Міністерство освіти і науки України
Національний технічний університет «Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента Бочіна Ігоря Ігоровича

академічної групи 125м-22-2

спеціальності 125 Кібербезпека

за освітньо-професійною програмою Кібербезпека

на тему Аналіз та обгрунтування методів штучного інтелекту для задач кібербезпеки

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., професор Корнієнко В.І.			
розділів:				
спеціальний	д.т.н., професор Корнієнко В.І.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викладач Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту *Бочіну Ігорю Ігоровичу* **академічної групи** *125м-22-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

за освітньо-професійною програмою *Кібербезпека*

на тему *Аналіз та обгрунтування методів штучного інтелекту для задач кібербезпеки*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 09.10.23 № 1227-с

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз та систематизація інформації про застосування методів штучного інтелекту у кібербезпеці	01.11.2022
Розділ 2	Впровадження штучного інтелекту. Рекомендації по розробці та впровадженню системи управління ризиками інформаційної безпеки в інформаційній системі	30.11.2022
Розділ 3	Визначення та аналіз показників економічної ефективності моделі управління	07.12.2022

Завдання видано _____ Валерій КОРНІЄНКО
(підпис керівника) (прізвище, ініціали)

Дата видачі: 17.10.2022р.

Дата подання до екзаменаційної комісії: 09.12.2022р.

Прийнято до виконання _____ Ігор БОЧІН
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 78 с., 7 рис., 7 табл., 4 додатки, 94 джерела.

Мета магістерської дипломної роботи: аналіз та обгрунтування використання методів ШІ у сфері кібербезпеки, а також вивчення потенціалу цих методів для підвищення ефективності захисту інформаційних систем від різноманітних кіберзагроз.

Об`єкт дослідження: інформаційні системи, які потребують захисту від кібератак, а предметом є методи ШІ, які застосовуються для забезпечення безпеки цих систем.

У першій частині проаналізована та систематизована інформація про застосування методів штучного інтелекту у кібербезпеці. В результаті була обрана модель аналізу ризиків.

У спеціальній частині була розроблена типова модель загроз, проведений аналіз ризиків та запропоновані методи зі зниження ризиків.

У економічній частині виконано розрахунок вартості запропонованих мір з захисту інформації. Надано оцінку економічної ефективності впровадження системи управління ризиками інформаційної безпеки.

В ході роботи розроблені типова модель загроз та приведений приклад використання ШІ для захисту інформаційних систем, водночас виокремлюючи ключові напрями для подальших досліджень у цій області.

ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ РИЗИКАМИ, МОДЕЛЬ ЗАГРОЗ, АНАЛІЗ РИЗИКІВ, ІНФОРМАЦІЙНИЙ РИЗИК, ШТУЧНИЙ ІНТЕЛЕКТ

THE ABSTRACT

Explanatory note: 78 pages, 7 figures, 7 tables, 4 appendices, 94 sources.

The purpose of the master's thesis: analysis and justification of the use of AI methods in the field of cyber security, as well as studying the potential of these methods to increase the effectiveness of protecting information systems from various cyber threats.

The object of research: information systems that need protection from cyber attacks, and the subject is AI methods that are used to ensure the security of these systems.

In the first part, information on the use of artificial intelligence methods in cyber security is analyzed and systematized. As a result, a risk analysis model was chosen.

In the special part, a typical threat model was developed, risk analysis was carried out, and risk reduction methods were proposed.

In the economic part, the cost of the proposed information protection measures was calculated. An assessment of the economic efficiency of the implementation of the information security risk management system is provided.

In the course of the work, a typical threat model was developed and an example of the use of AI for the protection of information systems was given, while at the same time identifying key areas for further research in this area.

INFORMATION SECURITY, RISK MANAGEMENT, THREAT MODEL, RISK ANALYSIS, INFORMATION RISK, ARTIFICIAL INTELLIGENCE

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІБ – інформаційна безпека;

ІТ – інформаційні технології;

ПЗ – програмне забезпечення;

IoT - Internet of Things (Інтернет речей);

ШІ – штучний інтелект;

SIEM - Системи виявлення та реагування на інциденти

КС – Комп’ютерні системи

ЗМІСТ

ВСТУП

У сучасному цифровому світі, де зростання обсягу даних та залежність від інформаційних технологій стрімко збільшується, питання кібербезпеки набуває особливої актуальності. Завдяки цьому, виникає вагома необхідність у розробці ефективних методів захисту інформаційних систем. Серед найперспективніших напрямків у цій сфері виділяються методи штучного інтелекту (ШІ), які відкривають нові можливості для вдосконалення механізмів кібербезпеки та реагування на кіберзагрози.

Метою даної роботи є аналіз та обгрунтування використання методів ШІ у сфері кібербезпеки, а також вивчення потенціалу цих методів для підвищення ефективності захисту інформаційних систем від різноманітних кіберзагроз. Об'єктом дослідження виступають інформаційні системи, які потребують захисту від кібератак, а предметом є методи ШІ, які застосовуються для забезпечення безпеки цих систем.

Дослідження базується на застосуванні широкого спектру методів, включаючи аналітичний підхід до вивчення існуючих літературних джерел, синтез інформації для виявлення ключових аспектів використання ШІ у кібербезпеці, а також емпіричний аналіз сучасних кейсів застосування ШІ в цій сфері.

Наукова новизна роботи полягає у комплексному аналізі та систематизації інформації про застосування методів штучного інтелекту у кібербезпеці, що включає оцінку ефективності цих методів, аналіз потенційних ризиків та переваг, а також вивчення передових практик і тенденцій у цій галузі. Таким чином, робота сприяє поглибленому розумінню важливості та можливостей використання ШІ для захисту інформаційних систем, водночас виокремлюючи ключові напрями для подальших досліджень у цій області.

РОЗДІЛ 1
СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Кібербезпека, класифікація і інструменти провдення кібератак

Кібербезпека в сучасному цифровому світі є однією з найважливіших тем, яка постійно розвивається і змінюється. Вона охоплює ряд методів та практик, спрямованих на захист систем, мереж і програм від цифрових атак. Ці атаки зазвичай мають на меті доступ, зміну або знищення чутливих даних; вимагання грошей від користувачів; або перешкоджання нормальному бізнес-процесам.

Уявлення про кібербезпеку постійно розвивається, оскільки нові технології, такі як хмарні обчислення, штучний інтелект та Інтернет речей, створюють нові можливості для кіберзлочинців. Тому, незважаючи на постійне вдосконалення заходів безпеки, кіберзагрози продовжують бути серйозною проблемою для організацій та індивідів. На рисунку 1.1 представлена статистика по кібератакам за січень-лютий 2023 року від Державної служби спеціального зв'язку та захисту інформації України.

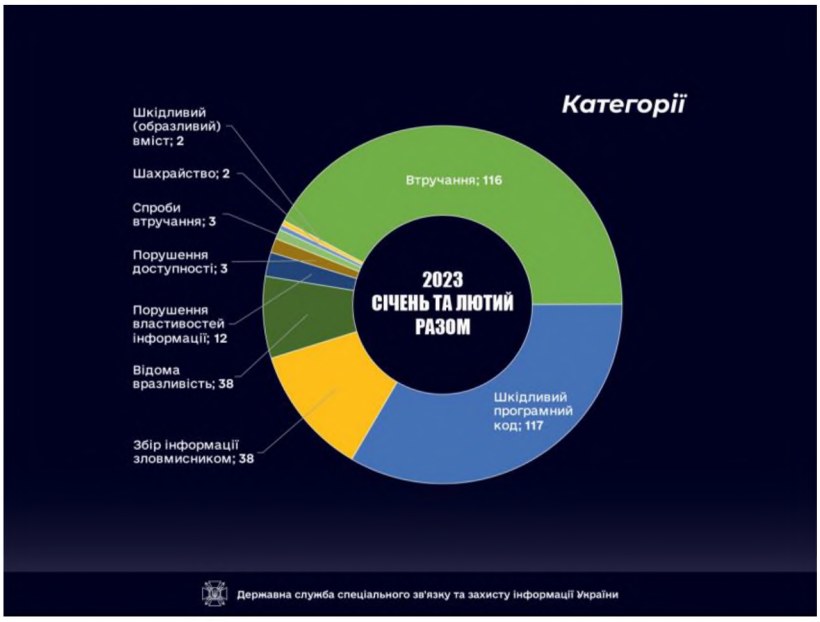

Рисунок 1.1 — Статистика кібератак за січень-лютий 2023 року

Кіберзагрози можуть приходити з різних джерел, включаючи зовнішніх хакерів, внутрішніх акторів, державні органи та навіть випадкові або несвідомі

дії співробітників. Види кібератак також дуже різноманітні. Вони включають в себе, але не обмежуються, вірусами та шкідливим програмним забезпеченням, фішинговими атаками, атаками на відмову в обслуговуванні (DoS), атаками "людини посередині", а також передовими постійними загрозами (APT).

Віруси та шкідливе програмне забезпечення часто розповсюджуються через інфіковані веб-сайти, електронну пошту або навіть через USB-пристрої. Ці програми можуть пошкодити систему, красти чутливі дані або навіть взяти під контроль заражені комп'ютери. Фішингові атаки використовують обманні електронні листи або веб-сайти, щоб змусити користувачів відкрити свої особисті дані, такі як паролі або номери кредитних карток.

Атаки на відмову в обслуговуванні мають на меті заблокувати доступ до ресурсів, змушуючи систему або мережу перевантажитися запитами. Такі атаки можуть бути особливо шкідливими для бізнесу, оскільки вони перешкоджають нормальній роботі компанії. Атаки "людини посередині" відбуваються, коли хакер перехоплює комунікацію між двома сторонами, щоб красти або маніпулювати даними.

Передові постійні загрози є складними та цілеспрямованими атаками, зазвичай виконуваними організованими групами, які цілять великі корпорації або державні установи. Ці атаки характеризуються тривалим проникненням і стеженням, що робить їх особливо небезпечними.

Для протидії цим загрозам, організації та індивіди повинні впроваджувати ряд заходів безпеки. Це включає в себе використання антивірусного програмного забезпечення, фаєрволів, систем виявлення та запобігання вторгнень, а також регулярне оновлення програмного забезпечення і систем. Освіта та навчання співробітників також відіграють ключову роль, оскільки багато атак використовують соціальну інженерію та фішинг.

Кібербезпека також вимагає комплексного підходу, який включає не тільки технічні заходи, але й організаційні. Це означає створення ефективних

політик та процедур, а також забезпечення, щоб усі співробітники були свідомі своєї ролі у захисті інформації. Важливою складовою ефективної кібербезпеки є регулярна оцінка ризиків та аудит безпеки.

Останнім часом все більше уваги приділяється не тільки захисту даних, але й їх відновленню після кібератак. Це означає, що організації повинні мати ефективні плани на випадок порушення безпеки, включаючи стратегії відновлення даних та відновлення систем.

Кібератака – це зловмисна діяльність, спрямована на проникнення, порушення, зміну або знищення інформаційних систем, мереж або цифрових ресурсів. Ця діяльність може мати різноманітні форми, включаючи, але не обмежуючись, шпигунськими програмами, вірусами, черв'яками, троянськими конями, фішингом, DDoS-атаками та іншими методами кіберзлочинності. Кібератаки можуть бути спрямовані на фізичні або віртуальні активи і часто призводять до значних фінансових втрат, порушення конфіденційності, недоступності сервісів та інших негативних наслідків.

Класифікація кібератак

1. Віруси та черв'яки: Програми, що самостійно розмножуються, поширюючись між системами та мережами. Віруси зазвичай прикріплюються до інших файлів, тоді як черв'яки розповсюджуються самостійно.
2. Троянські коні: Шкідливі програми, які маскуються під легітимний софт, даючи зловмисникам доступ до системи.
3. Фішинг та соціальна інженерія: Методи, що базуються на обмані користувачів для отримання конфіденційної інформації, такої як паролі та банківські дані.
4. DDoS-атаки (розподілені відмови в обслуговуванні): Направлені на перевантаження мережевих ресурсів, що робить веб-сайти та сервіси недоступними для користувачів.
5. Шпигунські програми та рекламне ПЗ: Програми, що стежать за діяльністю користувачів або нав'язують небажану рекламу.

6. Криптовалютний майнінг та криптоджекінг: Використання чужих ресурсів для майнінгу криптовалют без відома власника.
7. APT (розширені тривалі погрози): Комплексні та багатоетапні атаки, часто спрямовані на державні або великі корпоративні мережі, з метою довготривалого непомітного проникнення.
8. Man-in-the-Middle (MitM) атаки: Інтерцепція та модифікація комунікацій між двома сторонами без їх відома.
9. Експлоіти та нульові дні: Використання вразливостей у програмному забезпеченні, часто до того, як розробник встигне їх виправити.
10. Ransomware (Вимагальницьке ПЗ): Шкідливі програми, що блокують доступ до системи або файлів, вимагаючи викуп за їх розблокування.

Загрози від кібератак

Кібератаки створюють широкий спектр загроз, включаючи:

- Фінансові збитки: Втрати від шахрайства, крадіжки даних, втрати бізнесу через простої.
- Втрата конфіденційності: Несанкціоноване розголошення особистих, корпоративних чи державних даних.
- Порушення цілісності даних: Зміна або знищення важливої інформації.
- Загроза репутації: Підрив довіри клієнтів та партнерів через витоки даних чи інші інциденти.

Вплив кібератак на різні сектори

Кібератаки можуть мати різний вплив в залежності від цільового сектору. Наприклад:

- Фінансовий сектор: Атаки на банки та фінансові інститути можуть призвести до великих фінансових втрат, крадіжки кредитної інформації та порушення банківських операцій.
- Охорона здоров'я: Цільові атаки на медичні установи можуть призвести до втрати важливих медичних записів, порушення конфіденційності пацієнтів та навіть перерви в наданні життєво важливих медичних послуг.

- Урядові установи: Атаки на державні структури можуть мати наслідки для національної безпеки, втрату конфіденційної інформації та порушення громадських послуг.
- Освіта та дослідження: Університети та дослідницькі центри часто стають мішенями кібератак через великий обсяг інноваційної інтелектуальної власності.

Захист від кібератак

Захист від кібератак включає комплексний підхід, який поєднує технологічні, організаційні та освітні стратегії:

- Технологічні засоби: Включають антивірусне програмне забезпечення, фаєрволи, системи виявлення та запобігання вторгнень, шифрування даних та регулярні оновлення систем безпеки.
- Організаційні стратегії: Розробка та впровадження політик безпеки, регулярні аудити безпеки, розробка планів реагування на інциденти.
- Освіта та навчання персоналу: Освіта працівників щодо кращих практик кібергігієни, включаючи безпечне користування електронною поштою, створення сильних паролів та усвідомлення загроз фішингу.

Тенденції та майбутнє кібербезпеки

Зростання Інтернету речей (IoT), штучного інтелекту (AI) та хмарних технологій відкриває нові горизонти для кібербезпеки. Ці технології можуть не тільки створювати нові вектори атак, але й пропонувати інноваційні рішення для захисту. Наприклад, AI може бути використаний для автоматизації виявлення загроз та реагування на них, а IoT вимагає нових підходів до безпеки пристроїв та мереж.

У світі кібербезпеки, розуміння інструментів і засобів, які використовуються для проведення кібератак, є ключовим для розробки ефективних захисних стратегій. Кіберзлочинці використовують широкий спектр інструментів - від простих скриптів до складних програмних комплексів - для втручання в роботу комп'ютерних систем, крадіжки даних або виконання інших зловмисних дій.

Мережеві скануючі інструменти

Мережеві сканери, такі як Nmap або Wireshark, використовуються для виявлення відкритих портів, служб та потенційних вразливостей в цільових системах. Ці інструменти дозволяють зловмисникам зібрати інформацію про мережеву структуру, операційні системи та встановлене програмне забезпечення, що є критичним етапом підготовки більшості кібератак.

Експлоіти та використання вразливостей

Експлоіти - це спеціально розроблені програми або коди, призначені для використання вразливостей у програмному забезпеченні. Існують бази даних, такі як Metasploit, що містять велику кількість готових до використання експлоітів. Ці інструменти дозволяють зловмисникам проникнути в системи через відомі вразливості, часто без відома користувача або адміністратора.

Фішингові інструменти

Фішинг - це метод соціальної інженерії, який використовує обман для отримання конфіденційної інформації, такої як логіни та паролі. Інструменти для фішингу включають програми для створення підроблених веб-сторінок, електронних листів, що імітують легітимні запити, та інструменти для збору даних.

Інструменти для встановлення зворотного з'єднання

Зворотні шелли та троянські програми використовуються для встановлення зворотного з'єднання з цільовою системою. Це дозволяє зловмисникам віддалено керувати комп'ютером жертви, проводити подальші атаки або красти дані. Популярними інструментами є програми на кшталт Metasploit, які містять функції для створення та управління зворотними шеллами.

Розподілені системи для DDoS-атак

Для проведення DDoS-атак, зловмисники використовують ботнети - мережі інфікованих комп'ютерів, які можуть бути активовані для одночасного надсилання запитів до цільового сервера. Це призводить до перевантаження та відмови в обслуговуванні. Інструменти для створення та управління

ботнетами, такі як Mirai, стають все більш доступними і простими у використанні.

Інструменти для криптоджекінгу

Криптоджекінг - це процес незаконного використання чужих комп'ютерних ресурсів для майнінгу криптовалют. Інструменти для криптоджекінгу зазвичай включають шкідливе ПЗ, яке може бути приховано в легітимних програмах або розповсюджене через вразливості в веб-додатках.

Аналізатори трафіку та інтерцептори даних

Інструменти для аналізу мережевого трафіку, такі як Wireshark, та інтерцептори даних, такі як Burp Suite, використовуються для перехоплення та аналізу даних, що передаються через мережу. Це дозволяє зловмисникам виявити слабкі місця в мережевій безпеці, перехоплювати конфіденційну інформацію та маніпулювати даними.

Шкідливе ПЗ та віруси

Шкідливе програмне забезпечення, включаючи віруси, троянські програми, шпигунські та вимагальницькі програми, є основними інструментами для проведення кібератак. Ці програми можуть бути спроектовані для крадіжки даних, шпигунства, вимагання коштів або навіть для знищення даних.

Інструменти для Атак на Мобільні Пристрої

З розвитком мобільних технологій, кіберзлочинці все частіше використовують спеціалізоване шкідливе ПЗ для атак на мобільні пристрої. Це включає програми для крадіжки даних зі смартфонів, встановлення троянських програм та шпигунських додатків, які можуть відстежувати розташування користувача, перехоплювати дзвінки та повідомлення.

Інструменти для соціальної інженерії

Соціальна інженерія використовує психологічні прийоми для маніпулювання людьми, щоб вони виконували дії або розкривали конфіденційну інформацію. Інструменти для соціальної інженерії можуть

включати складні імітаційні сценарії, фальшиві телефонні дзвінки, електронні листи та повідомлення.

Хмарні інструменти для кібератак

Зі зростанням популярності хмарних технологій, зловмисники також адаптували свої стратегії для атак на хмарні сервіси та інфраструктури. Це може включати використання скомпрометованих облікових записів для викрадення даних з хмарних сховищ, атаки на конфігурацію хмарних сервісів та експлуатацію вразливостей у хмарних застосунках.

Інструменти для атак на промислові системи

Цільові атаки на промислові контрольні системи та інфраструктуру критично важливих об'єктів, таких як електростанції або водопостачання, вимагають спеціалізованих інструментів. Це може включати шкідливе ПЗ, спроектоване для переривання роботи промислових контрольних систем, таких як Stuxnet.

Анонімізуючі інструменти

Для приховування своєї діяльності та уникнення виявлення зловмисники часто використовують анонімізуючі інструменти, такі як VPN, проксі-сервери та мережу Tor. Ці інструменти дозволяють здійснювати атаки, ускладнюючи процес визначення реального місцезнаходження та ідентифікації зловмисників.

Автоматизовані інструменти для атак

Автоматизація грає ключову роль у проведенні кібератак. Інструменти для автоматичного сканування мереж, пошуку вразливостей та розгортання експлоітів значно підвищують ефективність та швидкість проведення атак. Це також включає використання скриптів та ботів для автоматизації рутинних завдань.

Інструменти для перехоплення даних

Зловмисники часто використовують інструменти для перехоплення даних, що передаються по нешифрованих або погано захищених каналах

зв'язку. Це включає інструменти для "sniffing" даних, такі як перехоплення паролів, кредитної інформації та інших важливих даних.

Інструменти для створення та розповсюдження шкідливого ПЗ

Розробка та розповсюдження шкідливого ПЗ є основною складовою більшості кібератак. Це включає використання інструментів для створення вірусів, троянських коней, шпигунських програм, а також стратегій для їх розповсюдження, таких як використання електронної пошти, фішингових сайтів або експлойт-кітів.

1.2 Сучасні методи забезпечення кібербезпеки

У контексті постійно зростаючої загрози кібератак, розробка та впровадження ефективних методів запобігання стає критично важливим. Сучасні методи запобігання кібератакам об'єднують технологічні, організаційні та освітні підходи для створення комплексної системи безпеки.

Розробка та впровадження політик безпеки

Фундаментальним кроком у запобіганні кібератак є розробка чітких політик безпеки. Це включає визначення стандартів, процедур та рекомендацій, які регулюють управління даними, доступ до систем, використання пристроїв та мережевих ресурсів. Ефективні політики безпеки мають бути доповнені регулярними перевірками та оновленнями, щоб відповідати новим загрозам.

Застосування сучасних технологій безпеки

Сучасні технології безпеки, включаючи антивірусне програмне забезпечення, фаєрволи, системи виявлення та запобігання вторгнень (IDS/IPS), шифрування даних та аутентифікація на основі багатьох факторів, є ключовими елементами стратегії запобігання кібератакам. Ці технології дозволяють виявляти, блокувати та повідомляти про спроби несанкціонованого доступу або інші підозрілі дії.

Регулярне оновлення та патчування

Регулярне оновлення та патчування програмного забезпечення та операційних систем є критично важливим для усунення вразливостей, які можуть бути використані зловмисниками. Організації мають встановлювати оновлення безпеки якнайшвидше після їх випуску.

Освіта та навчання персоналу

Освічений персонал може відігравати ключову роль у запобіганні кібератак. Навчання співробітників з кібергігієни, включаючи безпечне користування електронною поштою, створення сильних паролів, розпізнавання спроб фішингу та безпечне використання мобільних пристроїв та публічних мереж, є важливою частиною стратегії безпеки.

Захист фізичної інфраструктури

Фізичний захист інфраструктури, включаючи захист серверних приміщень, контроль доступу та моніторинг, є важливою складовою запобігання несанкціонованому доступу до критичних систем і даних.

Шифрування даних

Шифрування даних, як в процесі зберігання, так і передачі, є важливим засобом захисту конфіденційної інформації. Використання сучасних алгоритмів шифрування та ключових систем забезпечує захист даних від несанкціонованого доступу або крадіжки.

Використання облікових записів з обмеженими правами

Обмеження прав доступу користувачів та адміністраторів до мінімуму необхідного для виконання їхніх обов'язків допомагає запобігти можливості поширення шкідливих програм та доступу до конфіденційних даних.

Моніторинг та аналіз логів

Регулярний моніторинг та аналіз логів систем та мережевого трафіку дозволяють виявляти нестандартну поведінку, яка може вказувати на кібератаку. Це включає аналіз логів серверів, мережевого обладнання та систем безпеки.

Розробка плану реагування на інциденти

Маючи заздалегідь підготовлений план реагування на інциденти, організації можуть швидко та ефективно відновити роботу після атаки, зменшуючи потенційні збитки та відновлюючи довіру клієнтів.

Розширений аналіз загроз

Застосування технологій штучного інтелекту та машинного навчання для аналізу загроз дозволяє виявляти складні кібератаки, включаючи раніше невідомі варіанти шкідливого ПЗ та нові методи атак. Системи, здатні до самонавчання, можуть адаптуватися до постійно змінюваних стратегій кіберзлочинців.

Інтеграція систем безпеки

Інтеграція різних систем безпеки, таких як антивіруси, фаєрволи, IDS/IPS, та системи управління подіями та інформацією безпеки (SIEM), забезпечує комплексний підхід до захисту. Це дозволяє швидше реагувати на інциденти, обмінюватися інформацією про загрози та координувати заходи щодо їх нейтралізації.

Використання хмарних рішень для безпеки

Хмарні рішення для кібербезпеки пропонують гнучкість, масштабованість та оновлення в реальному часі. Вони можуть включати хмарні антивіруси, фаєрволи як послугу, хмарні системи виявлення вторгнень та управління ідентичністю.

Захист інфраструктури інтернету речей (IoT)

З огляду на зростаючу популярність IoT-пристроїв, важливо впроваджувати спеціалізовані заходи безпеки, включаючи шифрування, сильну аутентифікацію та регулярні оновлення ПЗ для захисту цих пристроїв від кібератак.

Використання блокчейну для забезпечення безпеки

Блокчейн пропонує нові можливості для забезпечення безпеки, включаючи створення незмінних та прозорих журналів для моніторингу та аудиту, що ускладнює несанкціоноване втручання або маніпулювання даними.

Адаптивна безпека

Адаптивна безпека включає в себе використання гнучких заходів безпеки, які можуть адаптуватися до зміни середовища та нових типів загроз. Це означає постійний аналіз ризиків, оцінку вразливостей та адаптацію політик безпеки.

Проактивне тестування безпеки

Регулярні аудити безпеки та пенетраційні тести допомагають ідентифікувати та виправляти потенційні вразливості перед тим, як їх можуть використати зловмисники. Це включає тестування веб-додатків, мережевої інфраструктури та інших критичних компонентів.

Стратегічне планування безпеки

Довгострокове стратегічне планування, яке враховує потенційні майбутні ризики та використовує передбачувальний аналіз, є важливою частиною запобігання кібератакам. Це включає планування інвестицій у безпеку, розвиток персоналу та вдосконалення технологій.

Залучення зовнішніх експертів

Співпраця з зовнішніми консультантами та експертами з кібербезпеки може допомогти організаціям оцінити їх поточний рівень безпеки, ідентифікувати слабкі місця та розробити більш ефективні стратегії захисту.

Створення культури безпеки

Побудова культури безпеки в організації, де кожен працівник усвідомлює свою роль у захисті інформації та активно дотримується політик безпеки, є ключовим фактором успіху у запобіганні кібератак.

Програмне забезпечення для виявлення та реагування на кібератаки є невід'ємною частиною стратегії кібербезпеки будь-якої організації. Ці системи використовують різні механіки та алгоритми для ідентифікації потенційних загроз та своєчасного реагування на них.

Механізми виявлення загроз

1. Підписи шкідливого ПЗ: Традиційно, антивірусне програмне забезпечення використовує бази даних з підписами відомого шкідливого ПЗ для їх виявлення. Це включає сканування файлів на наявність відомих підписів вірусів, троянів та іншого шкідливого коду.
2. Евристичний аналіз: Евристичні методи використовуються для виявлення раніше невідомих або модифікованих варіантів шкідливого ПЗ. Ці методи базуються на аналізі поведінки програм та виявленні підозрілих патернів або характеристик.
3. Аналіз поведінки: Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) аналізують мережевий трафік та активність системи для ідентифікації підозрілих змін або аномалій, які можуть свідчити про кібератаку.

4. Машинне навчання та штучний інтелект: Сучасні рішення все частіше включають компоненти штучного інтелекту та машинного навчання для виявлення складних атак, які не можуть бути ідентифіковані стандартними методами. Ці системи постійно навчаються на нових даних, покращуючи свою здатність до виявлення загроз.

Реагування на загрози

1. Автоматизоване втручання: При виявленні підозрілої діяльності, системи можуть автоматично вживати заходів для блокування атаки. Це може включати відключення інфікованих пристроїв від мережі, видалення або карантин шкідливого ПЗ.
2. Повідомлення та логування: Системи забезпечують детальне логування подій та повідомлення про виявлені інциденти. Це дозволяє аналітикам безпеки оцінити ситуацію та розробити план реагування.
3. Інтеграція з іншими системами безпеки: Інтеграція з системами управління інцидентами та іншими інструментами безпеки забезпечує координоване та ефективне реагування на інциденти.
4. Аналіз після інциденту: Після виявлення та реагування на інцидент, важливо провести глибокий аналіз, щоб визначити причини та знайти способи запобігання подібним атакам у майбутньому.

Адаптація до змінюваних загроз

Системи безпеки постійно адаптуються до змінюваних патернів загроз. Це включає оновлення баз даних підписів, вдосконалення алгоритмів машинного навчання та оновлення евристичних правил для кращого виявлення нових та складних видів атак.

Превентивні заходи

Сучасні рішення забезпечують не тільки виявлення та реагування на загрози, але й превентивні заходи. Це може включати аналіз вразливостей, прогнозування можливих векторів атак та рекомендації щодо зміцнення безпеки.

Покращення швидкості та точності виявлення

Сучасні системи безпеки фокусуються на зменшенні часу між проникненням зловмисника та його виявленням. Це включає вдосконалення алгоритмів для швидшого аналізу даних та точного виявлення аномалій, забезпечуючи швидке реагування на інциденти.

Автоматизація процесів безпеки

Автоматизація є ключовим аспектом сучасних систем безпеки, дозволяючи зменшити навантаження на фахівців та підвищити ефективність виявлення та реагування на загрози. Це може включати автоматичне блокування атак, самостійне виправлення вразливостей та автоматизовані повідомлення.

Контекстуалізація загроз

Розуміння контексту загрози є важливим для ефективного реагування. Системи виявлення та реагування на інциденти (SIEM) інтегрують дані з різних джерел, забезпечуючи повну картину загрози та дозволяючи зрозуміти, як краще реагувати.

Аналіз ризиків та вразливостей

Програмне забезпечення для виявлення кібератак часто включає інструменти для оцінки ризиків та вразливостей. Це дозволяє організаціям прогнозувати потенційні загрози та вживати проактивних заходів для їх запобігання.

Інтелектуальний аналіз загроз

Системи безпеки використовують інтелектуальний аналіз для ідентифікації складних шаблонів поведінки, які можуть вказувати на розширені тривалі погрози (APT) та інші складні атаки. Це включає вивчення міжмережевих взаємодій та користувацької поведінки для виявлення незвичайних дій.

Постійне оновлення та навчання

Ефективність систем безпеки залежить від їх здатності адаптуватися до нових загроз. Це включає регулярне оновлення баз даних загроз, алгоритмів

машинного навчання та правил поведінки, щоб врахувати змінні тактики та техніки зловмисників.

Співпраця та обмін інформацією

Сучасне програмне забезпечення для безпеки часто включає можливість співпраці та обміну інформацією між організаціями та приватним сектором. Це дозволяє ширше розуміння загроз та краще використання колективного інтелекту для боротьби з кіберзлочинністю.

Аналітика великих даних

Застосування аналітики великих даних дозволяє системам безпеки обробляти величезні обсяги інформації, виявляючи складні зв'язки та шаблони, які можуть вказувати на потенційні загрози або вразливості.

Використання хмарних технологій

Використання хмарних технологій у системах безпеки дозволяє використовувати гнучкість, масштабованість та постійні оновлення для захисту від найновіших загроз. Хмарні рішення також можуть надавати розширені можливості аналізу та обміну даними.

1.3 Використання методів штучного інтелекту для забезпечення кібербезпеки

У сучасному світі, де обсяги даних постійно зростають, а кіберзагрози стають все більш складними та різноманітними, використання штучного інтелекту (ШІ) для забезпечення кібербезпеки набуває особливого значення. ШІ може допомогти виявляти та протидіяти кібератакам шляхом аналізу великих обсягів даних, виявлення аномалій та автоматизації реагування на загрози.

Штучний інтелект (ШІ) — це інтелект машин або програмного забезпечення на відміну від інтелекту людей або тварин. Це галузь інформатики, яка розробляє та вивчає інтелектуальні машини. «ШІ» також може стосуватися самих машин.

Технологія ШІ широко використовується в промисловості, уряді та науці. Деякі популярні програми: розширені веб-пошукові системи (наприклад, Google Search), системи рекомендацій (використовуються YouTube, Amazon і Netflix), розуміння людської мови (такі як Siri та Alexa), безпілотні автомобілі (наприклад, Waymo).), генеративні або творчі інструменти (ChatGPT і AI art), а також змагання на найвищому рівні в стратегічних іграх (таких як шахи та го).[1]

Штучний інтелект був заснований як академічна дисципліна в 1956 році.[2] Сфера пройшла через кілька циклів оптимізму[3][4], а потім розчарування та втрати фінансування,[5][6] але після 2012 року, коли глибоке навчання перевершило всі попередні технології ШІ,[7] відбулося значне зростання фінансування та відсотки.

Різні підгалузі досліджень ШІ зосереджені навколо конкретних цілей і використання конкретних інструментів. Традиційні цілі досліджень штучного інтелекту включають міркування, представлення знань, планування, навчання, обробку природної мови, сприйняття та підтримку робототехніки.[a] Загальний інтелект (здатність вирішувати довільну проблему) є однією з довгострокових цілей галузі. [8] Щоб вирішити ці проблеми, дослідники ШІ

адаптували та інтегрували широкий спектр методів вирішення проблем, включаючи пошукову та математичну оптимізацію, формальну логіку, штучні нейронні мережі та методи, засновані на статистиці, дослідженні операцій та економіці.[b] ШІ також спирається на психологію, лінгвістику, філософію, неврологію та багато інших галузей.[9]

Загальна проблема моделювання (або створення) інтелекту була розбита на підпроблеми. Вони складаються з певних рис або можливостей, які дослідники очікують від інтелектуальної системи. Особливості, описані нижче, привернули найбільшу увагу та охоплюють сферу досліджень ШІ.[a]

Міркування, вирішення задач

Ранні дослідники розробили алгоритми, які імітували покрокові міркування, які люди використовують, коли розв'язують головоломки або роблять логічні висновки.[10] До кінця 1980-х і 1990-х років були розроблені методи роботи з невизначеною або неповною інформацією, використовуючи концепції ймовірності та економіки.[11]

Багато з цих алгоритмів є недостатніми для вирішення великих проблем міркування, тому що вони відчувають «комбінаторний вибух»: вони стали експоненціально повільнішими, оскільки проблеми ставали більшими.[12] Навіть люди рідко використовують покрокову дедукцію, яку могли моделювати ранні дослідження ШІ. Вони вирішують більшість своїх проблем, використовуючи швидкі, інтуїтивні судження.[13] Точне й ефективне міркування — невирішена проблема.

Репрезентація знань

Представлення знань та інженерія знань[14] дозволяють програмам штучного інтелекту розумно відповідати на запитання та робити висновки щодо фактів реального світу. Формальні представлення знань використовуються в індексуванні та пошуку на основі вмісту, [15] інтерпретації сцен, [16] підтримці клінічних рішень, [17] виявленні знань (видобуток «цікавих» і дієвих висновків із великих баз даних) [18] та інших областях [19]

База знань — це сукупність знань, представлених у формі, яка може використовуватися програмою. Онтологія — це набір об'єктів, відношень, понять і властивостей, які використовуються певною областю знань.[20] Бази знань мають представляти такі речі, як: об'єкти, властивості, категорії та зв'язки між об'єктами; [21] ситуації, події, стани та час; [22] причини та наслідки; [23] знання про знання (те, що ми знаємо про те, що знають інші люди); [24] міркування за замовчуванням (речі, які люди вважають істинними, доки не будуть сказане по-іншому і залишатиметься правдивим навіть тоді, коли інші факти змінюються); [25] і багато інших аспектів і сфер знання.

Серед найскладніших проблем у КР є: широта здорового глузду (набір атомарних фактів, які знає пересічна людина, є величезним); [26] і підсимволічна форма здорового глузду (багато з того, що люди знають, не представлені як «факти» або «твердження», які вони можуть висловити усно).[13]

Отримання знань є складною проблемою отримання знань для додатків штучного інтелекту. [c] Сучасний штучний інтелект збирає знання, «перебираючи» Інтернет (включно з Вікіпедією). Самі знання були зібрані волонтерами та професіоналами, які опублікували інформацію (які могли або не могли погодитися надати свою роботу компаніям зі штучним інтелектом).[29] Ця технологія «натовпу» не гарантує, що знання є правильними чи надійними. Знання великих мовних моделей (таких як ChatGPT) є дуже ненадійними — вони породжують дезінформацію та неправдиві відомості (відомі як «галюцинації»). Надання точних знань для цих сучасних програм штучного інтелекту є невирішеною проблемою.

Планування та прийняття рішень

«Агент» — це все, що сприймає та виконує дії у світі. Раціональний агент має цілі або переваги та вживає заходів, щоб їх реалізувати.[d][30] В автоматизованому плануванні агент має конкретну ціль.[31] У автоматизованому прийнятті рішень агент має переваги – є ситуації, в яких він хотів би опинитися, і деяких ситуацій, яких він намагається уникати. Агент,

який приймає рішення, присвоює кожній ситуації число (так званий «корисність»), яке вимірює, наскільки агент віддає перевагу цій ситуації. Для кожної можливої дії він може обчислити «очікувану корисність»: корисність усіх можливих результатів дії, зважених за ймовірністю того, що результат відбудеться. Потім він може вибрати дію з максимальною очікуваною корисністю.[32]

У класичному плануванні агент точно знає, яким буде ефект будь-якої дії.[33] Однак у більшості проблем реального світу агент може бути невпевнений щодо ситуації, в якій він перебуває (вона «невідома» або «недоступна»), і він може не знати напевно, що станеться після кожної можливої дії (це не «детермінований»). Він повинен вибрати дію, зробивши ймовірнісне припущення, а потім переоцінити ситуацію, щоб побачити, чи дія спрацювала.[34] У деяких проблемах уподобання агента можуть бути невизначеними, особливо якщо задіяні інші агенти або люди. Їх можна дізнатися (наприклад, за допомогою зворотного навчання з підкріпленням) або агент може шукати інформацію, щоб покращити свої переваги.[35] Теорія цінності інформації може бути використана для оцінки цінності пошукових або експериментальних дій.[36] Простір можливих майбутніх дій і ситуацій зазвичай нерозв'язно великий, тому агенти повинні вживати дій і оцінювати ситуації, не знаючи, яким буде результат.

Процес прийняття рішень Маркова має перехідну модель, яка описує ймовірність того, що певна дія змінить стан певним чином, і функцію винагороди, яка забезпечує корисність кожного стану та вартість кожної дії. Політика пов’язує рішення з кожним можливим станом. Політику можна розрахувати (наприклад, шляхом ітерації), бути евристичною або її можна вивчити.[37]

Теорія ігор описує раціональну поведінку кількох взаємодіючих агентів і використовується в програмах штучного інтелекту, які приймають рішення за участю інших агентів.[38]

навчання

Машинне навчання — це дослідження програм, які можуть автоматично покращувати свою продуктивність у виконанні певного завдання.[39] Він був частиною ШІ з самого початку.[e]

Існує кілька видів машинного навчання. Неконтрольоване навчання аналізує потік даних, знаходить закономірності та робить прогнози без будь-яких інших вказівок.[42] Контрольоване навчання вимагає, щоб людина спочатку позначила вхідні дані, і воно буває двох основних різновидів: класифікація (де програма повинна навчитися передбачати, до якої категорії належить вхід) і регресія (де програма повинна вивести числову функцію на основі числового введення).).[43] При навчанні з підкріпленням агент винагороджується за хороші відповіді та карається за погані. Агент вчиться вибирати відповіді, які класифікуються як «хороші».[44] Трансферне навчання – це коли знання, отримані з однієї проблеми, застосовуються до нової проблеми.[45] Глибоке навчання — це тип машинного навчання, який запускає вхідні дані через біологічно інспіровані штучні нейронні мережі для всіх цих типів навчання.[46]

Теорія обчислювального навчання може оцінювати учнів за обчислювальною складністю, за складністю вибірки (скільки даних потрібно) або за іншими поняттями оптимізації.[47]

Обробка природної мови

Обробка природної мови (NLP)[48] дозволяє програмам читати, писати та спілкуватися такими мовами, як англійська. Специфічні проблеми включають розпізнавання мовлення, синтез мовлення, машинний переклад, витяг інформації, пошук інформації та відповіді на запитання.[49]

Рання робота, заснована на генеративній граматиці та семантичних мережах Ноама Хомського, мала труднощі з усуненням неоднозначності [f], якщо не обмежуватись невеликими областями, які називаються «мікросвітами» (через проблему знання здорового глузду [26]).

Сучасні методи глибокого навчання для НЛП включають вбудовування слів (як часто одне слово з'являється поруч з іншим), [50] трансформери (які

знаходять шаблони в тексті) [51] та інші.[52] У 2019 році генеративні попередньо підготовлені трансформаторні (або «GPT») мовні моделі почали генерувати зв'язний текст [53] [54], а до 2023 року ці моделі змогли отримувати бали людського рівня на адвокатському іспиті, SAT, GRE, і багато інших реальних програм.[55]

1. Роль ШІ у Кібербезпеці

А. Автоматизація виявлення загроз

- Швидке виявлення: ШІ може аналізувати дані в режимі реального часу, швидко виявляючи підозрілу поведінку або аномалії, що можуть вказувати на кібератаку.
- Машинне навчання: Алгоритми машинного навчання можуть навчатися на історичних даних та підлаштовуватися під змінні моделі загроз.

Б. Прогнозування кібератак

- Аналіз тенденцій: ШІ може аналізувати тенденції та шаблони в даних, щоб прогнозувати потенційні майбутні атаки.
- Підвищення точності: Завдяки здатності до обробки великих обсягів даних, ШІ може зменшити кількість помилкових тривог.

2. Використання ШІ для Захисту Кіберпростору

А. Розпізнавання шаблонів

- Аналіз мережевого трафіку: Використання ШІ для аналізу мережевого трафіку дозволяє виявляти незвичайну активність, яка може вказувати на кібератаку.
- Виявлення аномалій: Алгоритми ШІ можуть ідентифікувати відхилення від нормального поводження системи, що є ключовим для виявлення нових або нестандартних атак.

Б. Боротьба з розширеними постійними загрозами (APT)

- Розширений аналіз: ШІ може допомогти в ідентифікації та відстеженні APT, які часто використовують складні та багатоетапні методи атак.
- Довгострокове спостереження: Автоматизоване спостереження за поведінкою системи допомагає виявляти тривалі нальоти атак APT.

3. ШІ у Відповіді на інциденти

А. Автоматизація реагування

- Швидке реагування: Алгоритми ШІ можуть автоматизувати реагування на інциденти, забезпечуючи швидке та ефективне усунення загроз.
- Оптимізація процесів: ШІ може допомогти в оптимізації процесів відповіді на інциденти, скорочуючи час та ресурси, необхідні для вирішення проблем.

Б. Підвищення резильєнтності

- Аналіз після атаки: Використання ШІ для аналізу кібератак допомагає в розумінні та вдосконаленні захисних механізмів.
- Навчання системи: Неперервне навчання системи на основі нових загроз підвищує її резильєнтність.

4. Виклики та Обмеження

А. Етичні та приватні виклики

- Захист даних: Необхідність забезпечення конфіденційності та захисту даних при використанні ШІ.
- Етичні запитання: Врахування етичних аспектів при використанні алгоритмів ШІ, особливо в контексті автоматизації рішень.

Б. Технологічні обмеження

- Залежність від даних: Ефективність ШІ залежить від якості та обсягу доступних даних.
- Вразливість ШІ: Потенційна вразливість систем ШІ до маніпуляцій або помилок.

5. Розвиток технологій ШІ для кібербезпеки

А. Розвиток алгоритмів ШІ

- Вдосконалення моделей машинного навчання: Постійний розвиток та оптимізація алгоритмів машинного навчання дозволяє краще виявляти складні кіберзагрози.

- Інтеграція різних підходів ШІ: Комбінування різних методик ШІ, таких як навчання з підкріпленням, глибоке навчання та нейронні мережі, для підвищення ефективності систем кібербезпеки.

Б. Автоматизація та оптимізація

- Автоматизація процесів кібербезпеки: Використання ШІ для автоматизації рутинних задач забезпечення безпеки, знижуючи навантаження на людський фактор.
- Оптимізація відповідей на інциденти: Впровадження ШІ для швидкого та ефективного реагування на кіберінциденти, зменшуючи час відновлення та вплив атаки.

6. Практичне застосування ШІ у кібербезпеці

А. Виявлення загроз

- Реальний час аналізу даних: Використання ШІ для моніторингу мережевого трафіку та системних журналів в реальному часі, що дозволяє оперативно виявляти підозрілу активність.
- Розпізнавання зразків поведінки: ШІ допомагає в ідентифікації незвичайних поведінкових зразків, які можуть вказувати на зловмисні дії.

Б. Профілактика витоків даних

- Захист від внутрішніх загроз: ШІ може виявляти потенційні витоки інформації зсередини організації, аналізуючи поведінку користувачів та транзакції даних.
- Попередження витоку даних: ШІ допомагає в ранньому виявленні та блокуванні спроб несанкціонованого доступу до конфіденційної інформації.

7. Майбутнє ШІ у кібербезпеці

А. Розвиток ШІ-заснованих захисних технологій

- Адаптивні системи безпеки: Розробка систем, які можуть адаптуватися до змінних умов та нових типів загроз, використовуючи алгоритми машинного навчання.

- Інтеграція ШІ з іншими технологіями: Комбінація ШІ з іншими передовими технологіями, такими як блокчейн або квантові обчислення, для створення більш надійних систем кібербезпеки.

Б. Етичні та юридичні виклики

- Прозорість та контроль: Важливість забезпечення прозорості роботи ШІ-систем та можливості їх контролю людьми для запобігання помилковим рішенням.
- Регулювання використання ШІ: Розробка та впровадження правових норм для регулювання використання ШІ в кібербезпеці, забезпечуючи етичне та відповідальне використання технологій.

8. Практичне впровадження ШІ в кібербезпеці

А. Кейс-стадії

- Використання ШІ для захисту клієнтських даних: Розглянемо випадок фінансової установи, яка використовує ШІ для аналізу патернів транзакцій та виявлення потенційних шахрайств.
- ШІ для автоматизації відповідей на інциденти: Розглянемо технологічну компанію, що впровадила систему ШІ для швидкого реагування на кіберінциденти, зменшуючи час відновлення після атак.

Б. Розробка та впровадження

- Інтеграція з існуючими системами: Необхідність інтеграції ШІ-рішень із вже існуючими системами кібербезпеки.
- Контроль та моніторинг: Створення інтерфейсів та панелей керування для моніторингу та контролю роботи ШІ.

9. Стратегії застосування ШІ у кібербезпеці

А. Оптимізація алгоритмів

- Навчання на реальних даних: Використання реальних даних для навчання алгоритмів ШІ, щоб забезпечити їхню релевантність та точність.

- Боротьба з фальшивими тривогами: Фокус на зниженні кількості фальшивих позитивних сигналів, які можуть сповільнювати робочі процеси.

Б. Адаптація до нових видів загроз

- Постійне оновлення: Оновлення алгоритмів для адаптації до нових та еволюційних видів кіберзагроз.
- Сценарії моделювання: Розробка та використання сценаріїв моделювання для прогнозування та підготовки до потенційних майбутніх атак.

10. Майбутні тренди та виклики

А. Розвиток ШІ

- Покращення моделей глибокого Навчання: Використання більш складних моделей глибокого навчання для аналізу кіберзагроз.
- Інтеграція ШІ з інтернетом речей (IoT): Застосування ШІ для захисту пристроїв IoT, які стають все більш поширеними та підвищують ризики кібербезпеки.

Б. Етичні та правові виклики

- Приватність та конфіденційність: Вирішення проблем приватності, особливо у світлі зростаючого використання даних користувачів.
- Нормативне регулювання: Вплив майбутнього нормативного регулювання на використання ШІ в кібербезпеці.

11. Застосування ШІ у різних галузях

А. Фінансовий сектор

- Шахрайство та фінансові злочини: Використання ШІ для виявлення та запобігання шахрайству, аналізу фінансових транзакцій для ідентифікації підозрілих дій.
- Ризик-менеджмент: Використання ШІ для прогнозування та управління ризиками, пов'язаними з кіберзагрозами.

Б. Здоров'я та медицина

- Захист медичних даних: Впровадження ШІ для захисту конфіденційних медичних даних, виявлення несанкціонованого доступу та витоків інформації.
- Моніторинг медичних систем: Використання ШІ для моніторингу медичного обладнання та систем, запобігання кібератакам, які можуть призвести до збоїв у роботі обладнання.

12. Технічні виклики та рішення

А. Великі обсяги даних

- Обробка біг дата: Використання ШІ для обробки великих обсягів даних, виявлення зразків та тенденцій, які можуть вказувати на кіберзагрози.
- Оптимізація зберігання та обробки: Розробка ефективних методів зберігання та обробки даних для оптимізації ресурсів.

Б. Точність і надійність

- Покращення точності моделей: Вдосконалення алгоритмів ШІ для зменшення помилок та підвищення точності виявлення.
- Тестування та валідація: Регулярне тестування та валідація моделей ШІ для забезпечення їх надійності та ефективності.

13. Майбутній розвиток та вплив

А. Розширення Можливостей ШІ

- Інновації у технологіях ШІ: Розвиток нових алгоритмів і методів машинного навчання, які можуть ефективніше виявляти та протидіяти кіберзагрозам.
- Інтеграція з іншими технологіями: Поєднання ШІ з іншими передовими технологіями для створення комплексних рішень у сфері кібербезпеки.

Б. Етичні та соціальні виміри

- Проблеми приватності та етики: Вирішення питань, пов'язаних з приватністю даних та етичним використанням ШІ.
- Регуляторні аспекти: Адаптація до змін у законодавстві та регуляторних рамках, що впливають на використання ШІ в кібербезпеці.

14. Продуктивне впровадження ШІ в кібербезпеці

А. Використання ШІ для захисту інфраструктури

- Захист мережі та систем: Розробка систем на основі ШІ, здатних аналізувати мережевий трафік на предмет аномальної поведінки та потенційних вторгнень.
- Охорона критичної інфраструктури: Використання ШІ для забезпечення безпеки критичних державних та приватних інфраструктур, включаючи енергетичні мережі, транспортні системи та фінансові установи.

Б. Інтеграція з існуючими захисними механізмами

- Сумісність з традиційними інструментами: Інтеграція ШІ з традиційними інструментами кібербезпеки, такими як антивіруси та файрволи, для створення більш комплексного захисту.
- Гармонійне співіснування: Розробка рішень, які гармонійно інтегруються з існуючою IT-інфраструктурою та не перешкоджають її роботі.

15. Покращення систем кібербезпеки за допомогою ШІ

А. Оновлення та підтримка

- Неперервне оновлення: Автоматичне оновлення систем кібербезпеки на основі ШІ для адаптації до нових видів загроз.
- Технічна підтримка та обслуговування: Надання якісної технічної підтримки для забезпечення стабільності та надійності роботи систем на основі ШІ.

Б. Вдосконалення алгоритмів

- Машинне та глибоке навчання: Постійне вдосконалення алгоритмів машинного та глибокого навчання для підвищення точності та ефективності виявлення загроз.
- Аналітика поведінки: Використання аналітики поведінки для виявлення складних кіберзагроз, які можуть не бути виявлені традиційними методами.

16. Майбутнє ШІ в кібербезпеці

А. Інноваційні Розв'язки

- Розвиток автономних захисних систем: Створення повністю автономних систем кібербезпеки, які можуть самостійно виявляти, аналізувати та нейтралізувати кіберзагрози без втручання людини.
- Інтеграція з іншими напрямками ШІ: Використання розвитків у галузі нейронних мереж, обробки природної мови та інших галузей штучного інтелекту для покращення захисних механізмів.

Б. Соціальні та етичні виклики

- Розробка етичних норм: Створення та впровадження етичних норм та правил для використання ШІ в кібербезпеці.
- Врахування соціальних аспектів: Оцінка соціальних впливів використання ШІ в кібербезпеці, зокрема на приватність та свободу інформації.

Використання штучного інтелекту в області кібербезпеки відкриває нові горизонти для захисту інформаційних систем і мереж. Від ефективного виявлення та реагування на загрози до розробки інноваційних захисних механізмів - потенціал ШІ в цій сфері є значним. Проте, необхідно також враховувати технічні, етичні та правові аспекти, які супроводжують цей шлях інновацій.

1.4 Постановка задачі

Завдання базується на аналізі проблеми використання штучного інтелекту для задач кібербезпеки на прикладі реального підприємства.

Відповідно до аналізу та вимог особливої частини нормативного документа необхідно виконати наступні роботи:

- Ознайомитись з особливостями підприємства;
- Проаналізувати фізичні характеристики об’єкту;
- Проаналізувати логічну характеристику об’єкту;
- Проаналізувати види інформації та особливості взаємодії інформації на об’єкті;
- Виявити загрози;
- Дати рекомендації стосовно впровадження штучного інтелекту для забезпечення кібербезпеки

РОЗДІЛ 2
СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про підприємство ТОВ «SoftSolutions»

Підприємство «SoftSolutions» підприємство в сфері інформаційних і телекомунікаційних технологій, основна діяльність якого полягає в створенні веб-сайтів «під ключ», охоплюючи всі етапи життєвого циклу розробки програмного забезпечення, починаючи від концептуального проектування і закінчуючи бета-тестуванням і аналітикою.

Компанія працює на ринку надання послуг зі створення програмного забезпечення з січня 2019 року і орендує офіс на третьому поверсі в бізнес-центрі за адресою м.Дніпро, вул. Воскресенська, 20.

Таблиця 2.1

Штат підприємства «SoftSolutions»

№	Посада	Роль в системі	Кількість працівників на посаді	Рівень кваліфікації	Стаж на підприємстві
1	Директор	Адміністратратор	1	Високий	2
2	HR-менеджер	Користувач	1	Середній	1
3	Тімлід	Користувач	1	Високий	2
4	Розробник	Користувач	4	Високий	1
5	Сайлз-менеджер	Користувач	1	Високий	2
6	Офіс-менеджер	Користувач	1	Низький	2

В обов’язки директора входить повне вирішення всіх податкових і економічних питань компанії, взаємодія з сайлз-менеджером і тімлідами, часткова взаємодія з клієнтами при необхідності. Окрім цього, директор виконує функціонал бухгалтера.

HR-менеджер займаються підбором та прийомом на роботу персоналу.

Тімліди відповідають за вірну роботу команд розробників, включаючи строки проектів, правки, тощо.

Сайлз-менеджер менеджер відповідає за пошук клієнтів і всі взаємодії з ними. Деякі взаємодії проходять при участі тімлідів.

Офіс-менеджер — широкопрофільний співробітник, який відповідає за доставку продуктів в офіс, замовлення і доставку меблів, техніки, тощо. Окрім цього виконує функціонал локального системного адміністратора.

Структура підприємства зображена на рисунку 2.1

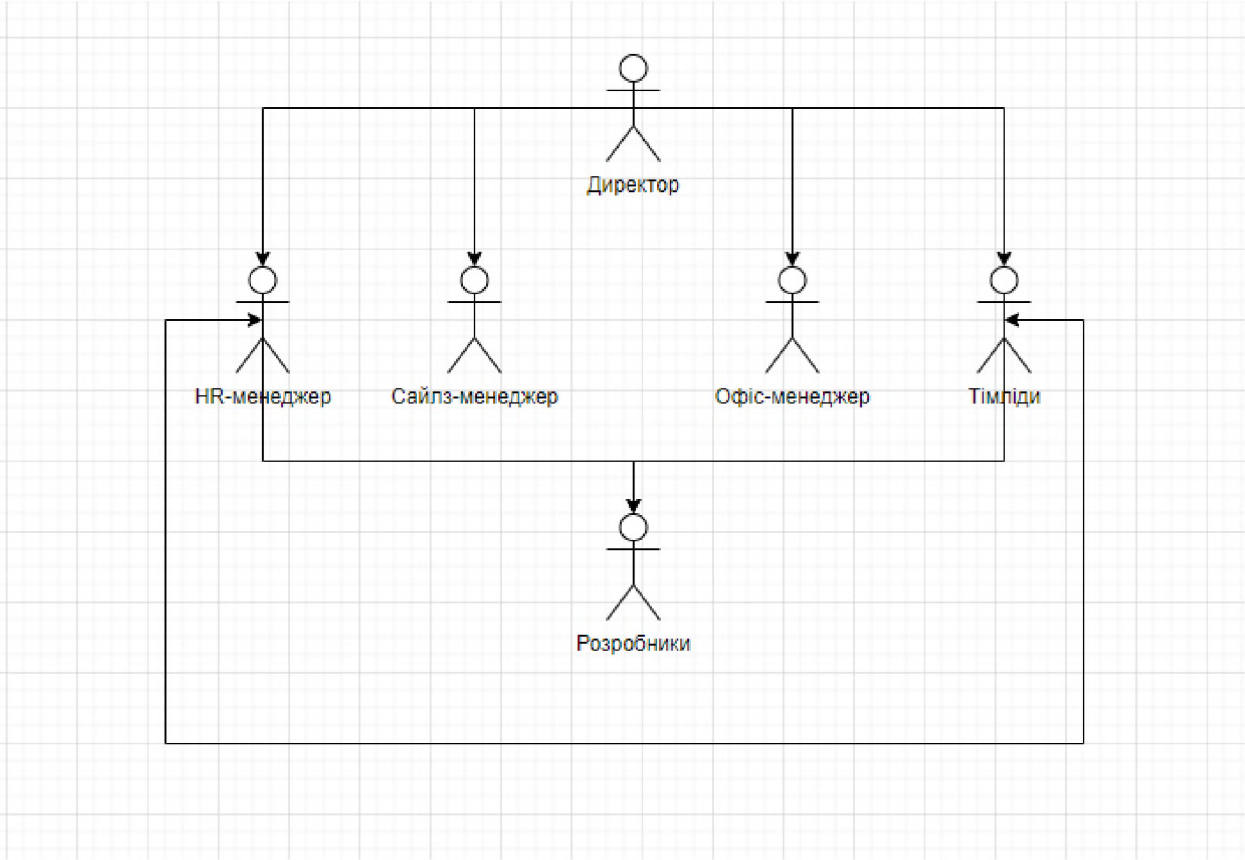

Рисунок 2.1 — Схема структури підприємства

2.2 Аналіз підприємства

Опис програмного забезпечення та його локалізація на комп'ютерах підприємства «SoftSolutions» представлено в таблиці 2.2.

Таблиця 2.2

Програмне забезпечення в інформаційній системі підприємства

№	Назва ПО	Тип	Ліцензія	Призначення	Термін дії	Встановлено
1	Windows 11	Системне	Commercial	Операційна система	Безстроковий	PC1…PC9
2	Microsoft Word	Прикладне	Commercial	Редактор тексту	Безстроковий	PC1…PC9
3	Microsoft Excel	Прикладне	Commercial	Редактор таблиць	Безстроковий	PC1…PC3, PC8, PC9
4	Adobe Photoshop	Прикладне	Commercial	Графічний редактор	Безстроковий	PC6…PC9
5	Unity	Прикладне	Commercial	Ігровий двигун	Безстроковий	PC4…PC7
6	Visual Studio 2022	Прикладне	Commercial	Інтегроване середовище розробки	Безстроковий	PC4…PC7
7	PyCharm 2022 Professional Edition	Прикладне	Commercial	Інтегроване середовище розробки	Безстроковий	PC4…PC7

Система складається з 9 персональних комп'ютерів, 2 принтерів, 3 комутаторів, 1 роутера.

На рисунку 2.2 зображено схему інформаційної системи підприємства.

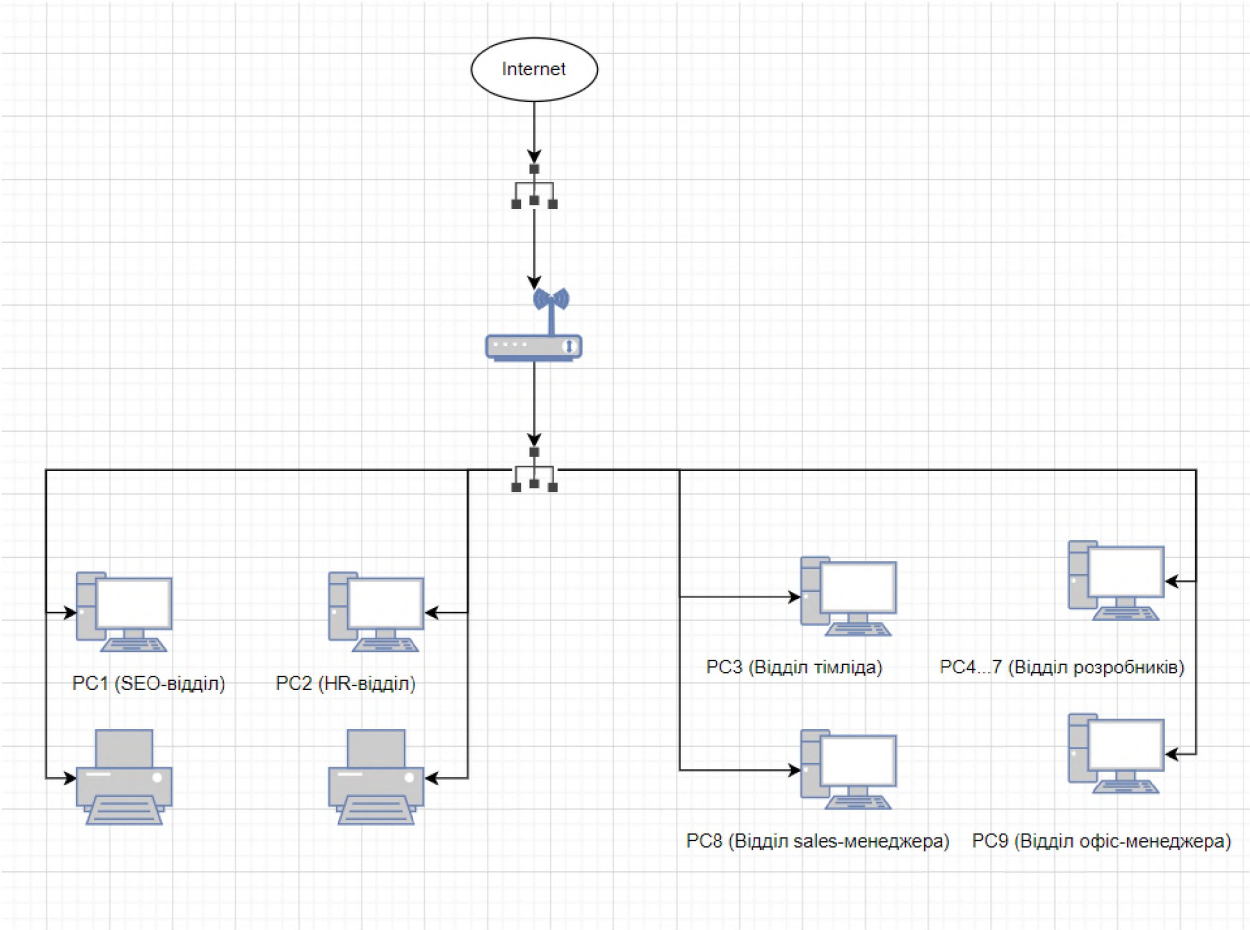

Рисунок 2.2 — Схема інформаційної системи підприємства

2.3 Обстеження об’єкту інформаційної діяльності

2.3.1 Ситуаційний план

Приміщення компанії, є об’єктом інформаційної діяльності (ОІД), що досліджується в кваліфікаційній роботі. Об’єкт інформаційної діяльності розташований на 3 поверсі бізнес-центру за адресою м. Дніпро, вул. Вознесенська, 20.

Контрольована зона (далі КЗ) обмежена зовнішніми стінами будівлі з усіх сторін, знизу - підлогою, під якою розташоване підвальне приміщення, фітнес-центр, студія краси та інші офіси та магазини, а зверху - стелею.

Територія позаду будинку огороджена невисоким парканом із шлагбаумом, асфальтована, наявні ділянки із кущами, є місця для паркування авто, які вказані на рисунку 2.3

Рисунок 2.3 — Схема ситуаційного плану ОІД

До даного будинку підключені наступні комунікації:

- електропостачання - від трансформаторної підстанції через підземні

комунікації до розподільного щитка, який розташований на стіні всередині будинку біля кімнати охорони;

- каналізація та водопостачання - підключені до міських магістралей та заходять до підвального приміщення даного будинку;
- система опалення - централізована, труби стояку йдуть з 0 поверху до приміщень на 1 поверсі, а потім до офісів вище.

Схема заземлення зображена на Ситуаційному плані Рисунку 2.3 Заземлення іде від трансформаторної підстанції до розподільного щита. Безпосередньо в офісі заземлення немає.

КЗ розташована в офісному будинку, комунікації, а саме труби системи опалення, лінія електропостачання та лінія комп'ютерної мережі виходять за межі КЗ. Інформація про навколишні будинки та споруди приведена у Таблиці 2.2.

Таблиця 2.2

Характеристика будівель та споруд.

№	Найменування	К-ть поверхів	Адреса	Відстань до ОІД, м
1	Житловий будинок	4	Мечнікова, 1	28
2	Адміністративна будівля	4	Мечнікова, 6	21
3	Трансформаторна підстанція ТП-102	1	Біля адміністративної будівлі №4	17
4	Адміністративна будівля	5	проспект Дмитра Яворницького, 75а	22
5	Житловий будинок	5	проспект Науки, 38а	20
6	Ремонтована будівля	5	Воскресенська, 18	7
7	Адміністративна будівля	2	Воскресенська, 16	12

Прилеглі вулиці відносно ОІД вказані у Таблиці 2.3.

Таблиця 2.3

Прилеглі вулиці відносно ОІД

Назва	Опис
вул. Мечнікова	Відносно ОІД вулиця розташована на заході. Автомобільний трафік становить 80 - 120 машин на годину.
вул. Воскресенська	Відносно ОІД вулиця розташована на сході. Автомобільний трафік становить 180 - 230 машин на годину.
вул. Челюскіна	Відносно ОІД вулиця розташована на півдні. Автомобільний трафік становить 70 - 100 машин на годину.

2.3.2 Опис генерального плану

- площа ОІД: 68м^2;
- висота стелі — 2.89м. Поверх — 3-ій;
- стеля (матеріал бетон, товщина — 0,5м.), підлога (матеріал бетон+металеві конструкції+деревина, товщина 1.5м.), стіни (матеріал цегла+гіпсокартон, товщина 0,6м);
- вікно (кількість — 6 шт, матеріал пластик (ПВХ)), розміри: 2.5м х 1,1м. Вікна виходять на двір. Сектор прямої видимості — це адміністративні будівлі та вулиці Воскресенська та Мечнікова;
- лінія електропостачання іде до поверхового щитка у підвалі, а звідти — до основного електрощита;
- сигналізація підключена до ПКП біля входу;
- лінія комп'ютерної мережі — оптичний кабель: Wi-Fi роутер підключений до мережевого обладнання провайдеру;
- система опалення — горизонтальна.

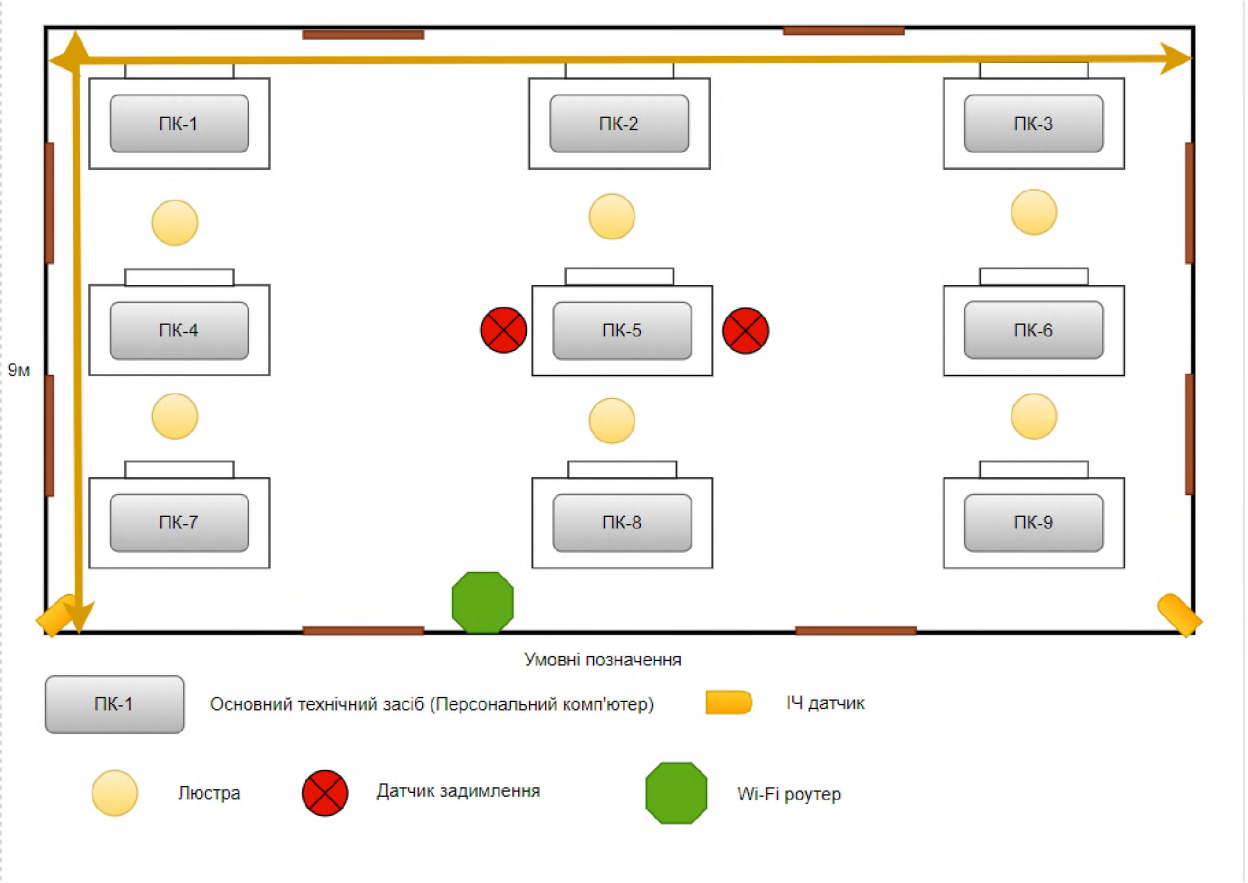

Рисунок 2.4 — Генеральний план

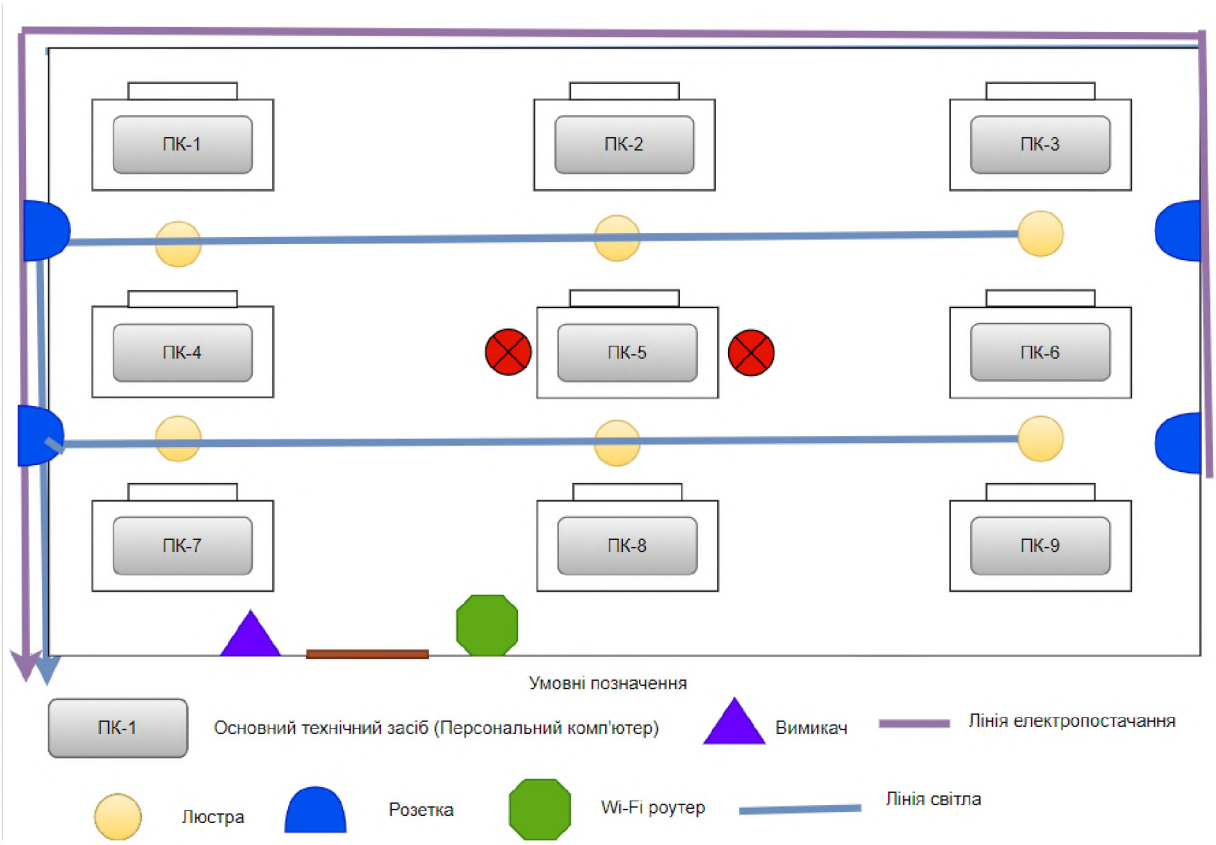

Рисунок 2.5 — Генеральний план. Схема систем електропостачання та освітлення

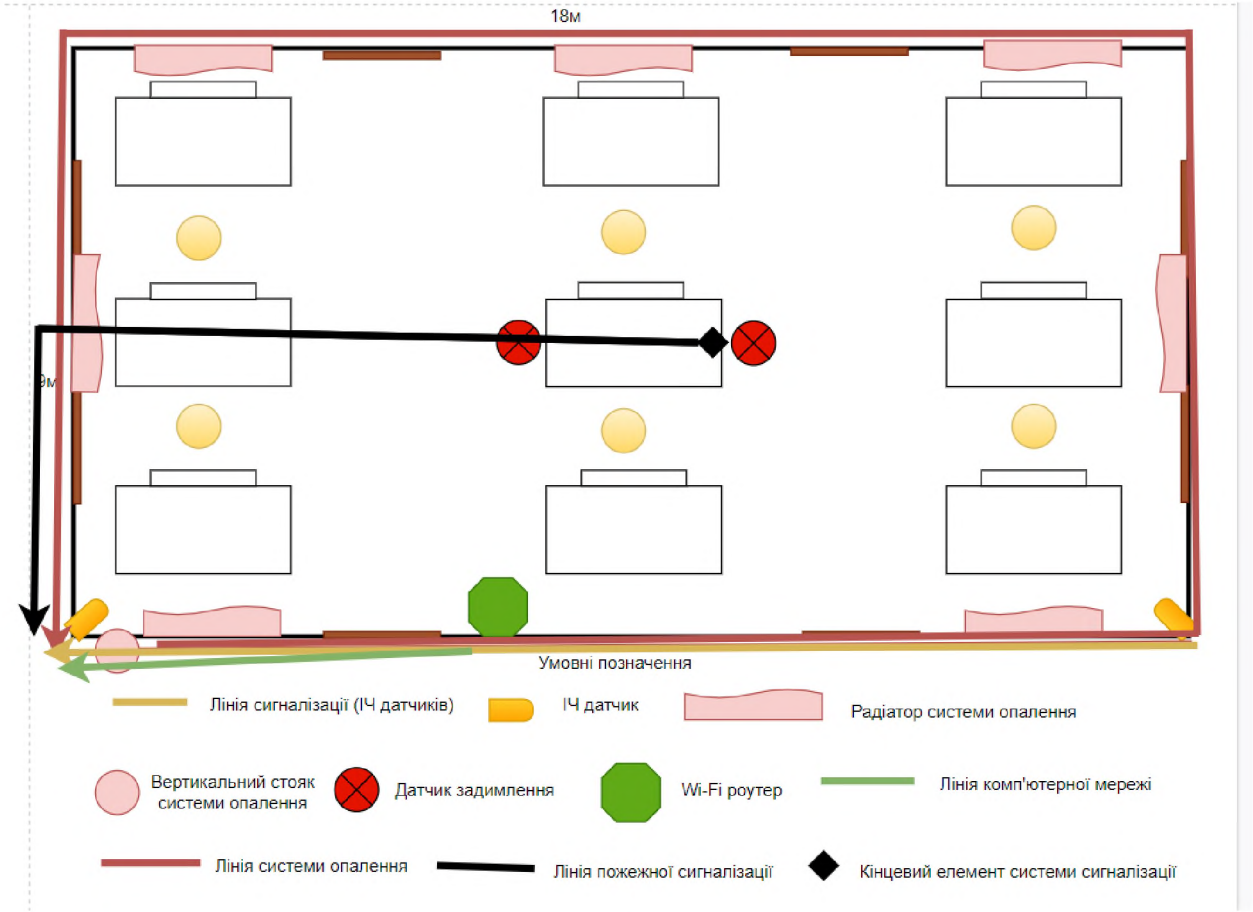

Рисунок 2.6 — Генеральний план. Схеми ліній комп'ютерної мережі, системи сигналізації та системи опалення

Режим КЗ забезпечується таким чином:

- у робочий час забезпечується співробітниками охоронної організації та системою контролю управління доступом. Чергові знаходяться біля контрольно-пропускного пункту, біля входу у будівлю;
- у неробочий час забезпечується силами охорони з використанням засобів відеоспостереження, решіток на вікнах, вхідними металопластиковими дверями, які закриваються на ключ. Також

застосовується автономна сигналізація приміщень всього будинку, яка підключена до приймально-контрольного пристрою, який знаходяться біля чергових ПКП. Чергові мають тривожну кнопку, яка застосовується для виклику наряду представників охоронної організації. Сигналізація КЗ входить до составу системи сигналізації усієї будівлі.

Комунікаційні системи КЗ вказані у Таблиці 2.4. Вони також відображені на генеральному плані (Рисунки 2.4-2.6).

Таблиця 2.4

Комунікаційні системи

Вид комунікації	Характеристика
Система електропостачання	від трансформаторної підстанції через підземні комунікації до розподільного щитка, який розташований на стіні всередині будинку біля входу до приміщення.
Система опалення	Централізована, труби стояку йдуть з 0 поверху до КЗ, а потім до офісів вище.
Система каналізації	Підключені до міських магістралей та заходять до підвального приміщення даного будинку
Система водопостачання	
Телефонна лінія та Інтернет	Підключені до Інтернет-провайдера «Укртелеком» . Кабель локальної мережі являє собою неекранована вита пара
Система сигналізації	Складається з інфрачервоних датчиків, датчиків задимлення, системи відеоспостереження. Керується службою безпеки власника будівлі.

2.4 Модель загроз

За результатами впливу на інформацію та систему її обробки, загрози поділяються на чотири класи:

1 Порушення конфіденційності інформації (К) - отримання інформації користувачами або процесами всупереч встановленим правилам розмежування доступу до інформації.

2 Порушення цілісності інформації (Ц) - повне або часткове знищення, викривлення, модифікація інформації, нав'язування хибної інформації тощо.

3 Порушення доступності інформації (Д) - часткова або повна втрата працездатності системи, блокування доступу до інформації в результаті некоректних дій адміністраторів, технічного обслуговуючого персоналу.

4 Втрата спостережності (керованості системою) (С) - порушення процедур ідентифікації та автентифікації адміністраторів або процесів і надання їм повноважень, втрата контролю за їх діяльністю, можливість відмови від отримання або пересилання повідомлень.

Потенційно загрози можуть завдати шкоди обробляємої інформації, працівникам, кліентам, технічним засобам і процесам. Загрози також можна поділити на:

- навмисні (Н);
- випадкові (В);
- природні (П).

Потрібно ідентифікувати як випадкові, так і навмисні джерела загроз.

Загрози можуть бути ідентифіковані в загальному вигляді або за типами.

Зроблено яшсну оцінку ймовірності реалізації загрози та визначено сукупний рівень загрози. Результати аналізу викладені в таблиці 2.5.

Таблиця 2.5

Результати аналізу загроз та разливостей інформації в ІТС.

№	Вразливість	Загроза	Ймовірність	Порушення	Рівень загрози	Загально
1	Вразливості системи охорони; Порушення правил використання КС; Відсутність системи ролей.	Несанціонований доступ до системи	3	КЦДС	4	3,5
2	Зловживання можливостями адміністраторів; Невірне розподілення ролей	Порушення правил, встановлених ролями користувачів	3	КЦДС	5	4
3	Відсутність політики безпеки щодо копіювання даних; Недотримання політики безпеки.	Копіювання конфіденційних даних	3	КЦДС	5	4

4	Відсутність політики безпеки, яка регулює використання дозволених програмних засобів.	Крадіжка конфіденційних даних з використанням стороннього ПЗ.	2	КЦДС	3	2,5
5	Відсутність антивірусів, наявність вільних каналів руху інформації.	Використання вірусів для отримання або пошкодження даних	2	КЦДС	3	2,5
6	Погано підібраний персонал; Низька заробітна плата та мотивації співробітників	Доступ до конфіденційних даних через співробітників	2	КЦДС	2	2
7	Відсутність правил використання системи	Використання системи в корисних цілях	4	С	1	2,5
8	Відсутність політики інформаційної безпеки	Неправомірне використання системи	4	КЦДС	2	3

9	Погана робота співробітників служби безпеки	Порушення роботи системи	1	С	4	2,5
10	Відсутність системи ролей. Неліцензійне програмне забезпечення.	Втручання в роботу системи з неправомірною метою	3	КЦДС	3	3

Серед найбільш критичних загроз можна виділити:

- несанкціонований доступ до системи;
- копіювання конфіденційних даних;
- використання неліцензійного ПЗ;
- використання забороненого ПЗ.

2.5 Рекомендації стосовно впровадження штучного інтелекту в систему захисту

Захист корпоративних систем є критично важливим для будь-якого сучасного підприємства. Зростання кількості кіберзагроз вимагає розробки більш вдосконалених методів захисту. Штучний інтелект (ШІ) надає нові можливості для підвищення рівня безпеки, дозволяючи більш ефективно виявляти та реагувати на потенційні загрози.

Огляд сучасних загроз

Сучасні загрози безпеки КС включають в себе несанкціонований доступ, фішинг, програми-вимагачі, а також внутрішні загрози, наприклад, від недобросовісних співробітників. Ці загрози можуть призвести до значних фінансових втрат, витоку конфіденційної інформації, а також до негативного впливу на репутацію підприємства.

Роль ШІ у захисті КС

ШІ може грати ключову роль у захисті КС, виконуючи такі завдання:

1. Аналіз поведінки користувачів: ШІ може аналізувати поведінку користувачів, виявляючи незвичні дії, які можуть свідчити про несанкціонований доступ або інші порушення безпеки.
2. Прогнозування та виявлення загроз: Використовуючи алгоритми машинного навчання, ШІ може прогнозувати потенційні загрози на основі аналізу великих обсягів даних, включаючи історичні дані про безпеку та актуальні тренди кіберзлочинності.
3. Адаптивні механізми захисту: ШІ може допомогти у розробці адаптивних механізмів захисту, які здатні самонавчатися та самовдосконалюватися, реагуючи на нові види загроз.
4. Автоматизоване реагування на інциденти: ШІ може автоматизувати процеси реагування на інциденти безпеки, забезпечуючи швидке та ефективне вирішення проблем.

Інтеграція ШІ в систему охорони

Інтеграція ШІ у систему охорони КС включає наступні аспекти:

1. Обладнання: Використання камер та сенсорів з можливостями розпізнавання образів та поведінки, здатних ідентифікувати підозрілі дії.
2. Програмне забезпечення: Розробка програмного забезпечення, яке використовує алгоритми машинного навчання для аналізу даних з камер і сенсорів, а також для моніторингу мережевого трафіку.
3. Дані та аналітика: Збір та аналіз великих обсягів даних для виявлення шаблонів, що можуть вказувати на загрози безпеки.
4. Навчання та адаптація: Постійне навчання та адаптація системи на основі нових даних і змін у поведінці користувачів або загроз.

Виклики та можливі рішення

При інтеграції ШІ у систему охорони КС необхідно враховувати такі виклики:

1. Захист даних та приватність: Потрібно забезпечити, щоб система дотримувалася всіх вимог щодо захисту даних та приватності користувачів.
2. Складність та вартість розробки: Впровадження ШІ вимагає значних ресурсів, включаючи кваліфіковані кадри та фінансові інвестиції.
3. Потреба у спеціалізованому персоналі: Для ефективного управління та обслуговування системи необхідні фахівці з глибокими знаннями у галузі кібербезпеки та ШІ.

Використання ШІ для покращення системи охорони та моніторингу КС є стратегічно важливим кроком для забезпечення вищого рівня безпеки підприємства. Хоча це вимагає значних ресурсів та спеціалізованого персоналу, потенційні переваги у вигляді зниження ризиків та підвищення ефективності реагування на загрози є вагомими.

РОЗДІЛ 3
ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ ДОЦІЛЬНОСТІ РОЗРОБКИ ПОЛІТИКИ БЕЗПЕКИ

3.1 Економічне обгрунтування доцільності впровадження політики безпеки інформації

Для економічного обгрунтування доцільності розробки політики безпеки інформації з використанням методів штучного інтеоекту ТОВ «SoftSolutions» потрібно провести розрахунки, щоб визначити економічну ефективність використання основних результатів, які будуть отримані після розрахунків.

Економічна доцільність визначається:

- розрахунками капітальних витрат, що потребує розроблена політика безпеки;
- розрахунками експлуатаційних витрат;
- розрахунками річного економічного ефекту від розробки інформаційної політики безпеки.

3.1.1 Розрахунок суми витрат на розробку політики безпеки інформації

Спочатку розраховується трудомістшсть розробки політики безпеки інформації, для цього потрібно скласти час, який знадобиться для кожної робочої операції:

$$t = tmз + tв + ta + tвз + tозб + товр + tд, \text{ годин, де}$$

- tmз - тривалість складання ТЗ на розробку ПБІ = 50 годин;
- tв - тривалість розробки концепції безпеки інформації у організації = 30 годин;
- ta - тривалість процесу аналізу ризиків = 36 годин;
- tак - тривалість визначення вимог заходів, методів та засобів захисту = 18 годин;

- tозб - тривалість виробу основних рішень з забезпечення БІ = 56 годин;
- товр - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організацій = 120 години;
- tд - тривалість документального оформлення політики безпеки = 20 годин.

$$t = 50 + 30 + 36 + 18 + 56 + 120 + 20 = 330 \text{ годин.}$$

3.1.2 Розрахунок суми витрат на реалізацію політики безпеки інформації.

Сума витрат на розробку політики безпеки {Kpn) складається з витрат на:

- Заробітну плату спеціаліста з кібербезпеки — Ззп, грн;
- Вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації — Змч.

$$Kpn = Ззп + Змч = 27411 \text{ грн}$$

Заробітна плата спеціаліста складається з основної та додаткової заробітної плати, соціальних виплат та визначається за формулою:

$$Ззп = t * Зіб = 24750{,}00 \text{ грн}$$

де t — загальна тривалість розробки політики безпеки інформації = 330 годин;

Зіб — середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями = 12000 / 160 = 75, грн/годину

Вартість машинного часу для розробки політики безпеки інформації на ІТК визначається за формулою:

$$Змч = t * Смч = 2661 \text{ грн}$$

де t — трудомістшсть підготовки документації на ІТК =4 години;

Смч — вартість 1 години машинного часу ПК, грн./година (5,6 грн).

Відповідно до розроблених рекомендацій, планується використання ліцензійних програмних засобів, як вже встановлених, так і нових.

Розрахована вартість розробки політики безпеки інформації Kpn ь складовою одноразових капітальних витрат разом з витратами на придбання програмних засобів, як рекомендовані для використання.

Отже фіксована сума капітальних витрат на розробку політики безпеки інформації складае:

$$К = Kpn + Кзпз + Каз + Кнавч + Кн = 61411 \text{ грн.}$$

$$К = 27411 + 11150 + 7850 + 9400 + 5600 = 61411 \text{ грн}$$

де *К* — вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх спеціалістів, тис. грн;

Кзпз — вартість закупівлі ліцензійного основного і додаткового програмного забезпечення (ПЗ), тис. грн;

Крп — вартість розробки політики безпеки інформації, тис. грн;

Каз — вартість закупівлі апаратного забезпечення та допоміжних матеріалів,

Кнавч вартість витрати на навчання технічних фахівців і обслуговуючого персоналу = 5600 грн;

Кн — витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

3.2 Оцінка можливого збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

tn — час простою вузла або сегмента корпоративної мережі внаслідок атаки, 1 година;

tв — час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

tви — час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі 2 години;

Зо — заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 5500 грн./міс.;

Зс — заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 11000 грн./міс.;

Чо — чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особа;

Чс — чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 7 осіб.;

О — обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 2 млн грн. у рік;

Пзч — вартість заміни устаткування або запасних частин, грн; I — число атакованих сегментів корпоративної мережі, 1;

N — середнє число атак на рік, 10.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U=Пп +Пв +V=11740,4,$$

де Пп — оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

Пв — вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V — втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\sum Зс}{F} * t_n,$$

Пп = ((11000 *7)/176)*3 = 1312,5 грн,

де F — місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на повторне введення інформації Пви розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви:

Пви = ((11000 *7)/176)*4 = 1750 грн,

Витрати на заміни устаткування або запасних частин можуть скласти 3200

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

Пв = 1312,5 + 1750 + 125 = 1875 грн.

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

В = 1 * 14 * 13764,4 = 192700 грн.

3.3 Розрахунок економічного ефекту

Економічний ефект в сфері проектування рішення:

$$Е_{пр}=Ц_а-Ц_п \qquad (3.21)$$

$Е_{пр}$ = 65000,0 – 61411,6 = 3588,4 грн.

Річний економічний ефект в сфері експлуатації:

$$Е_{кс}=В_{еа}-В_{еп}$$

$Е_{кс}$ = 24544,8 - 16354,8 = 8190 грн.

Додатковий економічний ефект у сфері експлуатації:

$$\Delta E_{екс} = \sum_{t=1}^{T} E_{екс}(1+R)^{T-t}$$

$$\Delta E_{екс} = \sum_{t=1}^{5} 8190 * (1+0{,}16)^{5-t} = 56323.7 \text{ грн.}$$

Сумарний ефект складає:

$$E = E_{пр} + \Delta E_{екс} = 414{,}4 + 56323.7 = 56738{,}1 \text{ грн}$$

Таблиця 3.1.

Показники економічної ефективності проектного рішення

№	Найменування	Одиниці вимірювання	Значення показників	
			Базовий варіант	Новий варіант
1	Капітальні вкладення	Грн.	-	3527,38
2	Ціна придбання	Грн.	5000,0	4585,6
3	Річні експлуатаційні витрати	Грн.	5922,0	3956,4
4	Ціна споживання	Грн.	24544,8	16354,8
5	Економічний ефект в сфері проектування	Грн.	-	3588,4
6	Річний економічний ефект в сфері експлуатації	Грн.	-	8190
7	Додатковий ефект в сфері експлуатації	Грн.	-	56738,1
8	Сумарний ефект	Грн.	60362,5	

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

ROSI = E / K, частки одиниці

де — E загальний ефект від впровадження системи інформаційної безпеки грн.; K — капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

60362,5 / 60423,5 = 0,99

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

Розрахункове значення коефіцієнта повернення інвестицій:

0,99 > 0,95

Термін окупності капітальних інвестицій To показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

T = 1/0,99 = 1.01 років.

Висновок до третього розділу

Розробка політики інформаційної безпеки з використанням методів штучного інтелекту для ТОВ «SoftSolutions» є економічно доцільною, оскільки коефіцієнт повернення інвестицій ROSI складає 0,99, що означає отримання 0,99 грн. економічного ефекту на кожну гривню капітальних вкладень на розробку політики інформаційної безпеки підприємства. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів.

ВИСНОВКИ

У результаті проведеного дослідження, було виявлено, що впровадження методів штучного інтелекту (ШІ) у сфері кібербезпеки відкриває значні перспективи для покращення захисту інформаційних систем. ШІ демонструє високу ефективність у виявленні та протидії кіберзагрозам завдяки своїм здібностям до швидкого аналізу великих обсягів даних, виявлення аномалій та адаптації до нових видів атак.

Водночас, застосування ШІ у кібербезпеці несе в собі певні виклики, зокрема, пов'язані з необхідністю забезпечення захисту даних та приватності, а також потребою в постійному оновленні та вдосконаленні ШІ-систем для адаптації до постійно еволюціонуючих кіберзагроз. Незважаючи на ці виклики, можливості, які відкриваються завдяки використанню ШІ, є значно ширшими та перспективнішими.

Дослідження також показало, що успішне впровадження ШІ у кібербезпеці вимагає комплексного підходу, що включає не тільки технічне вдосконалення систем, але й розробку відповідних правових та етичних рамок, а також забезпечення відповідного рівня освіти та підготовки фахівців.

У підсумку, можна стверджувати, що інтеграція ШІ в кібербезпеку є не тільки актуальною, але й невід'ємною частиною стратегії захисту інформаційних систем від сучасних та майбутніх кіберзагроз. Розвиток та застосування методів ШІ у цій галузі відкриває нові можливості для зміцнення кібербезпеки, підвищуючи її ефективність та адаптивність у відповідь на швидко змінюване кіберпростір.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. "AlphaGo – Google DeepMind". Archived from the original on 10 March 2016.
2. Alter, Alexandra; Harris, Elizabeth A. (20 September 2023), "Franzen, Grisham and Other Prominent Authors Sue OpenAI", The New York Times
3. Altman, Sam; Brockman, Greg; Sutskever, Ilya (22 May 2023). "Governance of Superintelligence". openai.com. Archived from the original on 27 May 2023. Retrieved 27 May 2023.
4. Anderson, Susan Leigh (2008). "Asimov's "three laws of robotics" and machine metaethics". AI & Society. 22 (4): 477–493. doi:10.1007/s00146-007-0094-5. S2CID 1809459.
5. Anderson, Michael; Anderson, Susan Leigh (2011). Machine Ethics. Cambridge University Press.
6. Arntz, Melanie; Gregory, Terry; Zierahn, Ulrich (2016), "The risk of automation for jobs in OECD countries: A comparative analysis", OECD Social, Employment, and Migration Working Papers 189
7. "Artificial intelligence: Google's AlphaGo beats Go master Lee Se-dol". BBC News. 12 March 2016. Archived from the original on 26 August 2016. Retrieved 1 October 2016.
8. Asada, M.; Hosoda, K.; Kuniyoshi, Y.; Ishiguro, H.; Inui, T.; Yoshikawa, Y.; Ogino, M.; Yoshida, C. (2009). "Cognitive developmental robotics: a survey". IEEE Transactions on Autonomous Mental Development. 1 (1): 12–34. doi:10.1109/tamd.2009.2021702. S2CID 10168773.
9. "Ask the AI experts: What's driving today's progress in AI?". McKinsey & Company. Archived from the original on 13 April 2018. Retrieved 13 April 2018.
10. Barfield, Woodrow; Pagallo, Ugo (2018). Research handbook on the law of artificial intelligence. Cheltenham, UK: Edward Elgar Publishing. ISBN 978-1-78643-904-8. OCLC 1039480085.

11. Beal, J.; Winston, Patrick (2009), "The New Frontier of Human-Level Artificial Intelligence", IEEE Intelligent Systems, 24: 21–24, doi:10.1109/MIS.2009.75, hdl:1721.1/52357, S2CID 32437713
12. Berdahl, Carl Thomas; Baker, Lawrence; Mann, Sean; Osoba, Osonde; Girosi, Federico (7 February 2023). "Strategies to Improve the Impact of Artificial Intelligence on Health Equity: Scoping Review". JMIR AI. 2: e42936. doi:10.2196/42936. ISSN 2817-1705. S2CID 256681439. Archived from the original on 21 February 2023. Retrieved 21 February 2023.
13. Berlinski, David (2000). The Advent of the Algorithm. Harcourt Books. ISBN 978-0-15-601391-8. OCLC 46890682. Archived from the original on 26 July 2020. Retrieved 22 August 2020.
14. Berryhill, Jamie; Heang, Kévin Kok; Clogher, Rob; McBride, Keegan (2019). Hello, World: Artificial Intelligence and its Use in the Public Sector (PDF). Paris: OECD Observatory of Public Sector Innovation. Archived (PDF) from the original on 20 December 2019. Retrieved 9 August 2020.
15. Bertini, M; Del Bimbo, A; Torniai, C (2006). "Automatic annotation and semantic retrieval of video sequences using multimedia ontologies". MM '06 Proceedings of the 14th ACM international conference on Multimedia. 14th ACM international conference on Multimedia. Santa Barbara: ACM. pp. 679–682.
16. Bostrom, Nick (2014). Superintelligence: Paths, Dangers, Strategies. Oxford University Press.
17. Bostrom, Nick (2015). "What happens when our computers get smarter than we are?". TED (conference). Archived from the original on 25 July 2020. Retrieved 30 January 2020.
18. Bowling, Michael; Burch, Neil; Johanson, Michael; Tammelin, Oskari (9 January 2015). "Heads-up limit hold'em poker is solved". Science. 347 (6218): 145–149. Bibcode:2015Sci...347..145B. doi:10.1126/science.1259433. ISSN 0036-8075. PMID 25574016. S2CID

3796371. Archived from the original on 1 August 2022. Retrieved 30 June 2022.

19. Brooks, Rodney (10 November 2014). "artificial intelligence is a tool, not a threat". Archived from the original on 12 November 2014.
20. Brooks, Rodney (1990). "Elephants Don't Play Chess" (PDF). Robotics and Autonomous Systems. 6 (1–2): 3–15. CiteSeerX 10.1.1.588.7539. doi:10.1016/S0921-8890(05)80025-9. Archived (PDF) from the original on 9 August 2007.
21. Buiten, Miriam C (2019). "Towards Intelligent Regulation of Artificial Intelligence". European Journal of Risk Regulation. 10 (1): 41–59. doi:10.1017/err.2019.8. ISSN 1867-299X.
22. Bushwick, Sophie (16 March 2023), "What the New GPT-4 AI Can Do", Scientific American
23. Butler, Samuel (13 June 1863). "Darwin among the Machines". Letters to the Editor. The Press. Christchurch, New Zealand. Archived from the original on 19 September 2008. Retrieved 16 October 2014 – via Victoria University of Wellington.
24. Buttazzo, G. (July 2001). "Artificial consciousness: Utopia or real possibility?". Computer. 34 (7): 24–30. doi:10.1109/2.933500.
25. Cambria, Erik; White, Bebo (May 2014). "Jumping NLP Curves: A Review of Natural Language Processing Research [Review Article]". IEEE Computational Intelligence Magazine. 9 (2): 48–57. doi:10.1109/MCI.2014.2307227. S2CID 206451986.
26. Cellan-Jones, Rory (2 December 2014). "Stephen Hawking warns artificial intelligence could end mankind". BBC News. Archived from the original on 30 October 2015. Retrieved 30 October 2015.
27. Chalmers, David (1995). "Facing up to the problem of consciousness". Journal of Consciousness Studies. 2 (3): 200–219. Archived from the original on 8 March 2005. Retrieved 11 October 2018.

28. Chen, Stephen (25 March 2023). "Artificial intelligence, immune to fear or favour, is helping to make China's foreign policy | South China Morning Post". Archived from the original on 25 March 2023. Retrieved 26 March 2023.
29. Christian, Brian (2020). The Alignment Problem: Machine learning and human values. W. W. Norton & Company. ISBN 978-0-393-86833-3. OCLC 1233266753.
30. Ciresan, D.; Meier, U.; Schmidhuber, J. (2012). "Multi-column deep neural networks for image classification". 2012 IEEE Conference on Computer Vision and Pattern Recognition. pp. 3642–3649. arXiv:1202.2745. doi:10.1109/cvpr.2012.6248110. ISBN 978-1-4673-1228-8. S2CID 2161592.
31. Clark, Jack (2015b). "Why 2015 Was a Breakthrough Year in Artificial Intelligence". Bloomberg.com. Archived from the original on 23 November 2016. Retrieved 23 November 2016.
32. CNA (12 January 2019). "Commentary: Bad news. Artificial intelligence is biased". CNA. Archived from the original on 12 January 2019. Retrieved 19 June 2020.
33. Cybenko, G. (1988). Continuous valued neural networks with two hidden layers are sufficient (Report). Department of Computer Science, Tufts University.
34. Deng, L.; Yu, D. (2014). "Deep Learning: Methods and Applications" (PDF). Foundations and Trends in Signal Processing. 7 (3–4): 1–199. doi:10.1561/2000000039. Archived (PDF) from the original on 14 March 2016. Retrieved 18 October 2014.
35. Dennett, Daniel (1991). Consciousness Explained. The Penguin Press. ISBN 978-0-7139-9037-9.
36. DiFeliciantonio, Chase (3 April 2023). "AI has already changed the world. This report shows how". San Francisco Chronicle. Archived from the original on 19 June 2023. Retrieved 19 June 2023.

37. Dickson, Ben (2 May 2022). "Machine learning: What is the transformer architecture?". TechTalks. Retrieved 22 November 2023.
38. Dockrill, Peter (27 June 2022), "Robots With Flawed AI Make Sexist And Racist Decisions, Experiment Shows", Science Alert, archived from the original on 27 June 2022
39. Domingos, Pedro (2015). The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World. Basic Books. ISBN 978-0465065707.
40. Dreyfus, Hubert (1972). What Computers Can't Do. New York: MIT Press. ISBN 978-0-06-011082-6.
41. Dreyfus, Hubert; Dreyfus, Stuart (1986). Mind over Machine: The Power of Human Intuition and Expertise in the Era of the Computer. Oxford: Blackwell. ISBN 978-0-02-908060-3. Archived from the original on 26 July 2020. Retrieved 22 August 2020.
42. Dyson, George (1998). Darwin among the Machines. Allan Lane Science. ISBN 978-0-7382-0030-9. Archived from the original on 26 July 2020. Retrieved 22 August 2020.
43. Eapen, Tojin T.; Finkenstadt, Daniel J.; Folk, Josh; Venkataswamy, Lokesh (16 June 2023). "How Generative AI Can Augment Human Creativity". Harvard Business Review. ISSN 0017-8012. Archived from the original on 20 June 2023. Retrieved 20 June 2023.
44. Edelson, Edward (1991). The Nervous System. New York: Chelsea House. ISBN 978-0-7910-0464-7. Archived from the original on 26 July 2020. Retrieved 18 November 2019.
45. Edwards, Benj (17 May 2023). "Poll: AI poses risk to humanity, according to majority of Americans". Ars Technica. Archived from the original on 19 June 2023. Retrieved 19 June 2023.
46. Evans, Woody (2015). "Posthuman Rights: Dimensions of Transhuman Worlds". Teknokultura. 12 (2). doi:10.5209/rev_TK.2015.v12.n2.49072.

47. Fearn, Nicholas (2007). The Latest Answers to the Oldest Questions: A Philosophical Adventure with the World's Greatest Thinkers. New York: Grove Press. ISBN 978-0-8021-1839-4.
48. Ford, Martin; Colvin, Geoff (6 September 2015). "Will robots create more jobs than they destroy?". The Guardian. Archived from the original on 16 June 2018. Retrieved 13 January 2018.
49. Fox News (2023). "Fox News Poll" (PDF). Fox News. Archived (PDF) from the original on 12 May 2023. Retrieved 19 June 2023.
50. Frangoul, Anmar (14 June 2019). "A Californian business is using A.I. to change the way we think about energy storage". CNBC. Archived from the original on 25 July 2020. Retrieved 5 November 2019.
51. Frey, Carl Benedikt; Osborne, Michael A (1 January 2017). "The future of employment: How susceptible are jobs to computerisation?". Technological Forecasting and Social Change. 114: 254–280. CiteSeerX 10.1.1.395.416. doi:10.1016/j.techfore.2016.08.019. ISSN 0040-1625.
52. "From not working to neural networking". The Economist. 2016. Archived from the original on 31 December 2016. Retrieved 26 April 2018.
53. Galvan, Jill (1 January 1997). "Entering the Posthuman Collective in Philip K. Dick's "Do Androids Dream of Electric Sheep?"". Science Fiction Studies. 24 (3): 413–429. JSTOR 4240644.
54. Geist, Edward Moore (9 August 2015). "Is artificial intelligence really an existential threat to humanity?". Bulletin of the Atomic Scientists. Archived from the original on 30 October 2015. Retrieved 30 October 2015.
55. Gertner, Jon (18 July 2023). "Wikipedia's Moment of Truth – Can the online encyclopedia help teach A.I. chatbots to get their facts right — without destroying itself in the process? + comment". The New York Times. Archived from the original on 18 July 2023. Retrieved 19 July 2023.
56. Gibbs, Samuel (27 October 2014). "Elon Musk: artificial intelligence is our biggest existential threat". The Guardian. Archived from the original on 30 October 2015. Retrieved 30 October 2015.

57. Goffrey, Andrew (2008). "Algorithm". In Fuller, Matthew (ed.). Software studies: a lexicon. Cambridge, Mass.: MIT Press. pp. 15–20. ISBN 978-1-4356-4787-9.
58. Good, I. J. (1965), Speculations Concerning the First Ultraintelligent Machine
59. Goodfellow, Ian; Bengio, Yoshua; Courville, Aaron (2016), Deep Learning, MIT Press., archived from the original on 16 April 2016, retrieved 12 November 2017
60. Goodman, Bryce; Flaxman, Seth (2017). "EU regulations on algorithmic decision-making and a 'right to explanation'". AI Magazine. 38 (3): 50. arXiv:1606.08813. doi:10.1609/aimag.v38i3.2741. S2CID 7373959.
61. Government Accountability Office (13 September 2022). Consumer Data: Increasing Use Poses Risks to Privacy. gao.gov (Report).
62. Grant, Nico; Hill, Kashmir (22 May 2023). "Google's Photo App Still Can't Find Gorillas. And Neither Can Apple's". The New York Times.
63. Goswami, Rohan (5 April 2023). "Here's where the A.I. jobs are". CNBC. Archived from the original on 19 June 2023. Retrieved 19 June 2023.
64. Harari, Yuval Noah (October 2018). "Why Technology Favors Tyranny". The Atlantic. Archived from the original on 25 September 2021. Retrieved 23 September 2021.
65. Harari, Yuval Noah (2023). "AI and the future of humanity". YouTube.
66. Haugeland, John (1985). Artificial Intelligence: The Very Idea. Cambridge, Mass.: MIT Press. ISBN 978-0-262-08153-5.
67. Heath, Nick (11 December 2020). "What is AI? Everything you need to know about Artificial Intelligence". ZDNet. Archived from the original on 2 March 2021. Retrieved 1 March 2021.
68. Henderson, Mark (24 April 2007). "Human rights for robots? We're getting carried away". The Times Online. London. Archived from the original on 31 May 2014. Retrieved 31 May 2014.
69. Hinton, G.; Deng, L.; Yu, D.; Dahl, G.; Mohamed, A.; Jaitly, N.; Senior, A.; Vanhoucke, V.; Nguyen, P.; Sainath, T.; Kingsbury, B. (2012). "Deep Neural

Networks for Acoustic Modeling in Speech Recognition – The shared views of four research groups". IEEE Signal Processing Magazine. 29 (6): 82–97. Bibcode:2012ISPM...29...82H. doi:10.1109/msp.2012.2205597. S2CID 206485943.

70. Holley, Peter (28 January 2015). "Bill Gates on dangers of artificial intelligence: 'I don't understand why some people are not concerned'". The Washington Post. ISSN 0190-8286. Archived from the original on 30 October 2015. Retrieved 30 October 2015.
71. Hornik, Kurt; Stinchcombe, Maxwell; White, Halbert (1989). Multilayer Feedforward Networks are Universal Approximators (PDF). Neural Networks. Vol. 2. Pergamon Press. pp. 359–366.
72. Horst, Steven (2005). "The Computational Theory of Mind". The Stanford Encyclopedia of Philosophy. Archived from the original on 6 March 2016. Retrieved 7 March 2016.
73. Howe, J. (November 1994). "Artificial Intelligence at Edinburgh University: a Perspective". Archived from the original on 15 May 2007. Retrieved 30 August 2007.
74. IGM Chicago (30 June 2017). "Robots and Artificial Intelligence". www.igmchicago.org. Archived from the original on 1 May 2019. Retrieved 3 July 2019.
75. Iphofen, Ron; Kritikos, Mihalis (3 January 2019). "Regulating artificial intelligence and robotics: ethics by design in a digital society". Contemporary Social Science. 16 (2): 170–184. doi:10.1080/21582041.2018.1563803. ISSN 2158-2041. S2CID 59298502.
76. Jordan, M. I.; Mitchell, T. M. (16 July 2015). "Machine learning: Trends, perspectives, and prospects". Science. 349 (6245): 255–260. Bibcode:2015Sci...349..255J. doi:10.1126/science.aaa8415. PMID 26185243. S2CID 677218.
77. Kahn, Gretel (11 April 2023). "Will AI-generated images create a new crisis for fact-checkers? Experts are not so sure". Reuters Institute for the Study of

Journalism. Archived from the original on 28 May 2023. Retrieved 28 May 2023.

78. Kahneman, Daniel (2011). Thinking, Fast and Slow. Macmillan. ISBN 978-1-4299-6935-2. Archived from the original on 15 March 2023. Retrieved 8 April 2012.
79. Kahneman, Daniel; Slovic, D.; Tversky, Amos (1982). "Judgment under uncertainty: Heuristics and biases". Science. New York: Cambridge University Press. 185 (4157): 1124–1131. Bibcode:1974Sci...185.1124T. doi:10.1126/science.185.4157.1124. ISBN 978-0-521-28414-1. PMID 17835457. S2CID 143452957.
80. Kasperowicz, Peter (1 May 2023). "Regulate AI? GOP much more skeptical than Dems that government can do it right: poll". Fox News. Archived from the original on 19 June 2023. Retrieved 19 June 2023.
81. Katz, Yarden (1 November 2012). "Noam Chomsky on Where Artificial Intelligence Went Wrong". The Atlantic. Archived from the original on 28 February 2019. Retrieved 26 October 2014.
82. "Kismet". MIT Artificial Intelligence Laboratory, Humanoid Robotics Group. Archived from the original on 17 October 2014. Retrieved 25 October 2014.
83. Kissinger, Henry (1 November 2021). "The Challenge of Being Human in the Age of AI". The Wall Street Journal. Archived from the original on 4 November 2021. Retrieved 4 November 2021.
84. Kobielus, James (27 November 2019). "GPUs Continue to Dominate the AI Accelerator Market for Now". InformationWeek. Archived from the original on 19 October 2021. Retrieved 11 June 2020.
85. Kolirin, Lianne (18 April 2023). "Artist rejects photo prize after AI-generated image wins award". CNN. Archived from the original on 28 May 2023. Retrieved 28 May 2023.
86. Kuperman, G. J.; Reichley, R. M.; Bailey, T. C. (1 July 2006). "Using Commercial Knowledge Bases for Clinical Decision Support: Opportunities, Hurdles, and Recommendations". Journal of the American Medical

Informatics Association. 13 (4): 369–371. doi:10.1197/jamia.M2055. PMC 1513681. PMID 16622160.

87. Kurzweil, Ray (2005). The Singularity is Near. Penguin Books. ISBN 978-0-670-03384-3.

88. Langley, Pat (2011). "The changing science of machine learning". Machine Learning. 82 (3): 275–279. doi:10.1007/s10994-011-5242-y.

89. Laskowski, Nicole (November 2023). "What is Artificial Intelligence and How Does AI Work? TechTarget". Enterprise AI. Retrieved 30 October 2023.

90. Lenat, Douglas; Guha, R. V. (1989). Building Large Knowledge-Based Systems. Addison-Wesley. ISBN 978-0-201-51752-1.

91. Lighthill, James (1973). "Artificial Intelligence: A General Survey". Artificial Intelligence: a paper symposium. Science Research Council.

92. Larson, Jeff; Angwin, Julia (23 May 2016). "How We Analyzed the COMPAS Recidivism Algorithm". ProPublica. Archived from the original on 29 April 2019. Retrieved 19 June 2020.

93. Law Library of Congress (U.S.). Global Legal Research Directorate, issuing body. (2019). Regulation of artificial intelligence in selected jurisdictions. LCCN 2019668143. OCLC 1110727808.

94. Lee, Timothy B. (22 August 2014). "Will artificial intelligence destroy humanity? Here are 5 reasons not to worry". Vox. Archived from the original on 30 October 2015. Retrieved 30 October 2015.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	1 Розділ	30	
5	А4	2 Розділ	16	
6	А4	3 Розділ	9	
7	А4	Висновки	1	
8	А4	Перелік посилань	10	
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	

ДОДАТОК Б. Перелік матеріалів на оптичному носії

Бочін_О.С._125м-22-2.docx

Бочін_О.С._125м-22-2.pptx

Бочін_О.С._125м-22-2.pdf

ДОДАТОК В. Відгук керівника економічного розділу

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 75 б. («добре»).

Керівник розділу _____ доц. Пілова Д.П.
(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

Відгук

на кваліфікаційну роботу студента групи 125м-22-2 Бочіна Ігоря Ігоровича на тему: «Аналіз та обгрунтування методів штучного інтелекту для задач кібербезпеки»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 78 сторінках.

Метою кваліфікаційної роботи є аналіз та обгрунтування використання методів ШІ у сфері кібербезпеки, а також вивчення потенціалу цих методів для підвищення ефективності захисту інформаційних систем від різноманітних кіберзагроз.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз джерел загроз інформаційної системи та кібербезпеки на підприємстві, а також методів та засобів впровадження штучного інтелекту в систему захисту.

Приведені приклади впровадження штучного інтелекту та рекомендації по розробці та впровадженню системи управління ризиками інформаційної безпеки в інформаційній системі.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Бочін І.І. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації магістра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему запобігання та виявлення плагіату НТУ «Дніпровська політехніка»".

Кваліфікаційна робота заслуговує оцінки «__» (_____).

Керівник роботи _____ _____

(підпис) (ініціали, прізвище)