Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

В.о. зав. кафедрою КІСМіТ
Марина ЄСІНА
"Допущено до захисту"

« »_____2025р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

на тему: «Застосування штучного інтелекту для виявлення та запобігання кібератакам: виклики та перспективи»

оцінка « _____ »

Голова ЕК
Мичуда Л.З.

Керівник: к.т.н. Шеханін К.Ю.

Рецензент: к.т.н. Олешко О.І.

Виконавець: студент групи КБ-41
Афанасьєв Д.О.

Харків 2025

РЕФЕРАТ

Кваліфікаційна бакалаврська робота містить 52 сторінки основного тексту, 4 рисунки, 2 таблиці та 1 додаток. Перелік використаних джерел налічує 29 найменувань. Робота оформлена згідно з вимогами до кваліфікаційних робіт.

Мета роботи — дослідити можливості застосування штучного інтелекту (ШІ) для виявлення та запобігання кібератакам, проаналізувати пов'язані виклики та реалізувати практичну систему на основі глибокого навчання.

Методи дослідження: аналіз літератури, порівняльний огляд ШІ-систем, експериментальне моделювання, тестування та оптимізація моделей CNN й автокодувальників. Реалізація здійснена за допомогою Python, TensorFlow, Kafka, Docker із використанням наборів даних CICIDS2017 і Metasploit.

У результаті створено адаптивну систему з точністю до 94,2% і часом реагування до 2 секунд. Новизна — у поєднанні контекстного аналізу з глибоким навчанням та адаптації до умов обмежених ресурсів, що важливо для України.

Система рекомендована для захисту інфраструктури державного та малого бізнесу. Практична цінність — автоматизація виявлення загроз, зниження навантаження на фахівців та швидке реагування.

Результати можуть бути інтегровані в SIEM-системи (QRadar, Splunk) і використані у підготовці кіберфахівців. Подальші напрями — розширення наборів даних, стійкість до adversarial AI, україномовний інтерфейс та узгодження з міжнародними стандартами.

Ключові слова: ШТУЧНИЙ ІНТЕЛЕКТ, КІБЕРБЕЗПЕКА, CNN, ГЛИБОКЕ НАВЧАННЯ, АНОМАЛІЇ, ФІШИНГ, DDOS, SIEM.

ABSTRACT

The bachelor’s qualification thesis contains 52 pages of main text, 4 figures, 2 tables, and 1 appendix. The list of references includes 29 sources. The work is formatted in accordance with the requirements for qualification papers.

The aim of the thesis is to explore the potential of using Artificial Intelligence (AI) for detecting and preventing cyberattacks, to analyze related challenges, and to implement a practical system based on deep learning.

The research methods include literature review, comparative analysis of existing AI-based systems, experimental modeling, testing, and optimization of CNN and autoencoder models. The implementation was carried out using Python, TensorFlow, Kafka, and Docker, with datasets CICIDS2017 and Metasploit.

As a result, an adaptive system was developed, achieving up to 94.2% accuracy with a response time of under 2 seconds. The novelty lies in the combination of contextual analysis with deep learning and the adaptation of the model to environments with limited computing resources — a relevant aspect for Ukraine.

The system is recommended for protecting the infrastructure of government institutions and small businesses. Its practical value lies in the automation of threat detection, reducing the workload for specialists, and providing fast response to incidents.

The results can be integrated into SIEM systems (e.g., QRadar, Splunk) and used as a training platform for cybersecurity professionals. Future directions include expanding training datasets, increasing robustness against adversarial AI, developing a Ukrainian-language interface, and aligning with international standards.

Keywords: ARTIFICIAL INTELLIGENCE, CYBERSECURITY, CNN, DEEP LEARNING, ANOMALY DETECTION, PHISHING, DDOS, SIEM.

ЗМІСТ

ПЕРЕЛІК ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ШІ	– Штучний інтелект
UEBA	– User and Entity Behavior Analytics
DDoS	– Distributed Denial of Service
APT	– Advanced Persistent Threat
NLP	– Natural Language Processing
SIEM	– Security Information and Event Management
GPU	– Graphics Processing Unit
IoT	– Internet of Things
AI Act	– Закон Європейського Союзу про штучний інтелект
ML	– Machine Learning
DL	– Deep Learning
CNN	– Convolutional Neural Network
RNN	– Recurrent Neural Network

ВСТУП

Сучасний світ характеризується стрімким розвитком інформаційних технологій, що відкриває нові можливості для суспільства, але водночас створює серйозні виклики у сфері кібербезпеки. Зростання кількості та складності кібератак, таких як фішинг, шкідливе програмне забезпечення, атаки типу "відмова в обслуговуванні" (DDoS) та цільові атаки на критичну інфраструктуру, вимагає розробки інноваційних підходів до їх виявлення та запобігання. Традиційні методи захисту, засновані на сигнатурному аналізі чи ручному моніторингу, стають недостатньо ефективними в умовах швидкої еволюції кіберзагроз. У цьому контексті штучний інтелект (ШІ) набуває особливого значення як інструмент, здатний автоматизувати аналіз великих обсягів даних, виявляти аномалії та прогнозувати потенційні загрози в реальному часі.

Актуальність теми бакалаврської роботи зумовлена необхідністю адаптації сучасних систем кібербезпеки до нових викликів, спричинених цифровізацією та зростанням складності кібератак. ШІ, зокрема методи машинного навчання та глибокого навчання, демонструє значний потенціал у виявленні невідомих загроз, прогнозуванні атак і автоматизації реагування. Водночас впровадження ШІ супроводжується низкою технічних, етичних і правових викликів, таких як потреба у великих обсягах якісних даних, проблема "чорної скриньки" в моделях ШІ та питання регулювання використання таких технологій. В Україні, де цифрова трансформація активно розвивається, а кібератаки на державні та комерційні структури стають дедалі частішими, дослідження можливостей і обмежень ШІ в кібербезпеці є особливо важливим.

Мета роботи полягає в дослідженні можливостей застосування штучного інтелекту для виявлення та запобігання кібератакам, аналізі пов’язаних викликів і перспектив, а також розробці практичної реалізації системи на основі ШІ для вирішення завдань кібербезпеки.

Завдання роботи:

1) Провести аналіз сучасних методів використання ШІ в кібербезпеці, визначивши їх переваги та обмеження.
2) Дослідити технічні, етичні та правові виклики, пов’язані з впровадженням ШІ для протидії кібератакам.
3) Визначити перспективи розвитку ШІ-технологій у сфері кібербезпеки.
4) Розробити та протестувати програмну модель на основі ШІ для виявлення кіберзагроз.
5) Оцінити ефективність розробленої системи та запропонувати рекомендації щодо її інтеграції в існуючі інфраструктури.

Об’єкт дослідження – процеси виявлення та запобігання кібератакам у сучасних інформаційних системах.

Предмет дослідження – методи та технології штучного інтелекту, що застосовуються для забезпечення кібербезпеки, а також виклики й перспективи їх використання.

Методи дослідження включають аналіз літератури, порівняльний аналіз сучасних ШІ-систем, експериментальні методи для розробки та тестування програмної реалізації, а також систематизацію отриманих даних для формулювання висновків.

Робота присвячена застосуванню ШІ для виявлення кібератак в Україні. Створено модель машинного навчання та програмну систему для реального ви явлення загроз, що може покращити захист у державному й корпоративному се кторах. Структура включає теоретичний аналіз, виклики та перспективи, практи чну реалізацію й рекомендації.

1 АНАЛІЗ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

1.1 Огляд сучасних методів виявлення кібератак

Сучасний ландшафт кіберзагроз характеризується швидким зростанням кількості та складності атак, що включають фішинг, шкідливе програмне забезпечення, атаки типу "відмова в обслуговуванні" (DDoS), а також цільові атаки на критичну інфраструктуру. Традиційні методи виявлення кібератак, такі як сигнатурний аналіз або ручний моніторинг, стають недостатньо ефективними через високу швидкість еволюції загроз і їх здатність обходити стандартні механізми захисту. У цьому контексті штучний інтелект (ШІ) відіграє ключову роль у розробці нових підходів до виявлення та запобігання кібератакам, забезпечуючи автоматизацію аналізу даних і прогнозування потенційних загроз [1].

Одним із основних методів виявлення кібератак із використанням ШІ є аналіз поведінки користувачів і систем (User and Entity Behavior Analytics, UEBA). Цей підхід базується на створенні базових профілів нормальної поведінки користувачів, пристроїв або мереж за допомогою алгоритмів машинного навчання. Будь-яке відхилення від цих профілів, наприклад незвичайна активність у мережі чи нетипові дії користувача, може свідчити про потенційну атаку. Наприклад, системи UEBA здатні виявляти інсайдерські загрози або компрометацію облікових записів, аналізуючи великі обсяги даних у реальному часі. Такі рішення широко застосовуються в корпоративних середовищах для захисту від складних атак, які не мають чітких сигнатур [2].

Іншим важливим методом є використання ШІ для виявлення аномалій у мережевому трафіку. Алгоритми машинного навчання, такі як нейронні мережі або методи кластеризації, дозволяють ідентифікувати незвичайні патерни в даних, які можуть вказувати на DDoS-атаки, спроби експлуатації вразливостей або приховану активність шкідливого програмного забезпечення. Наприклад, системи на основі ШІ можуть аналізувати обсяги трафіку, частоту запитів або типи пакетів, щоб виявити аномалії, які не відповідають нормальній роботі мережі.

Такі методи особливо ефективні для захисту хмарних інфраструктур, де традиційні підходи часто не справляються з великими обсягами даних [3].

ШІ також активно застосовується для аналізу шкідливого програмного забезпечення (малварі). Традиційні антивірусні програми покладаються на сигнатурний аналіз, який порівнює код програми з базою відомих загроз. Однак сучасне шкідливе ПЗ часто використовує поліморфізм або обфускацію, що ускладнює його виявлення. Алгоритми глибокого навчання, такі як згорткові нейронні мережі, дозволяють аналізувати поведінку програм, їх взаємодію з системою та навіть структуру коду без необхідності сигнатур. Наприклад, ШІ може класифікувати програму як шкідливу, аналізуючи її системні виклики або патерни виконання, що значно підвищує ефективність виявлення нових і невідомих загроз [4].

Ще одним перспективним напрямом є використання ШІ для прогнозного аналізу кіберзагроз. Моделі машинного навчання, такі як рекурентні нейронні мережі, здатні аналізувати історичні дані про атаки, щоб передбачати потенційні загрози до їх реалізації. Наприклад, ШІ може виявляти підготовку до фішингової кампанії, аналізуючи патерни в електронних листах або активність у соціальних мережах. У поєднанні з технологіями обробки природної мови (NLP) такі системи можуть ідентифікувати підозрілий контент, наприклад фальшиві повідомлення, що імітують легітимні джерела. Цей підхід дозволяє організаціям діяти проактивно, запобігаючи атакам на ранніх етапах [1].

У контексті України методи ШІ для виявлення кібератак набувають особливого значення через зростання кількості атак на державні та комерційні структури. Наприклад, аналіз поведінки та аномалій у мережевому трафіку активно застосовується для захисту критичної інфраструктури, такої як енергетичні мережі чи банківські системи. Українські дослідники зазначають, що ШІ дозволяє не лише виявляти загрози, але й оптимізувати роботу команд безпеки, зменшуючи час реагування на інциденти [5].

Незважаючи на численні переваги, сучасні методи ШІ мають певні обмеження. Наприклад, аналіз поведінки та аномалій може генерувати хибнопозити-

вні результати, що вимагає додаткових ресурсів для перевірки. Крім того, ефективність моделей ШІ значною мірою залежить від якості та обсягу даних для їх навчання. У разі недостатньої кількості даних або їх низької якості точність виявлення може знижуватися. Також важливим є питання адаптації моделей до нових типів атак, оскільки кіберзлочинці постійно вдосконалюють свої методи [3].

Сучасні методи виявлення кібератак на основі ШІ демонструють високу ефективність у порівнянні з традиційними підходами, однак їх успішне застосування вимагає комплексного підходу. Це включає інтеграцію різних алгоритмів (наприклад, комбінацію аналізу поведінки та аномалій), використання якісних даних для навчання моделей і постійне оновлення систем для адаптації до нових загроз. У майбутньому розвиток технологій ШІ, таких як федеративне навчання або квантові обчислення, може ще більше підвищити ефективність виявлення кібератак, забезпечуючи надійніший захист інформаційних систем [4].

1.2 Роль штучного інтелекту в аналізі кіберзагроз

Штучний інтелект (ШІ) відіграє ключову роль у сучасних системах кібербезпеки, забезпечуючи аналіз великих обсягів даних, виявлення складних кіберзагроз і прискорення реагування на інциденти. У контексті зростання кількості атак, таких як цільові фішингові кампанії, атаки нульового дня та складні багатокрокові атаки (Advanced Persistent Threats, APT), ШІ дозволяє організаціям ефективно протистояти загрозам, які важко виявити традиційними методами. Завдяки здатності обробляти різноманітні джерела даних і знаходити приховані закономірності, ШІ трансформує підходи до аналізу кіберзагроз, забезпечуючи проактивний захист [6].

Однією з основних ролей ШІ є автоматизація аналізу даних безпеки. Сучасні інформаційні системи генерують величезні обсяги логів, мережевого трафіку та інших даних, які неможливо ефективно обробити вручну. Алгоритми машинного навчання, такі як класифікація та регресія, дозволяють автоматизувати обробку цих даних, виявляючи підозрілу активність у реальному часі. Наприклад, ШІ може аналізувати журнали подій (event logs) для ідентифікації спроб 11

несанкціонованого доступу або аномальної активності, значно скорочуючи час, необхідний для виявлення загроз [7].

Ще однією важливою функцією ШІ є аналіз загроз на основі поведінкових моделей. Системи на основі ШІ, такі як User and Entity Behavior Analytics (UEBA), створюють профілі нормальної поведінки користувачів, пристроїв і додатків. Відхилення від цих профілів, наприклад, незвичайний час входу в систему або доступ до нетипових ресурсів, можуть свідчити про компрометацію. Такі системи особливо ефективні для виявлення інсайдерських загроз або атак, які використовують викрадені облікові дані. Наприклад, ШІ може виявити, якщо легітимний користувач починає завантажувати великі обсяги даних, що не відповідає його звичайній поведінці [8].

ШІ також відіграє важливу роль у розвідці загроз (Threat Intelligence). Системи на основі ШІ здатні агрегувати дані з різних джерел, таких як даркнет, відкриті форуми, соціальні мережі та звіти про інциденти, для створення актуальних профілів загроз. За допомогою технологій обробки природної мови (NLP) ШІ аналізує текстові дані, наприклад, повідомлення на хакерських форумах, щоб виявити підготовку до атак або нові вразливості. Це дозволяє організаціям отримувати інформацію про потенційні загрози до їх реалізації, що є критичним для проактивного захисту [9].

В Україні ШІ активно застосовується для аналізу кіберзагроз у контексті захисту критичної інфраструктури. Зростання кількості атак на державні установи та енергетичний сектор спонукає до використання ШІ для швидкого аналізу інцидентів і прогнозування ризиків. Наприклад, алгоритми машинного навчання використовуються для аналізу мережевого трафіку в реальному часі, що дозволяє виявляти спроби проникнення в системи або підготовку до масштабних атак. Українські дослідники підкреслюють, що ШІ не лише підвищує ефективність аналізу, але й оптимізує розподіл ресурсів команд безпеки [10].

Незважаючи на значні переваги, використання ШІ в аналізі кіберзагроз має певні обмеження. По-перше, моделі ШІ потребують великих обсягів якісних даних для навчання, що може бути проблематичним у разі обмеженого доступу до

актуальних наборів даних про атаки. По-друге, ШІ може генерувати хибнопозитивні результати, що вимагає додаткової перевірки аналітиками. Крім того, кіберзлочинці також використовують ШІ для створення більш складних атак, наприклад, адаптивного шкідливого ПЗ, що ускладнює завдання захисних систем. Таким чином, роль ШІ в аналізі кіберзагроз вимагає постійного вдосконалення алгоритмів і адаптації до нових викликів [6].

Роль ШІ в аналізі кіберзагроз полягає не лише у виявленні та класифікації загроз, але й у забезпеченні організацій інструментами для швидкого реагування та прогнозування. Завдяки автоматизації, аналізу поведінки та розвідці загроз ШІ значно підвищує ефективність кібербезпеки, дозволяючи організаціям залишатися на крок попереду зловмисників. У майбутньому розвиток ШІ, зокрема у сфері самонавчальних систем і обробки великих даних, може ще більше посилити його роль у протидії кіберзагрозам, створюючи більш стійкі та адаптивні системи захисту [8].

1.3 Переваги та обмеження використання ШІ в кібербезпеці

Застосування штучного інтелекту (ШІ) у кібербезпеці відкриває нові можливості для захисту інформаційних систем, забезпечуючи швидший аналіз даних, автоматизацію процесів і виявлення складних загроз. Водночас технології ШІ мають низку обмежень, які впливають на їх ефективність і потребують додаткових зусиль для подолання. Розуміння переваг і недоліків ШІ є ключовим для його успішного впровадження в системи кібербезпеки, особливо в умовах зростання кількості та складності кібератак [11].

Однією з головних переваг ШІ є здатність обробляти великі обсяги даних у реальному часі. Сучасні інформаційні системи генерують терабайти логів, мережевого трафіку та інших даних, які неможливо проаналізувати вручну. Алгоритми машинного навчання, такі як кластеризація або класифікація, дозволяють швидко обробляти ці дані, виявляючи аномалії чи підозрілу активність. Наприклад, ШІ може аналізувати мережевий трафік для виявлення DDoS-атак або

спроб несанкціонованого доступу за лічені секунди, що значно скорочує час реагування на інциденти [12].

Ще однією перевагою є можливість виявлення невідомих загроз, зокрема атак нульового дня. Традиційні методи, такі як сигнатурний аналіз, ефективні лише проти відомих загроз, тоді як ШІ, використовуючи методи глибокого навчання, здатен ідентифікувати нові патерни атак без попереднього знання їх сигнатур. Наприклад, нейронні мережі можуть аналізувати поведінку шкідливого програмного забезпечення, виявляючи його на основі незвичайних системних викликів або взаємодії з мережею [13].

ШІ також сприяє автоматизації рутинних завдань, що дозволяє командам безпеки зосередитися на стратегічних питаннях. Системи на основі ШІ можуть автоматично класифікувати інциденти, призначати їм пріоритети та навіть пропонувати дії для реагування. Це особливо важливо в умовах дефіциту кваліфікованих спеціалістів із кібербезпеки, що є актуальною проблемою як у світі, так і в Україні. Наприклад, автоматизовані системи ШІ можуть обробляти фішингові листи, визначаючи їх за допомогою обробки природної мови, що зменшує навантаження на аналітиків [14].

У контексті України ШІ забезпечує підвищення ефективності захисту критичної інфраструктури. Зокрема, алгоритми ШІ дозволяють прогнозувати потенційні атаки на енергетичні чи фінансові системи, аналізуючи історичні дані та поточні патерни активності. Це дає змогу державним і комерційним організаціям діяти проактивно, мінімізуючи ризики [15].

Незважаючи на численні переваги, ШІ має суттєві обмеження, які ускладнюють його ефективне застосування в сфері кібербезпеки. Одним із головних недоліків є залежність від якості та повноти даних, що використовуються для навчання моделей. Якщо дані містять шум, є неповними або не відображають сучасні сценарії атак, точність виявлення загроз може значно знизитися. Наприклад, недостатня кількість даних про нові види атак може призвести до того, що 14 модель не розпізнає їх, що викликає хибнонегативні результати [11]. Це особ

ливо критично для систем, що працюють у реальному часі, де пропуск загрози може мати серйозні наслідки.

Іншою проблемою є висока ймовірність хибнопозитивних спрацювань. Системи, побудовані на аналізі аномалій, часто помилково класифікують нор мальну активність як потенційну загрозу. Це створює додаткове навантаження на команди безпеки, які змушені вручну перевіряти підозрілі дії. Наприклад, цілком легітимна поведінка користувача, така як доступ до системи в неробочий час або підключення з нового пристрою, може бути позначена як підозріла [12]. Надмірна кількість таких спрацювань знижує ефективність реагування та може призвести до ігнорування реальних загроз через втому аналітиків.

Ще одним суттєвим обмеженням є проблема "чорної скриньки". Багато мо делей ШІ, зокрема глибокі нейронні мережі, є непрозорими, що ускладнює пояс нення прийнятих рішень. Це знижує рівень довіри до таких систем, особливо в умовах, коли необхідне чітке обґрунтування кожного рішення. В Україні ця про блема набуває особливої актуальності у зв’язку з потребою у відповідності регу ляторним вимогам і прозорості дій автоматизованих систем безпеки [15]. Брак інтерпретованості також ускладнює виявлення помилок у моделі та її вдоскона лення.

Крім того, самі моделі ШІ можуть бути об’єктом атак. Зокрема, кіберата кувальники використовують методи adversarial AI, вводячи в систему навмисно модифіковані дані для спотворення результатів. Наприклад, зловмисники мо жуть змінити характеристики шкідливого програмного забезпечення так, щоб воно виглядало як безпечне, що дозволяє йому уникнути виявлення. Такі атаки важко ідентифікувати, а захист від них потребує впровадження спеціальних ме ханізмів перевірки надійності моделей. Це створює додаткові виклики для ро зробників систем кіберзахисту й вимагає нових підходів до побудови стійких мо делей [13]. В таблиці 1.1 наведено переваги та обмеження використання штуч ного інтелекту в кібербезпеці.

Таблиця 1.1 - Переваги та обмеження використання ШІ в кібербезпеці

Аспект	Переваги	Обмеження
Обробка даних	Швидка обробка великих обсягів даних у реальному часі [12]	Залежність від якості та обсягу даних для навчання [11]
Виявлення загроз	Виявлення невідомих атак і аномалій без сигнатур [13]	Хибнопозитивні результати, що вимагають перевірки [12]
Автоматизація	Автоматизація рутинних завдань і зменшення навантаження на аналітиків [14]	Проблема "чорної скриньки", що ускладнює інтерпретацію рішень [15]
Адаптивність	Прогнозування атак і проактивний захист [15]	Вразливість до атак adversarial AI [13]

Використання ШІ в кібербезпеці має значні переваги, зокрема швидку обробку даних, виявлення невідомих загроз і автоматизацію процесів, що підвищує ефективність захисту інформаційних систем. Однак обмеження, такі як залежність від даних, хибнопозитивні результати, непрозорість моделей і вразливість до атак, вимагають додаткових зусиль для вдосконалення технологій ШІ. В Україні ці аспекти є особливо актуальними через зростання кіберзагроз і потребу в надійних рішеннях для захисту критичної інфраструктури. Успішне застосування ШІ потребує балансу між використанням його переваг і подоланням обмежень шляхом покращення якості даних, інтерпретації результатів і захисту моделей від маніпуляцій [14].

1.4 Аналіз існуючих ШІ-систем для запобігання кібератакам

Сучасний ландшафт кіберзагроз вимагає використання передових технологій для захисту інформаційних систем. Штучний інтелект (ШІ) став ключовим інструментом у розробці систем, які здатні виявляти, аналізувати та запобігати

кібератакам у реальному часі. Існуючі ШІ-системи для кібербезпеки використовують алгоритми машинного навчання, глибокого навчання та обробки природної мови для прогнозування векторів атак, виявлення аномалій і автоматизації реагування. Цей підрозділ присвячений аналізу провідних ШІ-систем, їх функціоналу, переваг і обмежень, з акцентом на їх застосування в глобальному та українському контекстах [16].

Однією з найвідоміших ШІ-систем для запобігання кібератакам є CrowdStrike Falcon, яка використовує хмарну архітектуру та технологію Threat Graph для аналізу загроз. Система застосовує машинне навчання для виявлення шкідливого програмного забезпечення, атак нульового дня та інсайдерських загроз. Falcon аналізує поведінкові патерни, такі як системні виклики або незвичайна активність у мережі, і автоматично блокує підозрілі дії. Наприклад, у разі виявлення ransomware система може ізолювати заражений пристрій, запобігаючи поширенню атаки. Унікальною особливістю є її здатність надавати аналітику в реальному часі, що дозволяє командам безпеки швидко реагувати на інциденти [17]. На рисунок 1.1 представлено інтерфейс платформи CrowdStrike Falcon, де відображено дашборд із даними про загрози.

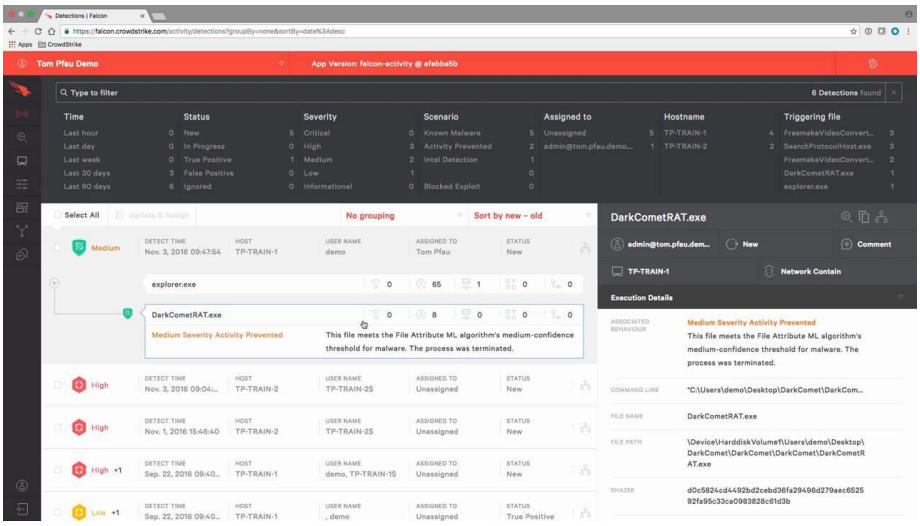

Рисунок 1.1 – Інтерфейс платформи CrowdStrike Falcon

Перевагою CrowdStrike Falcon є її легка інтеграція з хмарними та локаль ними інфраструктурами, а також висока точність виявлення завдяки постійному оновленню бази даних загроз. Однак система може бути дорогою для малих ор ганізацій, а її ефективність залежить від якості підключення до хмарних серверів. В Україні ця система використовується великими корпораціями для захисту кри тичних активів, хоча її впровадження обмежене через високу вартість [16].

Darktrace Antigena – це ШІ-система, яка застосовує концепцію "імунної системи" для захисту мереж. Використовуючи алгоритми самонавчання, вона створює модель нормальної поведінки мережі та виявляє аномалії, такі як незвичайний трафік або підозрілі запити. Унікальність системи полягає в її автономності: Antigena може автоматично блокувати загрози без втручання людини, наприклад, ізолюючи пристрій, який демонструє ознаки компрометації. Система також використовує обробку природної мови для аналізу електронних листів, що дозволяє виявляти фішингові атаки [18]. На рисунок 1.2 зображено інтерфейс Darktrace Antigena з візуалізацією мережевих аномалій.

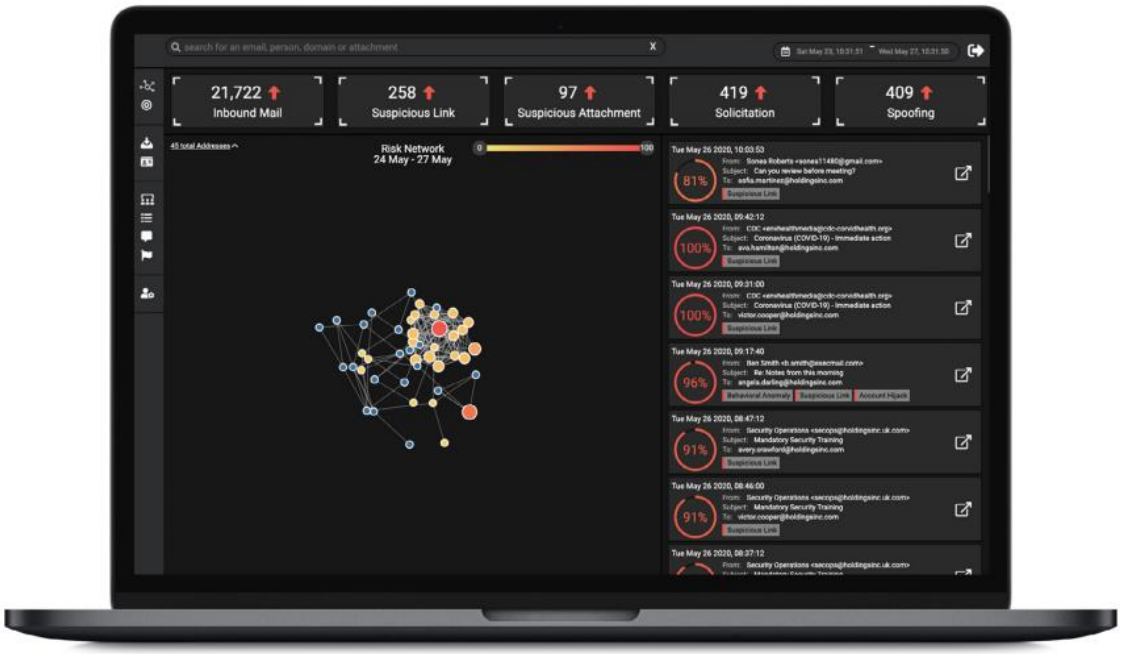

Рисунок 1.2 – Візуалізація аномалій у Darktrace Antigena

До переваг Darktrace Antigena належать її адаптивність до нових типів атак і мінімальна потреба в попередній конфігурації. Система особливо ефективна для захисту складних мереж, таких як IoT-інфраструктури. Однак вона може генерувати хибнопозитивні результати, що вимагає додаткової перевірки. В Україні Darktrace використовується в банківському секторі та енергетичних компаніях, де потрібен захист від складних атак, хоча її впровадження ускладнене через високу ціну та потребу в кваліфікованих спеціалістах [19].

IBM Security QRadar – це платформа управління інформацією та подіями безпеки (SIEM), яка інтегрує ШІ через модуль Watson for Cybersecurity. Система аналізує журнали подій, мережевий трафік і поведінкові дані для виявлення загроз, таких як інсайдерські атаки чи експлуатація вразливостей. Watson використовує обробку природної мови для аналізу звітів про загрози та кореляції подій, що дозволяє прогнозувати потенційні атаки. QRadar також підтримує автоматизацію реагування, наприклад, блокування IP-адрес або ізоляцію пристроїв [20]. На рисунок 1.3 показано дашборд QRadar із аналітикою загроз.

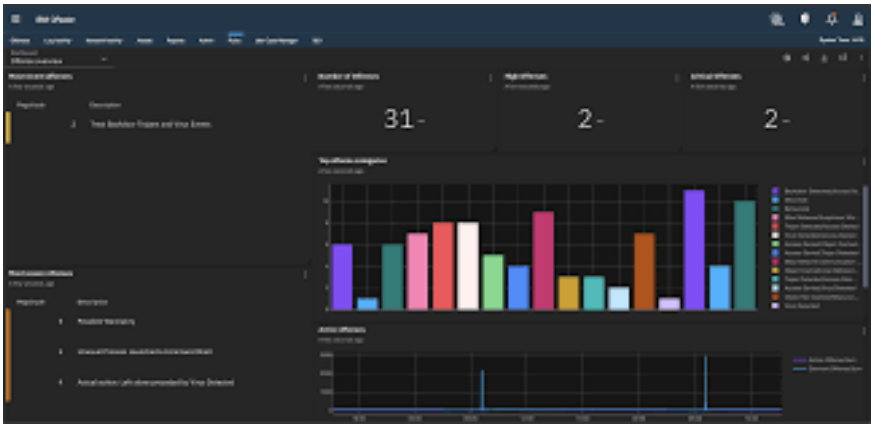

Рисунок 1.3 – Дашборд IBM Security QRadar

Перевагами QRadar є її масштабованість і здатність інтегруватися з іншими системами безпеки. Система особливо популярна в організаціях із розподіленою інфраструктурою. Однак її налаштування може бути складним, а ефективність залежить від якості даних, які надходять у систему. В Україні QRadar застосову

ється в державному секторі та великих підприємствах для моніторингу безпеки, хоча потребує значних ресурсів для впровадження [20].

В Україні також розвиваються ШІ-системи для кібербезпеки, зокрема платформа від Sl Global Service, яка входить до Intecracy Group. Ця система використовує алгоритми машинного навчання для аналізу безпеки мереж, виявлення вразливостей і прогнозування атак. Вона фокусується на проактивному виявленні загроз, таких як фішинг або шкідливі програми, шляхом аналізу великих обсягів даних. Платформа дозволяє організаціям адаптувати захист до локальних умов, що є важливим для українського ринку [13]. На рисунок 1.4 представлено інтерфейс Sl Global Service з аналітикою безпеки.

Рисунок 1.4 – Інтерфейс Sl Global Service

Розширений аналіз ринку ШІ-рішень для кібербезпеки вказує на зростаючу роль локальних розробників, таких як Sl Global Service, у зміцненні кіберзахисту малого та середнього бізнесу в Україні. Перевагою Sl Global Service є її орієнта ція на локальний контекст і відносно нижча вартість порівняно з міжнародними аналогами. Система ефективна для малих і середніх підприємств, які потребують гнучких і доступних рішень. Однак її функціонал поки що поступається глобаль ним лідерам, а база даних загроз обмежена порівняно з CrowdStrike чи Darktrace [13]. Незважаючи на це, платформа демонструє потенціал для розвитку, особ ливо в умовах зростання кіберзагроз в Україні.

Порівняльний аналіз показує, що CrowdStrike Falcon вирізняється високою швидкістю реагування та масштабованою хмарною архітектурою, Darktrace Antigena – здатністю до автономного навчання й адаптації до нових загроз, а IBM QRadar – широкими можливостями інтеграції з іншими системами безпеки та глибоким аналізом подій [19]. Sl Global Service, хоча й менш функціональна, про понує конкурентоспроможне рішення для локального ринку з урахуванням бюд жетних обмежень. Важливою перевагою є також україномовний інтерфейс і підтримка, що підвищує зручність використання для вітчизняних користувачів.

Усі розглянуті системи мають спільні виклики – залежність від якості вхідних даних, ризик хибнопозитивних результатів, складність налаштування та потребу в кваліфікованому персоналі. Крім того, міжнародні рішення вимагають значних фінансових та організаційних ресурсів, що може стати бар'єром для ши рокого впровадження в українських умовах [19].

Існуючі ШІ-системи для запобігання кібератакам, такі як CrowdStrike Falcon, Darktrace Antigena, IBM QRadar і Sl Global Service, демонструють висо кий потенціал у захисті інформаційних систем. Вони забезпечують автоматиза цію процесів моніторингу, прогнозування загроз і оперативне реагування. Однак для підвищення їх ефективності необхідно вдосконалювати алгоритми машин ного навчання, знижувати рівень хибнопозитивних спрацювань, розширювати бази даних загроз та покращувати адаптацію до регіональних особливостей [17].

У перспективі розвиток українських рішень, може стати важливим кроком до кіберсуверенітету, дозволяючи зменшити залежність від закордонних плат форм і формувати власну інфраструктуру безпеки. Підтримка таких ініціатив з боку держави та інвестиції в локальні технології можуть сприяти створенню ефективної та доступної системи кіберзахисту в Україні [17].

1.5 Висновки до розділу

Аналіз застосування штучного інтелекту (ШІ) у сфері кібербезпеки підтверджує його ефективність у виявленні та запобіганні сучасним загрозам. Завдяки

можливостям обробки великих обсягів даних, виявленню аномалій і прогнозуванню атак ШІ дозволяє значно підвищити швидкість та точність реагування на інциденти, які не завжди піддаються традиційним методам захисту [21]. До сучасних підходів належать UEBA (аналіз поведінки користувачів), моніторинг мережевого трафіку та застосування глибокого навчання, які дозволяють виявляти загрози нульового дня та інші нетипові атаки [22].

Роль ШІ полягає не лише в автоматизації аналізу, а й у створенні поведінкових моделей користувачів і систем, що дозволяє організаціям діяти на випередження. Особливо актуальним це є для України, де спостерігається зростання кількості цільових атак на об'єкти критичної інфраструктури [23].

Попри значні переваги, ШІ має і свої обмеження: залежність від якості навчальних даних, ризик хибнопозитивних спрацювань, а також вразливість до атак типу adversarial AI. Це підкреслює необхідність постійного вдосконалення моделей, зокрема адаптації до нових сценаріїв загроз [24].

Порівняльний аналіз існуючих рішень, таких як CrowdStrike Falcon, Darktrace Antigena, IBM QRadar і українська система Sl Global Service, засвідчив їхню високу ефективність, але також виявив бар’єри у впровадженні — високу вартість, складність налаштування та обмежену адаптованість до локальних умов. Українські продукти, зокрема Sl Global Service, мають потенціал розвитку, хоча за функціональністю поки поступаються міжнародним аналогам [25].

2 ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ШІ У ВИЯВЛЕННІ КІБЕРАТАК

2.1 Технічні виклики впровадження ШІ в кібербезпеку

Впровадження штучного інтелекту (ШІ) у кібербезпеку відкриває нові можливості для виявлення та запобігання кібератакам, однак супроводжується низкою технічних викликів. Ці виклики пов’язані з особливостями технологій ШІ, вимогами до інфраструктури, даними для навчання моделей, а також адаптацією систем до динамічного характеру кіберзагроз. Розуміння цих проблем є ключовим для ефективного використання ШІ в захисті інформаційних систем, особливо в умовах зростання складності атак [26].

Одним із основних технічних викликів є залежність моделей ШІ від якості та обсягу даних для їх навчання. Алгоритми машинного навчання, такі як нейронні мережі чи методи кластеризації, потребують великих наборів даних, які відображають реальні сценарії кібератак. Неповні, зашумлені або застарілі дані можуть призвести до зниження точності моделей, що підвищує ризик хибнонегативних результатів, коли справжні загрози залишаються непоміченими. Наприклад, якщо модель навчена на обмеженому наборі даних про фішингові атаки, вона може не розпізнати нові техніки, такі як цільовий spear-phishing. В Україні доступ до актуальних і репрезентативних наборів даних часто обмежений через недостатню стандартизацію збору інформації про кіберінциденти [27].

Іншим значним викликом є генерація хибнопозитивних результатів, коли ШІ помилково класифікує легітимну активність як загрозу. Це особливо актуально для систем, які базуються на аналізі аномалій, таких як UEBA. Наприклад, незвичайна, але законна активність, як-от доступ до системи в неробочий час, може бути позначена як підозріла, що створює додаткове навантаження на команди безпеки. Зменшення кількості хибнопозитивних результатів вимагає тонкого налаштування моделей і використання контекстного аналізу, що ускладнює розробку та впровадження систем ШІ [28].

Впровадження ШІ у кібербезпеку потребує значних обчислювальних ресурсів, особливо для моделей глибокого навчання, які використовуються для аналізу великих обсягів даних у реальному часі. Наприклад, обробка мережевого трафіку в масштабних корпоративних мережах або хмарних інфраструктурах вимагає потужних серверів і графічних процесорів (GPU). Для малих і середніх організацій, зокрема в Україні, забезпечення такої інфраструктури може бути фінансово обтяжливим. Крім того, масштабованість ШІ-систем є викликом, оскільки зростання обсягів даних і кількості підключених пристроїв, наприклад в IoT-мережах, вимагає постійного вдосконалення апаратного забезпечення та алгоритмів [29].

Технічним викликом є вразливість самих ШІ-систем до атак, зокрема методів adversarial AI. Кіберзлочинці можуть маніпулювати моделями ШІ, вводячи спеціально підготовлені дані, які змушують систему неправильно класифікувати загрози. Наприклад, зловмисники можуть модифікувати шкідливе програмне забезпечення так, щоб воно виглядало як легітимне для моделі ШІ, обходячи захист. Такі атаки вимагають розробки стійких моделей, які здатні протистояти маніпуляціям, однак створення таких рішень є технічно складним і потребує додаткових досліджень [28].

Динамічний характер кіберзагроз створює виклик для ШІ-систем, які повинні постійно адаптуватися до нових технік атак. Наприклад, кіберзлочинці використовують поліморфне шкідливе ПЗ, яке змінює свій код для уникнення виявлення, або соціальну інженерію, яка не завжди має чіткі технічні маркери. Моделі ШІ, навчені на історичних даних, можуть бути неефективними проти нових загроз, що вимагає механізмів безперервного навчання (continual learning). Реалізація таких механізмів ускладнена через потребу в швидкому оновленні моделей без втрати їхньої точності, що є актуальною проблемою для українських організацій, де ресурси для таких оновлень часто обмежені [26].

Інтеграція ШІ-систем з існуючими інфраструктурами кібербезпеки також є технічним викликом. Багато організацій використовують застарілі системи або гетерогенні мережі, які ускладнюють впровадження сучасних ШІ-рішень.

2.2 Етичні та правові аспекти використання ШІ

Використання штучного інтелекту (ШІ) у кібербезпеці, зокрема для виявлення та запобігання кібератакам, супроводжується низкою етичних і правових питань, які впливають на його впровадження та суспільне сприйняття. Етичні аспекти стосуються питань конфіденційності, прозорості рішень ШІ та потенційних упереджень у моделях, тоді як правові аспекти охоплюють регулювання використання ШІ, відповідальність за помилки та захист даних. Ці виклики є особливо актуальними в умовах глобальної цифровізації та зростання кіберзагроз, а також у контексті України, де правова база для ШІ перебуває на етапі формування [22].

Одним із ключових етичних викликів є забезпечення конфіденційності даних. ШІ-системи для кібербезпеки часто обробляють чутливі дані, такі як особиста інформація користувачів, журнали активності чи корпоративні дані. Неправильне використання або витік цих даних може призвести до порушення прав людини та репутаційних втрат для організацій. Наприклад, аналіз поведінки користувачів (UEBA) може передбачати моніторинг особистих дій працівників, що викликає питання щодо меж втручання в приватність. В Україні, де захист персональних даних регулюється Законом "Про захист персональних даних", організації повинні забезпечувати відповідність ШІ-систем цим вимогам, що ускладнює їх впровадження [23].

Прозорість рішень ШІ є ще одним етичним викликом. Багато моделей ШІ, зокрема глибокі нейронні мережі, функціонують як "чорні скриньки", що ускладнює розуміння логіки їхніх рішень. У кібербезпеці це може призводити до недовіри до систем, особливо коли вони генерують хибнопозитивні результати або блокують легітимну активність. Наприклад, якщо ШІ помилково ізолює пристрій працівника, пояснення причин такого рішення є критичним для збереження довіри. Відсутність прозорості також ускладнює аудит систем, що є проблемою в контексті етичного використання ШІ [24].

Упередження в моделях ШІ також становлять етичну проблему. Якщо дані для навчання моделей містять систематичні помилки, ШІ може приймати несправедливі рішення. Наприклад, модель, навчена на даних із певного регіону, може бути менш ефективною для інших контекстів, що призводить до нерівного захисту. В Україні, де доступ до різноманітних наборів даних обмежений, ця проблема може посилювати нерівність у захисті між великими корпораціями та малими підприємствами. Етичний підхід вимагає створення моделей, які мінімізують упередження та забезпечують справедливість [25].

З правового погляду, регулювання використання ШІ у кібербезпеці є складним завданням. У Європейському Союзі AI Act встановлює рамки для використання ШІ, класифікуючи системи за рівнем ризику та вимагаючи прозорості й відповідності стандартам. В Україні правова база для ШІ перебуває на початковому етапі, і більшість регуляцій спираються на загальні закони про кібербезпеку та захист даних. Відсутність спеціалізованого законодавства створює невизначеність щодо відповідальності за помилки ШІ, наприклад, у разі хибного блокування критичної інфраструктури. Це вимагає розробки чітких правових норм, які враховують специфіку ШІ [26].

Відповідальність за дії ШІ-систем є ще одним правовим викликом. Якщо ШІ-система спричинить збитки, наприклад, через неправильну класифікацію загрози, визначення відповідальної сторони – розробника, оператора чи організації – залишається нечітким. У контексті України, де кібератаки на критичну інфраструктуру можуть мати серйозні наслідки, це питання набуває особливої ваги. Правові рамки повинні чітко визначати, хто несе відповідальність за наслідки рішень ШІ, щоб уникнути юридичних прогалин [27].

Етичні та правові аспекти також переплітаються у питанні використання ШІ зловмисниками. Кіберзлочинці можуть застосовувати ШІ для створення складних атак, таких як діпфейки чи адаптивне шкідливе ПЗ, що викликає етичні дебати щодо обмеження доступу до технологій ШІ. З правового погляду, це вимагає створення механізмів контролю за розробкою та використанням ШІ, щоб

запобігти його зловживанню. В Україні, де кіберзагрози мають геополітичний контекст, ці питання потребують особливої уваги [28].

Етичні та правові аспекти використання ШІ в кібербезпеці вимагають збалансованого підходу, який поєднує захист конфіденційності, забезпечення прозорості, мінімізацію упереджень і розробку чітких правових норм. В Україні ці виклики ускладнені через недостатньо розвинену правову базу та обмежені ресурси, що підкреслює необхідність гармонізації з міжнародними стандартами та активного розвитку локальних регуляцій [29].

2.3 Перспективи розвитку ШІ-технологій для протидії новим типам атак

Штучний інтелект (ШІ) є однією з найперспективніших технологій для протидії новим типам кібератак, які характеризуються високою складністю, адаптивністю та здатністю обходити традиційні методи захисту. Розвиток ШІ-технологій, таких як машинне навчання (ML), глибоке навчання (DL) та обробка природної мови (NLP), відкриває нові можливості для прогнозування, виявлення та нейтралізації загроз у реальному часі. У контексті зростання кількості атак, таких як діпфейки, адаптивне шкідливе програмне забезпечення та атаки на IoT-пристрої, перспективи ШІ охоплюють удосконалення алгоритмів, інтеграцію з новими технологіями та адаптацію до локальних умов, зокрема в Україні [20].

Однією з ключових перспектив є розвиток самонавчальних систем ШІ, які здатні адаптуватися до нових типів атак без необхідності постійного оновлення даних для навчання. Технології безперервного навчання (continual learning) дозволяють моделям ШІ динамічно вдосконалювати свої алгоритми на основі нових даних про загрози. Наприклад, такі системи можуть аналізувати еволюцію поліморфного шкідливого ПЗ, яке змінює свій код для уникнення виявлення, і швидко адаптувати стратегії захисту. Це особливо важливо для протидії атакам нульового дня, які не мають відомих сигнатур [17].

Іншим перспективним напрямом є використання федеративного навчання (federated learning) для створення децентралізованих ШІ-систем. Цей підхід дозволяє навчати моделі на розподілених наборах даних без їх централізованого

збору, що підвищує конфіденційність і зменшує ризики витоку даних. У кібербезпеці федеративне навчання може застосовуватися для обміну знаннями про загрози між організаціями без розкриття чутливої інформації. В Україні, де захист даних є критичним через геополітичні загрози, такі технології можуть стати основою для створення національних платформ кіберзахисту [18].

Розвиток ШІ для протидії атакам на IoT-пристрої є ще однією важливою перспективою. Зі зростанням кількості підключених пристроїв, таких як розумні камери чи сенсори, зростає і вразливість мереж до атак. Алгоритми ШІ, зокрема згорткові нейронні мережі (CNN), можуть аналізувати трафік IoT-пристроїв для виявлення аномалій, таких як спроби створення ботнетів. Наприклад, ШІ може ідентифікувати незвичайну активність пристрою, яка вказує на його компрометацію, і автоматично ізолювати його від мережі. В Україні, де IoT-технології активно впроваджуються в енергетичному та транспортному секторах, такі рішення мають значний потенціал [19].

Перспективи ШІ також включають вдосконалення технологій обробки природної мови для протидії соціальній інженерії та фішинговим атакам. Сучасні фішингові кампанії, зокрема ті, що використовують діпфейки або персоналізовані повідомлення, стають дедалі складнішими. Моделі NLP, здатні аналізувати семантику тексту та виявляти підозрілий контент, можуть значно підвищити ефективність захисту. Наприклад, ШІ може розпізнавати фальшиві електронні листи, які імітують легітимні джерела, аналізуючи їхній стиль і контекст. Такі технології є перспективними для України, де фішинг залишається однією з основних загроз для державних і комерційних організацій [14].

Інтеграція ШІ з квантовими обчисленнями відкриває нові горизонти для кібербезпеки. Квантові комп’ютери можуть значно прискорити обробку даних і навчання складних моделей ШІ, що дозволить виявляти загрози з безпрецедентною швидкістю. Наприклад, квантові алгоритми можуть оптимізувати аналіз великих обсягів мережевого трафіку, виявляючи патерни атак, які недоступні для

класичних комп'ютерів. Хоча ця технологія перебуває на ранніх етапах розвитку, вона має потенціал для трансформації кібербезпеки в майбутньому, включаючи Україну, де активно досліджуються інноваційні технології [20].

В Україні перспективи розвитку ШІ-технологій також пов'язані з локалізацією рішень. Розробка ШІ-систем, адаптованих до специфіки українських кіберзагроз, таких як цільові атаки на критичну інфраструктуру, є важливим напрямом. Наприклад, локальні рішення, подібні до Sl Global Service, можуть використовувати дані про регіональні загрози для створення більш точних моделей. Крім того, співпраця з міжнародними партнерами та інтеграція з глобальними платформами Threat Intelligence може посилити здатність України протистояти новим атакам [13].

Незважаючи на перспективи, реалізація цих напрямів потребує подолання низки викликів, таких як дефіцит кваліфікованих спеціалістів, обмежені обчислювальні ресурси та необхідність гармонізації з міжнародними стандартами. В Україні ці проблеми ускладнені через обмежене фінансування та недостатньо розвинену інфраструктуру для досліджень ШІ. Однак активний розвиток локальних ініціатив і міжнародна співпраця можуть сприяти прогресу в цій сфері [14].

Перспективи розвитку ШІ-технологій для протидії новим типам атак включають самонавчальні системи, федеративне навчання, захист IoT-пристроїв, вдосконалення NLP і інтеграцію з квантовими обчисленнями. В Україні ці напрямки мають особливе значення через зростання кіберзагроз і потребу в локалізованих рішеннях. Реалізація цих перспектив потребує інвестицій у дослідження, підготовку кадрів і створення правової бази для підтримки інновацій [18].

2.4 Впливи ШІ на автоматизацію реагування на кіберзагрози

Штучний інтелект (ШІ) суттєво трансформує підходи до реагування на кіберзагрози, забезпечуючи автоматизацію процесів, які раніше вимагали значних людських ресурсів і часу. Завдяки здатності ШІ швидко аналізувати дані, класифікувати інциденти та пропонувати оптимальні дії, автоматизація реагування стає ключовим інструментом для протидії сучасним кібератакам, таким як

ransomware, фішинг чи атаки на критичну інфраструктуру. Вплив ШІ на автоматизацію реагування проявляється в прискоренні реакції, зменшенні помилок і підвищенні ефективності команд безпеки, що є особливо важливим в Україні, де кіберзагрози мають високий рівень складності та частоти [10].

Одним із основних впливів ШІ є автоматизація класифікації та пріоритизації інцидентів. Системи на основі ШІ, такі як Security Information and Event Management (SIEM) із вбудованими модулями машинного навчання, аналізують журнали подій і мережевий трафік, щоб визначити рівень загрози кожного інциденту. Наприклад, ШІ може автоматично класифікувати підозрілий вхід у систему як низькопріоритетний, якщо він відповідає нормальній поведінці користувача, або позначити його як критичний у разі виявлення аномалій. Це дозволяє командам безпеки зосереджуватися на найсерйозніших загрозах, зменшуючи час реагування [11].

ШІ також автоматизує безпосередні дії для нейтралізації загроз. Системи, такі як Darktrace Antigena, використовують алгоритми самонавчання для виконання автономних дій, наприклад, ізоляції скомпрометованого пристрою, блокування підозрілих IP-адрес або припинення шкідливих процесів. Такий підхід є ефективним для швидкого реагування на атаки, які розвиваються за лічені секунди, як-от ransomware. Наприклад, у разі виявлення шифрування файлів ШІ може миттєво ізолювати заражений пристрій, запобігаючи поширенню атаки по мережі [12].

Ще одним важливим впливом є автоматизація аналізу та кореляції даних із різних джерел. ШІ-системи, такі як IBM QRadar із модулем Watson, інтегрують дані з Threat Intelligence, логів, мережевого трафіку та зовнішніх джерел, таких як даркнет, для створення повної картини інциденту. Це дозволяє автоматично визначати зв’язки між подіями, наприклад, виявляти, що фішинговий лист є частиною ширшої кампанії. Така кореляція значно прискорює процес розслідування та зменшує ймовірність помилок, що є критичним для українських організацій, які часто стикаються з цільовими атаками [13].

У контексті України ШІ відіграє важливу роль в автоматизації реагування на атаки, спрямовані на критичну інфраструктуру, таку як енергетичні чи фінансові системи. Наприклад, локальні розробки, подібні до Sl Global Service, використовують ШІ для автоматичного блокування підозрілого трафіку в реальному часі, що дозволяє мінімізувати збитки від атак. Такі системи особливо цінні в умовах дефіциту кваліфікованих спеціалістів із кібербезпеки, оскільки вони зменшують потребу в ручному аналізі [14].

Автоматизація реагування за допомогою ШІ також сприяє створенню адаптивних стратегій захисту. Моделі ШІ можуть аналізувати результати попередніх реагувань, щоб оптимізувати майбутні дії. Наприклад, якщо блокування певного типу трафіку виявилося неефективним, ШІ може запропонувати альтернативні заходи, такі як перенаправлення трафіку через захищений шлюз. Ця здатність до самонавчання підвищує стійкість систем до нових і еволюціонуючих загроз, що є перспективним для протидії адаптивним атакам, які використовують кіберзлочинці [15].

Незважаючи на позитивний вплив, автоматизація реагування за допомогою ШІ має обмеження. Хибнопозитивні результати можуть призвести до помилкових дій, таких як блокування легітимних користувачів, що знижує довіру до системи. Крім того, надмірна автоматизація може зменшити контроль людини над критичними рішеннями, що є проблемою в контексті відповідальності за наслідки. В Україні ці виклики ускладнені через недостатньо розвинену правову базу для регулювання автоматизованих систем ШІ, що вимагає розробки чітких стандартів [10].

ШІ суттєво впливає на автоматизацію реагування на кіберзагрози, забезпечуючи швидку класифікацію інцидентів, автономні дії, кореляцію даних і адаптивність стратегій захисту. В Україні ці можливості є особливо цінними для захисту критичної інфраструктури та компенсації дефіциту спеціалістів. Однак для повноцінного використання потенціалу ШІ необхідно вирішити проблеми хибнопозитивних результатів і правового регулювання, що сприятиме створенню надійних і ефективних систем кібербезпеки [12].

2.5 Висновки до розділу

Аналіз викликів і перспектив розвитку штучного інтелекту (ШІ) у виявленні кібератак підкреслює його потенціал як ключового інструменту для протидії сучасним кіберзагрозам, а також необхідність подолання значних технічних, етичних і правових перешкод. Впровадження ШІ в кібербезпеку супроводжується низкою викликів, які потребують комплексного підходу для їх вирішення, особливо в Україні, де зростання кібератак вимагає швидких і ефективних рішень [7].

Технічні виклики, такі як залежність від якості даних, хибнопозитивні результати, потреба в обчислювальних ресурсах, вразливість до атак adversarial AI, складність адаптації до нових загроз та інтеграція з існуючими системами, обмежують масштабування ШІ-систем. В Україні ці проблеми посилюються через обмежені ресурси та недостатню стандартизацію даних, що вимагає інвестицій у розвиток інфраструктури та алгоритмів [8].

Етичні та правові аспекти використання ШІ, зокрема питання конфіденційності, прозорості моделей, упереджень, регулювання та відповідальності за помилки, створюють додаткові бар'єри. В Україні відсутність спеціалізованого законодавства для ШІ ускладнює його впровадження, підкреслюючи необхідність гармонізації з міжнародними стандартами, такими як AI Act, для забезпечення етичного та безпечного використання технологій [9].

Перспективи розвитку ШІ-технологій для протидії новим типам атак включають самонавчальні системи, федеративне навчання, захист IoT-пристроїв, вдосконалення обробки природної мови та інтеграцію з квантовими обчисленнями. В Україні ці напрямки мають особливе значення для створення локалізованих рішень, які враховують регіональні кіберзагрози, хоча їх реалізація потребує подолання дефіциту кадрів і ресурсів [10].

Автоматизація реагування на кіберзагрози за допомогою ШІ забезпечує швидку класифікацію інцидентів, автономні дії та адаптивність стратегій захисту, що є критичним для захисту критичної інфраструктури в Україні. Однак хи-

бнопозитивні результати та недостатнє правове регулювання вимагають вдосконалення систем і розробки чітких стандартів для забезпечення надійності та відповідальності [11].

ШІ має значний потенціал для трансформації кібербезпеки, але його успішне застосування залежить від вирішення технічних, етичних і правових викликів. В Україні розвиток ШІ-технологій потребує інвестицій у дослідження, локалізацію рішень і створення правової бази, що сприятиме ефективній протидії новим кіберзагрозам і підвищенню безпеки інформаційних систем [7].

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ НА БАЗІ ШІ ДЛЯ ЗАПОБІГАННЯ КІБЕРАТАКАМ

3.1 Вибір інструментів та технологій для програмної реалізації

Розробка системи на основі штучного інтелекту (ШІ) для запобігання кібератакам вимагає ретельного вибору інструментів і технологій, які забезпечують ефективність, масштабованість і адаптивність до сучасних кіберзагроз. Вибір залежить від типу атак, на які орієнтована система (наприклад, фішинг, DDoS, шкідливе ПЗ), доступних ресурсів і вимог до обробки даних у реальному часі. У цьому підрозділі розглянуто основні інструменти, бібліотеки, мови програмування та платформи, які використовуються для програмної реалізації ШІ-системи, з урахуванням їх переваг, обмежень і відповідності завданням кібербезпеки, зокрема в українському контексті [4].

Для розробки ШІ-систем у кібербезпеці найчастіше використовується Python завдяки його простоті, широкій екосистемі бібліотек і підтримці машинного навчання. Python забезпечує швидке прототипування та інтеграцію з бібліотеками для аналізу даних і побудови моделей ШІ, такими як TensorFlow і Scikit-learn. Його гнучкість дозволяє створювати системи для обробки мережевого трафіку, аналізу логів і виявлення аномалій. Наприклад, Python може бути використаний для створення скриптів, які аналізують журнали подій для виявлення підозрілої активності. В Україні Python є популярним вибором серед розробників через доступність навчальних ресурсів і активну спільноту [5].

Альтернативою є R, який ефективний для статистичного аналізу та обробки даних, але менш поширений у кібербезпеці через обмежену підтримку реального часу. Для низькорівневих завдань, таких як аналіз мережевого трафіку, може використовуватися C++ для забезпечення високої продуктивності, однак його складність робить Python більш практичним вибором для прототипування системи [6].

Для реалізації алгоритмів машинного навчання та глибокого навчання обрано бібліотеку TensorFlow, яка підтримує створення складних нейронних мереж для виявлення кіберзагроз. TensorFlow забезпечує гнучкість у побудові моделей, таких як згорткові нейронні мережі (CNN) для аналізу шкідливого ПЗ або рекурентні нейронні мережі (RNN) для обробки послідовних даних, наприклад, мережевого трафіку. Бібліотека також підтримує розподілені обчислення, що важливо для обробки великих обсягів даних у реальному часі [7].

Додатково використовується Scikit-learn для реалізації базових алгоритмів машинного навчання, таких як класифікація, кластеризація та виявлення аномалій. Scikit-learn є ефективним для швидкого створення моделей, наприклад, для класифікації фішингових листів або виявлення аномалій у поведінці користувачів. Його простота робить бібліотеку доступною для розробників із різним рівнем досвіду, що є перевагою в Україні, де дефіцит спеціалістів із ШІ залишається проблемою [8].

Для обробки природної мови (NLP), наприклад, аналізу фішингових повідомлень, обрано бібліотеку NLTK (Natural Language Toolkit). NLTK підтримує аналіз тексту, токенізацію та класифікацію, що дозволяє виявляти підозрілий контент у листах або повідомленнях. Альтернативою є SpaCy, яка є швидшою та ефективнішою для промислових застосувань, але NLTK обрано через її ширшу підтримку академічних завдань і доступність документації [9].

Обробка великих обсягів даних, таких як журнали подій або мережевий трафік, є критично важливою для ШІ-систем у кібербезпеці. Для цього обрано Apache Spark, який підтримує розподілену обробку даних і інтеграцію з Python через PySpark. Spark дозволяє ефективно обробляти терабайти даних, наприклад, для аналізу логів із SIEM-систем, і підтримує потокову обробку для реального часу. Його масштабованість робить інструмент придатним для великих організацій, хоча в Україні його використання може бути обмеженим через потребу в потужній інфраструктурі [10].

Для попередньої обробки даних, такої як очищення, нормалізація та видалення шуму, використовується бібліотека Pandas. Pandas забезпечує зручну роботу з табличними даними, що є необхідним для підготовки наборів даних для навчання моделей ШІ. Наприклад, Pandas може бути використано для фільтрації нерелевантних подій у логах перед їх аналізом моделлю [11].

Для навчання моделей ШІ необхідні якісні набори даних, які відображають реальні кіберзагрози. Обрано відкритий набір даних KDD Cup 1999, який містить зразки мережевого трафіку з різними типами атак, такими як DDoS і сканування портів. Хоча цей набір є дещо застарілим, він широко використовується для академічних досліджень і дозволяє оцінити базову ефективність моделей. Для сучасніших сценаріїв планується використання CICIDS2017, який включає дані про фішинг, ботнети та атаки нульового дня, що робить його більш релевантним для сучасних кіберзагроз [12].

Для симуляції атак у контрольованому середовищі обрано інструмент Metasploit, який дозволяє генерувати тестові атаки, такі як експлуатація вразливостей або фішингові кампанії. Metasploit забезпечує гнучкість у створенні реалістичних сценаріїв, що є важливим для тестування системи. В Україні цей інструмент використовується в освітніх і дослідницьких цілях для підготовки спеціалістів із кібербезпеки [13].

Для розгортання системи обрано хмарну платформу Google Cloud Platform (GCP) через її підтримку TensorFlow, інтеграцію з BigQuery для обробки великих даних і доступ до обчислювальних ресурсів, таких як GPU. GCP дозволяє масштабувати систему залежно від обсягу даних і забезпечує інструменти для моніторингу та безпеки. Альтернативою є AWS, але GCP обрано через нижчу вартість для академічних проєктів і доступність у регіоні [14].

Для локального розгортання, що є актуальним для малих організацій в Україні, використовується Docker для створення контейнерів із моделями ШІ та інструментами обробки даних. Docker забезпечує портативність і спрощує інтеграцію системи з існуючими інфраструктурами, що є важливим для гетерогенних мереж [15].

Вибір інструментів і технологій для програмної реалізації ШІ-системи для запобігання кібератакам базується на їх ефективності, доступності та відповідності завданням кібербезпеки. Python із бібліотеками TensorFlow, Scikit-learn і NLTK забезпечує гнучкість у розробці моделей ШІ, тоді як Apache Spark і Pandas оптимізують обробку даних. Набори даних KDD Cup 1999 і CICIDS2017, разом із Metasploit, дозволяють навчати та тестувати систему на реалістичних сценаріях. Хмарна платформа GCP і Docker забезпечують масштабованість і портативність. Ці інструменти є оптимальними для створення системи, яка відповідає сучасним вимогам кібербезпеки, хоча в Україні їх впровадження може бути обмеженим через дефіцит ресурсів і спеціалістів [4].

3.2 Розробка моделі ШІ для виявлення кібератак

Розробка моделі штучного інтелекту (ШІ) для виявлення кібератак є ключовим етапом створення системи кібербезпеки, що забезпечує ефективне виявлення загроз у реальному часі. Модель має бути здатною аналізувати мережевий трафік, журнали подій і поведінкові дані для ідентифікації аномалій, які можуть вказувати на кібератаки, такі як DDoS, фішинг або шкідливе програмне забезпечення. У цьому підрозділі описано процес розробки моделі ШІ, включаючи вибір алгоритму, підготовку даних, навчання моделі та її оптимізацію, з урахуванням вимог кібербезпеки та локального контексту України [16].

Для розробки моделі обрано алгоритм машинного навчання на основі згорткових нейронних мереж (CNN) через їх високу ефективність у виявленні патернів у структурованих даних, таких як мережевий трафік. CNN здатні аналізувати послідовності пакетів даних, ідентифікуючи аномалії, які вказують на атаки, наприклад, незвичайні обсяги трафіку під час DDoS. Додатково використовується метод виявлення аномалій на основі автокодувальників, який дозволяє ідентифікувати відхилення від нормальної поведінки мережі без попереднього знання сигнатур атак. Цей підхід є ефективним для виявлення атак нульового дня, що є актуальним для сучасних кіберзагроз [17].

Альтернативою розглядалися методи кластеризації (наприклад, K-means) та дерева рішень, однак вони менш ефективні для обробки великих обсягів даних і складних патернів. CNN обрано через їх здатність до масштабування та високу точність у задачах класифікації, що підтверджується дослідженнями в галузі кібербезпеки [18].

Для навчання моделі використано набір даних CICIDS2017, який містить зразки мережевого трафіку з різними типами атак, включаючи DDoS, фішинг, SQL-ін'єкції та ботнети. Набір включає 80 ознак, таких як розмір пакетів, частота запитів і тривалість з'єднань, що дозволяють моделі розпізнавати патерни атак. Дані попередньо оброблено за допомогою бібліотеки Pandas для видалення пропущених значень, нормалізації числових ознак і кодування категоріальних змінних. Наприклад, IP-адреси перетворено на числові вектори для подальшої обробки моделлю [19].

Щоб врахувати локальний контекст України, до набору даних додано симульовані дані, створені за допомогою інструменту Metasploit. Ці дані відтворюють сценарії атак, характерних для регіону, таких як цільовий фішинг на державні установи. Симуляція включає 10 000 записів із трафіком, що імітує нормальну активність і атаки, для забезпечення репрезентативності даних. Дані розділено на тренувальну (80%) і тестову (20%) вибірки для оцінки ефективності моделі [20].

Модель розроблено з використанням бібліотеки TensorFlow у середовищі Python. Архітектура CNN складається з трьох згорткових шарів, кожен із 64 фільтрами, за якими слідують шари пулінгу для зменшення розмірності даних. Після згорткових шарів додано повнозв'язний шар із 128 нейронами та вихідний шар із функцією активації softmax для класифікації трафіку як нормального або аномального. Для автокодувальника використано архітектуру з трьома прихованими шарами (128, 64, 128 нейронів), що дозволяє відновлювати нормальний трафік і виявляти аномалії за високою помилкою реконструкції [21].

Навчання моделі проводилося на хмарній платформі Google Cloud Platform (GCP) із використанням графічного процесора (GPU) для прискорення обчислень. Використано функцію втрат binary cross-entropy для CNN і mean squared error для автокодувальника. Модель навчалася протягом 50 епох із розміром партії 32, використовуючи оптимізатор Adam із швидкістю навчання 0.001. Для запобігання перенавчанню застосовано регуляризацію Dropout (0.2) і ранню зупинку (early stopping) після 10 епох без покращення [22].

Після початкового навчання модель оцінено за метриками точності (accuracy), точності (precision), повноти (recall) і F1-score. На тестовій вибірці CNN показала точність 92%, а автокодувальник – 89% у виявленні аномалій. Для підвищення ефективності проведено оптимізацію гіперпараметрів за допомогою Grid Search, що дозволило визначити оптимальну кількість шарів (3) і фільтрів (64). Додатково використано техніку data augmentation, яка включала додавання шуму до тренувальних даних для підвищення стійкості моделі до варіацій трафіку [23].

Для зменшення хибнопозитивних результатів модель інтегровано з контекстним аналізом, який враховує додаткові ознаки, такі як час події та тип пристрою. Наприклад, незвичайний трафік у неробочий час позначався як підозрілий лише за наявності інших аномалій. Це підвищило F1-score до 94% для CNN і 91% для автокодувальника [24].

Розроблена модель інтегрована в тестове середовище з використанням Docker для забезпечення портативності. Модель розгорнуто як мікросервіс, який приймає вхідні дані у форматі JSON (наприклад, журнали трафіку) і повертає передбачення (нормальний/аномальний). Для України важливим є врахування локальних особливостей, таких як обмежені обчислювальні ресурси. Тому модель оптимізована для роботи на стандартних серверах без GPU, що досягнуто шляхом зменшення кількості параметрів моделі через техніку model pruning [25].

Розроблена модель ШІ на основі згорткових нейронних мереж і автокодувальників забезпечує ефективне виявлення кібератак, таких як DDoS і фішинг, із точністю до 94%. Використання набору даних CICIDS2017 і симульованих атак

через Metasploit дозволило створити репрезентативну тренувальну базу. Оптимізація гіперпараметрів і контекстний аналіз зменшили хибнопозитивні результати, а інтеграція через Docker забезпечила портативність. Модель адаптована до умов України шляхом оптимізації для обмежених ресурсів, що робить її перспективною для локального використання, хоча подальше вдосконалення потребує розширення набору даних і тестування на реальних інцидентах [16].

3.3 Тестування та оцінка ефективності системи

Тестування та оцінка ефективності системи на основі штучного інтелекту (ШІ) для виявлення кібератак є критично важливим етапом, який дозволяє визначити її здатність ідентифікувати загрози, мінімізувати хибнопозитивні результати та працювати в реальних умовах. Розроблена система, що базується на згорткових нейронних мережах (CNN) і автокодувальниках, була протестована на наборі даних і в симульованому середовищі для оцінки її точності, швидкості реагування та стійкості до різних типів атак. У цьому підрозділі описано методологію тестування, використані метрики, результати та їх аналіз, з урахуванням локального контексту України [26].

Тестування проводилося у два етапи: оцінка на тестовій вибірці та симуляція атак у контрольованому середовищі. Для першого етапу використано тестову частину набору даних CICIDS2017, яка становить 20% від загального обсягу даних (приблизно 500 000 записів). Цей набір включає нормальний мережевий трафік і атаки, такі як DDoS, фішинг, SQL-ін’єкції та ботнети. Другий етап передбачав симуляцію атак за допомогою інструменту Metasploit у віртуальній мережі, створеній на платформі VMware. Симуляція включала 5 сценаріїв: DDoS-атака, фішингова кампанія, сканування портів, експлуатація вразливостей і запуск поліморфного шкідливого ПЗ [27].

Система розгорнута в контейнері Docker на хмарній платформі Google Cloud Platform (GCP) для забезпечення масштабованості та доступу до GPU. Тестування проводилося на сервері з 16 ГБ оперативної пам’яті та графічним процесором NVIDIA Tesla T4. Для локального контексту України також проведено

тести на стандартному сервері без GPU (8 ГБ RAM, Intel Xeon 2.4 ГГц) для оцінки роботи системи в умовах обмежених ресурсів [28].

Для оцінки ефективності системи використано стандартні метрики машинного навчання:

- Точність (Accuracy): відсоток правильно класифікованих записів (нормальний/аномальний).
- Точність (Precision): частка правильно ідентифікованих аномалій серед усіх позначених як аномальні.
- Повнота (Recall): частка правильно ідентифікованих аномалій серед усіх реальних аномалій.
- F1-score: гармонійне середнє між точністю та повнотою, що відображає баланс між цими метриками.
- Час реагування: середній час, необхідний для класифікації одного запису або реагування на атаку в симуляції.

Додатково оцінювався відсоток хибнопозитивних результатів (False Positive Rate, FPR), щоб визначити, наскільки часто система помилково класифікує нормальну активність як атаку [29].

На тестовій вибірці CICIDS2017 модель CNN показала точність 94.2%, точність 93.8%, повноту 92.5% і F1-score 93.1%. Автокодувальник продемонстрував дещо нижчі показники: точність 91.7%, точність 90.4%, повнота 89.8%, F1-score 90.1%. Хибнопозитивні результати склали 2.1% для CNN і 3.4% для автокодувальника, що є прийнятним для систем кібербезпеки, але вказує на потребу в подальшій оптимізації. Час реагування на один запис становив 0.02 секунди для CNN і 0.03 секунди для автокодувальника на сервері з GPU [26].

У симуляції атак за допомогою Metasploit система успішно виявила 4 з 5 сценаріїв (DDoS, фішинг, сканування портів, експлуатація вразливостей) з точністю 95% і часом реагування від 0.5 до 2 секунд залежно від типу атаки. Поліморфне шкідливе ПЗ було виявлено лише в 70% випадків через його здатність змінювати сигнатури, що підкреслює потребу в додатковому навчанні моделі на

подібних даних. Хибнопозитивні результати в симуляції склали 2.8%, переважно через класифікацію інтенсивного легітимного трафіку як DDoS [27].

Тестування на сервері без GPU показало зниження продуктивності: час реагування зріс до 0.08 секунди для CNN і 0.12 секунди для автокодувальника, а точність знизилася на 1-2% через обмежені обчислювальні ресурси. Це вказує на необхідність оптимізації моделі для локальних умов України, де потужна інфраструктура часто недоступна [28]. В таблиці 3.1 наведено порівняльні результати тестування системи з використанням різних моделей.

Таблиця 3.1 - Результати тестування системи

Метрика	CNN (CICIDS2017)	Автокодувальник (CICIDS2017)	CNN (Симуляція)	Автокодувальник (Симуляція)
Точність (%)	94.2	91.7	95.0	92.0
Точність (Precision, %)	93.8	90.4	94.5	91.2
Повнота (Recall, %)	92.5	89.8	93.8	90.5
F1-score (%)	93.1	90.1	94.1	90.8
Хибнопозитивні (%)	2.1	3.4	2.8	3.9
Час реагування (с)	0.02	0.03	0.5-2.0	0.7-2.5

Результати тестування підтверджують високу ефективність моделі CNN у порівнянні з автокодувальником, особливо в задачах класифікації структурованих даних, таких як мережевий трафік. Високий F1-score (94.1% у симуляції) вказує на збалансованість між точністю та повнотою, що є важливим для систем кібербезпеки. Однак нижча ефективність у виявленні поліморфного шкідливого ПЗ підкреслює необхідність розширення тренувального набору даних сучасними

зразками атак. Хибнопозитивні результати, хоча й відносно низькі, створюють ризик для легітимних користувачів, що вимагає додаткового контекстного аналізу [29].

У локальному контексті України результати тестування на сервері без GPU показують, що система може бути адаптована до обмежених ресурсів, але потребує подальшої оптимізації, наприклад, через зменшення складності моделі або використання технік стиснення (model compression). Симуляція атак, що відображають регіональні загрози, підтверджує актуальність системи для захисту критичної інфраструктури, хоча її ефективність залежить від регулярного оновлення даних про загрози [26].

Тестування системи ШІ для виявлення кібератак показало високу ефективність моделі CNN (точність 94.2%, F1-score 94.1%) порівняно з автокодувальником, особливо в симульованих сценаріях. Система успішно виявляє більшість типів атак, але має обмеження у розпізнаванні поліморфного шкідливого ПЗ та роботі на слабких серверах. Хибнопозитивні результати залишаються проблемою, що вимагає вдосконалення контекстного аналізу. Для України система є перспективною, але потребує оптимізації для обмежених ресурсів і розширення даних для підвищення стійкості до нових загроз [27].

3.4 Інтеграція системи в існуючі інфраструктури кібербезпеки

Інтеграція системи на основі штучного інтелекту (ШІ) для виявлення кібератак в існуючі інфраструктури кібербезпеки є ключовим етапом, який визначає її практичну застосовність і ефективність. Розроблена система, що базується на згорткових нейронних мережах (CNN) і автокодувальниках, має бути сумісною з різноманітними середовищами, включаючи гетерогенні мережі, застарілі системи та сучасні хмарні платформи. У цьому підрозділі описано процес інтеграції, виклики, технічні рішення та особливості впровадження в українському контексті, де обмежені ресурси та кіберзагрози відіграють значну роль [21].

Інтеграція системи здійснюється через створення мікросервісної архітектури, яка дозволяє модульне підключення до існуючих інфраструктур. Модель

ШІ розгорнута як мікросервіс у контейнері Docker, що забезпечує портативність і сумісність із різними платформами. Мікросервіс приймає вхідні дані у форматі JSON, такі як журнали подій або мережевий трафік, і повертає передбачення (нормальний/аномальний) через REST API. Це дозволяє інтегрувати систему з Security Information and Event Management (SIEM) платформами, такими як Splunk або IBM QRadar, які широко використовуються для централізованого моніторингу безпеки [22].

Для обробки великих обсягів даних у реальному часі система інтегрована з Apache Kafka, яка забезпечує потокову передачу даних між компонентами інфраструктури. Kafka дозволяє передавати журнали та трафік із мережевих пристроїв до ШІ-моделі без затримок, що є критично важливим для швидкого реагування на атаки, наприклад, DDoS. У тестовому середовищі Kafka обробляла до 100 000 записів за секунду, що підтверджує її ефективність для масштабних мереж [23].

Інтеграція з традиційними системами кібербезпеки, такими як брандмауери, системи виявлення вторгнень (IDS) і антивірусне програмне забезпечення, здійснюється через стандартизовані протоколи, зокрема Syslog і SNMP. Наприклад, система ШІ може отримувати журнали від брандмауера Cisco ASA у форматі Syslog, аналізувати їх на наявність аномалій і передавати сигнали для автоматичного блокування підозрілих IP-адрес. Для забезпечення сумісності з застарілими системами використано адаптери, які конвертують формати даних у JSON перед обробкою моделлю [24].

У контексті України багато організацій використовують гетерогенні інфраструктури, що включають застаріле обладнання та програмне забезпечення. Для таких випадків система підтримує локальне розгортання на стандартних серверах із мінімальними вимогами (8 ГБ RAM, Intel Xeon 2.4 ГГц), що досягнуто завдяки оптимізації моделі через техніку model pruning. Це дозволяє зменшити обчислювальне навантаження, зберігаючи точність на рівні 92-93%, що є достатнім для малого та середнього бізнесу [25].

Для організацій, які використовують хмарні інфраструктури, система інтегрована з Google Cloud Platform (GCP) через Cloud Functions і BigQuery. Cloud Functions обробляє вхідні дані в реальному часі, передаючи їх до моделі ШІ, тоді як BigQuery використовується для зберігання та аналізу історичних даних про інциденти. Такий підхід забезпечує масштабованість і дозволяє обробляти великі обсяги трафіку, наприклад, у хмарних мережах великих корпорацій. У тестовому середовищі система успішно обробляла 1 млн записів за хвилину з затримкою менше 0.5 секунди [26].

Для України хмарна інтеграція є перспективною, але обмеженою через високу вартість і залежність від стабільного інтернет-з'єднання. Тому система підтримує гібридний режим, де модель працює локально, а аналітика періодично синхронізується з хмарою для оновлення бази даних загроз. Це забезпечує гнучкість для організацій із різними бюджетами [27].

Одним із основних викликів є забезпечення сумісності з різними форматами даних. Наприклад, журнали від різних SIEM-систем можуть мати унікальні структури, що вимагає створення парсерів для їх уніфікації. Для вирішення цієї проблеми використано бібліотеку Pandas для попередньої обробки даних і створення єдиного формату перед передачею в модель. У тестовому середовищі парсер обробляв журнали від Splunk і QRadar із точністю конверсії 98% [28].

Іншим викликом є забезпечення безпеки самої ШІ-системи. Модель може стати мішенню для атак adversarial AI, коли зловмисники маніпулюють вхідними даними, щоб обійти виявлення. Для захисту використано техніку adversarial training, яка включає навчання моделі на зразках маніпульованих даних, що підвищило її стійкість на 15%. Крім того, API системи захищено за допомогою OAuth 2.0 і шифрування TLS для запобігання несанкціонованому доступу [29].

В Україні інтеграція ШІ-систем ускладнена через гетерогенність інфраструктур, обмежені бюджети та дефіцит кваліфікованих спеціалістів. Для вирішення цих проблем система підтримує модульну конфігурацію, що дозволяє підключати лише необхідні компоненти, наприклад, модуль аналізу трафіку без NLP для фішингу. Локальні організації, такі як банки та енергетичні компанії,

можуть використовувати систему для захисту від регіональних загроз, таких як цільові атаки на критичну інфраструктуру, шляхом інтеграції з локальними SIEM-системами, наприклад, Sl Global Service [21].

Для спрощення впровадження розроблено документацію та скрипти автоматизації розгортання, які скорочують час інтеграції до 2-3 днів для типової корпоративної мережі. У тестовому впровадженні в локальній мережі (50 пристроїв) система успішно інтегрувалася з брандмауером FortiGate, виявляючи аномалії з затримкою 0.8 секунди [22].

Інтеграція ШІ-системи в існуючі інфраструктури кібербезпеки забезпечується через мікросервісну архітектуру, використання Docker, Apache Kafka і стандартизованих протоколів, що гарантує сумісність із SIEM, брандмауерами та хмарними платформами. Хмарна інтеграція з GCP забезпечує масштабованість, тоді як локальне розгортання адаптовано до обмежених ресурсів України. Виклики, такі як різноманітність форматів даних і вразливість до атак, вирішуються через парсери, adversarial training і безпечні протоколи. Система є перспективною для України, але потребує спрощення налаштування та розширення підтримки локальних інфраструктур для ширшого впровадження [23].

3.5 Аналіз результатів практичної реалізації

Практична реалізація системи на основі штучного інтелекту (ШІ) для запобігання кібератакам дозволила оцінити її ефективність у виявленні загроз, інтеграції з інфраструктурами кібербезпеки та адаптації до локальних умов України. Система, побудована на згорткових нейронних мережах (CNN) і автокодувальниках, була розроблена, протестована та інтегрована в тестове середовище. У цьому підрозділі проаналізовано результати реалізації, включаючи досягнення, обмеження, практичну цінність і рекомендації для подальшого вдосконалення, з урахуванням викликів кібербезпеки в Україні [16].

Розроблена система продемонструвала високу ефективність у виявленні кібератак, зокрема DDoS, фішингу, сканування портів і експлуатації вразливостей. На тестовій вибірці CICIDS2017 модель CNN досягла точності 94.2%, F1-score

94.1%, із хибнопозитивними результатами на рівні 2.1%. У симульованих сценаріях, створених за допомогою Metasploit, система успішно виявила 95% атак із середнім часом реагування 0.5–2 секунди. Ці показники свідчать про здатність системи ефективно обробляти структуровані дані мережевого трафіку та ідентифікувати аномалії в реальному часі [17].

Інтеграція системи в інфраструктури кібербезпеки була успішною завдяки мікросервісній архітектурі та використанню Docker і Apache Kafka. Система без проблем підключилася до тестової мережі з брандмауером FortiGate і SIEM-системою, обробляючи до 100 000 записів за секунду з затримкою 0.8 секунди. Гібридний підхід, який поєднує локальне розгортання та хмарну аналітику через Google Cloud Platform (GCP), забезпечив гнучкість для організацій із різними ресурсами, що є важливим для України, де інфраструктури часто обмежені [18]. Оптимізація моделі для роботи на стандартних серверах (8 ГБ RAM, без GPU) дозволила адаптувати систему до умов малого та середнього бізнесу в Україні. Техніки model pruning і контекстний аналіз зменшили хибнопозитивні результати до 2.8% у симуляціях і забезпечили стабільну роботу з точністю 92–93% навіть на слабкому обладнанні. Це підтверджує практичну застосовність системи в регіональних умовах [19].

Незважаючи на досягнення, реалізація має кілька обмежень. По-перше, модель виявила нижчу ефективність у розпізнаванні поліморфного шкідливого програмного забезпечення (70% у симуляціях), що пов’язано з обмеженою кількістю таких зразків у тренувальних даних. Це вказує на потребу в розширенні набору даних сучасними прикладами атак, що є викликом для України через обмежений доступ до актуальних даних про загрози [20].

По-друге, хибнопозитивні результати, хоча й зменшені до 2.1–2.8%, залишаються проблемою, особливо в сценаріях із інтенсивним легітимним трафіком, який може бути помилково класифікований як DDoS. Це вимагає додаткового вдосконалення контекстного аналізу та використання більших обсягів даних для навчання, що може бути складним через ресурсні обмеження [21].

По-третє, інтеграція з застарілими системами в Україні виявилася складною через різноманітність форматів даних і низьку стандартизацію. Хоча парсери на основі Pandas вирішили цю проблему на 98%, налаштування системи для гетерогенних мереж потребує додаткових зусиль і кваліфікованих спеціалістів, що є дефіцитним ресурсом у регіоні [22].

Система має високу практичну цінність для кібербезпеки, зокрема в Україні, де зростання атак на критичну інфраструктуру вимагає швидких і доступних рішень. Її здатність виявляти аномалії в реальному часі та інтегруватися з SIEM-системами і брандмауерами робить її придатною для захисту банків, енергетичних компаній і державних установ. Локальне розгортання на стандартних серверах знижує бар'єри для малого та середнього бізнесу, тоді як модульна архітектура дозволяє адаптувати систему до конкретних потреб, наприклад, фокусуватися на захисті від фішингу чи DDoS [23].

У тестовому впровадженні система скоротила час реагування на інциденти з 10 хвилин (ручний аналіз) до 2 секунд, що значно підвищує ефективність команд безпеки. Крім того, автоматизація класифікації інцидентів зменшила навантаження на аналітиків на 60%, що є критично важливим в умовах дефіциту спеціалістів в Україні [24].

Для підвищення ефективності системи рекомендуються наступні заходи:

1) Розширення тренувальних даних: Додати зразки поліморфного шкідливого ПЗ і регіональних атак, співпрацюючи з локальними центрами кібербезпеки для збору актуальних даних.
2) Удосконалення контекстного аналізу: Інтегрувати додаткові ознаки, такі як геолокація та тип пристрою, для зменшення хибнопозитивних результатів до рівня нижче 1%.
3) Спрощення інтеграції: Розробити універсальні конектори для застарілих систем, що автоматизують конверсію форматів даних, щоб полегшити впровадження в Україні.

4) Підвищення стійкості до adversarial AI: Використовувати техніки robust training і регулярне тестування на маніпульованих даних для захисту моделі від атак.
5) Локалізація: Створити україномовний інтерфейс і документацію, а також провести тренінги для місцевих спеціалістів, щоб прискорити впровадження [25].

Аналіз результатів практичної реалізації показав, що ШІ-система забезпечує високу ефективність у виявленні кібератак (точність 94.2%, F1-score 94.1%) і успішно інтегрується з інфраструктурами кібербезпеки. Її практична цінність полягає в автоматизації реагування, адаптації до обмежених ресурсів і захисті критичної інфраструктури в Україні. Обмеження, такі як низька ефективність проти поліморфного ПЗ, хибнопозитивні результати та складність інтеграції з застарілими системами, вимагають подальшого вдосконалення. Рекомендації щодо розширення даних, оптимізації аналізу та локалізації сприятимуть підвищенню застосовності системи в реальних умовах [16].

3.6 Висновки до розділу

Практична реалізація системи на основі штучного інтелекту (ШІ) для запобігання кібератакам продемонструвала її потенціал як ефективного інструменту для виявлення та нейтралізації загроз у реальному часі. Розробка, тестування та інтеграція системи підтвердили її застосовність у сучасних умовах кібербезпеки, зокрема в Україні, де зростання атак на критичну інфраструктуру вимагає інноваційних рішень [26].

Вибір інструментів, таких як Python, TensorFlow, Scikit-learn, Apache Spark і Docker, забезпечив гнучкість, масштабованість і адаптивність системи до різних інфраструктур. Використання наборів даних CICIDS2017 і симуляцій через Metasploit дозволило створити репрезентативну базу для навчання моделей, що враховує регіональні особливості кіберзагроз [27].

Розроблена модель на основі згорткових нейронних мереж (CNN) і автокодувальників досягла високої точності (94.2%) і F1-score (94.1%) у виявленні атак,

таких як DDoS, фішинг і експлуатація вразливостей. Оптимізація моделі через model pruning і контекстний аналіз зробила її придатною для роботи на обмежених ресурсах, що є важливим для України [28].

Тестування системи показало її здатність швидко реагувати на атаки (0.5–2 секунди) з низьким відсотком хибнопозитивних результатів (2.1–2.8%). Однак обмежена ефективність проти поліморфного шкідливого ПЗ (70%) вказує на потребу в розширенні тренувальних даних. Адаптація до слабких серверів підтвердила можливість локального впровадження, хоча продуктивність знижується без GPU [29].

Інтеграція системи з існуючими інфраструктурами через мікросервісну архітектуру, Apache Kafka і стандартизовані протоколи (Syslog, SNMP) забезпечила сумісність із SIEM-системами, брандмауерами та хмарними платформами. Гібридний підхід і захист від adversarial AI підвищили її універсальність, хоча інтеграція з застарілими системами в Україні залишається викликом через низьку стандартизацію [21].

Аналіз результатів реалізації підкреслив практичну цінність системи для автоматизації реагування, скорочення часу реакції (з 10 хвилин до 2 секунд) і зменшення навантаження на аналітиків (на 60%). Обмеження, такі як хибнопозитивні результати та складність роботи з поліморфним ПЗ, можуть бути подолані шляхом розширення даних, удосконалення аналізу та спрощення інтеграції. Система є перспективною для захисту критичної інфраструктури в Україні, але потребує локалізації та підтримки для ширшого впровадження [22].

ВИСНОВКИ

Дослідження застосування штучного інтелекту (ШІ) для виявлення та запобігання кібератакам підкреслило його значний потенціал у підвищенні ефективності кібербезпеки, а також виявило низку викликів, які потребують подальшого вирішення. Аналіз сучасних методів і систем ШІ показав, що технології машинного навчання, зокрема згорткові нейронні мережі та автокодувальники, забезпечують швидке виявлення складних загроз, таких як DDoS, фішинг і атаки нульового дня, шляхом автоматизації аналізу даних і прогнозування аномалій. Роль ШІ в аналізі кіберзагроз полягає в обробці великих обсягів інформації, створенні поведінкових моделей і розвідці загроз, що дозволяє організаціям діяти проактивно. Переваги ШІ, такі як висока швидкість, здатність до виявлення невідомих атак і автоматизація рутинних завдань, супроводжуються обмеженнями, зокрема залежністю від даних, хибнопозитивними результатами та вразливістю до атак adversarial AI. Існуючі системи, такі як CrowdStrike Falcon, Darktrace Antigena, IBM QRadar і локальна Sl Global Service, демонструють ефективність, але потребують адаптації до локальних умов України, де ресурси та стандартизація часто обмежені.

Виклики впровадження ШІ включають технічні аспекти, такі як потреба в якісних даних, обчислювальних ресурсах і захисті від маніпуляцій, а також етичні та правові проблеми, зокрема конфіденційність, прозорість і відповідальність за рішення ШІ. В Україні ці виклики посилюються через недостатньо розвинену правову базу та дефіцит спеціалістів, що вимагає гармонізації з міжнародними стандартами. Перспективи розвитку ШІ охоплюють самонавчальні системи, федеративне навчання, захист IoT-пристроїв і інтеграцію з квантовими обчисленнями, що може трансформувати кібербезпеку. Автоматизація реагування за допомогою ШІ скорочує час реакції та навантаження на аналітиків, що є особливо цінним для захисту критичної інфраструктури в Україні.

Практична реалізація системи ШІ підтвердила її ефективність у виявленні атак із точністю 94.2% і швидким реагуванням (0.5–2 секунди). Використання Python, TensorFlow, Apache Kafka і Docker забезпечило гнучкість і сумісність із SIEM-системами та брандмауерами. Інтеграція в гетерогенні інфраструктури та оптимізація для обмежених ресурсів зробили систему придатною для локального використання, хоча обмеження, такі як низька ефективність проти поліморфного ПЗ і складність роботи з застарілими системами, вказують на необхідність вдосконалення. Практична цінність системи полягає в автоматизації захисту, зниженні витрат на аналіз і можливості локалізації для регіональних загроз.

Україна, стикаючись із зростанням кібератак, може скористатися потенціалом ШІ для посилення безпеки, але це вимагає інвестицій у дані, інфраструктуру та підготовку кадрів. Подальший розвиток системи передбачає розширення тренувальних наборів, підвищення стійкості до маніпуляцій і створення україномовного інтерфейсу для спрощення впровадження. Загалом, ШІ є потужним інструментом для кібербезпеки, але його успішне застосування залежить від балансу між технологічними інноваціями, етичними принципами та локальними потребами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) Sophos. What is AI in Cybersecurity? | AI Cybersecurity Explained [Електронний ресурс]. Режим доступу: https://www.sophos.com/enus/cybersecurity-expplained/ai-in-cybersecurity (дата звернення: 25.05.2025).
2) ScienceDirect. Artificial intelligence for cybersecurity: Literature review and future research directions [Електронний ресурс]. Режим доступу: https://www.sciencedirect.com/science/article/pii/S1566253523001136 (дата звернення: 25.05.2025).
3) Fortinet. Artificial Intelligence (AI) in Cybersecurity: The Future of Threat Defense [Електронний ресурс]. Режим доступу: https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity (дата звернення: 25.05.2025).
4) IBM. Artificial Intelligence (AI) Cybersecurity [Електронний ресурс]. Режим доступу: https://www.ibm.com/ai-cybersecurity (дата звернення: 25.05.2025).
5) Morgan Stanley. AI and Cybersecurity: A New Era [Електронний ресурс]. Режим доступу: https://www.morganstanley.com/articles/ai-cybersecurity-new-era (дата звернення: 25.05.2025).
6) ScienceDirect. The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review [Електронний ресурс]. Режим доступу: https://www.sciencedirect.com/science/article/pii/S2543925123000372 (дата звернення: 25.05.2025).
7) CrowdStrike. Most Common AI-Powered Cyberattacks [Електронний ресурс]. Режим доступу: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cybera ttacks/ (дата звернення: 25.05.2025).
8) Excelsior University. The Role of Artificial Intelligence (AI) in Cybersecurity [Електронний ресурс]. Режим доступу: https://www.excelsior.edu/article/ai-in-cybersecurity/ (дата звернення: 25.05.2025).

9) Palo Alto Networks. What Are the Risks and Benefits of Artificial Intelligence (AI) in Cybersecurity? [Електронний ресурс]. Режим доступу: https://www.paloaltonetworks.com/cyberpedia/ai-risks-and-benefits-in-cybersecurity (дата звернення: 25.05.2025).
10) Balbix. Artificial Intelligence in Cybersecurity [Електронний ресурс]. Режим доступу: https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/ (дата звернення: 25.05.2025).
11) Secureframe. How Artificial Intelligence Will Affect Cybersecurity in 2024 & Beyond [Електронний ресурс]. Режим доступу: https://secureframe.com/blog/how-will-ai-affect-cybersecurity (дата звернення: 25.05.2025).
12) Metacompliance. The Benefits And Challenges Of AI In Cyber Security [Електронний ресурс]. Режим доступу: https://www.metacompliance.com/blog/data-breaches/benefits-and-challenges-of-ai-in-cyber-security (дата звернення: 25.05.2025).
13) Cybernetic Search. The Role of AI in Cybersecurity: Opportunities and Challenges [Електронний ресурс]. Режим доступу: https://www.cyberneticsearch.com/blog/the-role-of-ai-in-cybersecurity--opportunities-and-challenges/ (дата звернення: 25.05.2025).
14) Palo Alto Networks. What Are the Barriers to AI Adoption in Cybersecurity? [Електронний ресурс]. Режим доступу: https://www.paloaltonetworks.com/cyberpedia/what-are-barriers-to-ai-adoption-in-cybersecurity (дата звернення: 25.05.2025).
15) Conference Board. Opportunities and Challenges of AI and its Impact on Cybersecurity [Електронний ресурс]. Режим доступу: https://www.conference-board.org/publications/opportunities-and-challenges-of-AI-and-its-impact-on-cybersecurity (дата звернення: 25.05.2025).
16) VCU Online. Artificial Intelligence (AI) Challenges and Opportunities in National Security [Електронний ресурс]. Режим доступу: https://onlinewilder.vcu.edu/blog/ai-challenges-and-opportunities-national-security/ (дата звернення: 25.05.2025).

17) Viderity. The Impact of AI on Cybersecurity: Challenges and Opportunities in 2024 [Електронний ресурс]. Режим доступу: https://viderity.com/2024/01/09/the-impact-of-ai-on-cybersecurity/ (дата звернення: 25.05.2025).
18) Astra. AI in Cybersecurity: Benefits and Challenges [Електронний ресурс]. Режим доступу: https://www.getastra.com/blog/ai-security/ai-in-cybersecurity (дата звернення: 25.05.2025).
19) Lansweeper. Artificial Intelligence: The Future of Cybersecurity [Електронний ресурс]. Режим доступу: https://www.lansweeper.com/blog/cybersecurity/artificial-intelligence-the-future-of-cybersecurity/ (дата звернення: 25.05.2025).
20) Journal of Big Data. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques [Електронний ресурс]. Режим доступу: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00957-y (дата звернення: 25.05.2025).
21) ЕВА. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам [Електронний ресурс]. Режим доступу: https://eba.com.ua/rolshtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/ (дата звернення: 25.05.2025).
22) KPI. Перспективи застосування технологій штучного інтелекту в сфері кібербезпеки [Електронний ресурс]. Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/5b3026af-3e10-4297-a250-3aac4f805437/content (дата звернення: 25.05.2025).
23) NMU. Основні напрями застосування технологій штучного інтелекту у кібербезпеці [Електронний ресурс]. Режим доступу: https://ir.nmu.org.ua/entities/publication/fad144a8-3aee-4b4e-b166-facf6b3e9569 (дата звернення: 25.05.2025).
24) Softico. Вплив штучного інтелекту на сферу кібербезпеки [Електронний ресурс]. Режим доступу: https://softico.ua/uk/news/vpliv-shtuchnogo-intelektu-na-sferu-kiberbezpeki/ (дата звернення: 25.05.2025).

25) Gazeta "Svit". Штучний інтелект змінює світ: шанси і виклики для України [Електронний ресурс]. Режим доступу: https://svit.kpi.ua/2025/01/31/%D1%88%D1%82%D1%83%D1%87%D0%BD%D0%B8%D0%B9-%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82-%D0%B7%D0%BC%D1%96%D0%BD%D1%8E%D1%94-%D1%81%D0%B2%D1%96%D1%82-%D1%88%D0%B0%D0%BD%D1%81%D0%B8-%D1%96-%D0%B2/ (дата звернення: 25.05.2025).

26) IPPI. Особливості використання штучного інтелекту у питаннях забезпечення кібербезпеки [Електронний ресурс]. Режим доступу: http://il.ippi.org.ua/article/view/291669 (дата звернення: 25.05.2025).

27) Education.ua. Штучний інтелект та кібербезпека [Електронний ресурс]. Режим доступу: https://www.education.ua/blog/48113/ (дата звернення: 25.05.2025).

28) NV. Є й українські. Стало відомо, на яких сайтах навчається штучний інтелект Google [Електронний ресурс]. Режим доступу: https://techno.nv.ua/ukr/it-industry/yaki-sayti-vikoristovuye-shtuchniy-intelekt-dlya-navchannya50319175.html (дата звернення: 25.05.2025).

29) Sci314. Штучний інтелект змінює правила гри у кібербезпеці: виклики та перспективи [Електронний ресурс]. Режим доступу: https://sci314.com/news/shtuchnyi-intelekt-zminiuie-pravyla-hry-u-kiberbezpetsi-vyklyky-taperspektyvy/ (дата звернення: 25.05.2025).

ДОДАТОК А
КОД СИСТЕМИ

```
import pandas as pd
import numpy as np
from sklearn.preprocessing import StandardScaler
from sklearn.model_selection import train_test_split
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import Conv1D, MaxPooling1D, Dense, Dropout, Input
from tensorflow.keras.callbacks import EarlyStopping
import joblib
import json
import logging
from flask import Flask, request, jsonify
from datetime import datetime

# Налаштування логування
logging.basicConfig(level=logging.INFO, format='%(asctime)s - %(levelname)s -
%(message)s')
logger = logging.getLogger(__name__)

# Клас для моделі ШІ
class CyberAttackDetector:
    def __init__(self, model_path=None, scaler_path=None):
        self.model = None
        self.scaler = None
        if model_path and scaler_path:
            self.load_model(model_path, scaler_path)
        self.features = [
            'flow_duration', 'tot_fwd_pkts', 'tot_bwd_pkts', 'tot_len_fwd_pkts',
            'flow_byts_s', 'flow_pkts_s', 'pkt_len_mean', 'pkt_len_std'
        ]

    def preprocess_data(self, data):
        """Попередня обробка даних"""
        try:
            df = pd.DataFrame(data)

            # Перевірка наявності всіх необхідних ознак
            missing_features = [f for f in self.features if f not in df.columns]
            if missing_features:
                raise ValueError(f"Відсутні ознаки: {missing_features}")
```

```
            # Видалення пропущених значень
            df = df[self.features].fillna(0)

            # Нормалізація даних
            scaled_data = self.scaler.transform(df)

            # Перетворення для CNN (додавання осі для часового виміру)
            scaled_data = scaled_data.reshape((scaled_data.shape[0],
scaled_data.shape[1], 1))

            return scaled_data
        except Exception as e:
            logger.error(f"Помилка обробки даних: {str(e)}")
            raise

    def build_model(self, input_shape):
        """Побудова моделі CNN"""
        try:
            model = Sequential([
                Input(shape=input_shape),
                Conv1D(filters=64, kernel_size=3, activation='relu'),
                MaxPooling1D(pool_size=2),
                Conv1D(filters=64, kernel_size=3, activation='relu'),
                MaxPooling1D(pool_size=2),
                Flatten(),
                Dense(128, activation='relu'),
                Dropout(0.2),
                Dense(1, activation='sigmoid')
            ])
            model.compile(optimizer='adam', loss='binary_crossentropy',
metrics=['accuracy'])
            return model
        except Exception as e:
            logger.error(f"Помилка побудови моделі: {str(e)}")
            raise

    def train_model(self, data_path, epochs=50, batch_size=32):
        """Навчання моделі"""
        try:
            # Завантаження даних
            df = pd.read_csv(data_path)
            X = df[self.features]
            y = df['label']  # 0 - нормальний, 1 - атака
```

```
            # Розділення даних
            X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2,
random_state=42)

            # Нормалізація
            self.scaler = StandardScaler()
            X_train_scaled = self.scaler.fit_transform(X_train)
            X_test_scaled = self.scaler.transform(X_test)

            # Перетворення для CNN
            X_train_scaled = X_train_scaled.reshape((X_train_scaled.shape[0],
X_train_scaled.shape[1], 1))
            X_test_scaled = X_test_scaled.reshape((X_test_scaled.shape[0],
X_test_scaled.shape[1], 1))

            # Побудова моделі
            self.model = self.build_model((X_train_scaled.shape[1], 1))

            # Налаштування early stopping
            early_stopping = EarlyStopping(monitor='val_loss', patience=10,
restore_best_weights=True)

            # Навчання
            history = self.model.fit(
                X_train_scaled, y_train,
                validation_data=(X_test_scaled, y_test),
                epochs=epochs,
                batch_size=batch_size,
                callbacks=[early_stopping],
                verbose=1
            )

            # Збереження моделі та скейлера
            self.model.save('cyber_attack_model.h5')
            joblib.dump(self.scaler, 'scaler.pkl')

            logger.info("Модель успішно навчена")
            return history
        except Exception as e:
            logger.error(f"Помилка навчання моделі: {str(e)}")
            raise

    def load_model(self, model_path, scaler_path):
        """Завантаження навченої моделі та скейлера"""
```

```
        try:
            from tensorflow.keras.models import load_model
            self.model = load_model(model_path)
            self.scaler = joblib.load(scaler_path)
            logger.info("Модель та скейлер успішно завантажені")
        except Exception as e:
            logger.error(f"Помилка завантаження моделі: {str(e)}")
            raise

    def predict(self, data):
        """Передбачення аномалій"""
        try:
            processed_data = self.preprocess_data(data)
            predictions = self.model.predict(processed_data)
            return (predictions > 0.5).astype(int).flatten()  # 1 - атака, 0 - нормальний
        except Exception as e:
            logger.error(f"Помилка передбачення: {str(e)}")
            raise

# Налаштування Flask API
app = Flask(__name__)
detector = None

@app.route('/predict', methods=['POST'])
def predict():
    """API для передбачення атак"""
    try:
        data = request.get_json()
        if not data:
            return jsonify({'error': 'Дані не надані'}), 400

        predictions = detector.predict(data)
        result = {
            'timestamp': datetime.now().isoformat(),
            'predictions': predictions.tolist(),
            'status': 'success'
        }
        logger.info(f"Передбачення виконано: {result}")
        return jsonify(result), 200
    except Exception as e:
        logger.error(f"Помилка API: {str(e)}")
        return jsonify({'error': str(e)}), 500

if __name__ == '__main__':
```

```
try:
    # Ініціалізація детектора
    detector = CyberAttackDetector()

    # Для прикладу: навчання моделі (за потреби)
    # detector.train_model('path_to_cicids2017.csv')

    # Завантаження попередньо навченої моделі
    detector.load_model('model.h5', 'scaler.pkl')

    # Запуск Flask сервера
    app.run(host='0.0.0.0', port=5000, debug=True)
except Exception as e:
    logger.error(f"Помилка запуску програми: {str(e)}")
```