизації є атаки типу adversarial attacks, коли зловмисники намагаються маніпулювати вхідними даними для впливу на нейронні мережі. Подібна атака може ввести систему в оману, змушуючи її ухвалювати неправильні рішення, що може спричинити серйозні кібератаки на організацію [[14]].

Ще однією проблемою є відсутність людського контролю в автоматизованих системах. Людина зазвичай відіграє важливу роль у перевірці рішень, ухвалених алгоритмами ШІ, і виключення цього фактора може призвести до помилкових рішень, які залишаться непоміченими. Це особливо актуально в контексті реагування на загрози, де швидкість і точність рішень є критично важливими. У разі помилкового спрацьовування автоматизованої системи може бути ухвалене рішення, яке негативно вплине на бізнес-процеси або навіть призведе до зупинки діяльності компанії [[15]].

Етичні аспекти використання нейронних мереж у кібербезпеці також охоплюють питання алгоритмічної упередженості. Нейронні мережі можуть підсвідомо ухвалювати упереджені рішення на основі даних, на яких вони були навчені. Якщо ці дані містять перекоси або упередження, це може призвести до дискримінації або неправильного визначення загроз. Наприклад, мережевий трафік з певних регіонів може бути помилково ідентифікований як більш загрозливий через наявність таких патернів у даних [[17]].

Ще одним важливим етичним викликом є забезпечення справедливості у використанні нейронних мереж для виявлення загроз. Усі суб'єкти повинні мати рівні можливості для захисту своїх даних, а моделі ШІ мають бути відкритими для аудиту та відповідати стандартам справедливості й етичності.

Етичні та правові аспекти використання нейронних мереж у кібербезпеці є одними з найважливіших і найскладніших питань. Прозорість алгоритмів, захист даних, управління ризиками автоматизації та етична відповідальність — це ключові аспекти, які потребують особливої уваги з боку розробників, користувачів і регуляторів. У майбутньому роль етичних принципів та правових норм у кібербезпеці лише зростатиме, а розвиток штучного інтелекту вимагатиме впровадження нових підходів до управління технологіями та захисту прав людини.

Одним із найважливіших напрямків розвитку є використання глибоких нейронних мереж (Deep Neural Networks, DNN) для створення складніших і точніших моделей виявлення загроз. Завдяки здатності обробляти великі обсяги даних та самонавчатися, DNN можуть виявляти нові види атак, зокрема атаки нульового дня (zero-day attacks), які неможливо виявити за допомогою традиційних систем, заснованих на сигнатурах. Наприклад, DNN здатні аналізувати величезні масиви даних у реальному часі, що є критично важливим для сучасного кіберзахисту [[14]].

Ще однією важливою тенденцією є розвиток трансформерів — моделей штучного інтелекту, здатних аналізувати дані в режимі реального часу з високою точністю.

Трансформери вже продемонстрували свою ефективність у сфері обробки природної мови, однак їхнє використання в кібербезпеці може стати проривом у виявленні аномалій та аналізі мережевого трафіку. Наприклад, трансформери здатні виявляти відхилення від нормальної поведінки в режимі реального часу, що сприятиме запобіганню атакам на хмарні сервіси та Інтернет речей (IoT) [[15]].

Інтеграція нейронних мереж у повсякденні інструменти кібербезпеки також стане ключовою тенденцією. Адаптивні системи безпеки, що використовують штучний інтелект, зможуть динамічно реагувати на зміни в кіберпросторі, коригуючи свої стратегії захисту у відповідь на нові загрози. Це надасть компаніям можливість не лише реагувати на атаки, а й передбачати їх на основі аналізу попередніх дій зловмисників [[14]].

Одним із найбільш перспективних напрямків є поєднання квантових обчислень і нейронних мереж, що відкриє нові горизонти в галузі кібербезпеки. Квантові нейронні мережі (Quantum Neural Networks, QNN) можуть значно підвищити ефективність обробки інформації і дадуть змогу аналізувати великі обсяги даних з набагато вищою швидкістю, ніж традиційні методи. Наприклад, квантові обчислення можуть виконувати складні математичні операції, як-от розкладання великих чисел, що підвищить ефективність криптографічних методів і захист від нових загроз [[14]].

Проте розвиток квантових нейронних мереж також принесе нові виклики. Зокрема, існує ризик, що зловмисники, отримавши доступ до квантових обчислень, зможуть використовувати їх для зламу сучасних систем шифрування. Це змусить компанії оновлювати свої методи захисту даних, щоб протидіяти новим видам атак [[17]].

Незважаючи на значний потенціал нейронних мереж для покращення кібербезпеки, існують кілька викликів, які залишатимуться актуальними в найближчі роки. Одним із головних викликів є adversarial attacks, коли зловмисники маніпулюють вхідними даними для введення нейронної мережі в оману. Такі атаки можуть призвести до того, що система ШІ розпізнає безпечні дії як загрозу або не виявить реальну атаку. Наприклад, у фінансовому секторі такі атаки можуть дозволити шахраям обійти системи виявлення шахрайства [[15]].

Іншим викликом є необхідність постійної адаптації нейронних мереж до нових загроз. Оскільки зловмисники постійно вдосконалюють свої методи, нейронні мережі мають швидко адаптуватися, щоб зберігати свою ефективність. Це потребує регулярного навчання моделей на основі нових даних, що створює додаткові складнощі, особливо у контексті захисту конфіденційності даних і виконання вимог регуляторів, таких як GDPR [[15]].

Міжнародні регулятори відіграватимуть ключову роль у розвитку нейронних мереж у сфері кібербезпеки. Такі органи, як Європейська комісія та Національний інститут стандартів і технологій США (NIST), продовжуватимуть впроваджувати вимоги щодо захисту даних, стимулюючи компанії до розробки та впровадження технологій ШІ відповідно до встановлених стандартів [[14]].

Наразі регулятори розробляють нові законодавчі акти, зокрема AI Act, який регулюватиме використання штучного інтелекту в критично важливих сферах, таких як кібербезпека. Це введе додаткові вимоги до прозорості алгоритмів і підзвітності систем ШІ, що є важливим для забезпечення безпеки даних і запобігання кіберзагрозам [[15]]. Майбутні тенденції у сфері нейронних мереж і кібербезпеки демонструють величезний потенціал цих технологій у протидії новим загрозам. Проте їхній розвиток не мине без викликів, таких як адаптація до нових видів атак, вирішення етичних питань та відповідність вимогам регуляторів. З огляду на це, компаніям та урядам необхідно співпрацювати для забезпечення безпечного й етичного використання нейронних мереж у кіберпросторі.

Окрім технічних досягнень, використання нейронних мереж у кібербезпеці пов'язане з викликами, що стосуються регуляторних вимог і етичних аспектів. Такі стандарти, як GDPR, NIS Directive і ISO 27001, відіграють ключову роль у впровадженні цих технологій, встановлюючи вимоги щодо захисту даних та прозорості алгоритмів. Однак проблема «чорної скриньки» нейронних мереж і ризик атак типу adversarial attacks потребують додаткової уваги з боку розробників та регуляторів.

Подальший розвиток нейронних мереж у кібербезпеці також пов'язаний із їх інтеграцією з іншими інноваційними технологіями, такими як блокчейн і квантові обчислення. Це дасть змогу створювати стійкіші до загроз системи. Проте для реалізації повного потенціалу цих технологій необхідно вдосконалювати регуляторні рамки, підвищувати етичну відповідальність і забезпечувати прозорість процесів ШІ.

Висновки. Таким чином, нейронні мережі є перспективним інструментом для боротьби з кіберзагрозами. Однак їхня ефективність значною мірою залежатиме від здатності компаній і урядів вирішувати виклики, пов'язані з конфіденційністю, етичними питаннями та технічними вразливостями.

Робота виконана в рамках держбюджетної науково-дослідної роботи № 0124U000550 «Моделювання механізмів протидії організованій та транснаціональній кіберзлочинності у воєнний та післявоєнний часи».

Список літератури

[1]. Adebunmi, O., Adewusi, U., Okoli, T., Ejuma, A., Donald, O. Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA review. World Journal Of Advanced Research and Reviews, 2024. doi: 10.30574/wjarr.2024.21.1.0313.

[2]. AI Risk Management Framework. NIST. URL: https://www.nist.gov/itl/ai-risk-management-framework (дата звернення: 21.09.2024).

[3]. Artificial Intelligence Act: MEPs adopt landmark law. European Parliament. URL: https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law (date of access: 21.09.2024).

[4]. Brown, T. B., et al. Language models are few-shot learners. Advances in Neural Information Processing Systems, 2020.

[5]. Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine. URL: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ (дата звернення: 21.09.2024).

[6]. EU data protection rules. European Commission. URL: https: // commission.europa.eu / law /law-topic/data-protection/eu-data-protection-rules_en (дата звернення: 21.09.2024).

[7]. Hansen, R., Venables, P. Introducing Google's Secure AI Framework. Google. URL: https://blog.google

/technology/safety-security/introducing-googles-secure-ai-framework/ (дата звернення: 21.09.2024).

[8]. ISO/IEC 27032 cybersecurity guideline. ISO 27001 information security standards. URL: https:// www.iso27001security.com / html / 27032.html (дата звернення: 21.09.2024).

[9]. NIS directive. ENISA. URL: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new (дата звернення: 21.09.2024).

[10]. Palani, K., Kethar, J., Prasad, S., Torremocha, V. Impact of AI and Generative AI in transforming Cybersecurity. J Stud Res, 2024, 13(2), May.

[11]. Regulation - 2016/679 - EN - GDPR - EUR-Lex. EUR-Lex – Access to European Union law – choose your language. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 21.09.2024).

[12]. Shevchuk, R., Martsenyuk, V. Neural Networks Toward Cybersecurity: Domain Map Analysis of State-of-the-Art Challenges. IEEE Access, 2024, 12, 81265-81280. doi: 10.1109/ACCESS.2024.3411632.

[13]. Ssetimba, I. D., Kato, J., Othieno, P. E., Twineamatsiko, E., Nakayenga, H. N., Muhangi, E. Advancing electronic communication Compliance and fraud detection Through Machine Learning, NLP and generative AI: A Pathway to Enhanced Cybersecurity and Regulatory Adherence. World Journal Of Advanced Research and Reviews, 2024, 23(2), pp. 697-707. doi: 10.30574/wjarr.2024.23.2.2364.

[14]. Suman, Kashyap. The Influence of Artificial Intelligence on Cybersecurity. International Journal of Innovative Research in Computer and Communication Engineering, 2024. doi: 10.15680/ijircce.2024.1203503.

[15]. Thapaliya, S. Examining the Influence of AI-Driven Cybersecurity in Financial Sector Management. The Batuk, 2024, 10(2), 129-144. doi: 10.3126/batuk.v10i2.68147.

[16]. What is Attention Mechanism?. H2O.ai | Convergence of The World's Best Predictive & Generative AI. URL: https://h2o.ai/wiki/attention-mechanism/ (дата звернення: 21.09.2024).

[17]. Zharama, M., Llarena. Code development of regulatory technology for legitimacy of cybersecurity adjudication. International journal of political science and governance, 2022, 4(1), 06-09. doi: 10.33545/26646021.2022.v4.i1a.126.

[18]. Регулювання штучного інтелекту. Стандарт ISO/IEC 42001:2023 - AIN. Інтернет-бізнес в Україні. URL: https://ain.ua/2024/04/04/regulyuvannya-shtuchnogo-intelektu-standart-iso-iec-420012023/ (дата звернення: 21.09.2024).

[19]. Шевченко, А., Застело, Г., Шпачинський, Є. Аналіз застосування методів машинного навчання на основі штучних нейронних мереж для виявлення кіберзагроз. 2019, 7(1), 79-90. doi: 10.20535/2411-1031.2019.7.1.184327.

УДК 654.071

Kushnerev O., Pozovna I., Sokol V. Influence of neuronal networks on development cybersecurity in the conditions of regulatory changes

Abstract. *The article studies the influence of neural networks on the development of cybersecurity in conditions of constant changes in the regul-torus field. In today's digital world, where the complexity and frequency of cyber attacks are growing rapidly, traditional security methods are becoming insufficient. Neural networks, as one of the key technologies of state-of-the-art intelligence, open up new opportunities for increasing the efficiency of cyber defense systems for automation of threat detection, anomaly analysis and attack prevention. The integration of neural networks with other emerging technologies, such as blockchain and quantum computing, opens up new horizons for creating more sustainable systems. However, challenges such as adversarial attacks, opacity of the (the "black box" problem) and compliance with regulatory requirements, in particular GDPR and ISO 27001, demand special attention. The study also examines the ethical and legal aspects of using non-neural networks in cybersecurity, emphasizing the importance of developing explanatory artificial intelligence (XAI) and maintaining human control for safe and ethical implementation. The article makes it a dream that neural networks are a promising tool in the fight against cyber threats, but their effects will depend on the ability of organizations and states to solve privacy problems, ethical issues and technical vulnerabilities.*

Keywords: *neural networks, cybersecurity, artificial intelligence, cyberattacks, system vulnerabilities, regulatory standards.*

Кушнерьов Олександр Сергійович, старший викладач кафедри економічної кібернетики, Сумський державний університет, Україна.
Oleksandr Kushnerev, senior lecturer at the Department of Economic Cybernetics, Sumy State University, Ukraine.

Позовна Ірина Вікторівна, старша викладачка кафедри економічної кібернетики, Сумський державний університет, Україна.
Iryna Pozovna, senior lecturer at the Department of Economic Cybernetics, Sumy State University, Ukraine.

Сокол Владислав, кандидат технічних наук, докторант за спеціальністю 125 «Кібербезпека та захист інформації», Національний технічний університет «Харківський політехнічний інститут», Україна.
Vladyslav Sokol, candidate of technical sciences, doctoral student in specialty 125 "Cybersecurity and information protection", National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Отримано *31 травня 2024 року,* затверджено редколегією *26 червня 2024 року*