



[DOI 10.28925/2663-4023.2024.25.318329](https://doi.org/10.28925/2663-4023.2024.25.318329)

УДК 004.056.5:510.22(043.3)

Ільєнко Анна Вадимівна

кандидат технічних наук, доцент, завідувач кафедри кібербезпеки

Національний авіаційний університет, Київ, Україна

ORCID ID: 0000-0001-8565-1117

ilyenko.a.v@nau.edu.ua

Ільєнко Сергій Сергійович

кандидат технічних наук, доцент,

доцент кафедри автоматизації та енергоменеджменту

Національний авіаційний університет, Київ, Україна

ORCID ID: 0000-0002-0437-0995

ilyenko.s.s@nau.edu.ua

Яковенко Олеся Леонідівна

старший викладач кафедри кібербезпеки

Національний авіаційний університет, Київ, Україна

ORCID ID: 0000-0003-2998-9767

olesia.yakovenko@npp.nau.edu.ua

Галич Євгенія Олександрівна

студентка кафедри кібербезпеки

Національний авіаційний університет, Київ, Україна

ORCID ID: 0009-0008-2610-1439

7405781@stud.nau.edu.ua

Павленко Владислав Георгійович

студент кафедри кібербезпеки

Національний авіаційний університет, Київ, Україна

ORCID ID: 0009-0008-8072-5525

7328430@stud.nau.edu.ua

ПЕРСПЕКТИВИ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМИ КІБЕРБЕЗПЕКИ

Анотація. Стаття детально розглядає застосування штучного інтелекту (ШІ) у сфері кібербезпеки, підкреслюючи його ключову роль у прогнозуванні та запобіганні кібератакам в умовах зростаючих кіберзагроз. Дослідження показує, що 51% великих організацій вже використовують ШІ для виявлення загроз, а 12% змогли зменшити витрати на кібербезпеку завдяки його впровадженню. Автори пропонують теоретичну модель, що включає етапи сканування системи на наявність вразливостей, оцінку можливих наслідків їх експлуатації, прогнозування атак на основі аналізу історичних даних та поведінкових шаблонів зловмисників, а також розробку комплексних стратегій захисту. Теоретична модель, запропонована в статті, демонструє, як інтеграція ШІ може значно підвищити ефективність систем кібербезпеки, забезпечуючи більш глибоке розуміння загроз та більш ефективні методи їхнього прогнозування та запобігання. Особлива увага приділяється новітнім технологіям ШІ, таким як ChatGPT від OpenAI, які базуються на принципах навчання з підкріпленням із зворотним зв'язком від людини. Практична реалізація цієї моделі з використанням новітніх технологій ШІ, таких як GPT-4, може стати важливим кроком у посиленні захисту інформаційних систем від зростаючих кіберзагроз. Стаття наголошує на необхідності тісної співпраці між людиною та технологією для досягнення оптимальних результатів у протидії кіберзагрозам. Впровадження ШІ вимагає ретельного планування та постійної адаптації стратегій до нових викликів. Таким чином, застосування штучного інтелекту у сфері кібербезпеки відкриває нові можливості для виявлення, прогнозування та запобігання кіберзагрозам.



Ключові слова: штучний інтелект; кібербезпека; прогнозування атак; вразливості; загроза.

ВСТУП

Кібербезпека є однією з найактуальніших та найобширніших проблем, з якою стикається весь Інтернет-простір. Зростаюча кількість і складність кіберзагроз вимагають новаторських підходів до захисту інформаційних систем. Інциденти кібербезпеки, такі як крадіжка даних, атаки на критичну інфраструктуру та кібертероризм, можуть мати серйозні наслідки для економічної стабільності та національної безпеки.

Одним з найперспективніших напрямків у кібербезпеці, безумовно, є застосування штучного інтелекту (ШІ). Технології ШІ, зокрема машинне навчання та глибоке навчання, надають нові можливості для вдосконалення стратегій кіберзахисту. ШІ здатен аналізувати великі обсяги даних, виявляти аномалії, прогнозувати потенційні атаки та автоматизувати реагування на інциденти. ШІ відкриває нові можливості для виявлення кіберзагроз і реагування на них, дозволяючи автоматизувати низку процесів, які раніше вимагали ручного втручання. Зокрема, ШІ можна використовувати для виявлення та оцінки вразливостей системи, прогнозування потенційних кібератак, виявлення шкідливого програмного забезпечення та аномалій мережевого трафіку, а також для автоматизації реагування на інциденти безпеки.

Однією з найбільших переваг ШІ є його здатність навчатися на великих обсягах даних. Це дозволяє ШІ постійно вдосконалювати свої алгоритми і моделі для боротьби з новими типами кіберзагроз. Інструменти на основі ШІ, такі як системи виявлення вторгнень, антивірусне програмне забезпечення та платформи управління інцидентами безпеки, стають все більш важливими для забезпечення кіберзахисту компанії.

Важливість ШІ у сфері кібербезпеки неможливо не оцінити: технологія ШІ надає нові інструменти для протидії кібератакам, роблячи їх більш ефективними та результативними. Однак для того, щоб повністю реалізувати потенціал ШІ, його інтеграція в існуючі системи безпеки повинна бути ретельно продумана, а стратегії повинні постійно адаптуватися до нових викликів.

Постановка проблеми. Науково-дослідний інститут французької компанії Cargemini, яка є однією з провідних у світі в області консалтингу, інформаційних технологій та аутсорсингу, провів глибокий аналіз ролі ШІ в кібербезпеці. Результати цього дослідження підкреслюють критичну значимість інтеграції ШІ у стратегії кіберзахисту для сучасних організацій. Завдяки впровадженню ШІ, організації мають змогу удосконалювати моделі для виявлення нових і потенційно небезпечних загроз. Респонденти вказують, що кіберзлочинці також активно використовують технології ШІ для реалізації атак, що посилює необхідність впровадження передових технологій захисту. Зокрема, 51% великих світових організацій вже інтегрували ШІ для ідентифікації кіберзагроз, 69% вважають, що ШІ є критично важливим для реагування на кібератаки, а 64% відзначають, що ШІ допомагає скоротити час та ресурси, необхідні для виявлення, розслідування та усунення загроз. Додатково, 12% організацій змогли зменшити витрати на кібербезпеку завдяки впровадженню технологій ШІ. Ці дані підкреслюють важливість розуміння того, що ШІ може бути корисним інструментом для захисту інформаційних систем від зростаючих кіберзагроз [1] – [6], [9], [10]. Задача, що постає перед практиками в галузі кібербезпеки, полягає в розробці теоретичної моделі для прогнозування кібератак з використанням технологій ШІ, зокрема на основі



алгоритмів машинного навчання та глибокого навчання. Ця модель повинна включати етапи сканування систем на наявність вразливостей, оцінки ризиків, прогнозування атак та розробки заходів захисту.

Метою статті є створення та впровадження ефективної системи кібербезпеки, яка б використовувала можливості ШІ для автоматизації процесів виявлення та запобігання кібератакам. Реалізація порактичної та теоретичної моделі на базі ШІ включає в себе: розробку алгоритмів для сканування вразливостей та оцінки ризиків; використання історичних даних для прогнозування можливих атак; автоматизацію реагування на інциденти безпеки; інтеграцію розробленої моделі в існуючі системи безпеки організацій.

Таким чином, реалізація цієї мети дозволить значно підвищити ефективність захисту інформаційних систем, знизити ризики кіберзагроз та адаптувати стратегії безпеки до нових викликів у сфері кібербезпеки.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Сучасні технології, такі як ChatGPT, розроблені компанією OpenAI, на основі моделі GPT-3.5, демонструють значний потенціал у сфері кібербезпеки. ChatGPT є потужним інструментом завдяки своїй здатності обробляти і генерувати текст на природній мові, що відкриває нові можливості для автоматизації процесів прогнозування та запобігання кібератакам. Його функціонал базується на принципах навчання з підкріпленням із зворотним зв'язком від людини (Reinforcement Learning with Human Feedback — RLHF), що дозволяє моделі покращувати свою точність і ефективність завдяки постійному вдосконаленню.

У рамках даної роботи для розробки та реалізації моделі прогнозування кібератак буде використано технологію GPT-4, розроблену OpenAI. GPT-4 є останньою версією генеративної передбачувальної моделі, яка є значним вдосконаленням порівняно з попередньою версією GPT-3.5. GPT-4 має значні поліпшення порівняно з попередньою версією, GPT-3.5, зокрема в аспектах розуміння складних запитів, контекстуальної обробки даних та точності відповідей. Ці покращення дуже важливі для кібербезпеки, де точність даних і здатність прогнозувати та аналізувати потенційні загрози є критичними.

Модель складається з кількох ключових етапів, кожен з яких є важливим для забезпечення комплексного підходу до виявлення і запобігання кіберзагрозам.

1. Сканування: На цьому етапі ШІ використовується для сканування системи або мережі на наявність вразливостей. Сканування здійснюється на основі актуальних баз даних вразливостей, які містять інформацію про відомі слабкі місця в програмному забезпеченні або системних конфігураціях. ШІ аналізує дані і визначає потенційні ризики, що можуть бути експлуатовані зловмисниками.

2. Оцінка: Після ідентифікації потенційних вразливостей ШІ проводить оцінку можливих наслідків їхньої експлуатації. Цей процес включає аналіз ступеню шкоди, яку може завдати атака, якщо вразливість буде використана. Оцінка базується на таких факторах, як рівень доступу, що забезпечує вразливість, потенційні збитки для системи та даних, а також можливість подальшого поширення зловмисного впливу. Для цього використовуються метрики Common Vulnerability Scoring System — CVSS (спосіб охопити основні характеристики вразливості та отримати числову оцінку, що відображає її серйозність).



3. Прогнозування атак: Використання ШІ для прогнозування можливих кібератак є одним з ключових аспектів цієї моделі. ШІ аналізує історичні дані про атаки, вивчає поведінкові шаблони зловмисників та використовує алгоритми машинного навчання для ідентифікації потенційних майбутніх атак. Це дозволяє фахівцям з кібербезпеки своєчасно реагувати та запобігати можливим загрозам.

4. Захист: Останній етап моделі включає розробку та впровадження заходів захисту для запобігання кібератакам. ШІ допомагає у формуванні комплексних стратегій захисту, що включають технічні (антивірусні програми, мережеві брандмауери), організаційні (навчання персоналу, розробка політик безпеки) та правові (відповідність законодавству) заходи [5] – [7].

Теоретична модель демонструє, як інтеграція ШІ може значно підвищити ефективність систем кібербезпеки, забезпечуючи більш глибоке розуміння загроз та більш ефективні методи їхнього прогнозування та запобігання.

Практична реалізація теоретичної моделі передбачає створення програмного забезпечення спільними діями людини та ШІ, яке інтегрує різні інструменти для сканування вразливостей, оцінює ризики на основі отриманих даних, прогнозує можливі кібератаки та надає рекомендації щодо їх запобігання. Основна мета демонстрації можливості цієї реалізації — показати можливість забезпечення автоматизації процесів кібербезпеки за допомогою технологій ШІ, знизити ризики кіберзагроз та підвищити загальний рівень захищеності систем.

Важливо наголосити, у випадку реалізації моделі в реальних умовах, втручання людини є обов'язковим. ШІ надає лише ідеї для впровадження. Для кращого результату важлива підтримка фахівців. Щоб почати працювати над реалізацією моделі, людина має навчитися співпрацювати з ШІ. Першочергово, необхідно пояснити нейромережі план дій. Введемо запит до чат-боту, що містить наступну інформацію: «Запропонуй сценарій реалізації теоретичної моделі». Отримано наступну відповідь: Для організації реалізації теоретичної моделі і демонстрації того, як ця модель може допомогти компаніям в підвищенні їхньої кібербезпеки, можна запропонувати такий підхід, який включає розробку пілотного проекту, використання реальних сценаріїв тестування та аналіз ефективності рішення:

1. Розробка пілотного проекту

Вибір компанії-партнера: Співпраця з компанією, яка зацікавлена в тестуванні та інтеграції рішення ШІ для кібербезпеки. Це може бути компанія, яка стикається з високим рівнем кіберзагроз або великим обсягом даних для моніторингу.

Визначення вимог та цілей: Спільне обговорення та встановлення ключових вимог та бізнес-цілей проекту. Це дозволить зосередитись на найбільш актуальних задачах та визначити метрики для оцінки успіху проекту.

2. Впровадження та інтеграція

Розробка індивідуалізованого рішення: Адаптація теоретичної моделі під специфіку та потреби компанії. Це може включати налаштування алгоритмів сканування, оцінки та прогнозування з урахуванням конкретних технологій та інфраструктури компанії.

Інтеграція з існуючими системами: Підключення розробленого рішення до існуючих інформаційних систем компанії для забезпечення збору даних, їх аналізу та відповідного реагування на інциденти безпеки.

3. Тестування та оптимізація



Проведення тестувань: Виконання серії тестів для перевірки ефективності рішення в реальних умовах. Це може включати симуляції кібератак, стрес-тестування системи та аналіз здатності системи вчасно виявляти та реагувати на потенційні загрози.

Аналіз результатів та оптимізація: Оцінка зібраних даних та фідбеку від компанії для вдосконалення рішення. Оптимізація алгоритмів та процесів на основі отриманих результатів.

4. Розгортання та моніторинг

Розгортання рішення: Повноцінне впровадження рішення в операційну діяльність компанії після успішного завершення пілотного проекту та оптимізації.

Налаштування моніторингу та підтримки: Встановлення постійного моніторингу рішення та забезпечення технічної підтримки для оперативного усунення можливих проблем або оновлення системи відповідно до нових кіберзагроз.

Опираючись на відповідь чат-боту можна зрозуміти, що ШІ може дати вектор проекту для реальних компаній. Основні кроки для розробки такого продукту згідно відповідей ШІ є:

1. Вимоги та проектування

Збір вимог:

- Визначення бізнес-вимог та технічних специфікацій;
- Визначення ключових функцій та користувачів системи.

Архітектура системи:

- Вибір архітектурного стилю (наприклад, мікросервіси);
- Проектування модульної структури, що включає компоненти для збору даних, обробки, аналізу та візуалізації.

2. Розробка основних компонентів

Компонент сканування:

- Інтеграція з існуючими інструментами сканування вразливостей (наприклад, Nessus, OpenVAS);
- Розробка інтерфейсу для отримання та обробки даних сканування.
- Компонент оцінки:
- Використання алгоритмів оцінки ризику, таких як Common Vulnerability Scoring System (CVSS);
- Розробка логіки для обчислення потенційної шкоди від виявлених вразливостей.

Компонент прогнозування:

- Використання методів машинного навчання для аналізу історичних даних про кібератаки;
- Розробка моделей для прогнозування можливих атак на основі виявлених патернів.

Компонент захисту:

- Інтеграція з системами управління кібербезпекою для автоматизації реагування (наприклад, налаштування брандмауерів, впровадження патчів);
- Розробка інтерфейсу для взаємодії з користувачами та відображення рекомендацій щодо захисту.

3. Тестування та валідація

Розробка тестових сценаріїв:

- Створення сценаріїв для тестування всіх компонентів системи;
- Виконання функціональних, інтеграційних та навантажувальних тестів.



Валідація моделі:

- Перевірка точності моделей прогнозування на тестових наборах даних;
- Оцінка ефективності рішень щодо захисту в реальних умовах.

4. Розгортання та інтеграція

Інтеграція з існуючою інфраструктурою:

- Інтеграція з системами управління логами, SIEM-системами та іншими інструментами кібербезпеки.

Розгортання:

- Використання контейнерних технологій (наприклад, Docker) для спрощення розгортання та масштабування;
- Налаштування безперервної інтеграції та доставки (CI/CD) для швидкого впровадження оновлень.

5. Моніторинг та підтримка

Моніторинг продуктивності:

- Налаштування системи моніторингу для відстеження продуктивності та виявлення можливих проблем;
- Використання інструментів для аналізу логів і метрик (наприклад, ELK Stack).
- Технічна підтримка:
- Забезпечення технічної підтримки для користувачів системи;
- Регулярне оновлення моделі та системи на основі нових даних про загрози та зворотного зв'язку від користувачів.

Сценарій використання програмного продукту

1. Користувач заходить у систему і запускає сканування мережі.

- Система інтегрується з інструментами сканування і збирає дані про вразливості.

2. Система аналізує зібрані дані і виконує оцінку ризику.

- Використовується модель оцінки, що враховує важливість вразливостей і можливі наслідки їх експлуатації.

3. На основі результатів оцінки система виконує прогнозування можливих атак.

- Модель прогнозування визначає потенційні сценарії атак і надає рекомендації щодо захисту.

4. Система генерує звіт та рекомендації для користувача.

- Користувач отримує детальний звіт про виявлені вразливості, оцінку ризиків і рекомендації щодо заходів захисту.

5. Користувач застосовує рекомендації системи і моніторить результат.

- Система надає можливість автоматизованого впровадження певних заходів захисту і відстежує їх ефективність [6] – [8].

Проте для демонстрації як технології ШІ можуть допомогти у реалізації моделі без доступу до даних реальної компанії, було введено запит до чат-боту з наступним вмістом: «Оскільки автори не мають доступу до інформації реальної компанії, приймаємо рішення про імітацію реалізації практичного застосування». Отримано наступну відповідь: Для реалізації теоретичної моделі з точки зору програмного продукту, необхідно створити інтегроване програмне рішення, яке буде виконувати основні етапи моделі: сканування, оцінку, прогнозування та захист.



Далі на практиці перейдемо до детальному опису кожного етапу теоретичної моделі та її практичної реалізації, включаючи:

1. Інтеграцію зі сканерами (Nmap, Nessus,);
2. Аналіз вразливостей та оцінку ризиків за допомогою метрики CVSS;
3. Використання алгоритмів машинного навчання для прогнозування можливих кібератак;
4. Розробку та впровадження рекомендацій для усунення вразливостей.

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ

Для реалізації програмного забезпечення для сканування та оцінки захищеності веб-додатків, виділення основних типів наявних загроз і оцінки згідно CVSS, будемо використовувати Python як основну мову програмування через її широку підтримку бібліотек для кібербезпеки та інтеграції зі сканерами. Нижче наведено покрокову реалізацію по-блоково:

1. Інтеграція зі сканерами

1.1. Nmap

```
import subprocess
def scan_with_nmap(target):
    command = ["nmap", "-sV", "--script=vulners", target]
    result = subprocess.run(command, capture_output=True, text=True)
    return result.stdout
if __name__ == "__main__":
    target_ip = "192.168.1.1"
    print(scan_with_nmap(target_ip))
```

Функція `scan_with_nmap(target)`: Запускає сканування Nmap для визначеного target (IP-адреса чи URL). Використовує параметри `-sV` для виявлення версій сервісів та `—script=vulners` для використання скриптів Nmap для виявлення вразливостей.

1.2. Nessus

```
import requests
def scan_with_nessus(target, nessus_url, api_key):
    headers = {
        "X-ApiKeys": f"accessKey={api_key}"
    }
    # Запуск сканування
    scan_data = {
        "uuid": "YOUR_SCAN_UUID",
        "settings": {
            "name": "Scan",
            "text_targets": target
        }
    }
    response = requests.post(f"{nessus_url}/scans", json=scan_data, headers=headers)
    return response.json()
if __name__ == "__main__":
    nessus_url = "https://localhost:8834"
    api_key = "YOUR_API_KEY"
    target_ip = "192.168.1.1"
```



```
print(scan_with_nessus(target_ip, nessus_url, api_key))
```

Функція `scan_with_nessus(target, nessus_url, api_key)`: Запускає сканування за допомогою Nessus API. Після аутентифікації з використанням API ключа, функція створює нове сканування для визначеного `target`.

2. *Аналіз вразливостей*

```
def analyze_vulnerabilities(scan_results):  
    vulnerabilities = []  
    for result in scan_results:  
        # Проста фільтрація для прикладу  
        if "vulnerability" in result:  
            vulnerabilities.append(result)  
    return vulnerabilities  
if __name__ == "__main__":  
    sample_results = ["vulnerability1", "info1", "vulnerability2"]  
    print(analyze_vulnerabilities(sample_results))
```

Функція `analyze_vulnerabilities`: Аналізує результати сканування та виділяє виявлені вразливості.

3. *Оцінка згідно CVSS*

```
def calculate_cvss(vulnerability):  
    # Приклад розрахунку  
    base_score = 7.5  
    impact_score = 6.0  
    exploitability_score = 3.9  
    overall_score = (base_score + impact_score + exploitability_score) / 3  
    return overall_score  
if __name__ == "__main__":  
    vulnerability = "Sample vulnerability"  
    print(calculate_cvss(vulnerability))
```

Містить скрипти для аналізу вразливостей та оцінки ризиків згідно CVSS.

4. *Основний файл програми*

```
from scanners.zenmap_scanner import scan_with_nmap  
from scanners.nessus_scanner import scan_with_nessus  
from scanners.openvas_scanner import scan_with_openvas  
from analysis.vulnerability_analysis.py import analyze_vulnerabilities  
from analysis.cvss_calculator import calculate_cvss  
def main():  
    # Для імітації запуску використана довільна IP- адреса  
    target = "192.168.1.1"  
    # Вибір сканера (наприклад, Zenmap)  
    scan_results = scan_with_nmap(target)  
    # Аналіз вразливостей  
    vulnerabilities = analyze_vulnerabilities(scan_results)  
    # Оцінка ризиків згідно CVSS  
    for vulnerability in vulnerabilities:  
        score = calculate_cvss(vulnerability)  
        print(f"Vulnerability: {vulnerability}, CVSS Score: {score}")  
if __name__ == "__main__":  
    main()
```


Основний файл програми, який інтегрує всі компоненти. У ході проведення реалізації програмного забезпечення для сканування та оцінки захищеності веб-додатків необхідно провести імітацію запуску та аналізу. Так як конкретні дані про реальну організацію та комерційні версії програмного забезпечення, які використовуються для сканування вразливостей та їх аналізу відсутні, було запущено фіктивний веб-додаток у віртуальній оболонці чат-боту Chat GPT. Він містив у собі певну вразливість — SQL — ін'єкцію, для можливості перевірки моделі.

Проведемо імітацію запуску та перевірки програми.

```
Запустимо програму для аналізу результатів сканування:  
sh  
python main.py  
Результат роботи програми:  
sql  
Vulnerability: Potential SQL Injection found in parameter 'query', CVSS Score: 8.1666666
```

Рис. 1. Запуск програми ШІ

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Використання ШІ та автоматизованих інструментів для виявлення, оцінки та усунення вразливостей стає все більш актуальним. У ході розгляду питання застосування засобів ШІ в кібербезпеці. Використання ШІ, зокрема технологій машинного навчання та глибокого навчання, відкриває нові можливості для виявлення, прогнозування та запобігання кібератакам. Завдяки здатності аналізувати великі обсяги даних, ШІ може виявляти аномалії, оцінювати вразливості систем, прогнозувати потенційні атаки та автоматизувати реагування на інциденти безпеки. Використано теоретичну модель, що включає етапи сканування, оцінки, прогнозування та захисту, і розглядали її практичну реалізацію. Практична реалізація цієї теоретичної моделі передбачає створення інтегрованого програмного рішення, яке автоматизує основні етапи кібербезпеки:

1. Сканування: Інтеграція зі сканерами (Zenmap, Nessus) дозволяє автоматизувати процес виявлення вразливостей. Використання інструментів сканування забезпечує точне та ефективне виявлення потенційних загроз у системах.

2. Оцінка: Використання метрики Common Vulnerability Scoring System (CVSS) для оцінки вразливостей дозволяє отримати числову оцінку ризику для кожної вразливості. Це допомагає пріоритизувати заходи захисту та ефективно розподілити ресурси для усунення найбільш критичних загроз.

3. Прогнозування: Використання алгоритмів машинного навчання для аналізу історичних даних та прогнозування можливих кібератак дозволяє своєчасно реагувати на потенційні загрози та запобігати їх реалізації.



4. Захист: Розробка та впровадження рекомендацій для усунення вразливостей та підвищення загальної безпеки систем. Інтеграція з існуючими системами управління безпекою дозволяє автоматизувати впровадження заходів захисту.

Однак, у рамках цієї роботи проведено лише імітацію практичної реалізації моделі через відсутність доступу до даних реальних компаній та комерційних версій програмного забезпечення, які використовуються для сканування вразливостей. Імітація дозволила продемонструвати потенційні можливості та ефективність моделі у контрольованому середовищі. Важливо відзначити, що, хоча ШІ та автоматизовані інструменти значно підвищують ефективність кібербезпеки, вони не можуть повністю замінити участь кваліфікованих фахівців. Спеціалісти з кібербезпеки повинні брати активну участь у налаштуванні та адаптації моделі під конкретні потреби організації, забезпечуючи їй відповідність специфічним вимогам і умовам. Дана робота демонструє важливість інтеграції сучасних технологій у процеси кібербезпеки та підкреслює значення комплексного підходу до захисту інформаційних систем у цифровому світі. Успішна інтеграція ШІ в кібербезпеку у поєднанні з досвідом і знаннями фахівців дозволяє створити надійну та адаптивну систему захисту від кіберзагроз, що в свою чергу сприяє більш ефективному реагуванню на кібератаки. Це дозволяє організаціям не лише знижувати ризики, але й підвищувати загальний рівень захищеності, адаптуючи свої стратегії до швидко змінюваного кіберпростору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bhardwaj, A., & Kaushik, K. (2022). Predictive analytics-based cybersecurity framework for cloud infrastructure. *International Journal of Cloud Applications and Computing (IJCAC)*, 12(1), 1–20.
2. Meister, J. A., Akram, R. N., & Markantonakis, K. (2019). Deep learning application in security and privacy—theory and practice: A position paper. In *Information Security Theory and Practice: 12th IFIP WG 11.2 International Conference, WISTP 2018, 12*, 129–144.
3. Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, 19(1), 57–106.
4. Welukar, J. N., & Bajoria, G. P. (2021). Artificial Intelligence in Cyber Security-A Review. *International Journal of Scientific Research in Science and Technology*, 488, 488–491.
5. Das, R., & Sandhane, R. (2021). Artificial intelligence in cyber security. In *Journal of Physics: Conference Series*, 1964(4).
6. Tolido, R., Thieullent, A.-L., van der Linden, G. (n. d.). *Reinventing Cybersecurity with Artificial Intelligence*. https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf
7. Ilyenko, A. V., Galich, E., & Pavlenko, V. (2024). Application of artificial intelligence tools in cybersecurity. *Problems of cybersecurity of information and telecommunication systems (PCSITS): VI international scientific and practical conference*, 21–22.
8. *Artificial intelligence Chat GPT*. (n. d.). <https://chatgpt.com/>
9. Ilyenko, A., Ilyenko, S., Kravchuk, I., & Herasymenko, M. (2022). Prospective directions of traffic analysis and intrusion detection based on neural networks. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, 1(17), 46–56. <https://doi.org/10.28925/2663-4023.2022.17.4656>
10. Ilyenko, A., Ilyenko, S., Diana, K., & Mazur, Y. (2023). Practical approaches to detecting vulnerabilities in information and telecommunication networks. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, 3(19), 96–108. <https://doi.org/10.28925/2663-4023.2023.19.96108>

**Ilyenko Anna**

Candidate of Technical Sciences, Associate Professor,
Head of the Cybersecurity Department
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0001-8565-1117
ilyenko.a.v@nau.edu.ua

Ilyenko Sergii

Candidate of Technical Sciences, Assistant Professor,
Assistant Professor of Automation and Energy Management Department
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0002-0437-0995
ilyenko.s.s@nau.edu.ua

Yakovenko Olesia

Senior Lecturer of the Cybersecurity Department
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0003-2998-9767
olesia.yakovenko@npp.nau.edu.ua

Halych Yevheniia

Student of the Cyber Security Department
National Aviation University, Kyiv, Ukraine
ORCID ID: 0009-0008-2610-1439
7405781@stud.nau.edu.ua

Pavlenko Vladyslav

Student of the Cyber Security Department
National Aviation University, Kyiv, Ukraine
ORCID ID: 0009-0008-8072-5525
7328430@stud.nau.edu.ua

PROSPECTS OF INTEGRATION OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY SYSTEMS

Abstract. The article examines in detail the application of artificial intelligence (AI) in the field of cybersecurity, emphasizing its key role in predicting and preventing cyber attacks in the face of growing cyber threats. The study shows that 51% of large organizations already use AI to detect threats, and 12% were able to reduce cybersecurity costs thanks to its implementation. The authors propose a theoretical model that includes the stages of scanning the system for vulnerabilities, assessing the possible consequences of their exploitation, predicting attacks on based on the analysis of historical data and behavioral patterns of attackers, as well as the development of complex protection strategies. The theoretical model proposed in the article demonstrates how the integration of AI can significantly increase the effectiveness of cyber security systems, providing a deeper understanding of threats and more effective methods of their prediction and prevention. Special attention is paid to the latest AI technologies, such as OpenAI's ChatGPT, which is based on the principles of reinforcement learning with human feedback. The practical implementation of this model using the latest AI technologies, such as GPT-4, can be an important step in strengthening the protection of information systems against growing cyber threats. The article emphasizes the need for close cooperation between people and technology to achieve optimal results in countering cyber threats. Implementation of AI requires careful planning and constant adaptation of strategies to new challenges. Thus, the use of artificial intelligence in the field of cybersecurity opens up new opportunities for detecting, predicting and preventing cyber threats.

Keywords: artificial intelligence; cyber security; prediction of attacks; vulnerabilities; threat.



REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Bhardwaj, A., & Kaushik, K. (2022). Predictive analytics-based cybersecurity framework for cloud infrastructure. *International Journal of Cloud Applications and Computing (IJCAC)*, 12(1), 1–20.
2. Meister, J. A., Akram, R. N., & Markantonakis, K. (2019). Deep learning application in security and privacy—theory and practice: A position paper. In *Information Security Theory and Practice: 12th IFIP WG 11.2 International Conference, WISTP 2018*, 12, 129–144.
3. Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, 19(1), 57–106.
4. Welukar, J. N., & Bajoria, G. P. (2021). Artificial Intelligence in Cyber Security-A Review. *International Journal of Scientific Research in Science and Technology*, 488, 488–491.
5. Das, R., & Sandhane, R. (2021). Artificial intelligence in cyber security. In *Journal of Physics: Conference Series*, 1964(4).
6. Tolido, R., Thieullent, A.-L., van der Linden, G. (n. d.). *Reinventing Cybersecurity with Artificial Intelligence*. https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf
7. Ilyenko, A. V., Galich, E., & Pavlenko, V. (2024). Application of artificial intelligence tools in cybersecurity. *Problems of cybersecurity of information and telecommunication systems (PCSITS): VI international scientific and practical conference*, 21–22.
8. *Artificial intelligence Chat GPT*. (n. d.). <https://chatgpt.com/>
9. Ilyenko, A., Ilyenko, S., Kravchuk, I., & Herasymenko, M. (2022). Prospective directions of traffic analysis and intrusion detection based on neural networks. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, 1(17), 46–56. <https://doi.org/10.28925/2663-4023.2022.17.4656>
10. Ilyenko, A., Ilyenko, S., Diana, K., & Mazur, Y. (2023). Practical approaches to detecting vulnerabilities in information and telecommunication networks. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, 3(19), 96–108. <https://doi.org/10.28925/2663-4023.2023.19.96108>

