ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ
КАФЕДРА КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Пояснювальна записка

до дипломного проекту (роботи)
Магістр
(освітньо-кваліфікаційний рівень)

на тему *Дослідження методів захисту від атак на основі штучного інтелекту в корпоративних мережах*

Research of protection methods against attacks based on artificial intelligence in corporate networks

Виконав: студент *6* курсу, групи *6КСМ*
напряму підготовки (спеціальності)
123 «Комп'ютерна інженерія»
(шифр і назва напряму підготовки, спеціальності)
Оліховський С.В,
(прізвище та ініціали)
Керівник *Дідик О.О.*
(прізвище та ініціали)
Рецензент *Вороненко М.О.*
(прізвище та ініціали)

м. Хмельницький – 2024 року

ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Інститут, факультет, відділення *Інформаційних технологій та дизайну*

Кафедра, циклова комісія *Комп'ютерних систем та мереж*

Освітньо-кваліфікаційний рівень *магістр*

Напрям підготовки _____

(шифр і назва)

Спеціальність *123 "Комп'ютерна інженерія"*

(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри, голова циклової комісії _____
комп'ютерних систем та мереж
_____ А.А. Григорова
«___» _____ 2024 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Оліховському Сергію Валентиновичу

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) *Дослідження методів захисту від атак на основі штучного інтелекту в корпоративних мережах*

Research of protection methods against attacks based on artificial intelligence in corporate networks

керівник проекту (роботи) *Дідик Олексій Олександрович, к.т.н., доцент.*

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від «18» жовтня 2024 року №569-с

2. Строк подання студентом проекту(роботи) 01.12.2024

3. Вихідні дані до проекту (роботи) *Методичні рекомендації до виконання дипломного проекту. Матеріали практики*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) *Аналіз методів проведення атак, Методі забезпечення захисту у мережі, Дослідження штучного інтелекту, Підготовка штучного інтелекту, Моделювання роботи мережі під час атаки*

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1.	Вивчення предметної області	13.09.2024	
2.	Постановка завдання	21.09.2024	
3.	Дослідження методів атак	11.10.2024	
4.	Дослідження існуючих методів захисту	16.10.2024	
5.	Моделювання захисту	11.11.2024	
6.	Оцінка отриманих результатів	21.11.2024	
7.	Оформлення пояснювальної записки	04.12.2024	
8.	Захист роботи	20.12.2024	
9.			
10.			
11.			
12.			
13.			

Студент _____ Оліховський С.В.
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ Дідик О.О.
(підпис) (прізвище та ініціали)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ШІ	Штучний інтелект
DoS	Denial of Service
DDoS	Distributed Denial of Service
DNS	Domain Name Service
ПЗ	Програмне забезпечення
XSS	Cross Site Scripting
NAC	Network Access Control
IPS	Intrusion Prevention System

ВСТУП

Актуальність проблеми

З розвитком технологій зростають і загрози, створені хакерами та кіберзловмисниками.

Зростає кількість кіберзлочинів, таких як фішинг, шахрайство та крадіжка даних, що наражає організації на небезпеку. Для боротьби з цими загрозами організації звертаються до кваліфікованих команд кібербезпеки, оснащених передовими технологіями, зокрема штучним інтелектом (ШІ), які швидко виявляють і протидіють зловмисним діям, захищаючи мережі від загроз.

Визнання потенціалу штучного інтелекту змусило 76% підприємств віддати перевагу штучному інтелекту та машинному навчанню у своїх IT-бюджетах, керуючись величезним обсягом даних, які потребують аналізу для виявлення загроз безпеці та ефективної боротьби з ними.

З підключеними пристроями, за прогнозами, до 2025 року згенерують приголомшливі 79 зетабайт даних, ручний аналіз людини стає непрактичним, що робить ШІ незамінним інструментом у боротьбі з кіберзлочинністю.

Об’єкт дослідження: штучний інтелект.

Ціль роботи: Визначення можливості застосування штучного інтелекту для захисту комп’ютерних мереж від атак.

Для визначення можливості застосування штучного інтелекту для захисту комп’ютерних мереж:

1. Дослідити методи атак на комп’ютерні мережі.
2. Визначити інструменти захисту мереж від атак.
3. Проаналізувати застосування штучного інтелекту для захисту мереж.
4. Провести моделювання захисту мережі від атак при використанні захисту зі штучним інтелектом.

Наукова новизна кваліфікаційної роботи магістра полягає в проведені комплексного дослідження штучного інтелекту для захисту комп’ютерних мереж.

Метою кваліфікаційної роботи магістра є визначити процент атак, що здатний визначити або зупинити штучний інтелект в умовах невизначеності.

Практична значимість є у отриманні можливості застосування штучного інтелекту у захисті комп’ютерних мереж.

Публікації. Тематика магістерської роботи була представлена у публікації:

Оліховський С.В., Іванчук О.В., Дідик О.О. Аналіз сфери застосування штучного інтелекту. *Сучасні комп’ютерні системи та мережі в управлінні* : матеріали VII Всеукраїнської науково-практичної інтернет-конференції студентів, аспірантів та молодих вчених. Хмельницький, 2024 р.

Структура й об'єм роботи

Кваліфікаційна робота магістра складається з вступу, 5 глав, висновку й списку використаних джерел, викладених на 79 сторінках машинописного тексту, що включає 4 таблиць, 10 рисунків і список літературних джерел з 50 посилань.