Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Розробка навчальної системи для збору персональних даних з використанням штучного інтелекту та соціальної інженерії"

Виконав: студент VI курсу, групи СБм-62
Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Прокопенко О.Є.
підпис (прізвище та ініціали)

Керівник Козак Р.О.
підпис (прізвище та ініціали)
Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)
за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)
Студенту Прокопенку Олегу Євгеновичу
(прізвище, ім'я, по батькові)
1. Тема роботи Розробка навчальної системи для збору персональних даних з використанням штучного інтелекту та соціальної інженерії

Керівник роботи: Козак Руслан Орестович, кандидат технічних наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
Затверджені наказом ректора від «20» 11 2024 року № 4/7-1112
2. Термін подання студентом завершеної роботи 16.12.2024
3. Вихідні дані до роботи

4. Зміст роботи (перелік питань, які потрібно розробити)
Теоретичні основи збору персональних даних та соціальної інженерії
Розробка архітектури навчальної системи для симуляції методу соціальної інженерії
Впровадження системи збору персональних даних
Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1.Тема роботи, 2.Наукова новизна дослідження, 3.Актуальність теми роботи, 4.Мета та Завдання дослідження,5.Актуальність та проблеми соціальної інженерії, 6.Впровадження ШІ в роботу, 7.Архітектура навчальної системи 8. Практичне впровадження системи, 9.Результати тестування навчальної системи, 10.Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент	10.12.2024	
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 23.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.09 – 22.09	Виконано
2.	Підбір джерел для аналізу впливу соціальної інженерії	25.09 – 10.10	Виконано
3.	Опрацювання джерел в галузі дослідження	11.10 – 15.10	Виконано
4.	Налаштування тестового лабораторного середовища	16.10 – 25.10	Виконано
5.	Розроблення оптимізованої навчальної системи бота	25.10 - 30.10	Виконано
6.	Оформлення розділу «Теоретичні основи збору персональних даних та соціальної інженерії»	30.10 – 05.11	Виконано
7.	Оформлення розділу «Розробка архітектури навчальної системи для симуляції методу соціальної інженерії»	06.11 – 10.11	Виконано
8.	Оформлення розділу «Впровадження системи збору персональних данних»	11.11 – 25.11	Виконано
9.	Виконання завдання до підрозділу «Охорона праці та безпека в надзвичайних ситуаціях»	26.11-01.12	
10.	Оформлення кваліфікаційної роботи	02.12 – 10.12	Виконано
11.	Нормоконтроль	15.12 – 16.12	Виконано
12.	Перевірка на плагіат	18.12 – 19.12	Виконано
13.	Попередній захист кваліфікаційної роботи	25.12 – 26.12	Виконано
14.	Захист кваліфікаційної роботи	27.12.2024	

Студент _____ Прокопенко О.Є.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Козак Р.О.
(підпис) (прізвище та ініціали)

ЗМІСТ

АНОТАЦІЯ

Розробка навчальної системи для збору персональних даних з використанням штучного інтелекту та соціальної інженерії» // Прокопенко Олег // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-62 // Тернопіль, 2024 // С. 54, рис. – 6, табл. – 1 , кресл. – 0, додат. – ____.

Ключові слова: ПЕРСОНАЛЬНІ ДАНІ, СОЦІАЛЬНА ІНЖЕНЕРІЯ, ШТУЧНИЙ ІНТЕЛЕКТ, НАВЧАЛЬНІ СИСТЕМИ, КІБЕРБЕЗПЕКА.

У кваліфікаційній роботі магістра було створено середовище, що дозволяє ефективно імітувати атаку для збору персональних даних з метою підвищення рівня обізнаності користувачів.

У першому розділі представлено огляд технологій соціальної інженерії, методів збору даних та сучасних алгоритмів штучного інтелекту, які можуть бути використані в даній сфері. Визначено основні вразливості користувачів та організацій, що експлуатуються атакуючими.

У другому розділі розроблено архітектуру навчальної системи, яка включає модулі моделювання атак на основі соціальної інженерії, штучного інтелекту для адаптації сценаріїв навчання. Було проведено аналіз вже готових систем та інструментів

У третьому розділі проведено тестування розробленої системи на вибірці користувачів, яке підтвердило її ефективність у виявленні вразливостей у поведінці користувачів та підвищенні їхньої обізнаності про методи протидії атакам. Зроблено висновки щодо подальших напрямів вдосконалення системи для її інтеграції в корпоративне середовище.

ABSTRACT

Development of a training system for collecting personal data using artificial intelligence and social engineering" // Prokopenko Oleg // Ivan Pulyuy Ternopil National Technical University, Faculty of Computer and Information Systems and Software Engineering, Department of Cybersecurity, Group SBм-62 // Ternopil, 2024 // P. 54, fig. – 6, tab. – 1 , drawing – 0, append. – ____.

Keywords: PERSONAL DATA, SOCIAL ENGINEERING, ARTIFICIAL INTELLIGENCE, TRAINING SYSTEMS, CYBERSECURITY.

In the master's qualification work, an environment was created that allows effectively simulating the attack of collecting personal data in order to increase user awareness.

The first section presents an overview of social engineering technologies, data collection methods and modern artificial intelligence algorithms that can be used in this area. The main vulnerabilities of users and organizations exploited by attackers were identified.

In the second section, the architecture of the training system was developed, which includes modules for modeling attacks based on social engineering, artificial intelligence for adapting training scenarios. An analysis of ready-made systems and tools was conducted

In the third section, the developed system was tested on a sample of users, which confirmed its effectiveness in identifying vulnerabilities in user behavior and increasing their awareness of methods for countering attacks. Conclusions were drawn on further areas of system improvement for its integration into the corporate environment.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ACID – Atomicity, Consistency, Isolation, Durability

API – IApplication Programming Interface

CEH – Certified Ethical Hacker

GPT –Generative Pre-trained Transformer

ICMP –Internet Control Message Protocol

IP – (Internet Protocol

IT – Інформаційні технології.

NLP –Natural Language Processing

ORM –Object-Relational Mapping

OSCP –Offensive Security Certified Professional

SANS – Інститут кібербезпеки (SANS Institute

SET – Social-Engineer Toolkit

SMS – Short Message Service

SQL –Structured Query Language

GDPR – Загальний регламент захисту даних (General Data Protection Regulation).

ШІ – Штучний інтелект.

ВСТУП

Актуальність теми роботи визначається стрімким розвитком цифрових технологій, що супроводжується зростанням ризиків у сфері кібербезпеки. У сучасному суспільстві персональні дані стали важливим ресурсом, який активно використовується не лише для покращення користувацького досвіду, але й для зловмисних цілей. Одним із ключових методів отримання таких даних є соціальна інженерія — форма маніпуляції, яка експлуатує людську довірливість, недосвідченість і неуважність. В умовах збільшення кількості фішингових атак і кіберзагроз зростає потреба в розробці ефективних навчальних рішень, які дозволяють підвищувати обізнаність користувачів і зменшувати їхню вразливість до таких атак.

Мета дослідження полягає у створенні навчальної системи для симуляції збору персональних даних із використанням методів соціальної інженерії та штучного інтелекту. Ця система спроектована з метою ідентифікації слабких місць у поведінці користувачів і підвищення їхньої обізнаності щодо ризиків соціальної інженерії.

Основні задачі дослідження включають:

- Аналіз існуючих методів соціальної інженерії та їх впливу на безпеку персональних даних.
- Розробку концепції навчальної системи для моделювання соціальної інженерії.
- Інтеграцію технологій штучного інтелекту в систему для збору та аналізу даних.
- Реалізацію Telegram-бота як основного інструмента симуляції взаємодії.
- Проведення тестування системи та аналіз її ефективності.
- Розробку рекомендацій щодо покращення цифрової грамотності користувачів і захисту персональних даних.

Об’єкт дослідження — процеси збору персональних даних.

Предмет дослідження — система збору даних з використанням технологій штучного інтелекту для моделювання і навчання користувачів.

Методи дослідження включають теоретичний аналіз літературних джерел із кібербезпеки, моделювання сценаріїв соціальної інженерії, використання алгоритмів штучного інтелекту для обробки та аналізу даних, експериментальне тестування навчальної системи.

Наукова новизна одержаних результатів полягає у розробці інтерактивної системи, яка поєднує алгоритми штучного інтелекту та принципи соціальної інженерії для навчання користувачів у контрольованому середовищі. Запропонований підхід дозволяє ефективно моделювати ризики, пов’язані з витоком даних, і формувати навички безпечної поведінки.

Практичне значення результатів роботи полягає у можливості застосування розробленої системи для підготовки користувачів до виявлення фішингових атак, навчання працівників організацій основам кібербезпеки та створення рекомендацій для вдосконалення політик захисту персональних даних. Система також може використовуватися як база для подальших досліджень і вдосконалення методів навчання в галузі кібербезпеки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗБОРУ ПЕРСОНАЛЬНИХ ДАНИХ ТА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

1.1 Персональні дані: поняття, класифікація, правове регулювання

1.1.1 Визначення персональних даних

Персональні дані визначаються як будь-яка інформація, яка дозволяє прямо або опосередковано ідентифікувати фізичну особу. Ці дані можуть бути як окремими елементами, так і їх комбінацією. Наприклад, ім’я та прізвище можуть бути недостатніми для ідентифікації у глобальному контексті, але у певному локальному середовищі вони стають ключовими ідентифікаторами.

До персональних даних відносять широкий спектр інформації, включаючи базові відомості, такі як ім’я, прізвище, дата народження, та більш чутливі дані, наприклад, медичні записи, біометричні параметри або фінансову інформацію. Важливим аспектом є те, що навіть непрямі дані, такі як IP-адреса або геолокація, можуть використовуватися для визначення особи у поєднанні з іншими даними.

Персональні дані поділяються за їхніми характеристиками. Залежно від функціонального призначення, вони можуть бути ідентифікаційними (номер паспорта, ідентифікаційний код), контактними (адреса, номер телефону), поведінковими (історія відвідувань вебсайтів) або біометричними (відбитки пальців, сканування обличчя). Ця класифікація важлива для розуміння їхньої ролі у сучасному цифровому суспільстві.

Особливістю персональних даних є їх контекстуальність. Дані, що у певному випадку здаються нейтральними, можуть стати чутливими у іншому. Наприклад, дані про місцезнаходження особи в реальному часі є надзвичайно конфіденційними, якщо вони збираються без її згоди.

Джерела персональних даних можна умовно поділити на три основні групи. Перша — це дані, які надаються самими користувачами, наприклад, при реєстрації у сервісах чи заповненні анкет. Друга група охоплює дані, зібрані через спостереження, такі як відеонагляд або трекери активності. Третя група — це

аналітичні дані, які генеруються системами через аналіз поведінки користувачів, їхніх уподобань чи взаємодій у цифровому середовищі.

На міжнародному рівні визначення персональних даних регулюється законодавством та стандартами. Зокрема, у Європейському Союзі це визначення закріплене у Загальному регламенті про захист даних (GDPR), який трактує персональні дані максимально широко, включаючи будь-яку інформацію, що дозволяє ідентифікувати особу. Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI. Цей закон встановлює правові основи для обробки персональних даних, визначає права суб'єктів даних і обов'язки осіб, які їх обробляють, а також гарантує захист персональної інформації. Українське законодавство у сфері захисту персональних даних також встановлює відповідні норми, однак його імплементація потребує подальшого вдосконалення для врахування сучасних викликів цифрового світу.

1.1.2 Класифікація персональних даних

Класифікація персональних даних є ключовим аспектом для їхнього аналізу, обробки та захисту. Існує кілька основних підходів до класифікації, кожен із яких базується на різних характеристиках даних, таких як їхнє функціональне призначення, ступінь чутливості, джерело отримання та спосіб обробки.

За функціональним призначенням:

- Ідентифікаційні дані: це дані, які використовуються для прямої ідентифікації особи. До них відносяться паспортні дані, ідентифікаційні номери, ідентифікатори у цифрових сервісах.

- Контактні дані: включають адресу проживання, номер телефону, електронну пошту, що забезпечують зв'язок із особою.

- Фінансові дані: інформація про банківські рахунки, кредитні картки, податкові дані.

- Медичні дані: включають історію хвороб, результати аналізів, відомості про поточний стан здоров'я.

Поведінкові дані: інформація про дії користувача у цифровому середовищі, включаючи історію пошуку, вподобання та інші параметри активності.

За ступенем чутливості:

- Загальнодоступні дані: інформація, яка публічно доступна і не потребує спеціального захисту (наприклад, ім’я та прізвище у соціальних мережах).

- Конфіденційні дані: інформація, що вимагає захисту через потенційні ризики неправомірного використання (наприклад, медичні або фінансові дані).

- Особливо чутливі дані: це дані, обробка яких вимагає дотримання спеціальних умов, зокрема біометричні та генетичні дані.

За джерелом отримання:

- Надані суб’єктом даних: інформація, яку користувач добровільно -надає, наприклад, під час реєстрації у сервісі.

- Зібрані через спостереження: дані, отримані без прямої участі користувача, наприклад, через відеонагляд або аналіз поведінки у мережі.

- Виведені дані: інформація, отримана через аналіз інших даних, наприклад, через машинне навчання або статистичні моделі.

За способом обробки:

- Автоматизовані дані: обробляються без участі людини за допомогою програмного забезпечення.

- Неавтоматизовані дані: обробляються вручну, зазвичай у традиційних системах обліку.

Ця класифікація є основою для розробки стратегій захисту персональних даних, вибору методів обробки та створення ефективних систем управління даними. У сучасному світі класифікація даних також визначає вимоги до їх зберігання, використання і передачі відповідно до міжнародних стандартів та законодавчих норм.

1.1.3 Виклики у сфері захисту персональних даних

У сучасних умовах, особливо в контексті війни України з Росією, сфера захисту персональних даних стикається з безпрецедентними викликами. Гібридна війна, яка включає не лише фізичні бойові дії, а й кібернетичні атаки, інформаційні кампанії та маніпуляції, ставить перед Україною складні завдання у захисті даних громадян та державних організацій. Одним із головних викликів є активізація кібератак з боку ворожих державних і недержавних акторів. Атаки спрямовані на злам баз даних, викрадення інформації про українських громадян, військовослужбовців, волонтерів та осіб, що підтримують Збройні сили України. Особливо небезпечним є використання цих даних для шантажу, дискредитації або проведення психологічних операцій проти українського населення. Іншим важливим аспектом є ризик компрометації критичної інфраструктури, зокрема державних реєстрів, банківських систем та систем охорони здоров'я. Злом таких систем може призвести до масштабного витоку конфіденційної інформації, яка може бути використана для підриву національної безпеки та економіки України. Ще одним викликом є недостатній рівень цифрової грамотності серед значної частини населення, що робить його вразливим до соціальної інженерії. Наприклад, шахрайські схеми, фішингові атаки та інші методи маніпуляції використовуються для отримання доступу до персональних даних через довірливість користувачів. Окремої уваги заслуговує проблема недостатньої гармонізації українського законодавства з міжнародними стандартами захисту даних, такими як Загальний регламент про захист даних (GDPR). Відсутність сучасних механізмів регулювання та нагляду ускладнює ефективне реагування на нові загрози.

У воєнний час також виникають етичні дилеми, пов'язані із захистом персональних даних. Наприклад, необхідність збору інформації для забезпечення безпеки може суперечити принципам конфіденційності. В умовах евакуації населення або роботи гуманітарних організацій існує ризик неналежного зберігання або передачі даних третім сторонам.

Додатково, варто зазначити, що інформаційна війна значно ускладнює захист даних у медіа-просторі. Пропагандистські кампанії можуть використовувати зібрані персональні дані для поширення дезінформації або створення фейкових новин, спрямованих на підрив довіри до державних інституцій та міжнародних партнерів України.

Усі ці виклики вимагають комплексного підходу до захисту персональних даних, включаючи розробку сучасних технологічних рішень, підвищення обізнаності населення та вдосконалення законодавчої бази.

1.2 Соціальна інженерія: визначення, методи, приклади використання

1.2.1 Визначення соціальної інженерії

Соціальна інженерія — це форма маніпуляції, спрямована на отримання конфіденційної інформації, доступу до систем чи виконання певних дій шляхом використання психологічних методів впливу на людей. Ця концепція є однією з ключових складових кібербезпеки, оскільки саме людський фактор залишається найвразливішою ланкою в будь-якій системі захисту.

Основні характеристики соціальної інженерії:

Людський фактор як об'єкт атаки. Соціальна інженерія спрямована на використання людських слабкостей, таких як довірливість, страх, незнання чи бажання допомогти. Вона враховує психологічні та поведінкові аспекти людини, що робить її більш ефективною, ніж технічні методи атак.

Маніпуляція емоціями. Соціальні інженери часто викликають у жертви страх, цікавість, терміновість або довіру, щоб змусити її виконати бажану дію. Наприклад, повідомлення про “злом акаунта” або термінову необхідність змінити пароль часто використовуються для досягнення мети.

Широке використання технік впливу. До них належать фішинг, вішинг (голосові дзвінки з метою отримання даних), смішинг (фішинг через SMS), а також фізичні методи, такі як проникнення у приміщення під виглядом працівника компанії.

Соціальна інженерія охоплює широкий спектр методів і технік, спрямованих на обман людини з метою:

- отримання конфіденційної інформації (наприклад, паролів, фінансових даних);
- отримання доступу до систем або фізичних об'єктів;
- впливу на дії жертви в інтересах зловмисника.

Ключовим аспектом соціальної інженерії є те, що вона не вимагає високого рівня технічних знань. Основна увага приділяється маніпуляції людською психологією, що робить її доступною для широкого кола зловмисників.

Соціальна інженерія поділяється на такі основні типи:

- Технічна соціальна інженерія. Використання технологічних засобів для досягнення цілей. Прикладом є підроблені вебсайти, електронні листи чи програми, які імітують легітимні сервіси.
- Нетехнічна соціальна інженерія. Фізичні чи вербальні взаємодії, наприклад, спроби проникнення в офіс під виглядом обслуговуючого персоналу або проведення телефонних розмов для отримання доступу до секретної інформації.
- Мішані методи. Поєднання технічних і нетехнічних підходів, наприклад, коли електронний лист з фішингом супроводжується телефонним дзвінком для підвищення довіри жертви.

Соціальна інженерія знаходить застосування в різних сценаріях:

- Атаки на корпоративні мережі. Зловмисники отримують доступ до корпоративних систем, надсилаючи співробітникам фішингові електронні листи або телефоном видаючи себе за адміністратора IT-відділу.
- Крадіжка персональних даних. Фішинг-сайти, які імітують легітимні сервіси (банки, поштові клієнти), використовуються для отримання логінів і паролів користувачів.
- Соціальна маніпуляція в фізичному середовищі. Зловмисники можуть видавати себе за кур'єрів, працівників технічної підтримки або відвідувачів для отримання доступу до конфіденційної інформації.

Соціальна інженерія становить значну загрозу, оскільки вона обходить традиційні засоби захисту, такі як антивірусні програми, фаєрволи та системи шифрування. Навіть найкраще налаштовані технічні засоби не здатні забезпечити повний захист, якщо співробітники чи користувачі недостатньо обізнані про загрози та методи соціальної інженерії.

Таким чином, ефективна протидія соціальній інженерії вимагає комплексного підходу, який включає навчання користувачів, впровадження багаторівневого захисту та регулярні перевірки на вразливість до подібних атак.

1.2.2 Приклади успішних атак

В контексті війни між Україною та Росією соціальна інженерія стала інструментом ведення інформаційної війни та кібератак. Нижче наведено приклади успішних атак, які ілюструють роль соціальної інженерії в цьому конфлікті:

Фішингові кампанії проти урядових органів України є однією з найпоширеніших тактик. Зловмисники надсилали електронні листи із підробленими повідомленнями, що нібито надходили від офіційних установ чи міжнародних організацій. Ці листи містили шкідливе програмне забезпечення, яке активувалося після відкриття вкладень. У багатьох випадках зловмисники успішно отримували доступ до внутрішніх мереж державних органів України, що дозволяло викрадати конфіденційну інформацію або саботувати роботу систем.

Російські хакери також здійснювали атаки на критичну інфраструктуру через фейкові запити. Було зафіксовано випадки, коли співробітникам енергокомпаній надходили телефонні дзвінки від нібито представників регулюючих органів із проханням надати доступ до серверів для "екстрених перевірок". Унаслідок цього зловмисники отримували доступ до систем управління енергетичними об'єктами.

Дезінформаційні кампанії для деморалізації населення також стали важливим інструментом. Через соціальні мережі та месенджери розповсюджувалися повідомлення, спрямовані на деморалізацію українського суспільства та військових. Наприклад, поширювалися фейкові новини про нібито капітуляцію

Збройних Сил України або про загрозу масових техногенних катастроф. Такі повідомлення часто містили посилання на підроблені сайти, які заражали пристрої користувачів шкідливим програмним забезпеченням.

Крім того, використовувалися соціальні мережі для вербування та шантажу. Російські спецслужби активно використовували соціальні мережі для виявлення цільових осіб, які мають доступ до секретної інформації або є вразливими до шантажу. Через фальшиві акаунти вони налагоджували зв'язок із такими особами, отримуючи від них конфіденційну інформацію або схиляючи до співпраці(див. рисунок 1.1)

Приклади успішних атак показують, що соціальна інженерія є ефективним інструментом у сучасних конфліктах, особливо коли вона комбінується з технічними методами. Для протидії цим загрозам необхідно підвищувати рівень обізнаності користувачів та впроваджувати багаторівневі системи захисту.

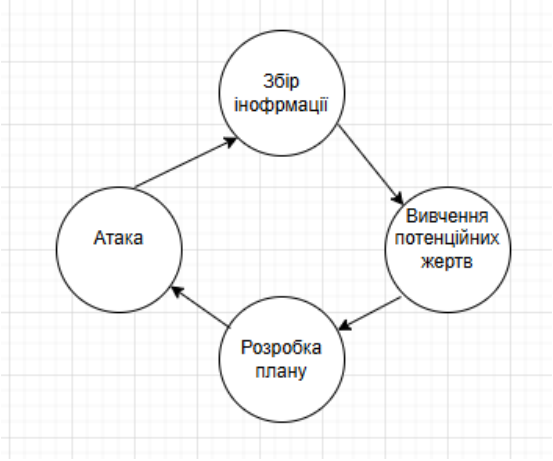

Рисунок 1.1 - Огляд картини плану

1.2.4 Наслідки атак соціальної інженерії

Атаки соціальної інженерії мають значний вплив на людей, що проявляється в різних аспектах їхнього життя. Наслідки таких атак можна поділити на кілька категорій. На рисунку 1.2 зображено основні наслідки

Рисунок 1.2 - Насділки атак соціальної інженерії

Люди, які стали жертвами соціальної інженерії, часто відчувають страх, тривогу та втрату довіри до оточення. Наприклад, викрадення персональних даних або фінансових коштів може спричинити глибокий емоційний дискомфорт.

Одним із найпоширеніших наслідків є викрадення грошей. Зловмисники можуть використовувати отриману інформацію для доступу до банківських рахунків, що призводить до значних фінансових втрат для жертв.

Поширення персональних даних, отриманих через соціальну інженерію, може спричинити проблеми з конфіденційністю, включаючи шантаж або небажану публікацію особистої інформації.

Жертви атак часто починають сумніватися у надійності цифрових систем, банківських установ чи навіть власного робочого середовища, що ускладнює їхнє повсякденне життя.

Масштабні кампанії дезінформації можуть призводити до суспільної паніки, деморалізації населення або підриву довіри до урядових структур. Це може впливати на соціальну стабільність та взаємодію між громадянами.

Наслідки атак соціальної інженерії є багатогранними і часто мають довготривалий характер. Для зменшення шкоди необхідно не лише впроваджувати технічні заходи захисту, але й підвищувати рівень обізнаності населення щодо потенційних загроз та методів їх уникнення.

1.3 Технології штучного інтелекту у зборі та аналізі персональних даних

Автоматизація збору даних стала ключовим інструментом у сучасному світі, особливо у контексті великих даних та аналітики. Штучний інтелект (ШІ) значно спрощує процес збору, обробки та аналізу даних, забезпечуючи ефективність та точність навіть за відсутності традиційних підрозділів для цього процесу. Цей розділ присвячений розгляду того, як ШІ може сприяти автоматизації збору даних про людей, організації чи події.

1.3.1 Автоматизація збору даних за допомогою штучного інтелекту

ШІ може використовуватись для автоматичного збору даних з відкритих джерел, таких як веб-сайти, соціальні мережі або публічні бази даних. Алгоритми машинного навчання допомагають аналізувати та структуризувати ці дані, витягуючи лише релевантну інформацію. Наприклад, за допомогою NLP (Natural Language Processing, обробка природної мови) можна аналізувати текстові дані та витягувати ключові факти.

Технології комп'ютерного зору, що базуються на ШІ, дозволяють автоматизувати збір біометричних даних, таких як обличчя, голос, відбитки пальців. Це може бути корисним у багатьох галузях, включаючи безпеку, маркетинг чи соціальні дослідження.

Чат-боти, що працюють на основі ШІ, можуть збирати дані безпосередньо від користувачів через інтерактивні сесії. Це можуть бути демографічні дані, уподобання, відгуки або інші форми зворотного зв'язку. Такий підхід зменшує потребу в людському втручанні та прискорює процес збору даних.

Пристрої IoT, що підтримуються ШІ, здатні збирати великі обсяги даних про поведінку користувачів, їх середовище та інші аспекти. Наприклад, розумні годинники, системи "розумного будинку" чи транспортні засоби оснащені датчиками, які автоматично передають дані в реальному часі.

Соціальні мережі є багатим джерелом даних про людей. ШІ може допомогти автоматизувати збір даних про поведінку користувачів, їхні інтереси, зв'язки та активність. Алгоритми дозволяють не лише збирати дані, а й аналізувати їх для виявлення трендів та створення персоналізованих профілів.

ШІ дозволяє збирати великі обсяги даних за короткий час, що є недосяжним для традиційних методів. Точність, алгоритми ШІ зменшують кількість помилок, пов'язаних із людським фактором. Гнучкість, ШІ-системи можуть адаптуватися до різних типів даних та джерел. Зменшення витрат, Автоматизація зменшує потребу в людських ресурсах, що призводить до економії.

Автоматизація збору даних також піднімає важливі питання етики. Наприклад, збирання персональних даних без згоди користувачів може порушувати їхні права на конфіденційність. Прозорість у використанні технологій збору даних, відповідність до регуляторних норм, таких як GDPR, захист зібраних даних від несанкціонованого доступу.

Штучний інтелект відкриває широкі можливості для автоматизації збору даних, що дозволяє підвищити ефективність бізнесу, досліджень та багатьох інших сфер. Однак використання таких технологій має супроводжуватися дотриманням етичних стандартів та забезпеченням конфіденційності даних. У майбутньому подальший розвиток ШІ ще більше вдосконалить процеси збору та обробки даних, роблячи їх доступнішими та зручнішими.

1.3.2 Використання штучного інтелекту для аналізу даних із соціальних мереж

Аналіз даних із соціальних мереж є однією з ключових сфер застосування штучного інтелекту (ШІ), особливо в умовах постійного зростання обсягів інформації, що генерується користувачами. Завдяки потужним алгоритмам машинного навчання та аналізу даних, ШІ дозволяє отримувати цінну інформацію, яка може бути використана в навчальних, дослідницьких або практичних цілях.

У контексті навчання ШІ допомагає не лише збирати дані, але й проводити їх глибокий аналіз. Збирання даних зазвичай здійснюється за допомогою API (Application Programming Interface), веб-скрейпінгу або моніторингу ключових слів і трендів. Використовуються виключно публічно доступні дані з дотриманням етичних норм.

Проте основна цінність ШІ полягає у здатності аналізувати зібрані дані, перетворюючи їх на цінну інформацію. Наприклад:

- Сентимент-аналіз дозволяє визначити емоційне забарвлення текстів, таких як пости чи коментарі. Це особливо корисно для вивчення громадської думки або аналізу реакції на певні події.
- Аналіз тексту допомагає виявляти ключові теми, розуміти контекст і знаходити закономірності у великих обсягах даних.
- Кластеризація використовується для групування схожих даних, що сприяє ідентифікації трендів або створенню сегментованих профілів.
- Візуалізація даних полегшує сприйняття результатів аналізу через графіки, діаграми чи карти.

Крім того, ШІ автоматизує обробку даних. Процеси очищення, нормалізації та анонімізації забезпечують підготовку високоякісного матеріалу для досліджень. Наприклад, видалення спаму чи дубльованої інформації значно покращує точність аналізу.

Етичні аспекти також відіграють важливу роль. Усі зібрані дані мають бути анонімними та використовуватися лише для освітніх цілей. Дотримання цих принципів гарантує відповідальне використання технологій.

Таким чином, використання ШІ для аналізу даних із соціальних мереж у навчальних цілях дозволяє студентам і дослідникам отримувати цінні знання, вивчати сучасні технології та розвивати практичні навички роботи з великими обсягами інформації.

1.4 Етичні та правові аспекти використання штучного інтелекту у зборі даних

1.4.1 Проблеми приватності та конфіденційності

Приватність та конфіденційність є фундаментальними аспектами сучасного цифрового світу, однак вони стикаються з численними викликами, які впливають на безпеку даних та особисту свободу. Однією з ключових проблем є масовий збір даних. Технологічні компанії, уряди та інші організації збирають величезні обсяги інформації про користувачів, що часто відбувається без їхньої явної згоди або усвідомлення. Ця інформація може включати особисті дані, звички користувачів, геолокацію, фінансові дані та навіть інтимні аспекти життя, що створює ризики для приватності.

Ще однією проблемою є недостатня прозорість у тому, як обробляються дані. Багато організацій не повідомляють чітко, як вони зберігають, використовують або передають інформацію. Це може призводити до зловживань, таких як продаж даних третім сторонам або їх використання для цілей, які не відповідають інтересам користувачів.

Важливим питанням є також ризики кіберзлочинності. Хакерські атаки, витоки даних та несанкціонований доступ до інформації можуть мати серйозні наслідки для індивідуумів і організацій. Наприклад, викрадення особистих даних може призводити до фінансових втрат, репутаційних ризиків та навіть до загроз фізичній безпеці.

Крім того, проблема приватності стає особливо актуальною в умовах поширення інтернету речей (IoT). Розумні пристрої, які збирають дані про користувачів, часто мають слабкі механізми захисту, що робить їх легкою мішенню

для кіберзлочинців. Такі пристрої також можуть збирати інформацію без чітко вираженої згоди користувачів, створюючи ризики для їхньої приватності.

Законодавчі аспекти також залишають бажати кращого. У багатьох країнах регулювання захисту даних є недостатньо розвиненим або не відповідає сучасним викликам. Навіть у випадках існування відповідних законів їхнє виконання часто залишається проблематичним через брак ресурсів або політичну волю.

Окремою проблемою є культура поведінки самих користувачів. Багато людей недостатньо обізнані про важливість захисту своєї інформації або нехтують базовими заходами безпеки, такими як використання надійних паролів чи двофакторної автентифікації. Це створює додаткові ризики для їхньої конфіденційності.

У сукупності ці виклики свідчать про те, що проблеми приватності та конфіденційності є комплексними і потребують узгоджених зусиль з боку урядів, бізнесу та громадянського суспільства. Захист персональних даних та забезпечення прозорості у використанні інформації мають стати пріоритетом для всіх учасників цифрового середовища, аби гарантувати безпечний і відповідальний розвиток сучасних технологій.

1.4.2 Етичні дилеми

У сучасному цифровому середовищі з’являються нові етичні дилеми, зокрема щодо зловживання даними та нечіткої відповідальності за дії автоматизованих систем, які потребують комплексного підходу та активної взаємодії урядів, бізнесу та громадянського суспільства.

Можливість зловживання даними в комерційних і політичних цілях є однією з найсерйозніших проблем. Величезні обсяги персональних даних, які збираються через онлайн-платформи, соціальні мережі та інші цифрові інструменти, можуть бути використані для маніпулювання поведінкою людей. У комерційному секторі це проявляється в таргетованій рекламі, коли компанії використовують зібрані дані для переконання користувачів у здійсненні покупки, навіть якщо вони не мали

наміру купувати товар. Часто ці дані продаються чи передаються третім сторонам, що порушує принципи конфіденційності. У політичному контексті зловживання даними може призводити до маніпулювання виборцями, як це сталося під час виборів 2016 року в США, де аналіз даних використовувався для створення політичних кампаній, що впливали на громадську думку. Ці технології також можуть сприяти поширенню фальшивих новин, що ускладнює процес інформування виборців і може негативно впливати на демократичні процеси.

Однією з найбільших проблем є відсутність прозорості у використанні персональних даних. Користувачі часто не розуміють, як їхні дані збираються, обробляються та передаються третім особам. Крім того, умови згоди на обробку даних зазвичай є складними і неповними, що ставить під загрозу приватність і права користувачів.

Нечіткість відповідальності за дії автоматизованих систем є ще однією серйозною етичною проблемою. Розвиток технологій штучного інтелекту та автоматизованих систем створює ситуації, коли важко визначити, хто несе відповідальність за рішення, ухвалені системами. Наприклад, коли автономний автомобіль потрапляє в аварію, хто має нести відповідальність — розробники програмного забезпечення, виробники автомобіля чи сама система? Це питання ще ускладнюється, якщо автоматизовані системи використовуються в інших галузях, наприклад, у фінансах чи медицині. Без чіткої правової бази, що регулює роботу таких систем, виникає ризик того, що ні одна зі сторін не візьме на себе відповідальність за наслідки помилок автоматизованих систем.

Ще одна проблема полягає в тому, що автоматизовані системи можуть бути налаштовані таким чином, щоб ухвалювати дискримінаційні рішення, що може призвести до соціальної нерівності, наприклад, в питаннях кредитування чи працевлаштування. Тому необхідно розробити правові норми, які забезпечать чесність і прозорість у використанні автоматизованих технологій.

Для ефективного вирішення цих етичних дилем потрібні чіткі правові норми, що регулюють використання даних та автоматизованих систем. Це включає забезпечення прозорості у використанні даних, захист персональної інформації,

визначення відповідальності за дії автоматизованих систем і розробку етичних стандартів для створення таких систем. Крім того, важливо забезпечити взаємодію між урядами, бізнесом і громадянським суспільством, щоб технології не завдавали шкоди людям і суспільству, а також гарантувати безпечний і відповідальний розвиток цифрового середовища.

1.4.3 Баланс між безпекою та приватністю

Баланс між безпекою та приватністю є важливою етичною дилемою в сучасному цифровому середовищі, де необхідно враховувати як потреби держави у забезпеченні національної безпеки, так і права громадян на захист їхньої особистої інформації. З одного боку, технології, що дозволяють збір та обробку персональних даних, є потужними інструментами для забезпечення безпеки: від боротьби з тероризмом та організованою злочинністю до протидії кіберзагрозам і запобігання загрозам на глобальному рівні. Дані, отримані з різних джерел — соціальних мереж, онлайн-платформ, систем відеоспостереження, фінансових операцій — дозволяють державним органам своєчасно виявляти потенційні загрози та приймати необхідні заходи для їхнього усунення.

З іншого боку, ці ж технології можуть стати інструментом порушення приватності. Постійний моніторинг, збирання і зберігання особистих даних без належного контролю можуть призвести до порушень прав людини. Якщо держави чи корпорації можуть без обмежень отримувати доступ до особистої інформації, це створює ризик для свободи слова, приватності та навіть для особистої безпеки громадян. Без належного захисту ці дані можуть бути використані не лише для боротьби з кримінальними загрозами, а й для політичних маніпуляцій, дискримінації чи економічної експлуатації.

Тому важливо знайти правильний баланс між цими двома потребами. Суспільство повинно мати гарантії, що його права на приватність не будуть порушені в ім’я безпеки. Водночас держави та бізнес повинні розробити чіткі механізми для контролю за використанням особистих даних і забезпеченням їхньої безпеки, аби уникнути зловживань і забезпечити прозорість у процесах збору і

обробки даних. Цей баланс може бути досягнутий тільки через активну взаємодію урядів, технологічних компаній та громадянського суспільства для розробки етичних стандартів і правових норм, що захищають як безпеку, так і приватність осіб.

1.5 Висновки до розділу 1

У сучасному світі питання збору, обробки та захисту персональних даних стає дедалі важливішим, оскільки вони є основою функціонування цифрового суспільства. Різноманітність персональних даних та їх класифікація за функціональним призначенням, ступенем чутливості та способами обробки дозволяють визначити важливі аспекти їхнього використання й забезпечення безпеки. Одним із серйозних викликів є зростання кількості кібератак, зокрема через використання соціальної інженерії, яка спрямована на маніпуляцію людьми для отримання конфіденційної інформації. Військові конфлікти, як, наприклад, війна між Україною та Росією, лише підвищують значення захисту персональних даних, оскільки зловмисники активно використовують методи соціальної інженерії та кібератаки для саботажу, шантажу та викрадення даних. У цих умовах необхідно посилювати цифрову грамотність населення, впроваджувати багаторівневі системи захисту і забезпечувати гармонізацію національного законодавства з міжнародними стандартами. Проблеми, пов'язані з етикою та правовими аспектами збору даних, також набувають значення, оскільки порушення прав на приватність та конфіденційність можуть призвести до серйозних наслідків як для індивідуумів, так і для суспільства загалом. Використання штучного інтелекту для збору та аналізу даних відкриває нові можливості, однак потребує ретельного контролю та дотримання етичних стандартів. Останні тенденції вимагають пошуку балансу між безпекою та правами громадян, де повинні враховуватися інтереси держави та забезпечення конфіденційності особистої інформації, що вимагає спільних зусиль урядів, бізнесу та громадянського суспільства для створення ефективної та справедливої нормативної бази.

РОЗДІЛ 2. РОЗРОБКА АРХІТЕКТУРИ НАВЧАЛЬНОЇ СИСТЕМИ ДЛЯ СИМУЛЯЦІЇ МЕТОДУ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

2.1 Огляд сучасних навчальних систем для вивчення соціальної інженерії

У цьому розділі ми розглянемо існуючі навчальні платформи, що вже використовуються для навчання соціальної інженерії. Ці системи включають онлайн-курси, тренінги, а також інструменти для симуляцій атак. На основі аналізу цих систем було створено телеграм-бота знайомств, який дозволяє користувачам застосовувати отримані теоретичні знання про соціальну інженерію в інтерактивному чаті. Бот використовує принципи соціальної інженерії для навчання користувачів взаємодії в онлайн-середовищі, створюючи практичний досвід, що наближається до реальних ситуацій.

2.1.1 Coursera. Курси з соціальної інженерії

Coursera — одна з найбільших онлайн-освітніх платформ, що пропонує курси з різних дисциплін, включаючи кібербезпеку. Одним з найбільш популярних курсів є "Social Engineering: The Art of Human Hacking" від університету Мічігану, який навчає базовим принципам соціальної інженерії. Курс охоплює різноманітні методи атак, такі як фішинг, вишинг і скамерство, а також вивчає психологічні аспекти, які використовуються для маніпуляції людьми. Також надаються стратегії захисту, що допомагають виявити і зупинити ці атаки.

Контент курсу: Основи соціальної інженерії, методи атак, психологія маніпуляцій, стратегії захисту, практичні завдання.

Переваги: Безкоштовний доступ до лекцій (якщо не потрібен сертифікат), можливість отримати сертифікат після завершення курсу, визнана міжнародна платформа.

Недоліки: Курси зосереджені на теоретичних знаннях, відсутність глибоких практичних навичок.

2.1.2 Offensive Security: OSCP та інструменти для соціальної інженерії

Offensive Security є провідною платформою для навчання етичних хакерів. Їхня сертифікаційна програма OSCP (Offensive Security Certified Professional) включає елементи соціальної інженерії, даючи студентам можливість розуміти та застосовувати різні методи проникнення в системи, зокрема через маніпулювання людьми. Програма включає навчання роботі з Social-Engineer Toolkit (SET) та Phishing Frenzy, що дозволяє студентам відтворювати фішингові атаки в контрольованому середовищі.

Контент курсу: Використання інструментів для фішингових атак, практичні завдання з проникнення через соціальну інженерію, симуляція реальних сценаріїв атак.

Переваги: Глибоке занурення в практичні аспекти тестування безпеки, використання реальних інструментів, можливість отримати сертифікат.

Недоліки: Підходить для досвідчених фахівців, може бути складно для початківців.

2.1.3 SANS Institute. Навчання з кібербезпеки

SANS Institute є однією з найвідоміших освітніх організацій, що пропонує сертифікаційні курси з кібербезпеки. У курсі SEC301: Introduction to Cyber Security викладаються основи соціальної інженерії, зокрема методи фішингу, вишингу та бейтінгу, а також застосування інструментів для виявлення цих загроз. Курс містить інтерактивні лабораторії та практичні завдання, що дозволяють учасникам застосовувати теоретичні знання на практиці.

Контент курсу: Вивчення методів соціальної інженерії, інструменти для захисту, практичні завдання з тестування безпеки.

Переваги: Інтерактивні лабораторії, міжнародно визнана сертифікація, комплексний підхід.

Недоліки: Вартість навчання може бути високою, підходить більше для фахівців середнього та високого рівня.

2.1.4 KnowBe4: Тренінги з обізнаності в сфері безпеки

KnowBe4 спеціалізується на навчанні співробітників компаній щодо безпеки через тренінги з соціальної інженерії. Платформа пропонує симуляції фішингових атак, навчання розпізнаванню підозрілих повідомлень і загроз, а також модулі для підвищення загальної обізнаності про кіберзагрози. Крім того, KnowBe4 пропонує спеціалізовані програми для різних категорій співробітників.

Контент курсу: Симуляції фішингових атак, тренінги з розпізнавання соціальних маніпуляцій, інтерактивні модулі.

Переваги: Регулярне оновлення курсу, спеціалізовані тренінги для різних працівників.

Недоліки: Орієнтовано на організації, що може бути менш корисним для індивідуальних користувачів.

2.1.5 Udemy: Курси з кібербезпеки та соціальної інженерії

Інструменти, такі як Cofense та Proofpoint, дозволяють організаціям створювати та запускати симуляції фішингових атак, допомагаючи навчити співробітників реагувати на реальні загрози. Ці інструменти дозволяють створювати умовні фішингові атаки, оцінювати ефективність захисту і навчати користувачів правильно реагувати на підозрілі ситуації.

Контент курсу: Симуляції фішингових атак, тренування на виявлення підозрілих повідомлень, відстеження результатів і аналітика.

Переваги: Можливість адаптувати сценарії під потреби організації, реалістичні симуляції

Udemy — це популярна онлайн-платформа для навчання, що надає численні курси з кібербезпеки, зокрема з соціальної інженерії. Курси на Udemy часто

включають практичні приклади реальних атак та тренінги з виявлення фішингових атак. Деякі з курсів з соціальної інженерії є доступними за низькою ціною, що робить платформу доступною для більш широкої аудиторії.

Контент курсу: Основи соціальної інженерії, реальні приклади атак, фішинг, скамерство, стратегії захисту.

Переваги: Широкий вибір курсів на будь-який рівень підготовки, доступні ціни та часті знижки.

Недоліки: Якість курсів може змінюватись в залежності від інструктора, багато матеріалів потребують додаткового контексту для новачків.

2.1.6 EC-Council: Курси з етичного хакерства та соціальної інженерії

EC-Council є відомою організацією, що спеціалізується на навчанні етичних хакерів. Вона пропонує курс Certified Ethical Hacker (CEH), в якому велика увага приділяється соціальній інженерії, як частині тестування на проникнення та методів, що використовуються при виявленні слабких місць у безпеці. Курси сертифікації CEH включають практичні завдання, де учасники навчаються використовувати інструменти, такі як Social-Engineer Toolkit (SET).

Контент курсу: Інструменти для фішингових атак, маніпулювання людьми, етичне тестування безпеки, принципи соціальної інженерії.

Переваги: Визнана міжнародна сертифікація, фокус на реальних сценаріях атак.

Недоліки: Вартість сертифікації може бути високою, що обмежує доступ для деяких користувачів.

Розглянуті навчальні платформи та інструменти є важливими ресурсами для вивчення соціальної інженерії. Курси на Coursera, Offensive Security, SANS Institute, KnowBe4, а також інструменти для симуляцій фішингових атак допомагають фахівцям з кібербезпеки розвивати необхідні навички для виявлення та протидії соціальним атакам. На основі цього аналізу був створений телеграм-бот знайомств, який використовує елементи соціальної інженерії для навчання

користувачів взаємодії через чат. Бот дозволяє застосовувати теоретичні знання про соціальну інженерію в безпечному і контрольованому середовищі, що сприяє розвитку практичних навичок у реальному часі.

2.2 Концепція навчальної системи

Метою створення навчальної системи є підвищення обізнаності користувачів про методи соціальної інженерії, які базуються на маніпуляціях людськими емоціями, довірою та бажанням взаємодії. Для цього пропонується розробка Telegram-бота, який симулюватиме платформу для знайомств. Такий підхід дозволяє ефективно продемонструвати користувачам, як звичайне спілкування може використовуватись для збору персональних даних, що є однією з ключових технік соціальної інженерії.

Telegram обрано як платформу для розробки з кількох причин. По-перше, це один із найпопулярніших месенджерів в Україні, який має велику аудиторію користувачів. По-друге, Telegram забезпечує широкий набір інструментів для розробки ботів, таких як інтерактивні меню, обробка повідомлень та інші функції, що дозволяють створити зручний і зрозумілий інтерфейс для навчання.

Навчальний бот працюватиме за принципом платформи для знайомств. Користувачі будуть взаємодіяти з ботом, який у формі діалогу поступово запитуватиме різну інформацію: базові персональні дані (ім’я, вік, місце проживання), уподобання, звички та навіть відповіді на сценарії, що можуть здаватися дружніми або невинними. Таким чином, бот демонструватиме, як дані, надані добровільно, можуть бути використані для створення баз даних.

2.3 Використання штучного інтелекту у зборі персональних даних та його аналіз у використанні в навчальній архітектурі

Штучний інтелект (ШІ) є одним із найбільш інноваційних інструментів сучасності, здатним значно спрощувати та автоматизувати процеси збору, аналізу

та обробки даних. Однак його використання у сфері персональних даних створює серйозні ризики для конфіденційності користувачів. Завдяки потужним алгоритмам машинного навчання, ШІ дозволяє створювати автоматизовані системи, здатні виконувати складні завдання, які раніше потребували участі людини. У контексті соціальної інженерії ці технології стають ще небезпечнішими, оскільки дозволяють масштабувати атаки, робити їх персоналізованими та практично невидимими для жертв.

Одна з основних загроз ШІ – це автоматизація створення фейкових профілів. Генеративні моделі ШІ можуть створювати реалістичні анкети, що включають вигадані імена, фотографії, професії, уподобання та іншу персональну інформацію, яка виглядає достовірно. Такі фейкові профілі можуть бути інтегровані в Telegram-боти, які симулюють сервіси знайомств. Боти, оснащені алгоритмами ШІ, здатні вести діалоги, які імітують реальну поведінку людини, викликати довіру та спонукати користувачів ділитися особистою інформацією.

Ця технологія також дозволяє масштабувати атаки. Один бот із застосуванням ШІ може взаємодіяти з тисячами користувачів одночасно, збираючи дані про кожного з них. Зібрана інформація може включати базові персональні дані (ім'я, вік, місце проживання), соціальні зв’язки, інтереси та навіть відповіді на сценарії, що здаються невинними. Усе це використовується для створення великих баз даних, які можуть бути продані, використані для таргетованих атак або для інших шкідливих цілей.

Ще однією небезпекою є адаптивність алгоритмів ШІ. Вони здатні аналізувати поведінку користувачів у реальному часі та підлаштовувати стратегію взаємодії, щоб максимально ефективно збирати інформацію. Наприклад, якщо користувач проявляє недовіру, бот може змінити тон або зменшити кількість запитів, поки не отримає потрібну відповідь.

У розробленій навчальній архітектурі Telegram-бота також буде застосовано технології ШІ для демонстрації потенційних загроз. Бот симулюватиме фейкові профілі, створені на основі генеративних моделей, які включатимуть реалістичні фотографії та дані, що виглядають правдоподібно. Крім того, завдяки алгоритмам

обробки природної мови (NLP), бот зможе вести динамічні діалоги, які адаптуються до відповіді користувача, імітуючи реальну взаємодію. Це дозволить на практиці продемонструвати, як ШІ використовується для маніпулювання людьми та збору інформації.

У рамках навчального сценарію користувачі зможуть побачити, як фейковий профіль викликає довіру та поступово збирає персональні дані. Такий підхід не тільки покаже ризики, пов'язані із соціальною інженерією, але й продемонструє реальні механізми роботи ШІ, підвищуючи цифрову грамотність користувачів. Таким чином, інтеграція ШІ в навчальну архітектуру Telegram-бота дозволяє створити реалістичну та ефективну платформу для навчання, яка допоможе користувачам зрозуміти сучасні ризики та методи захисту від атак соціальної інженерії.

В наступних підрозділах обґрунтуємо вибір програмного середовища.

2.4 Фреймворк Aiogram

Для створення чат-бота, що збирає персональні дані користувачів з навчальною метою, було обрано фреймворк aiogram. Це Python-фреймворк, який займає лідируючі позиції серед інструментів розробки Telegram-ботів завдяки своїй гнучкості, потужності та простоті використання. Його використання забезпечує численні переваги, які є ключовими для ефективної реалізації сучасних програмних рішень.

Aiogram побудований на основі бібліотеки asyncio, що дозволяє обробляти багато запитів одночасно, оптимізуючи використання ресурсів. Завдяки асинхронній архітектурі, бот здатний швидко реагувати на дії користувачів, навіть за умов високого навантаження. Це робить його ідеальним рішенням для платформ, орієнтованих на масштабованість і швидкодію.

Aiogram пропонує інтуїтивно зрозумілий інтерфейс для взаємодії з Telegram Bot API. Усі операції, від відправлення повідомлень до обробки мультимедійних

файлів, реалізуються через зрозумілі й добре документовані методи. Це значно скорочує час на розробку функціональності та мінімізує ризик помилок.

Завдяки потужним механізмам маршрутизації, таким як Dispatcher та система фільтрів, aiogram дозволяє налаштовувати обробку повідомлень з високою точністю. Це особливо важливо для ботів, які працюють із персональними даними, оскільки необхідно забезпечити коректну валідацію введеної інформації та її подальшу обробку.

Aiogram підтримує модульну архітектуру, що дозволяє розробникам структурувати код у логічно ізольовані блоки. Це сприяє легкості в обслуговуванні, тестуванні та розширенні функціональності. Наприклад, можна створити окремі модулі для обробки реєстрації користувачів, збору аналітики або інтеграції сторонніх сервісів.

Фреймворк дозволяє легко інтегруватися з різними базами даних, забезпечуючи збереження та обробку персональних даних користувачів. Використання ORM-бібліотек, таких як SQLAlchemy або Peewee, або пряме підключення до баз даних, наприклад, PostgreSQL чи SQLite, надає розробникам широкий вибір засобів для організації зручної та безпечної роботи з даними.

Aiogram має активну спільноту розробників, яка постійно оновлює документацію та ділиться прикладами реалізації складних задач. Це суттєво спрощує навчання, дає змогу знаходити готові рішення для типових проблем та підтримує впевненість у виборі цього інструменту.

Завдяки гнучким налаштуванням, aiogram дозволяє створювати унікальні сценарії роботи бота, інтегрувати зовнішні сервіси, налаштовувати вебхуки та розширювати функціональність відповідно до потреб проєкту. Це відкриває широкі можливості для створення висококласних програмних рішень.

Aiogram забезпечує високий рівень захисту персональних даних, використовуючи шифрування та засоби контролю доступу. Це критично важливо для забезпечення конфіденційності інформації, що обробляється ботом, особливо у випадку роботи з чутливими даними користувачів.

Завдяки регулярним оновленням фреймворку, aiogram завжди відповідає актуальним вимогам Telegram Bot API. Це дозволяє розробникам швидко адаптувати бота до нових функцій та змін у платформі, гарантуючи безперебійну роботу навіть у довгостроковій перспективі.

Використання aiogram для створення чат-бота є оптимальним вибором завдяки його продуктивності, гнучкості, безпеці та зручності у використанні. Фреймворк дозволяє швидко та ефективно реалізувати навіть найскладніші функціональні вимоги, забезпечуючи стабільність і високу якість кінцевого продукту. Його можливості роблять його потужним інструментом як для навчальних, так і для комерційних проєктів, сприяючи успішній реалізації цілей та розвитку сучасних технологій.

2.5 База даних SQL

У рамках розробки бота для знайомств з навчальною метою було використано базу даних SQLite для збереження та управління персональними даними користувачів. SQLite є ефективним інструментом для забезпечення зручного та структурованого способу роботи з даними, що дозволяє реалізувати широкий спектр функціональності бота та досягти навчальних і дослідницьких цілей.

SQLite було обрано через низку її переваг. По-перше, це автономна база даних, яка не потребує встановлення серверного середовища. Всі дані зберігаються в одному файлі, що робить її легкою у використанні та інтеграції. По-друге, SQLite є дуже легкою за ресурсоспоживанням, що дозволяє ефективно використовувати її навіть у малих проєктах, таких як бот для знайомств. Крім того, вона забезпечує високу швидкість роботи та підтримує можливість шифрування даних для підвищення безпеки.

База даних була використана для зберігання персональних даних користувачів, включаючи ім'я, вік, інтереси, місцезнаходження та іншу

інформацію, введену користувачами. Підтримки функціональності бота, такої як пошук відповідних співрозмовників або створення динамічних відповідей.

Особливу увагу приділено використанню персональних даних у навчальних цілях. У рамках проєкту було передбачено моделювання створення фішингових розсилок, що дозволяє дослідити механізми соціальної інженерії. Індивідуалізовані повідомлення, створені на основі зібраних даних, допомагають вивчити вплив таких факторів на поведінку користувачів. Це також підкреслює важливість захисту персональних даних та необхідність розробки ефективних заходів інформаційної безпеки.

Розроблено таблиці для зберігання різних типів даних, таких як профілі користувачів, історія взаємодій та параметри вподобань.

Використано механізми перевірки даних, включаючи обмеження на рівні бази, щоб уникнути дублювання та забезпечити коректність інформації.

Застосовано індексацію для підвищення швидкості виконання основних операцій, таких як пошук відповідностей серед користувачів.

Зважаючи на чутливий характер даних, важливим аспектом реалізації стало впровадження заходів безпеки. Було використано методи шифрування для зберігання конфіденційних даних, а також обмеження доступу до бази даних. Це дозволило знизити ризик несанкціонованого доступу та забезпечити конфіденційність інформації.

Завдяки використанню SQLite вдалося досягти як практичних, так і теоретичних результатів. З одного боку, це забезпечило повноцінну роботу бота, який ефективно взаємодіє з користувачами. З іншого боку, було розкрито потенційні ризики, пов'язані з використанням персональних даних, що сприяє кращому розумінню необхідності їх захисту.

Досвід, отриманий у процесі роботи, дозволяє не лише поглибити знання у сфері роботи з базами даних, але й підготувати рекомендації щодо впровадження інформаційної безпеки у подібних системах. Цей підхід демонструє важливість комплексного підходу до розробки сучасних інформаційних технологій.

2.6. Висновки до розділу 2

У сучасних умовах кіберзагроз та інформаційних маніпуляцій питання безпеки персональних даних і протидії соціальній інженерії набуло критичного значення. Особливо це стосується України, де війна з Росією супроводжується масованими атаками на цифрові системи та інформаційну інфраструктуру. У такій ситуації розробка системи, яка допомагає виявляти вразливості в поведінці користувачів і навчати їх ефективній протидії маніпуляціям, стає не просто актуальною, а необхідною.

Розроблена навчальна система має на меті не тільки імітувати сценарії атак, але й навчати користувачів на основі їх взаємодії з ботом. Вибір платформи Telegram для реалізації цього інструменту пояснюється її популярністю серед українських користувачів, а також гнучкістю API, що дозволяє створювати складні сценарії взаємодії. Інтерактивний формат бота надає можливість навчатися через практику, дозволяючи користувачам відчути на власному досвіді, як зловмисники можуть використовувати їхню довіру для збору конфіденційної інформації.

Необхідність створення саме такої системи обумовлена кількома ключовими факторами:

Під час війни кібератаки та маніпуляції з використанням персональних даних стають ще більш небезпечними. Атаки, які спрямовані на українських військових, волонтерів та громадян, мають на меті не лише збір даних, а й створення інформаційного хаосу, підрив морального духу та дискредитацію.

Успішність багатьох атак сьогодні залежить не стільки від технічних вразливостей, скільки від людського фактора. Люди залишаються найбільш уразливим елементом будь-якої системи захисту. Маніпуляції довірою, страхом або цікавістю дозволяють зловмисникам отримувати доступ до цінної інформації.

Більшість існуючих рішень для навчання в сфері кібербезпеки орієнтовані на фахівців і мають високу вартість. Розроблений бот пропонує доступний спосіб підвищити обізнаність про ризики соціальної інженерії для широкої аудиторії. На основі цього бота, можна показати успішний кейс збору даних користувачів, який

в подальшому може використовуватись про ти їх відому та може нашкодити користувачам, які потенційно можуть реєструватись на схожих сервісах.

Одним із важливих завдань було забезпечення етичності використання бота. Усі сценарії взаємодії розроблені так, щоб уникнути збирання чутливих даних або використання їх не за призначенням. Крім того, система акцентує увагу на важливості захисту приватності та етичному ставленні до обробки персональної інформації.

Бот здатний підлаштовувати сценарії під реакції користувача, що робить навчання більш персоналізованим.

Використання елементів штучного інтелекту дозволяє системі аналізувати відповіді користувачів і надавати зворотний зв’язок у реальному часі.

Telegram є популярною платформою, доступною на різних пристроях, що забезпечує широке охоплення аудиторії.

Тестування системи продемонструвало її здатність підвищувати обізнаність користувачів і допомагати їм уникати небезпечних ситуацій у реальному житті.

Війна в Україні висвітлила нові виклики для кібербезпеки, зокрема пов’язані з інформаційними маніпуляціями. Система навчання, що базується на реалістичних сценаріях, дозволяє ефективно імітувати можливі атаки й навчати користувачів протидіяти їм. Це не лише підвищує їхній рівень цифрової грамотності, а й зміцнює загальну кібербезпеку країни.

У подальшій роботі планується розширення функціоналу бота, додавання можливість інтеграції з іншими освітніми платформами. Крім того, розвиток системи може включати аналіз більш складних моделей поведінки користувачів за допомогою штучного інтелекту, що зробить бота ще ефективнішим.

РОЗДІЛ 3 ВПРОВАДЖЕННЯ СИСТЕМИ ЗБОРУ ПЕРСОНАЛЬНИХ ДАНИХ

3.1 Реалізація чат-бота для збору персональних даних

У цьому підрозділі детально розглядається процес створення, тестування та використання чат-бота, здатного автоматизовано збирати персональні дані. Цей інструмент був розроблений виключно у навчальних цілях і демонструє практичне застосування сучасних технологій штучного інтелекту для імітації кіберзагроз, таких як фішинг.

Основною метою розробки було підвищення обізнаності про методи, які використовуються зловмисниками для збору персональної інформації, а також вдосконалення навичок ідентифікації кіберзагроз серед цільової аудиторії. Чат-бот забезпечує моделювання реальних фішингових атак у контрольованому середовищі.

Чат-бот розроблено на базі фреймворку для створення Telegram-ботів із використанням мови програмування Python. Основні функціональні можливості включають:

- Динамічний діалог із користувачем: Бот здатний адаптувати свої відповіді залежно від введеної інформації, використовуючи алгоритми обробки природної мови (NLP).
- Збір даних через інтерактивні форми: Бот пропонує користувачам заповнювати форми з метою збору імені, віку, локації, уподобань тощо.
- Імітація фішингових методів: У сценарії роботи бота інтегровано функції, які імітують фішингові прийоми, наприклад:

Пропозиції вигідних акцій для стимулювання введення даних, імітація дизайну й комунікаційних стилів відомих сервісів, запити персональної інформації через анкети.

Зберігання даних у базі: Бот використовує локальну базу даних SQLite для тимчасового зберігання інформації, що допомагає аналізувати поведінку користувачів у межах експерименту.

Бот складається з таких основних компонентів:

- Модуль управління станами: Використовується для керування сценаріями взаємодії із користувачем.
- Сценарії збору даних: Розроблені для поступового отримання персональної інформації через запити, які виглядають максимально автентично.
- Функціонал зворотного зв'язку: Забезпечує миттєве реагування на відповіді користувачів, адаптуючи наступні запити.

Для дотримання етичних норм і забезпечення безпеки:

- Бот працює виключно в тестовому середовищі.
- Усі персональні дані знеособлюються та автоматично видаляються після завершення експерименту.
- Учасники експерименту попередньо дають згоду на участь у -дослідженні.
- Результати тестування.

Тестування бота показало його ефективність у моделюванні реальних фішингових сценаріїв. Було встановлено, що:

- Користувачі частіше вводять дані, якщо повідомлення виглядає офіційно.
- Автоматизація сценаріїв дозволяє ідентифікувати найбільш вразливі точки в поведінці користувачів.
- Інтеграція інструментів NLP значно покращує природність спілкування.

Таким чином, цей бот не тільки демонструє можливості сучасних технологій, але й підвищує рівень обізнаності про ризики, пов'язані з фішингом, серед цільової аудиторії.

3.2 Інтеграція штучного інтелекту в розробці

Штучний інтелект (ШІ) є потужним інструментом, що дозволяє автоматизувати різноманітні процеси, зокрема створення фейкових анкет для телеграм-ботів у навчальних цілях. У цьому розділі розглянуто, як саме ШІ допомагає виконувати цю задачу, які методи і технології використовуються, а також які є переваги та ризики такого підходу.

Основні етапи створення фейкових анкет:

- Збір вимог та аналіз даних. Перед початком генерації необхідно визначити, які саме дані повинні містити фейкові анкети. Це можуть бути такі параметри, як ім'я, вік, місто проживання, інтереси, професія тощо. Зібрані вимоги допомагають створити реалістичні профілі, які відповідатимуть очікуванням користувачів бота.

- Генерація текстових даних ШІ-моделі, такі як GPT (Generative Pre-trained Transformer), використовуються для створення текстових даних. Наприклад, вони можуть генерувати реалістичні імена, вигадані біографії або описи інтересів. Такі моделі навчаються на великих наборах текстових даних і здатні враховувати контекст для створення правдоподібної інформації.

- Синтетичні зображення Якщо анкета включає фотографії, для їх створення можна використовувати генеративно-змагальні мережі (GANs – Generative Adversarial Networks). Ці мережі здатні створювати реалістичні зображення осіб, які не існують у реальності. Важливим є те, що використання таких підходів дозволяє уникати порушення конфіденційності, адже створені особи є повністю вигаданими.

- Автоматизація процесу Для інтеграції з телеграм-ботом необхідно автоматизувати процес створення анкет. Це можна зробити за допомогою програмування на Python, використовуючи API для телеграм-ботів та бібліотеки, які забезпечують взаємодію зі ШІ-моделями. Автоматизація дозволяє генерувати анкети у великих кількостях і забезпечувати їх швидке завантаження в базу бота.

- Адаптація до специфіки бота Залежно від функціоналу телеграм-бота, можна створювати анкети, які підходять для певних сценаріїв використання. Наприклад, для чат-ботів, що спрямовані на соціальні опитування, анкети можуть містити більше деталей щодо особистих інтересів чи соціально-демографічних характеристик. Для ботів, які моделюють підтримку клієнтів, основний акцент робиться на коротких, чітких відповідях.

Переваги використання ШІ для генерації фейкових анкет:

- Швидкість і масштабованість. ШІ дозволяє створювати сотні або навіть тисячі анкет за короткий час.

- Реалістичність. Завдяки сучасним технологіям, створені анкети виглядають переконливо, що робить їх ідеальними для тестування.

- Зниження витрат. Використання ШІ зменшує потребу в ручній роботі, що економить час і ресурси.

- Гнучкість. Можливість адаптації під специфічні вимоги дозволяє використовувати анкети в різноманітних сценаріях.

Попри значні переваги, використання ШІ для створення фейкових анкет має і певні ризики:

- Етичні питання. Використання фейкових даних може викликати моральні дилеми, особливо якщо ці дані використовуються поза межами навчальних або дослідницьких цілей.

- Потенційне зловживання. Фейкові анкети можуть бути використані для шахрайства або дезінформації, якщо вони потраплять у руки недобросовісних осіб.

- Технічні обмеження. Навіть найкращі моделі іноді можуть генерувати некоректні або нелогічні дані, що впливає на якість анкет.

- Вплив на довіру. Використання фейкових даних у реальних умовах може знизити довіру до платформи або продукту, якщо користувачі дізнаються про це.

Попри все, в реалізації даної роботи було дотримано наступні правові та етичні норми:

- Використання лише в межах законодавства. Генерація фейкових анкет має відбуватися виключно у законних і етичних цілях.

- Прозорість. Для дослідницьких проєктів бажано зазначати, що анкети є синтетичними, щоб уникнути можливих непорозумінь.

- Контроль якості. Регулярна перевірка згенерованих даних допоможе уникнути помилок та недоліків.

Штучний інтелект відкриває широкі можливості для автоматизації процесу створення фейкових анкет у телеграм-ботах, що є особливо корисним у навчальних цілях. Використання таких технологій дозволяє прискорити тестування функціональності бота та створити реалістичні сценарії його взаємодії з

користувачами. Водночас необхідно враховувати етичні аспекти та дотримуватися принципів відповідального використання ШІ, щоб мінімізувати можливі ризики.

3.3 Тестування бота для збору персональних даних

3.3.1 Процес реєстрації

Реєстрація реалізована за допомогою станів (FSMContext), що дозволяє зберігати поточний етап і дані, введені користувачем, до моменту завершення процесу. Інтерактивні кнопки та повідомлення адаптовані до мови користувача (українська, або англійська). Бот використовує перевірки на кожному етапі, щоб уникнути некоректних даних.

Користувач може пропустити певні етапи (наприклад, завантаження фото), але все одно успішно завершити реєстрацію. Використання різних мов та персональних налаштувань дозволяє адаптувати бот до потреб користувачів. Користувачу надається чітке керівництво, що спрощує процес заповнення анкети. Таким чином, бот надає інтуїтивно зрозумілий та добре структурований процес реєстрації, забезпечуючи високу якість зібраних персональних даних.

Ініціація процесу реєстрації. Процес починається після того, як користувач надсилає команду /start або обирає кнопку " Створити анкету" в головному меню (рис 3.1.1). Бот відправляє привітальне повідомлення, яке залежить від мови, заданої для користувача. Якщо мова ще не вибрана, за замовчуванням використовується українська. Відразу після привітання бот запитує ім'я користувача, щоб розпочати створення анкети.

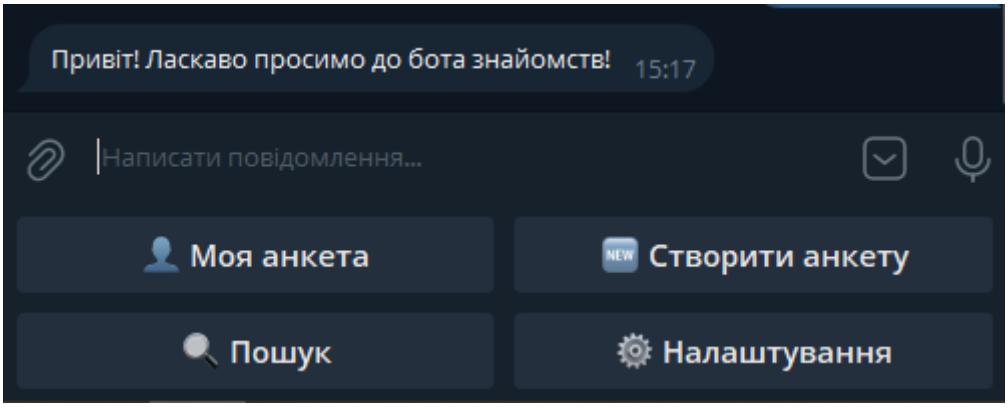

Рисунок.3.1 - Демонстрація головного меню

Процес збору даних розділений на кілька етапів, кожен з яких супроводжується перевіркою введених даних. Ось як це відбувається:

- Ім'я. Бот запитує ім'я користувача: *"Введіть ваше ім'я:"*. Перевіряє, щоб ім'я не було порожнім, і зберігає його у тимчасовому сховищі станів.
- Вік
- Наступний запит: *"Введіть ваш вік:"*.

Бот перевіряє, чи є введене значення числом, і чи знаходиться вік у дозволеному діапазоні (18-99 років). Якщо дані некоректні, бот просить ввести правильне значення.

Опис

Користувач отримує запит на короткий опис про себе: *"Розкажіть трохи про себе:"*.

Опис також перевіряється на заповненість.

Гендер

Бот пропонує вибрати гендер (чоловік чи жінка) за допомогою кнопок:

- "Чоловік"
- "Жінка"

Введений вибір зберігається, а бот переходить до наступного етапу рис(3.1.2).

Переваги

Користувач вказує, кого він шукає (чоловіків, жінок чи всіх). Це робиться через кнопки:

- "Чоловік"
- "Жінка"
- "Всі"
- Локація
- Запитується місто проживання: "Вкажіть ваше місто:".

Бот зберігає відповідь без додаткових перевірок.

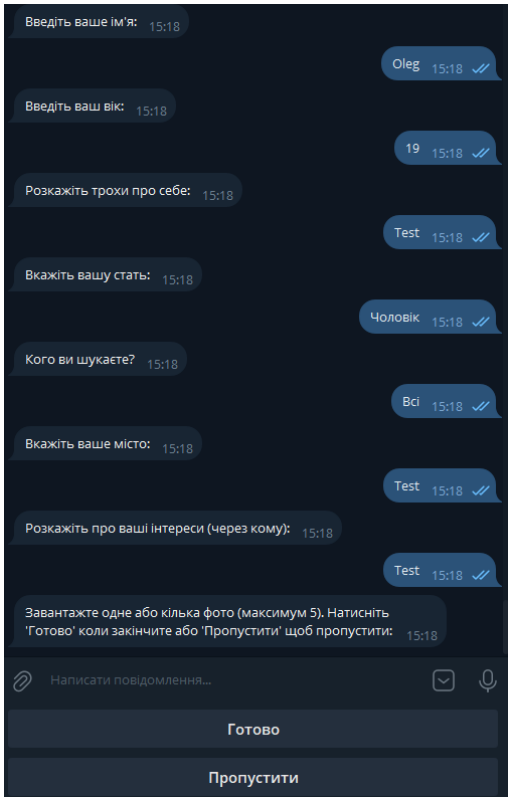

Рисунок. 3.2 - Демонстрація системи реєстрації.

Останній текстовий запит: *"Розкажіть про ваші інтереси (через кому):"*Користувач вводить список інтересів, який буде використаний для пошуку збігів.

Користувачу пропонується завантажити до п'яти фотографій для свого профілю.

На екрані відображається запит: "Завантажте одне або кілька фото (максимум 5). Натисніть 'Готово', коли закінчите, або 'Пропустити', щоб пропустити цей крок.".

Якщо користувач завантажує більше ніж п'ять фотографій, бот повідомляє про перевищення ліміту. Користувач також може натиснути кнопку *"Пропустити"*, щоб завершити реєстрацію без фотографій.

Після завершення збору всіх даних (або пропуску етапу завантаження фотографій), бот зберігає анкету користувача в базі даних SQLite. У базі створюється запис з такими полями:

- user_id – унікальний ідентифікатор користувача.

- name – ім'я.
- age – вік.
- bio – короткий опис.
- gender – гендер.
- preference – кого шукає.
- location – місто проживання.
- interests – інтереси.
- photos – список фото (або NULL, якщо фото відсутні).
- language – вибрана мова інтерфейсу.
- username – Telegram-юзернейм.

Бот надсилає повідомлення про успішне створення анкети: *"Анкета успішно створена!"*.

Користувач повертається до головного меню. Демонстрація готової анкети представлена на рисунку 3.3

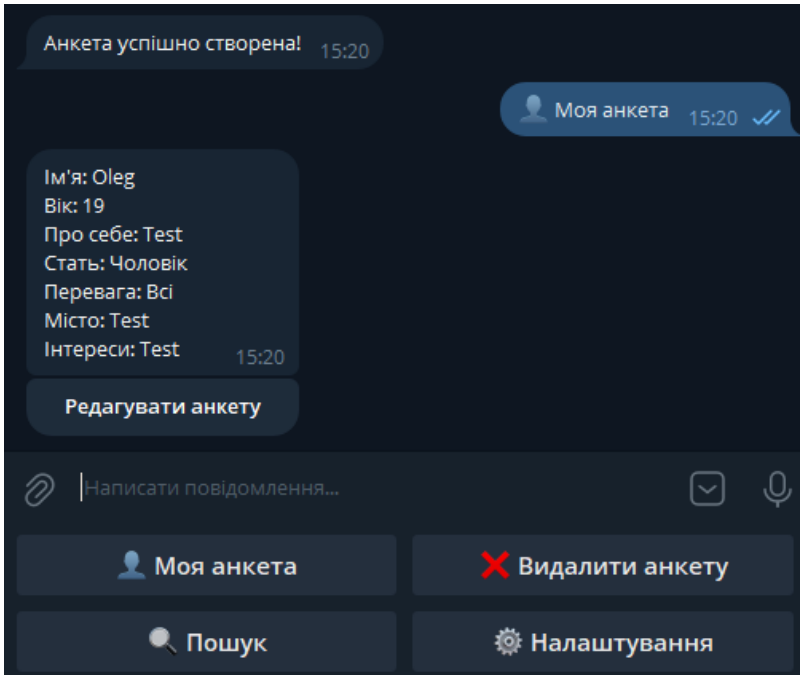

Рисунок.3.3 - Демонстрація готової анкети

Ця система збору персональних даних у навчальних цілях має такі особливості та можливості Завдяки зібраним даним (таким як унікальний ідентифікатор користувача, збережений у базі даних), можна чітко ідентифікувати кожного учасника. Це дає змогу відстежувати взаємодії користувачів із ботом і аналізувати їх поведінку в різних сценаріях. Час від часу бот може надсилати користувачам спеціальні повідомлення із посиланнями на умовно фішингові сайти. Ці повідомлення служать для імітації реальних загроз із метою навчити користувачів розпізнавати такі ризики. Система відстежує, як користувачі взаємодіють із фішинговими посиланнями — чи переходять за ними, чи ігнорують, чи повідомляють про підозрілі повідомлення. Це допомагає зрозуміти слабкі сторони у поведінці користувачів і розробити рекомендації для їх усунення.

Надсилання фішингових повідомлень із наступним поясненням їх небезпеки сприяє формуванню в користувачів навичок ідентифікації шахрайських схем. Це забезпечує підготовку до реальних кіберзагроз.

Дані та аналіз, отримані завдяки роботі цього чат-бота, можуть стати базою для створення більш ефективних систем кібербезпеки, а також програм навчання для широкої аудиторії.

Для першочергового заповнення бота було використано тенологію ШІ, яка автоматично генерує фейкові анкети користувачів, для більшого наповнення бота та прояву життєдіяльності боту для 3 осіб. На рисунку ви можете побачити як ШІ згенерував анкету фейкового користувача стосовно запитів бота

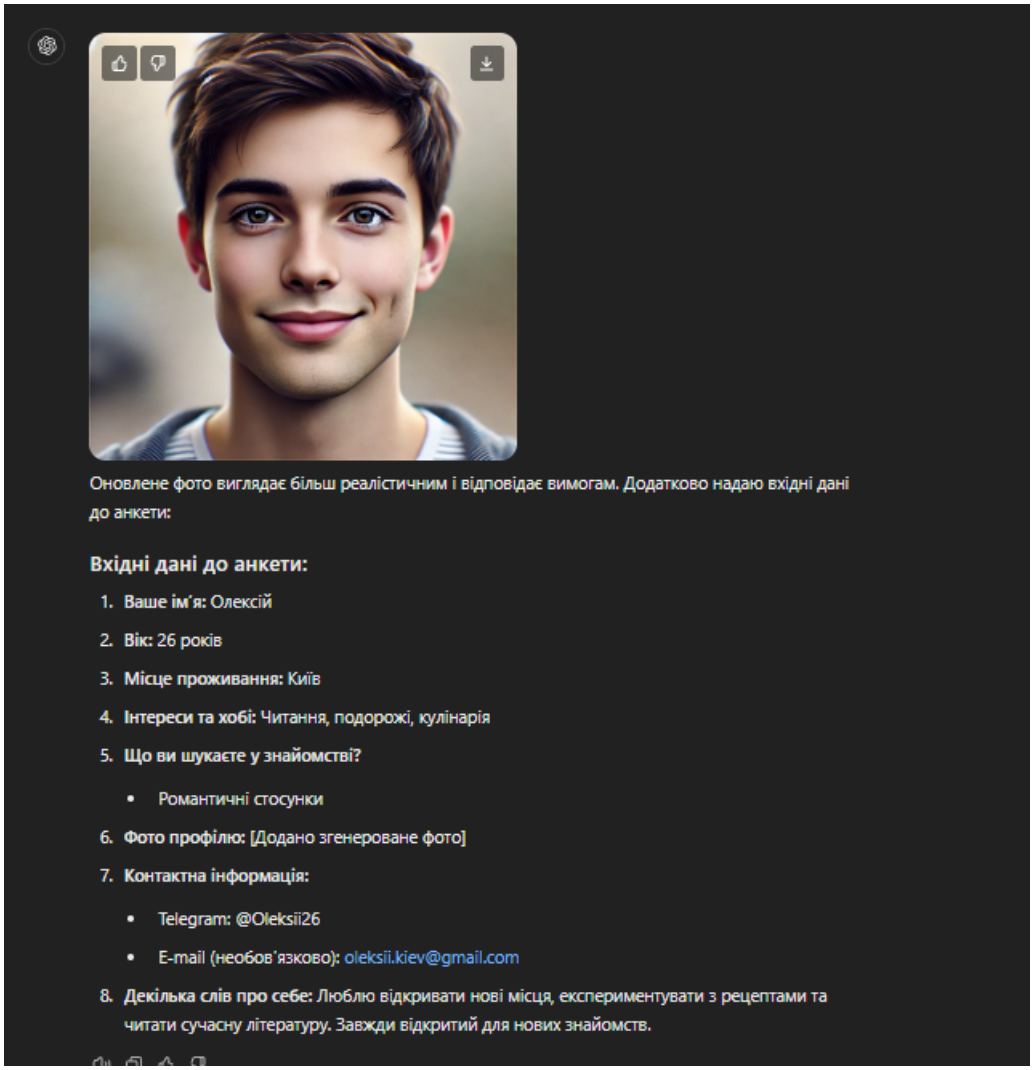

Рисунок 3.4 - Демонстрацію генерування анкети за допомогою ШІ

3.4 Архітектура системи зберігання даних на основі SQL

Система зберігання даних, побудована на основі бази даних SQL, забезпечує надійне зберігання та керування даними, зібраними з Telegram-бота. У цьому розділі розглянуто основну архітектуру системи, її складові та принципи роботи.

Telegram-бот є ключовим джерелом даних. Він забезпечує збір інформації від користувачів (запити, реєстрація, опитування тощо) та передає її до системи зберігання даних. API Telegram подає інтерфейс для отримання та обробки запитів. Це забезпечує точність даних та їх передачу в SQL-базу даних через серверний бік.Сервер робить перевірку даних на відповідність валідності та логіці перед

додаванням їх до SQL. Таким чином, знижується ймовірність помилок та дублювання даних.

База даних організована за принципами нормалізованої структури. Вона містить такі таблиці, як користувачі, запити, сесії та логи діяльності (див.рис3.4). Реляційна модель даних дозволяє ефективно структурувати та шукати їх.

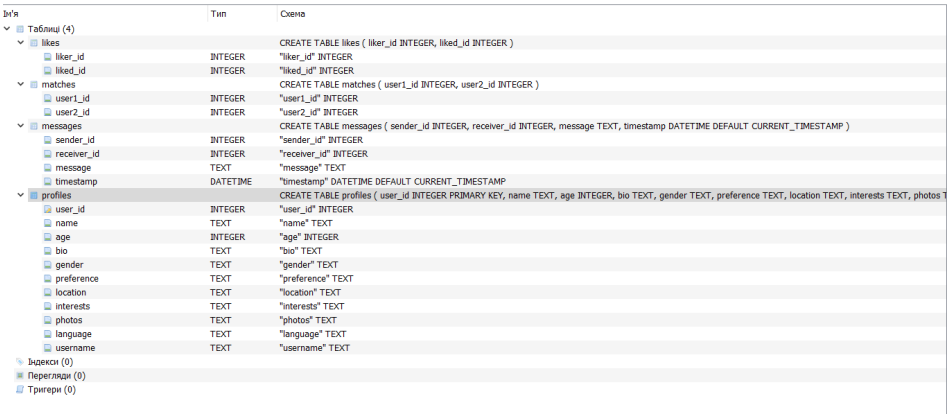

Рисунок 3.5 - Демонстрація структури бази даних

Telegram-бот отримує дані від користувача та поступово передає їх до API сервера.Дані перевіряються на відповідність формату та логіці. У випадку помилок бот повідомляє користувача про невірність даних. Валідні дані записуються в відповідні таблиці SQL-бази з урахуванням їх реляційних зв’язків.

На рисунку 3.6, ви можете побачити реалізовану структуру з даними користувачі.

user_id	name	age	bio	gender	preference	location	interests	photos	language	username
365208395	Я	22	Люблю спати	f	m	Майорка	Люблю спати, гладити кота, пити …	AgACAgIAAxkBAAICY2dcN2vDySpm1tYQEvj…	Українська	
669074640	Oleg	19	Test	m	all	Test	Test	NULL	Українська	
896577459	Григорій	24	Займаюсь спортом	m	f	Тернопіль	Бокс, туризм, плавання	AgACAgIAAxkBAAIB4WdcKpU6pWAkGFG_Wdo…	Українська	
947593185	Іван	18	Вчуся в політеці	m	f	Тернопіль	Крипто валюта	NULL	Українська	
1023058059	Степан	22		m	f	Тернопіль	Вчуся в університеті	NULL	Українська	

Рисунок 3.6 - Реалізована структура даних користувачів

Бази даних SQL є більш надійними завдяки своїй структурованій реляційній моделі, яка забезпечує цілісність і узгодженість даних. Основні принципи, такі як транзакційність (ACID-властивості), гарантують, що операції з даними виконуються повністю або не виконуються взагалі, навіть у разі збою системи.

Резервування даних через механізми бекапу та відновлення дозволяє зберігати дані у разі аварійних ситуацій. SQL також підтримує індексацію і оптимізацію запитів, що сприяє ефективному зберіганню та швидкому доступу до великих обсягів інформації. Додатково, засоби контролю доступу та захисту даних у SQL дозволяють обмежити несанкціонований доступ, що підвищує безпеку.

3.5 Висновки до розділу 3

У третьому розділі дослідження було реалізовано впровадження системи для збору персональних даних, що включало декілька важливих етапів. Основним елементом системи став чат-бот, розроблений для імітації реальних сценаріїв взаємодії з користувачами. Його ключовою метою було зібрати структуровані дані, а також виявити слабкі місця у поведінці користувачів, які могли б бути використані в атаках соціальної інженерії. Завдяки використанню сучасних технологій штучного інтелекту система отримала адаптивні можливості, що дозволило значно підвищити ефективність і точність збору даних. Інтеграція алгоритмів ШІ забезпечила персоналізований підхід до взаємодії з користувачами та допомогла враховувати їхні індивідуальні особливості.

Тестування системи показало її здатність ефективно виконувати поставлені завдання. Під час тестування було підтверджено, що чат-бот може не тільки ідентифікувати вразливості у поведінці користувачів, але й підвищувати їхню обізнаність щодо ризиків і методів соціальної інженерії. Це свідчить про можливість використання системи як навчального інструмента, спрямованого на формування у користувачів базових навичок цифрової грамотності та захисту особистих даних.

Одним із ключових аспектів впровадження стала розробка надійної архітектури для зберігання даних на основі бази даних SQL. Вона забезпечила високий рівень безпеки та конфіденційності, що є критично важливим у контексті роботи з персональною інформацією. Архітектура була спроектована таким чином,

щоб відповідати сучасним вимогам щодо захисту даних та їхнього належного зберігання.

У результаті впровадження розробленої системи було підтверджено її потенціал у сфері підвищення рівня кібербезпеки. Система демонструє високу ефективність у формуванні навичок протидії методам соціальної інженерії та може бути інтегрована в корпоративне середовище для навчання. Подальший розвиток і вдосконалення системи дозволять адаптувати її до різних галузей і забезпечити ще ширше охоплення аудиторії.

РОЗДІЛ 4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Метою розробки є створення навчального телеграм-бота, який ілюструє ризики, пов’язані із соціальною інженерією, через симуляцію типових атак. Основна задача системи — підвищити обізнаність користувачів у сфері інформаційної безпеки та допомогти уникнути витоку персональних даних у реальних ситуаціях.

Телеграм-бот використовує штучний інтелект для аналізу введених даних, адаптації сценаріїв взаємодії та створення персоналізованого досвіду для кожного користувача. Основою роботи бота є сценарії, побудовані на базі типових методів соціальної інженерії, таких як фішинг, маніпуляція довірою та психологічний вплив.

Процес розробки системи складався з кількох етапів:

- Аналіз та дослідження: було вивчено основні методи соціальної інженерії та помилки, які найчастіше допускають користувачі при взаємодії з потенційно небезпечними системами.

- Проектування: створена архітектура бота з інтеграцією модуля AI, а також детально розроблені сценарії для імітації реальних загроз.

- Реалізація: розробка здійснювалась з використанням Python та Telegram API, а алгоритми AI дозволили створити адаптивні сценарії.

- Тестування: проведено експериментальну перевірку системи із залученням добровольців для вдосконалення сценаріїв і підвищення ефективності.

Етичні аспекти розробки передбачають:

- Використання даних виключно для навчальних цілей без передачі третім особам.

- Дотримання законодавства та етичних норм у всіх сценаріях.

- Повідомлення користувачів про цілі системи та їх право на припинення участі у будь-який момент.

Завдяки інтеграції AI та соціальної інженерії, навчальний бот став ефективним інструментом для популяризації інформаційної безпеки. Він допомагає користувачам зрозуміти, як уникати потенційних загроз, що, у свою чергу, сприяє зменшенню кількості випадків витоку даних і підвищенню рівня цифрової грамотності.

4.2 Забезпечення електробезпеки користувачів ПК

Електробезпека — це система організаційних, технічних та експлуатаційних заходів, спрямованих на захист користувачів від ураження електричним струмом під час експлуатації електроприладів, зокрема персональних комп’ютерів (ПК). Оскільки сучасний ПК є складним електронним пристроєм, що працює від електромережі, питання забезпечення електробезпеки є надзвичайно важливим.

Основні фактори ризику

Під час роботи з ПК існує низка потенційних ризиків, пов'язаних із електробезпекою:

- Ураження електричним струмом через несправність ізоляції або пошкодження кабелів.

- Пожежонебезпека, спричинена коротким замиканням у внутрішніх компонентах ПК або перенавантаженням електромережі.

- Електромагнітне випромінювання, що може негативно впливати на здоров'я користувачів у разі порушення стандартів експлуатації.

- Статична електрика, яка може пошкодити внутрішні компоненти ПК або викликати дискомфорт у користувачів.

Нормативно-правова база електробезпеки

У питаннях забезпечення електробезпеки важливу роль відіграють державні стандарти, нормативні акти та правила:

Державні стандарти України (ДСТУ), які регламентують параметри електрообладнання та рівні безпеки.

Правила технічної експлуатації електроустановок споживачів.

Правила безпечної експлуатації електроустановок.

Санітарні норми та правила, що визначають допустимі рівні електромагнітного випромінювання.

Заходи забезпечення електробезпеки

1. Організаційні заходи

Інструктажі та навчання персоналу. Користувачі ПК повинні бути ознайомлені з основними правилами електробезпеки, такими як недопустимість торкання відкритих провідників, дотримання правил експлуатації електроприладів тощо.

Регулярна перевірка електрообладнання. Забезпечення контролю за справністю ПК та його периферійного обладнання через регулярні огляди й тестування.

Документальне забезпечення. Наявність інструкцій, правил і журналів обліку перевірок обладнання.

2. Технічні заходи

Заземлення та занулення. ПК повинні бути підключені до електромережі з правильно організованим заземленням для запобігання ураженню струмом у разі пошкодження ізоляції.

Використання автоматичних вимикачів та запобіжників. Встановлення захисних пристроїв, які відключають обладнання у разі короткого замикання або перенавантаження.

Екранування та фільтрація. Використання захисних екранів та фільтрів для зменшення впливу електромагнітного випромінювання.

Якісне електричне з'єднання. Застосування кабелів і роз'ємів, які відповідають стандартам безпеки.

3. Експлуатаційні заходи

Регулярне технічне обслуговування. Систематичний огляд кабелів, розеток, адаптерів і внутрішніх компонентів ПК на предмет пошкоджень.

Контроль за навантаженням на мережу. Використання джерел безперебійного живлення (ДБЖ) для запобігання стрибкам напруги.

Правильне розміщення обладнання. ПК повинні бути розміщені у добре провітрюваних місцях, на поверхнях, що не проводять електрику, аби уникнути перегріву чи короткого замикання.

Статична електрика і засоби її усунення

Одним із важливих аспектів є запобігання накопиченню статичної електрики, яка може пошкодити чутливі компоненти ПК. Для цього використовуються:

Антистатичні килимки та браслети.

Підтримання оптимальної вологості повітря у приміщенні (40–60%).

Використання антистатичних спреїв для обробки поверхонь.

Вимоги до приміщень

Приміщення, в яких експлуатуються ПК, повинні відповідати таким вимогам:

Наявність захисного заземлення та електрощита з автоматичними вимикачами.

Відповідна освітленість і відсутність вологи.

Підлога повинна бути виготовлена з матеріалів, що не накопичують статичну електрику.

Новітні технології для підвищення електробезпеки

Сучасні технології пропонують низку рішень для підвищення рівня електробезпеки користувачів ПК:

Інтелектуальні системи захисту. Використання розумних розеток і блоків живлення, які автоматично регулюють параметри електроживлення.

Моніторинг стану електромережі. Встановлення датчиків, які попереджають про можливі перевантаження чи стрибки напруги.

Безконтактні технології. Використання бездротових зарядних пристроїв і периферійного обладнання для зменшення кількості кабелів і з’єднань.

Забезпечення електробезпеки користувачів ПК є багатогранним завданням, що потребує системного підходу. Комплекс організаційних, технічних та експлуатаційних заходів дозволяє мінімізувати ризики ураження електричним струмом, зменшити вплив електромагнітного випромінювання та забезпечити надійну і безпечну експлуатацію комп’ютерної техніки.

Упровадження сучасних технологій, таких як інтелектуальні системи захисту, дозволяє значно підвищити рівень електробезпеки та зменшити ризики для здоров'я користувачів. Дотримання нормативних вимог, своєчасне технічне обслуговування та відповідальна експлуатація ПК забезпечують ефективну і тривалу роботу обладнання. Окрему увагу слід приділяти освіті користувачів, адже їхня обізнаність є ключовим фактором у запобіганні небезпеці. Враховуючи швидкий розвиток технологій, важливо регулярно оновлювати підходи до забезпечення електробезпеки, інтегруючи нові рішення та пристрої для захисту від можливих загроз.

ВИСНОВОК

У процесі дослідження була розроблена та реалізована інтерактивна навчальна система, яка дозволяє ефективно моделювати сценарії соціальної інженерії для підвищення обізнаності користувачів у сфері кібербезпеки. Завдяки інтеграції технологій штучного інтелекту Telegram-бот отримав здатність адаптуватися до поведінки користувачів, створювати реалістичні сценарії взаємодії та імітувати фішингові загрози в контрольованому середовищі.

Результати тестування продемонстрували ефективність запропонованого підходу, дозволивши ідентифікувати основні помилки в поведінці користувачів та надати рекомендації щодо їх виправлення. Система виявилася корисною як для індивідуальних користувачів, так і для організацій, зацікавлених у підвищенні рівня кібербезпеки своїх працівників.

Наукова новизна роботи полягає у застосуванні штучного інтелекту для створення динамічних навчальних сценаріїв, що сприяє більш глибокому розумінню ризиків та методів їх уникнення. Практичне значення роботи підтверджується можливістю її використання в освітніх програмах та дослідженнях у галузі кібербезпеки.

Подальший розвиток системи може включати розширення функціоналу бота, додавання нових сценаріїв взаємодії та інтеграцію з іншими платформами. Це дозволить ще більше підвищити її ефективність і адаптованість до реальних потреб користувачів.

Загалом, результати дослідження демонструють, що розроблена система є ефективним інструментом для навчання користувачів у сфері кібербезпеки. Вона дозволяє моделювати реальні загрози у контрольованому середовищі, сприяє підвищенню рівня цифрової грамотності та забезпечує формування практичних навичок протидії методам соціальної інженерії. Практичне значення роботи полягає у можливості використання системи як у навчальних закладах, так і в корпоративному середовищі для підвищення обізнаності співробітників. Розробка

також може слугувати базою для подальших досліджень у сфері інтерактивних навчальних технологій та кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17
2. General Data Protection Regulation (GDPR). European Commission. URL: https://gdpr-info.eu/
3. Cisco. What is Social Engineering? Methods and Prevention. Cisco. URL: https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html
4. Aiogram Framework Documentation. URL: https://docs.aiogram.dev/en/latest/
5. SQL Database Fundamentals. Microsoft Learn. URL: https://learn.microsoft.com/en-us/sql
6. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.
7. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.
8. Проблеми кіберзахисту під час воєнного стану. CERT-UA. URL: https://cert.gov.ua/articles
9. Тернопільський національний технічний університет. Внутрішня політика захисту персональних даних. URL: https://tntu.edu.ua
10. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
11. Mitnick, K. D., & Simon, W. L. (2011). The Art of Deception: Controlling the Human Element of Security. Wiley.
12. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
13. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.

14. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.
15. GDPR. (2016). General Data Protection Regulation (EU) 2016/679. Official Journal of the European Union.
16. Tymoshchuk, V., Pakhoda, V., Dolinskyi, A., Karnaukhov, A., & Tymoshchuk, D. (2024). MODELLING CYBER THREATS AND EVALUATING THE PERFORMANCE OF INTRUSION DETECTION SYSTEMS. Grail of Science, (46), 636–641. https://doi.org/10.36074/grail-of-science.29.11.2024.081
17. ENISA. (2020). European Union Agency for Cybersecurity: Threat Landscape Report. ENISA.
18. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.
19. AI Ethics Lab. (2020). Ethical Considerations in Artificial Intelligence Applications. AI Ethics Lab Publications.

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ПУЛЮЯ
НАУКОВЕ ТОВАРИСТВО ім. ШЕВЧЕНКА

М А Т Е Р І А Л И

XII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

18-19 грудня 2024 року

ТЕРНОПІЛЬ

2024

УДК 001

М34

ПРОГРАМНИЙ КОМІТЕТ

Голова: Приймак Микола – професор кафедри комп'ютерних систем та мереж, д.т.н., професо**р.**

Співголови: Марущак Павло – проректор з наукової роботи, докт. техн. наук, професор.

Баран Ігор – канд. техн. наук, доцент, декан факультету ФІС.

Науковий секретар: Надія Крива– старший викладач.

Члени: Василь Кривень - завідувач кафедри математичних методів в інженерії д.ф.-м.н., професор; Галина Осухівська – завідувач кафедри комп'ютерних систем та мереж, к.т.н., доцент; Микола Карпінський - професор кафедри кібербезпеки, д.т.н., професор; Жанна Баб'як - завідувач кафедри української та іноземних мов, к.пед. н., доцент; Ярослав Литвиненко – професор кафедри комп'ютерних наук, д.т.н., професор; Михайло Петрик - завідувач кафедри програмної іженерії, д.ф.-м.н., професор; Наталія Загородна – завідувач кафедри кібербезпеки, к.т.н., доцент.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова: Скоренький Юрій Любомирович – канд. техн. наук, доцент кафедри фізики.

Члени: доцент кафедри комп'ютерних наук, к.т.н. В. Никитюк; доцент кафедри програмної інженерії, к.т.н. Д. Михалик; доцент кафедри кібербезпеки, к.т.н. М. Стадник; доцент кафедри комп'ютерних систем та мереж, к.т.н. Є. Тиш; ст. викладач Л. Джиджора.

М34 Матеріали XII науково-технічної конфції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 18–19 грудня 2024 р.). – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024.

Адреса оргкомітету: ТНТУ ім. І. Пулюя, м. Тернопіль, вул. Руська, 56, 46001,

тел. (0352) 52-41-33, факс (0352) 25-49-83.

E-mail: conffis2024@gmail.com

Редагування, оформлення та верстка: Надія Крива

СЕКЦІЇ КОНФЕРЕНЦІЇ, ЯКІ ПРЕДСТВЛЕНІ В ЗБІРНИКУ

- Математичне моделювання
- Інформаційні системи та технології, кібербезпека
- Комп’ютерні системи та мережі
- Програмна інженерія та моделювання складних розподілених систем
- Новітні фізико-технічні та освітні технології

В збірнику надруковано тези доповідей XII науково-технічної конференції «Інформаційні моделі, системи та технології» (Тернопіль, 18–19 грудня 2024 р.) за такими науковими напрямками: математичне моделювання; інформаційні системи та технології, кібербезпека; комп’ютерні системи та мережі; програмна інженерія та моделювання складних розподілених систем; новітні фізико-технічні та освітні технології.

Розрахований на науковців, викладачів та студентів вузів.

За зміст тез та дотримання норм академічної доброчесності відповідальність несе автор.

УДК 004.056
Прокопенко Олег, студент гр.СБм-62
Тернопільський національний технічний університет імені Івана Пулюя

РОЗРОБКА НАВЧАЛЬНОЇ СИСТЕМИ ДЛЯ ЗБОРУ ПЕРСОНАЛЬНИХ ДАНИХ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ ТА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Prokopenko Oleh, student of gr СБм-62

DEVELOPMENT OF A TRAINING SYSTEM FOR COLLECTING PERSONAL DATA USING AI AND SOCIAL ENGINEERING

Сучасні конфлікти, зокрема війна між Україною та Росією, демонструють, що кіберпростір стає одним із ключових фронтів. Збір персональних даних через соціальну інженерію та їх використання для інформаційних атак став важливим інструментом агресора. Розробка навчальних систем із використанням штучного інтелекту допоможе не лише дослідити ці методи, але й підготувати фахівців для протидії таким загрозам.[1]

Штучний інтелект пропонує нові інструменти для збору та аналізу персональних даних, але водночас створює виклики, пов'язані з етикою та конфіденційністю. Навчальні системи, що симулюють сценарії соціальної інженерії, дозволяють зрозуміти поведінкові моделі та розробити механізми захисту. Це особливо актуально для країн, які перебувають у зоні геополітичної нестабільності, як Україна.[2]

Актуальність теми зумовлена масштабним використанням соціальної інженерії для маніпуляції громадською думкою, збору конфіденційної інформації та проведення інформаційних операцій. В умовах війни, такі дії можуть мати катастрофічні наслідки для безпеки держави. Навчальні системи на основі штучного інтелекту допоможуть моделювати реальні загрози, формувати критичне мислення та вдосконалювати розуміння стосовно цього. Україна вже кілька років стикається з інформаційними атаками, що є частиною гібридної війни з Росією. Розуміння механізмів збору даних допоможе протистояти таким загрозам. [3]

Основна робота зосереджена на створенні телеграм-бота, який імітує один із можливих методів збору інформації для соціальної інженерії. Telegram є популярним месенджером в Україні, що робить його ефективним середовищем для моделювання потенційних загроз і навчання користувачів реагувати на них. Цей бот демонструє вразливість до фішингових атак і навчає користувачів розпізнавати загрози. За допомогою цього бота, також можна продемонструвати анонімний збір персональних даних користувачів.

Сучасний світ дедалі більше залежить від цифрових технологій, що робить суспільство вразливим до атак, які використовують персональні дані. Тому запропонована модель демонстрації загрози має високий потенціал для вивчення цієї теми та в подальшому використанні методів захисту на основі запропонованого навчального бота/

Література:

1. Roles and Implications of AI in the Russian-Ukrainian Conflict URL:Warfarehttps://www.cnas.org/publications/commentary/roles-and-implications-of-ai-in-the-russian-ukrainian-conflict
2. RAND CorporationURL: https://www.rand.org/pubs/commentary/2022/11/ukraines-lessons-for-the-future-of-hybrid-warfare.html
3. Oxford AcademicURL: https://academic.oup.com/book/56111/chapter-abstract/442747673?redirectedFrom=fulltext&login=false