МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ПАЛАМАРЧУК ВЛАДИСЛАВ БОРИСОВИЧ

Допускається до захисту:
в.о. завідувача кафедри
інформаційних технологій
к. т. н., доцент
_____ О. В. Зелінська
«____»_____ 20__ р.

СИСТЕМА ВИЯВЛЕННЯ ШАХРАЙСТВА НА ОСНОВІ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ В СОЦІАЛЬНИХ МЕРЕЖАХ

Спеціальність 122 Комп’ютерні науки

Кваліфікаційна (магістерська) робота

Науковий керівник:
О. В. Зелінська, доцент кафедри
інформаційних технологій,
к. т. н., доцент
_____

Оцінка: _____ / _____ / _____
(бали/за шкалою ЄКТС/за національною шкалою)

Голова ЕК: _____

Вінниця — 2024

АНОТАЦІЯ

Паламарчук В.Б. Застосунок протидії шахрайству на основі аналізу поведінки користувачів інтернет. Спеціальність 122 «Комп’ютерні науки», Освітня програма «Комп’ютерні технології обробки даних (Data Science)». Донецький національний університет імені Василя Стуса, Вінниця, 2024.

"Система виявлення шахрайства на основі аналізу поведінки користувачів Інтернет" розглядає проблеми, пов'язані з шахрайством. У цій роботі досліджуються різні аспекти поведінкового аналізу, включаючи збір та обробку даних, використання алгоритмів машинного навчання та статистичних методів для виявлення аномальної поведінки, що може свідчити про шахрайство.

Ключові слова: застосунок, система опитування, дані, аналіз даних, методи запобігання шахрайству, Python.

62 с., 6 рис., 18 джерел.

Palamarchuk V.B. Application of fraud counteraction based on the analysis of Internet users' behaviour. Speciality 122 "Computer Science", Educational programme "Computer Technologies of Data Processing (Data Science)". Vasyl' Stus Donetsk National University, Vinnytsia, 2024.

"Fraud detection system based on the analysis of Internet users' behaviour" addresses the problems associated with fraud. This paper explores various aspects of behavioural analysis, including data collection and processing, the use of machine learning algorithms and statistical methods to detect abnormal behaviour that may indicate fraud.

Keywords: application, survey system, data, data analysis, fraud prevention methods, Python.

62 pages, 6 figures, 18 sources.

ЗМІСТ

ВСТУП

Проблема шахрайства в мережі Інтернету має значний вплив на користувачів та бізнес-середовище. Онлайн-шахрайство охоплює широкий спектр злочинів, які спрямовані на викрадення особистої інформації, фінансові шахрайства, крадіжку конфіденційних даних, шпигунство, фішинг, фармінг, обман користувачів та інші шахрайські дії.

Продовжуючи розмову про проблему шахрайства в мережі Інтернету, важливо зазначити, що ця проблема має серйозні наслідки для користувачів і бізнесів.

Для боротьби з проблемою шахрайства в мережі Інтернету необхідно підвищувати свідомість користувачів щодо безпеки в Інтернеті, використовувати надійне програмне забезпечення та антивіруси, не ділитися конфіденційною інформацією з ненадійними джерелами, регулярно оновлювати паролі і бути уважними до підозрілих дій та повідомлень в мережі.

Дослідження та розробка систем для боротьби з шахрайством є надзвичайно актуальними в сучасному світі. З огляду на зростаючу кількість користувачів Інтернету та збільшення обсягу онлайн-транзакцій і зв'язку, шахраї стають все більш винахідливими і впевненими в своїх діях. Тому розробка ефективних систем для виявлення, запобігання та реагування на шахрайство є надзвичайно важливою.

Ось кілька причин, чому дослідження та розробка систем шахрайства залишаються актуальними:

1. Еволюція шахрайства: Шахраї постійно змінюють свої методи і техніки, щоб уникнути виявлення та обійти захист. Вони використовують нові технології, соціальні мережі та інші інструменти для вчинення своїх злочинних дій. Тому постійне дослідження і розробка нових методів і систем для виявлення шахрайства є необхідними.

2. Збільшення загрози для користувачів та бізнесів: Шахраї здатні завдати серйозної шкоди як індивідуальним користувачам, так і бізнесам. Вони можуть викрадати фінансові реквізити, руйнувати репутацію, використовувати шпигунське програмне забезпечення для злому систем, крадіжки ідентичності та багато іншого. Розробка ефективних систем для захисту від таких загроз є надзвичайно важливою.
3. Законодавство та регулювання: Уряди та організації стежать за проблемою шахрайства і впроваджують законодавство та регулювання для боротьби з цим явищем. Дослідження та розробка систем шахрайства можуть допомогти виконувати ці законодавчі вимоги та забезпечити безпеку користувачів та бізнесів в Інтернеті.
4. Зростання використання штучного інтелекту та аналітики даних: Розвиток штучного інтелекту та аналітики даних надає нові можливості для виявлення шаблонів та аномалій, які можуть вказувати на шахрайську діяльність. Розробка систем, які використовують ці технології, дозволяє ефективно виявляти й запобігати шахрайству.

Усе вищезгадане свідчить про необхідність продовжувати дослідження та розробку систем шахрайства для забезпечення безпеки та захисту користувачів Інтернету.

РОЗДІЛ 1
ПОСТАНОВКА ЗАДАЧІ І ОГЛЯД АНАЛОГІВ ІСНУЮЧИХ МЕТОДІВ ТА СИСТЕМ ЗА ДАНОЮ ТЕМАТИКОЮ

1.1 Опис актуальності дослідження методів та систем протидії шахрайству

Дослідження методів та систем протидії шахрайству є надзвичайно актуальними і важливими з кількох причин:

1. Зростання шахрайства в мережі Інтернету: Шахрайство в Інтернеті постійно зростає і стає все більш складним і винахідливим. Шахраї постійно шукають нові способи шахрайства, використовуючи технологічний прогрес і нові методи, щоб обійти захист і отримати незаконну вигоду. Тому потрібні постійні дослідження для розуміння цих нових методів і розробки ефективних стратегій протидії.
2. Загрози для безпеки користувачів та організацій: Шахрайство в Інтернеті становить серйозну загрозу для безпеки як індивідуальних користувачів, так і організацій. Воно може призвести до фінансових втрат, крадіжки конфіденційної інформації, пошкодження репутації та інших негативних наслідків. Дослідження методів та систем протидії шахрайству допомагають зменшити ризики і забезпечити безпеку користувачів та організацій.
3. Розвиток нових технологій: З розвитком нових технологій, таких як штучний інтелект, машинне навчання, блокчейн, Internet of Things тощо, з'являються нові можливості для шахраїв і, в той же час, для розробки нових методів протидії шахрайству. Дослідження методів і систем протидії шахрайству допомагають

використовувати ці нові технології для забезпечення безпеки в Інтернеті.

4. Законодавчі вимоги та регулювання: Уряди та організації впроваджують законодавчі вимоги та регулювання для боротьби з шахрайством в Інтернеті. Дослідження методів та систем протидії шахрайству допомагають виконувати ці законодавчі вимоги і забезпечувати відповідність стандартам безпеки.

1.2 Огляд літератури

1.2.1 Дослідження попередніх робіт та існуючих систем протидії шахрайству.

Дослідники та експерти активно працюють над розробкою методів та систем протидії шахрайству в мережі Інтернету. Деякі з попередніх робіт і існуючих систем включають наступне:

1. Аналіз поведінки користувачів: Велику увагу приділяють аналізу поведінки користувачів для виявлення аномалій і підозрілих дій. Наприклад, використання машинного навчання та алгоритмів класифікації може допомогти виявити шаблони шахрайства на основі активності користувача.
2. Методи машинного навчання: Машинне навчання використовується для створення моделей, які можуть класифікувати шахрайську активність. Наприклад, моделі можуть навчатися розпізнавати фішингові електронні листи або шкідливе програмне забезпечення.
3. Аналіз тексту та мови: Використання аналізу тексту та мови дозволяє виявляти підозрілі заяви, обманливі оголошення або спамові повідомлення. Алгоритми можуть аналізувати семантику, тон та інші ознаки тексту для виявлення шахрайства.

4. Автоматичне виявлення фішингових веб-сторінок: Системи можуть використовувати аналіз веб-сторінок для виявлення фішингових сайтів та попередження користувачів про потенційно шахрайську діяльність.
5. Системи виявлення шахрайства в електронній комерції: Ці системи використовуються для виявлення шахрайських транзакцій та запобігання незаконним операціям. Вони аналізують різні фактори, такі як історія покупок, місцезнаходження, використані платіжні методи та інші ознаки, щоб виявити підозрілу активність.
6. Криптографічні протоколи та захист даних: Розробляються та вдосконалюються криптографічні протоколи для забезпечення безпеки під час передачі та зберігання інформації в Інтернеті. Також розробляються методи захисту даних, щоб унеможливити несанкціонований доступ до конфіденційної інформації.

Це лише деякі приклади попередніх робіт та існуючих систем протидії шахрайству. Завдяки постійному дослідженню та розробці нових методів і технологій, шахраї стикаються зі складнішими викликами, але науковці та розробники продовжують покращувати системи протидії шахрайству, щоб забезпечити безпеку та довіру в Інтернеті.

1.2.2 Огляд існуючих систем та методів для виявлення шахрайства

Існує ряд систем і методів, які використовуються для виявлення шахрайства в мережі Інтернету. Ось декілька з них:

1. Системи виявлення аномалій: Ці системи використовують статистичні аналізи та алгоритми машинного навчання для виявлення незвичних або підозрілих активностей. Вони порівнюють активність користувачів з нормальними моделями поведінки та сповіщають про можливі шахрайські дії.

2. Системи виявлення шаблонів: Ці системи використовують набір попередньо визначених шаблонів шахрайства або аномальної активності для виявлення відповідних сигналів. Вони можуть виявляти специфічні шаблони, такі як фішингові електронні листи або шахрайські веб-сайти.
3. Системи виявлення шахрайства на основі правил: Ці системи використовують набір правил та вимог, щоб виявляти потенційно шахрайські дії. Наприклад, вони можуть перевіряти деталі транзакцій на відповідність певним правилам, які вказують на можливе шахрайство.
4. Аналіз графів соціальних мереж: Шахраї часто використовують соціальні мережі для здійснення своїх дій. Аналіз графів соціальних мереж дозволяє виявляти підозрілі зв'язки та несподівані залежності між користувачами, що можуть свідчити про шахрайську активність.
5. Моніторинг веб-сайтів і онлайн-платформ: Багато веб-сайтів та онлайн-платформ мають власні системи моніторингу для виявлення шахрайської активності. Наприклад, системи захисту від шахрайства у банківській галузі можуть виявляти підозрілу активність на рахунках клієнтів або спроби несанкціонованого доступу.
6. Використання машинного навчання та штучного інтелекту: Методи машинного навчання та штучного інтелекту широко використовуються для аналізу великих обсягів даних та виявлення складних шаблонів шахрайства. Ці методи можуть автоматично навчатися на нових данних та покращувати свою ефективність з часом.

Ці системи і методи працюють в комбінації, допомагаючи виявляти та запобігати різноманітним видам шахрайства в мережі Інтернету. Важливо зауважити, що шахраї постійно вдосконалюють свої методи, тому системи

протидії шахрайству також тримаються в активному розвитку та оновлюються для боротьби зі змінюючимися загрозами.

1.2.3 Обгрунтування методів та підходів, які використовуються для дослідження

Дослідження шахрайства в соціальних мережах вимагає використання різноманітних методів та підходів для збору, аналізу та вивчення даних. Нижче наведено деякі ключові методи та підходи, які можна використовувати для дослідження цієї проблеми:

1. Аналіз змісту та текстовий аналіз:
   - Виявлення ключових слів та фраз: Використовуйте аналіз текстового змісту для виявлення ключових слів та фраз, які можуть вказувати на шахрайську діяльність.
   - Сентимент-аналіз: Оцінюйте тон та емоційний стан текстового матеріалу для виявлення підозрілих або шахрайських висловлювань.
2. Мережевий аналіз:
   - Аналіз соціальних мереж: Досліджуйте взаємодії та зв'язки між користувачами у соціальних мережах для виявлення несподіваних або підозрілих зв'язків.
   - Аналіз взаємодій: Вивчайте шаблони взаємодій між користувачами, оцінюючи типові сценарії шахрайської діяльності.
3. Машинне навчання та аналіз даних:
   - Класифікація поведінки користувачів: Використовуйте методи машинного навчання для класифікації поведінки користувачів на "нормальну" та "підозрілу".
   - Кластерний аналіз: Визначайте групи користувачів, які мають схожі характеристики або спільні риси.
4. Візуальний аналіз:

- Графічне представлення даних: Використовуйте діаграми та графіки для візуалізації розподілу даних та виявлення аномалій.
- Візуальний аналіз мереж: Вивчайте графіки взаємодій між користувачами для швидкого виявлення патернів.

5. Опитування та інтерв'ю:

- Дослідження користувачів: Проводьте опитування або інтерв'ю з користувачами для збору додаткової інформації про їхні досвіди та сприйняття шахрайства.

6. Моніторинг активності:

- Реальний час: Використовуйте системи моніторингу в реальному часі для виявлення підозрілої активності негайно після її виникнення.

7. Експертний аналіз:

- Експертна експертиза: Залучайте експертів у галузі кібербезпеки та соціальних мереж для оцінки складних випадків та ідентифікації шахрайських зразків.

8. Запобігання та освіта:

- Проактивна освіта: Здійснюйте превентивні заходи, такі як інформаційні кампанії та навчання користувачів щодо ризиків шахрайства.

Використання комбінації цих методів дозволяє створити комплексний підхід до дослідження шахрайства в соціальних мережах, сприяючи виявленню та запобіганню шахрайській діяльності.

1.3 Збір даних

1.3.1 Визначення типів даних, необхідних для аналізу поведінки користувачів.

Аналіз поведінки користувачів в інтернеті вимагає збору та аналізу різноманітних типів даних. Основні типи даних, необхідних для аналізу поведінки користувачів в Інтернеті, включають:

1. Історичні дані: Це дані, що відображають минулу активність користувачів, такі як журнали дій, історія відвідувань веб-сайтів, історія транзакцій, активність в соціальних мережах тощо. Історичні дані надають контекст і відомості про попередні дії користувачів.
2. Демографічні дані: Це дані, що характеризують особисті характеристики користувачів, такі як вік, стать, місцезнаходження, освіта, заняття тощо. Демографічні дані допомагають у розумінні контексту та особливостей поведінки користувачів.
3. Дані про використання пристроїв: Це дані, що відображають характеристики та параметри використання пристроїв, такі як тип пристрою, операційна система, веб-браузер, мобільні додатки, IP-адреси тощо. Ці дані можуть бути важливими для виявлення підозрілої або несанкціонованої активності.
4. Дані про взаємодію: Це дані, що відображають способи взаємодії користувачів з веб-сайтами або онлайн-сервісами, такі як кліки, наведення курсора, час перебування на сторінці, заповнення форм, взаємодія з елементами інтерфейсу тощо. Ці дані дозволяють аналізувати поведінкові патерни та звички користувачів.
5. Соціальні дані: Це дані, що відображають взаємодію користувачів у соціальних мережах, такі як коментарі, подобається, ділитися, підписки, список друзів тощо. Соціальні дані допомагають у розумінні соціального контексту та виявленні патернів поведінки.
6. Геолокаційні дані: Це дані, що відображають місцезнаходження користувачів, такі як GPS-координати, інформація про регіон,

місто, район тощо. Геолокаційні дані можуть бути важливими для виявлення незвичайної або шахрайської активності, зокрема в контексті безпеки.

Ці типи даних можуть бути зібрані з різних джерел, таких як серверні журнали, бази даних, веб-аналітичні інструменти, додатки моніторингу тощо. Аналізуючи ці дані, можна виявити патерни, аномалії та інші ознаки шахрайства в мережі Інтернету.

Додатково до типів даних, які я вже описав, існують інші важливі типи даних, які використовуються для аналізу поведінки користувачів в Інтернеті:

7. Фінансові дані: Це дані про фінансові транзакції, такі як купівля товарів або послуг, платежі, банківські перекази тощо. Аналіз фінансових даних дозволяє виявити підозрілу або шахрайську фінансову активність, таку як крадіжки ідентифікаційних даних, шахрайські платежі або фінансові маніпуляції.
8. Текстові дані: Це дані з текстових джерел, такі як електронні листи, повідомлення в соціальних мережах, коментарі, відгуки тощо. Аналіз текстових даних за допомогою технік обробки природної мови (Natural Language Processing, NLP) дозволяє виявити шахрайські схеми, спам, фішингові атаки та інші види шахрайства, що використовуються в текстовій формі.
9. Дані про поведінку на веб-сайті: Це дані, що відображають взаємодію користувачів з конкретним веб-сайтом, такі як сторінки, які вони відвідують, товари, які переглядають, час перебування на сторінці, дії, які вони здійснюють (натискання, додавання до кошика тощо). Аналіз цих даних допомагає розуміти користувацькі звички, інтереси та виявляти підозрілу активність.
10. Візуальні дані: Це дані, що відображають візуальну інформацію, наприклад, зображення, відео або графіки. Аналіз візуальних даних може бути застосований для виявлення шахрайства, такого

як використання фальшивих зображень, фотошоп або відеообробка для обману користувачів.

11. Ці типи даних використовуються разом для створення комплексних систем і алгоритмів аналізу поведінки користувачів в Інтернеті. Поєднання різноманітних джерел даних та застосування різних аналітичних технік дозволяють виявляти патерни, аномалії та визначати шахрайську активність для подальшого застосування в системах протидії шахрайству.

1.3.2 Розробка методів збору та збереження даних для подальшого аналізу.

Розробка методів збору та збереження даних є важливим етапом для подальшого аналізу поведінки користувачів в Інтернеті. Ефективна збір і збереження даних дозволяють забезпечити достатню кількість, якість та доступність даних для подальшого аналізу. Ось деякі методи, що можуть бути використані для цих цілей:

1. Логування: Використання серверних журналів або лог-файлів для запису дій користувачів, запитів до веб-сайту, транзакцій та інших взаємодій. Ці дані можуть включати інформацію про IP-адреси, дати та часи, типи запитів, відповіді сервера тощо.
2. Веб-аналітика: Використання спеціальних інструментів аналізу веб-сайту для збору інформації про відвідувачів, таких як відвідувані сторінки, джерела трафіку, час перебування на сторінках, конверсії та інші метрики. Ці дані можуть бути корисними для визначення користувацьких звичок та виявлення аномалій.
3. Соціальні мережі та API: Використання API соціальних мереж для збору даних про активність користувачів, включаючи взаємодію з

постами, лайки, коментарі тощо. Ці дані можуть допомогти у розумінні соціального контексту та виявленні патернів поведінки.

4. Системи управління базами даних (СУБД): Використання СУБД для збереження структурованих даних, таких як особиста інформація, фінансові дані, історія транзакцій тощо. Ці дані можуть бути організовані в таблиці, реляційні бази даних або інші формати, залежно від потреб проекту.
5. Системи збереження масштабованих даних: Використання спеціалізованих систем збереження даних, таких як Hadoop, Apache Cassandra, Elasticsearch тощо, для збереження великих обсягів даних, які можуть бути зібрані з різних джерел.
6. Методи анонімізації та захисту даних: Застосування методів анонімізації, шифрування та інших методів захисту даних для збереження конфіденційності та приватності користувачів.

При розробці методів збору та збереження даних необхідно враховувати правові та етичні аспекти, пов'язані зі збором та обробкою персональних даних користувачів.

Висновок до розділу 1

У даному розділі було розглянуто постановку задачі роботи, а також проведений огляд існуючих продуктів даної тематики, були окреслені їх плюси та мінуси. Наступний розділ буде присвячений аналізу існуючих методів вирішення транспортної задачі.

РОЗДІЛ 2
АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ОПТИМІЗАЦІЇ ТА БОРОТЬБИ З ШАХРАЙСТВОМ

2.1 Аналіз поведінки користувачів

2.1.1 Використання методів аналізу даних для виявлення аномалій та підозрілих патернів поведінки користувачів.

Використання методів аналізу даних для виявлення аномалій та підозрілих патернів поведінки користувачів є одним із ключових аспектів систем протидії шахрайству в мережі Інтернету. Дослідники та розробники використовують різні техніки та алгоритми для аналізу великого обсягу даних та виявлення незвичайних або підозрілих активностей. Ось кілька методів, які можуть бути застосовані:

1. Машинне навчання: Методи машинного навчання, такі як класифікація, кластеризація та асоціативні правила, використовуються для побудови моделей, які можуть виявляти аномалії та незвичайні патерни в даних користувачів. Навчання моделей може проводитись з використанням розмічених даних, де відомо, що є підозрілим або нормальним, або застосовуються методи навчання без учителя для виявлення аномалій без попередньої розмітки.
2. Аналіз графів: У випадках, коли дані користувачів можуть бути представлені у вигляді графової структури, такої як соціальні мережі або мережі зв'язків, аналіз графів може бути застосований для виявлення аномалій, вузлів з несподіваною активністю або взаємозв'язків, що відхиляються від норми.
3. Виявлення аномалій у часових рядах: Якщо дані про поведінку користувачів можуть бути впорядковані в часовий ряд, методи виявлення аномалій у часових рядах можуть бути застосовані. Це

включає використання статистичних методів, таких як аналіз зміни середнього, методи засновані на відхиленні стандартного відхилення, або складніші моделі, такі як авторегресійні моделі чи методи глибинного навчання.

4. Аналіз текстових даних: Якщо доступні тексові дані, такі як коментарі, повідомлення або відгуки користувачів, можуть застосовуватися методи обробки природної мови (NLP) для аналізу тексту. Це може включати виявлення схожості тексту, класифікацію на позитивні та негативні коментарі, аналіз емоцій тощо, що допоможе виявити підозрілі або шахрайські відгуки.

Ці методи можуть бути застосовані як окремо, так і у поєднанні, залежно від конкретного контексту та типу даних, які аналізуються. Комбінація різних методів дозволяє створити потужні системи для виявлення шахрайства та підозрілої поведінки користувачів в мережі Інтернету.

2.1.2 Розробка алгоритмів для класифікації поведінки як доброчесної або підозрілої.

Розробка алгоритмів для класифікації поведінки користувачів як доброчесної або підозрілої є важливим кроком у протидії шахрайству в Інтернеті. Ці алгоритми дозволяють автоматично аналізувати дані та виявляти ознаки підозрілого або шахрайського поведінки. Ось деякі загальні підходи до розробки таких алгоритмів:

1. Використання навчання з учителем: Цей підхід передбачає наявність розмічених даних, де для кожного прикладу поведінки користувача вказано, чи є вона доброчесною або підозрілою. За допомогою цих даних можна навчити класифікатор, який буде прогнозувати клас поведінки для нових прикладів. При цьому використовуються різні алгоритми класифікації, такі як

логістична регресія, дерева рішень, випадковий ліс, нейронні мережі тощо.

2. Використання навчання без учителя: У випадках, коли розмічених даних обмежено або їх немає взагалі, можуть бути використані методи навчання без учителя. Ці методи дозволяють виявляти приховані патерни або групи схожих поведінок у нерозмічених даних. Наприклад, можна застосувати кластерний аналіз для групування користувачів за схожістю їхньої поведінки, і потім провести додатковий аналіз кожного кластера для виявлення аномалій.
3. Використання комбінації ознак: Крім аналізу самої поведінки користувача, можуть бути використані інші ознаки, які допомагають відрізнити доброчесну поведінку від підозрілої. Наприклад, можуть бути використані дані про пристрій, IP-адресу, геолокацію, історію дій та інші метадані. Комбінація цих ознак із алгоритмами класифікації дозволяє створити більш точні моделі класифікації.
4. Використання експертних правил: Поряд з автоматичними методами аналізу даних, можуть бути використані експертні правила, які встановлюються на основі знань та досвіду фахівців. Ці правила можуть включати певні шаблони або узори поведінки, які свідчать про підозрілу активність. Комбінація правил з автоматичними методами аналізу даних дозволяє покращити точність виявлення підозрілої поведінки.

При розробці алгоритмів для класифікації поведінки як доброчесної або підозрілої необхідно враховувати специфіку конкретної сфери або домену, в якому використовується система. Різні види шахрайства можуть мати відмінні характеристики та ознаки, тому важливо підходити до розробки алгоритмів з урахуванням цих особливостей.

2.2 Виявлення шахрайства та прийняття рішень

2.2.1 Використання розроблених моделей та алгоритмів для виявлення шахрайських дій користувачів

Після розробки моделей і алгоритмів для виявлення шахрайських дій користувачів їх можна використовувати в реальному часі для моніторингу активності користувачів і виявлення підозрілих дій. Ось кілька способів використання розроблених моделей та алгоритмів:

1. Реалізація системи моніторингу: Розроблені моделі та алгоритми можна інтегрувати у систему моніторингу, яка перевіряє активність користувачів у реальному часі. Система може аналізувати дані про дії користувачів, їх поведінку, взаємодію з ресурсами та інші параметри, і використовувати розроблені моделі для виявлення підозрілих дій. Якщо модель виявляє підозрілу активність, система може спрацювати і вжити відповідних заходів, наприклад, блокування доступу користувача або сповіщення адміністратора.
2. Інтеграція з існуючими системами безпеки: Розроблені моделі та алгоритми можуть бути інтегровані з існуючими системами безпеки, такими як системи виявлення вторгнень (IDS) або системи управління безпекою (Security Information and Event Management, SIEM). Це дозволить розширити можливості існуючих систем і забезпечити виявлення шахрайських дій на рівні мережі або додатків. Наприклад, модель може аналізувати мережевий трафік або системні журнали, щоб виявити аномальну або підозрілу активність.
3. Побудова рішень на основі ризику: Розроблені моделі та алгоритми можуть бути використані для оцінки ризику шахрайства в конкретних сценаріях або доменах. Наприклад,

модель може присвоювати кожній дії користувача показник ризику, враховуючи його характеристики та контекст. На основі цього ризику можуть прийматися рішення щодо подальших кроків, таких як перевірка додаткової інформації, виклик високоризикових дій до перевірки адміністратором або автоматичне блокування підозрілих дій.

4. Постійне вдосконалення моделей: Результати, отримані з розроблених моделей і алгоритмів, можуть бути використані для постійного вдосконалення системи виявлення шахрайства. Наприклад, виявлені підозрілі дії можуть бути використані як навчальні дані для покращення моделей, їх адаптації до нових видів шахрайства або виявлення раніше невідомих шаблонів. Це дозволить системі стати більш ефективною та точною в виявленні шахрайської активності.

Загалом, використання розроблених моделей і алгоритмів для виявлення шахрайських дій користувачів допомагає покращити безпеку в інтернеті та зменшити вплив шахрайства на користувачів і організації.

2.2.2 Розробка системи прийняття рішень щодо подальших кроків після виявлення підозрілого поведінки

Розробка системи прийняття рішень щодо подальших кроків після виявлення підозрілого поведінки користувачів є важливою складовою процесу боротьби з шахрайством в Інтернеті. Основна мета такої системи полягає в тому, щоб ефективно виявляти, реагувати і запобігати шахрайським діям з мінімальними наслідками для законних користувачів. Ось кілька ключових етапів розробки такої системи:

1. Аналіз підозрілого поведінки: Першим етапом є аналіз підозрілої активності, виявленої за допомогою моделей і алгоритмів виявлення шахрайства. Цей аналіз може включати перевірку збігу

з попередньо відомими шаблонами шахрайської діяльності, оцінку ризику, аналіз відхилень від нормальних моделей поведінки тощо.

2. Визначення рівня загрози: Наступним етапом є визначення рівня загрози, пов'язаної з підозрілою активністю. Це може бути здійснено шляхом оцінки ризику, який базується на характеристиках дії, історії користувача, відомих шаблонах шахрайства тощо. Рівень загрози може бути визначений, наприклад, як низький, середній або високий.
3. Вибір подальших кроків: На основі визначеного рівня загрози система повинна вибрати подальші кроки, які потрібно підприйняти. Це може включати такі дії, як блокування доступу користувача, вимагання додаткової аутентифікації, сповіщення адміністратора, збір додаткової інформації або вжиття інших заходів безпеки.
4. Виконання вибраних кроків: Після вибору подальших кроків система повинна виконати їх. Це може включати автоматичне застосування обмежень або блокування доступу до ресурсів, надсилання сповіщень адміністратору або користувачу, аналіз додаткової інформації для підтвердження або спростування підозри тощо.
5. Постійне вдосконалення системи: Система прийняття рішень повинна бути піддана постійному вдосконаленню на основі набутого досвіду та нової інформації про шахрайські методи. Це включає аналіз результатів рішень, зворотний зв'язок від користувачів та аналітику, пошук нових шаблонів шахрайства та покращення моделей і алгоритмів виявлення.

Загалом, розробка системи прийняття рішень щодо подальших кроків після виявлення підозрілої активності вимагає комплексного підходу, що

включає аналіз, оцінку ризику та вибір відповідних заходів з мінімальним впливом на законних користувачів.

2.3 Юридичні аспекти та впровадження

2.3.1 Вивчення юридичних аспектів, пов'язаних зі збором та обробкою даних, а також використанням результатів аналізу для прийняття рішень

Вивчення юридичних аспектів, пов'язаних зі збором та обробкою даних, а також використанням результатів аналізу для прийняття рішень, є важливою складовою розробки системи протидії шахрайству в Інтернеті. Тут декілька ключових аспектів, які варто врахувати:

1. Законодавча відповідність: Перш за все, необхідно дослідити і розуміти юридичні вимоги, пов'язані зі збором, зберіганням та обробкою даних користувачів. Це можуть бути вимоги, встановлені загальними законами про захист персональних даних, як-от Загальний регламент про захист даних (GDPR) в Європейському Союзі або його еквіваленти в інших юрисдикціях. Також варто враховувати специфічні вимоги або обмеження, пов'язані зі збором та обробкою даних для цілей виявлення шахрайства.
2. Згода та прозорість: При зборі даних важливо мати ясну згоду користувачів на їх обробку. Користувачі повинні бути повідомлені про цілі та способи використання їх даних для виявлення шахрайства. Прозорість і зрозумілість процесів обробки даних є важливими для забезпечення довіри користувачів та дотримання законодавчих вимог.
3. Анонімізація та псевдонімізація: Для забезпечення конфіденційності та захисту особистих даних користувачів можна використовувати техніки анонімізації або псевдонімізації. Це дозволяє використовувати дані у вигляді,

який не дозволяє прямо ідентифікувати окремих користувачів, зменшуючи ризик порушення конфіденційності.

4. Збереження та захист даних: Дослідження юридичних вимог повинно включати вивчення вимог до збереження та захисту даних. Забезпечення безпеки та цілісності даних, а також використання відповідних технічних заходів для запобігання несанкціонованому доступу до даних є важливими аспектами уникнення порушень безпеки.
5. Дотримання принципів пропорційності та обмежень: При використанні результатів аналізу для прийняття рішень важливо дотримуватися принципів пропорційності та обмежень. Це означає, що обрані заходи повинні бути відповідними виявленому ризику, а також необхідно уникати непропорційних обмежень прав користувачів.

Підсумовуючи, вивчення юридичних аспектів, пов'язаних зі збором та обробкою даних, а також використанням результатів аналізу для прийняття рішень, є важливим для забезпечення законності та етичності процесу боротьби з шахрайством. При розробці системи варто співпрацювати з юристами та експертами з питань захисту персональних даних, щоб забезпечити відповідність всіх процесів вимогам законодавства та максимальну захищеність даних користувачів.

2.3.2 Розробка політик та процедур для використання системи шахрайства з дотриманням законодавства та приватності

Розробка політик та процедур для використання системи протидії шахрайству з дотриманням законодавства та приватності є важливим етапом у забезпеченні ефективного та етичного використання такої системи. Ось кілька ключових кроків у цьому процесі:

1. Вивчення законодавства: Перш за все, необхідно ретельно дослідити та зрозуміти відповідне законодавство, пов'язане зі

збором, зберіганням та обробкою даних, а також використанням результатів аналізу для прийняття рішень. Це можуть бути загальні закони про захист персональних даних, такі як GDPR, а також специфічні вимоги, які стосуються виявлення шахрайства. Вивчення цих вимог допоможе розробити політики та процедури, що відповідають законодавчим вимогам.

2. Визначення цілей і обмежень: Важливо чітко визначити цілі використання системи протидії шахрайству, а також обмеження, які слід дотримувати. Наприклад, можуть бути встановлені обмеження щодо обсягу збирання даних, збереження терміну зберігання, обмеження використання даних для інших цілей, критерії доступу до даних та інші аспекти.
3. Розробка політик конфіденційності та згоди: Важливо розробити політики, які визначають, як будуть збиратися, оброблятися та зберігатися дані користувачів, а також яким чином результати аналізу будуть використовуватися для прийняття рішень. Політики конфіденційності повинні бути зрозумілими для користувачів та включати вимогу згоди на обробку їх даних.
4. Забезпечення безпеки даних: Розробка процедур і заходів для забезпечення безпеки даних є важливим аспектом. Вони можуть включати технічні заходи безпеки, контроль доступу до даних, захист від несанкціонованого доступу та інші заходи, спрямовані на забезпечення конфіденційності та цілісності даних.
5. Стеження за змінами у законодавстві: Законодавство про захист даних постійно змінюється та розвивається. Важливо підтримувати відповідність із новими законодавчими вимогами та оновлювати політики та процедури відповідно. Регулярне оновлення і перегляд політик і процедур є необхідним для

забезпечення актуальності та відповідності вимогам законодавства.

6. Навчання та свідомість користувачів: Для успішного впровадження системи протидії шахрайству важливо навчати та підвищувати свідомість користувачів. Користувачі повинні розуміти, як їхні дані будуть збиратися та оброблятися, а також як використовуватимуться результати аналізу для прийняття рішень. Навчання користувачів про правила конфіденційності, заходи безпеки та їхні права може сприяти покращенню прийняття системи та забезпеченню довіри користувачів.

Враховуючи ці кроки, розробка політик та процедур для використання системи протидії шахрайству з дотриманням законодавства та приватності стане фундаментом для ефективного та етичного застосування системи, забезпечуючи захист даних користувачів і дотримання вимог законодавства.

2.3.3 Розгляд відповідності розробленої системи протидії шахрайству законодавству та етичним стандартам

Розгляд відповідності розробленої системи протидії шахрайству законодавству та етичним стандартам важливий для забезпечення правової і моральної легітимності системи. Нижче представлені ключові аспекти, які слід враховувати під час такого розгляду:

1. Законодавство:

- Захист приватності: Перевірити, чи система дотримується вимог законодавства про захист особистої інформації та приватності користувачів. Визначити, які дані система збирає, як вони обробляються та зберігаються.
- Електронна комерція: Якщо система включає функції електронної комерції або фінансові операції, переконайтеся, що вона відповідає вимогам законодавства щодо електронної торгівлі та фінансових операцій.

2. Захист прав споживачів:

- Вивчити законодавство, що стосується захисту прав споживачів, особливо якщо система працює з особистими даними та інформацією користувачів.

3. Антидискримінація та рівні можливості:

- Врахувати принципи антидискримінації та рівних можливостей у використанні системи. Уникати будь-яких аспектів, які можуть призвести до дискримінації користувачів.

4. Безпека та кібербезпека:

- Перевірити, чи система відповідає вимогам щодо кібербезпеки. Забезпечте захист інформації від несанкціонованого доступу та забезпечте безпеку та цілісність даних.

5. Етичні стандарти:

- Прозорість: Забезпечити прозорість у використанні системи, розкриваючи користувачам, як їхні дані збираються та використовуються.
- Відповідальність: Розглянути етичний аспект відповідального використання системи та можливі наслідки для користувачів.

6. Правила інтелектуальної власності:

- Впевнитись, що ваша система не порушує права інтелектуальної власності інших компаній або осіб.

7. Антитрестовське законодавство (якщо застосовується):

- Якщо система взаємодіє з іншими компаніями або займає домінуюче становище на ринку, вивчити антитрестовське законодавство та дотримуватися його вимог.

Забезпечення відповідності системи законодавству та етичним стандартам є необхідним етапом у розробці та впровадженні будь-якої системи, особливо тієї, яка має стосування до особистих даних та комунікацій користувачів в соціальних мережах.

2.3.4 Розгляд можливих впливів системи протидії шахрайству на приватність користувачів

Розгляд можливих впливів системи протидії шахрайству на приватність користувачів є важливим етапом при розробці та впровадженні такої системи. Нижче подані ключові аспекти, які слід враховувати при аналізі можливого впливу системи на приватність:

1. Збір та обробка особистої інформації:
- Визначити, які конкретно дані збирає ваша система для виявлення шахрайства. Це може бути інформація про активність користувача, даних авторизації, геолокація тощо.
- Розглянути, як ці дані будуть оброблятися та зберігатися, та чи існує можливість анонімізації або псевдонімізації.
2. Комунікація та повідомлення:
- Забезпечити прозорість щодо того, як система взаємодіє з користувачами та повідомляє їх про виявлені випадки шахрайства.
- Розробити чіткі правила та політики щодо сповіщення користувачів про будь-які дії системи, які можуть стосуватися їхньої приватності.
3. Захист особистої інформації:
- Впевнітись, що система надійно захищає особисті дані від несанкціонованого доступу та забезпечує конфіденційність користувачів.
- Розглянути використання шифрування для захисту передачі та зберігання конфіденційної інформації.
4. Права користувачів:
- Визначити, які права мають користувачі стосовно їхніх особистих даних у системі.

- Розробити механізми для доступу користувачів до їхніх даних, можливості видалення та контролю за їхньою приватністю.

5. Мінімізація обсягу збору даних:

- Спроектувати систему так, щоб збирати лише необхідні дані для ефективного виявлення шахрайства, мінімізуючи кількість збирається інформації.

6. Оцінка ризиків та аудит:

- Виконати оцінку ризиків з приводу можливих порушень приватності та розробіть план аудиту, щоб забезпечити відповідність приватності протягом експлуатації системи.

7. Інформування та навчання користувачів:

- Забезпечити ефективну систему інформування та навчання для користувачів щодо можливостей виявлення шахрайства та впливу системи на їхню приватність.

8. Врахування регуляторних вимог:

- Врахувати законодавство про захист особистих даних та інші регуляторні вимоги, які можуть стосуватися вашого регіону або цільової аудиторії.

Здійснення ретельного розгляду можливого впливу системи на приватність користувачів допомагає забезпечити баланс між ефективністю виявлення шахрайства та збереженням основних принципів приватності та етики.

2.4 Експерименти та оцінка системи

2.4.1 Розробка політик та процедур для використання системи шахрайства з дотриманням законодавства та приватності

Проведення експериментів з реальними даними є важливим етапом для оцінки ефективності системи протидії шахрайству. Основною метою цих експериментів є визначення того, наскільки добре система здатна

виявляти шахрайство і розрізняти його від законної діяльності. Ось деякі кроки, які можуть бути виконані під час проведення таких експериментів:

1. Збір реальних даних: Потрібно зібрати достатню кількість реальних даних, що включають в себе поведінку користувачів в інтернеті. Ці дані можуть бути отримані з веб-серверів, соціальних мереж, електронної пошти, транзакційних систем та інших джерел. Важливо врахувати конфіденційність та анонімність даних, а також дотримуватися вимог законодавства щодо захисту персональних даних.
2. Анотування даних: Для проведення експериментів необхідно анотувати дані, тобто вручну позначити підозрілі випадки шахрайства та нормальну діяльність. Це може вимагати експертного знання та участі фахівців з безпеки даних. Анотування даних допоможе створити набір для навчання моделей і оцінки їхньої ефективності.
3. Вибір метрик оцінки: Для оцінки ефективності системи потрібно вибрати підходящі метрики, які відображатимуть її точність, чутливість, специфічність та інші характеристики. Наприклад, такі метрики, як точність (precision), відсоток виявлених шахрайств (recall), F-мера (F-measure) та AUC-ROC (Area Under the Receiver)

2.4.2 Розробка політик та процедур для використання системи шахрайства з дотриманням законодавства та приватності

Визначення метрик успішності та порівняння результатів з існуючими системами та методами є важливим кроком при оцінці ефективності системи протидії шахрайству. Ось деякі типові метрики та підходи, які можуть бути використані в такому аналізі:

1. Точність (Precision): Ця метрика вимірює відсоток ідентифікованих підозрілих випадків, які насправді є

шахрайством, серед усіх виявлених підозрілих випадків. Висока точність означає, що система має низьку кількість помилкових спрацювань.

2. Повнота (Recall): Ця метрика вимірює відсоток ідентифікованих підозрілих випадків шахрайства серед усіх дійсно існуючих підозрілих випадків. Висока повнота означає, що система виявляє більшу кількість справжніх шахрайств.
3. F-мера (F-measure): Ця метрика об'єднує точність та повноту в одне значення, що дає збалансовану оцінку ефективності системи. F-мера розраховується на основі гармонічного середнього точності та повноти.
4. AUC-ROC (Area Under the Receiver Operating Characteristic curve): Ця метрика використовується для оцінки загальної здатності системи розрізняти між шахрайством та нормальною діяльністю. Вимірюється площа під кривою ROC, яка показує залежність між чутливістю (True Positive Rate) та специфічністю (1 - False Positive Rate) системи.
5. Порівняння з існуючими системами: Щоб оцінити ефективність системи, її результати можна порівняти з результатами існуючих систем та методів для боротьби з шахрайством. Це може включати порівняння метрик успішності, швидкості реакції, ступеня виявлення шахрайства та інших характеристик.

Важливо враховувати, що вибір метрик та порівняння з існуючими системами повинні бути здійснені з урахуванням конкретних особливостей контексту, типів шахрайства та цілей системи протидії.

Висновок до розділу 2

У даному розділі було розглянуто існуючі методи аналізу та противодії шахрайським діям . Наступний розділ буде присвячений вибору інструментів для розробки.

РОЗДІЛ 3
ОГЛЯД ТЕХНОЛОГІЙ ДЛЯ СТВОРЕННЯ ПРОГРАМНОГО ПРОДУКТУ

3.1 Мова програмування Python

Мова програмування Python є однією з найпопулярніших мов програмування, яка широко використовується у багатьох сферах, включаючи веб-розробку, наукові дослідження, аналіз даних та штучний інтелект. Ось огляд основних характеристик, переваг та недоліків мови Python:

Python є інтерпретованою, об'єктно-орієнтованою мовою програмування з динамічною типізацією. Вона була розроблена у 1990-х роках і має простий та зрозумілий синтаксис, що полегшує читання і розуміння коду.

Переваги мови Python:

1. Простота та читабельність: Python має лаконічний та зрозумілий синтаксис, що дозволяє легко розробляти й підтримувати код. Це сприяє прискоренню процесу розробки та полегшує спільну роботу в команді.
2. Велика кількість бібліотек: Python має широкий вибір сторонніх бібліотек та модулів, що робить його потужним інструментом для різних завдань. Наприклад, бібліотеки NumPy, Pandas, Matplotlib та SciPy дозволяють легко працювати з науковими обчисленнями та аналізом даних.
3. Портативність: Python підтримує багато платформ, включаючи Windows, macOS та різні дистрибутиви Linux. Це дозволяє розробникам писати код один раз і запускати його на різних операційних системах без необхідності значних змін.
4. Широке застосування: Python застосовується в різних галузях, включаючи веб-розробку, наукові дослідження, машинне

навчання, штучний інтелект, автоматизацію та багато іншого. Велика спільнота розробників дозволяє знайти підтримку та рішення для багатьох завдань.

5. Інтеграція з іншими мовами: Python підтримує механізми взаємодії з іншими мовами програмування, такими як C/C++, що дозволяє використовувати швидкі обчислення на мовах нижчого рівня та інтегрувати Python з існуючими проектами.

Недоліки мови Python:

1. Швидкодія: У порівнянні з деякими компільованими мовами, такими як C++ або Java, Python може бути повільнішим у виконанні. Це особливо важливо для обчислювально важких задач, де швидкодія є критичною.
2. Обмежена підтримка для мобільної розробки: Python не є найкращим вибором для мобільної розробки, оскільки не має широкої підтримки для платформ, таких як Android або iOS. Хоча існують деякі фреймворки, такі як Kivy, PySide, що дозволяють розробляти мобільні додатки на Python, але вони не настільки поширені, як інші мови програмування.
3. Обмежена підтримка для розробки ігор: Python не є першим вибором для розробки складних ігор, де швидкість та прямий доступ до апаратного забезпечення є важливими. Для розробки ігор використовуються інші мови програмування, такі як C++ або C#.
4. Обмеження в мобільних додатках: Якщо вам потрібен повний доступ до функціональності мобільних пристроїв, таких як GPS, камера або акселерометр, Python може мати обмежену підтримку. Для таких завдань використовуються мови, спеціалізовані на мобільній розробці, наприклад, Kotlin для Android та Swift для iOS.

5. Використання пам'яті: Python використовує багато пам'яті для збереження об'єктів, що може бути проблемою в обмежених ресурсах, таких як вбудовані системи або пристрої з обмеженими обсягами пам'яті.

Незважаючи на деякі недоліки, Python залишається однією з найбільш зручних та популярних мов програмування. Його простота, гнучкість та велика спільнота розробників роблять його потужним інструментом для широкого спектру завдань.

IDLE (Integrated Development and Learning Environment) - це інтегроване середовище розробки для мови програмування Python. IDLE поставляється разом зі стандартним пакетом Python і є одним з офіційних середовищ, які можна використовувати для розробки програм на Python.

Основні характеристики та можливості IDLE Python:

1. Редактор коду: IDLE надає текстовий редактор, в якому можна писати, редагувати та зберігати код Python. Редактор підтримує функції виділення синтаксису, автозавершення, перехід до визначення функції (Go to Definition) та інші корисні можливості.
2. Виконання коду: IDLE дозволяє виконувати Python-код безпосередньо з редактора. Ви можете виконати весь файл або вибрати окремий фрагмент коду для виконання.
3. Інтерактивний режим: IDLE надає інтерактивне середовище Python Shell, де ви можете вводити команди Python один за одним і бачити результати виконання негайно.
4. Модуль для візуального програмування: IDLE включає в себе модуль Tkinter, який дозволяє розробникам створювати графічні інтерфейси користувача (GUI) за допомогою візуального програмування.
5. Робота з файлами та проектами: Ви можете відкривати, зберігати та обробляти файли Python. IDLE також має підтримку для

створення проектів, що полегшує роботу з більшими кодовими базами.

6. Дебагер: IDLE має вбудований простий дебагер, який дозволяє вам встановлювати точки зупинки, крокувати код та аналізувати значення змінних під час виконання.
7. Допоміжні інструменти: IDLE містить інші корисні інструменти, такі як історія команд, довідкова система, автоматичне вирівнювання та інші.
8. Підтримка Unicode: IDLE підтримує Unicode, що дозволяє працювати з текстом у різних мовах та кодуваннях.
9. Платформонезалежність: IDLE є платформонезалежним і може використовуватися на різних операційних системах, таких як Windows, macOS та Linux.

IDLE Python є відмінним інструментом для новачків у програмуванні Python, а також зручним для швидкого виконання коду та експериментів в інтерактивному режимі. Для більш складних та розгалужених проектів можуть бути використані інші інтегровані середовища розробки (IDE).

3.2 Набір використаних бібліотек

1. customtkinter: це бібліотека інтерфейсу користувача Python, заснована на Tkinter, яка надає нові, сучасні і повністю настроювані віджети. Вони створюються та використовуються як звичайні віджети Tkinter, а також можуть використовуватися у поєднанні із звичайними елементами Tkinter. Кольори віджетів і вікон або адаптуються до зовнішнього вигляду системи, або до заданого вручну режиму (світлий, темний), а всі віджети та вікна CustomTkinter підтримують масштабування HighDPI (Windows, macOS). З CustomTkinter ви отримаєте одноманітний та сучасний вигляд на всіх настільних платформах (Windows, macOS, Linux).

2. tkinter: є стандартною бібліотекою для створення графічних інтерфейсів користувача (GUI) в мові програмування Python. Вона базується на бібліотеці Tk, яка розроблена для мови Tcl (Tool Command Language), але Tkinter надає обгортку для використання її в Python. Основним компонентом Tkinter є об'єкт Tk, який представляє вікно, де відбувається вся взаємодія з користувачем.
3. pymysql: це бібліотека для взаємодії з базами даних MySQL з допомогою мови програмування Python. Вона надає інтерфейс для виконання SQL-запитів та роботи з результатами в мові Python.
4. matplotlib: це потужна бібліотека для створення графіків та візуалізації даних в мові програмування Python. Вона надає широкий спектр можливостей для створення різноманітних видів графіків, включаючи лінійні графіки, стовбчасті діаграми, кругові діаграми, гістограми, контурні графіки та багато інших.

3.3 Машинне навчання та аналітика

CustomTkinter - це бібліотека інтерфейсу користувача Python, заснована на Tkinter, яка надає нові, сучасні і повністю настроювані віджети. Вони створюються та використовуються як звичайні віджети Tkinter, а також можуть використовуватися у поєднанні із звичайними елементами Tkinter. Кольори віджетів і вікон або адаптуються до зовнішнього вигляду системи, або до заданого вручну режиму (світлий, темний), а всі віджети та вікна CustomTkinter підтримують масштабування HighDPI (Windows, macOS). З CustomTkinter ви отримаєте одноманітний та сучасний вигляд на всіх настільних платформах (Windows, macOS, Linux).

Машинне навчання та аналітика є двома важливими галузями в сфері обробки даних, які використовуються для виявлення закономірностей, отримання інсайтів та прийняття рішень. Ось огляд цих галузей:

Машинне навчання (Machine Learning): Машинне навчання використовує статистичні та комп'ютерні методи для навчання комп'ютерних систем здійснювати завдання без явного програмування. Воно розглядається як підгалузь штучного інтелекту і базується на ідеї, що комп'ютер може навчитися з досвіду та покращувати свою продуктивність з часом.

Машинне навчання використовує алгоритми та моделі для аналізу даних та виявлення закономірностей. Це може бути поділеним на кілька підгалузей, включаючи навчання з учителем, навчання без учителя та підсилене навчання. Застосування машинного навчання включає розпізнавання образів, класифікацію, кластеризацію, прогнозування та багато іншого.

Аналітика (Analytics): Аналітика охоплює процес збору, обробки, аналізу та інтерпретації даних з метою здобуття інсайтів та прийняття обґрунтованих рішень. Це включає в себе використання різних методів, статистичних моделей, алгоритмів та інструментів для розуміння даних та виявлення корисної інформації.

Аналітика може бути розподілена на декілька типів, включаючи дескриптивну аналітику, прогностичну аналітику та прескриптивну аналітику. Дескриптивна аналітика фокусується на описі попередніх подій, прогностична аналітика займається передбаченням майбутніх подій, а прескриптивна аналітика рекомендує дії на основі отриманих даних.

Машинне навчання та аналітика взаємопов'язані та використовуються в комбінації для вирішення складних проблем і виявлення патернів у великих обсягах даних. Машинне навчання може бути використане для побудови моделей прогнозування на основі даних, а аналітика допомагає зрозуміти та пояснити результати цих моделей. Обидві галузі мають велике значення для бізнесу, науки, медицини та інших галузей, де прийняття рішень базується на даних та інформації.

3.4 Бази даних

База даних (Database) - це організована колекція даних, яка зберігається та управляється з допомогою певної системи керування базами даних (СКБД). Бази даних використовуються для ефективного збереження, організації, пошуку та маніпулювання великими обсягами даних.

Основні складові бази даних:

1. Структура даних: База даних містить структуровані дані, організовані за певними правилами та форматами. Найпоширенішими структурами даних є таблиці, поля, реляційні зв'язки та інші.
2. Мова запитів: Для взаємодії з базою даних використовується спеціальна мова запитів, яка дозволяє виконувати операції пошуку, вставки, оновлення та видалення даних. Сама поширена мова запитів - це SQL (Structured Query Language).
3. Система керування базами даних (СКБД): Це програмне забезпечення, яке дозволяє створювати, управляти та використовувати бази даних. Деякі популярні СКБД включають MySQL, PostgreSQL, Oracle, Microsoft SQL Server та SQLite.

Використання баз даних:

1. Зберігання даних: Бази даних використовуються для збереження великого обсягу даних у структурованому та безпечному форматі. Вони дозволяють ефективно організовувати та зберігати дані для подальшого використання.
2. Операції пошуку та фільтрації: Бази даних дозволяють виконувати складні операції пошуку, сортування та фільтрації даних. Це дозволяє швидко отримувати необхідну інформацію з бази даних.
3. Забезпечення цілісності даних: Бази даних мають механізми для забезпечення цілісності даних, що означає, що дані в базі завжди залишаються у вірному та консистентному стані.

4. Многокористувацький доступ: Бази даних дозволяють кільком користувачам одночасно отримувати доступ до даних, а також контролюють права доступу для кожного користувача.
5. Забезпечення резервного копіювання та відновлення: Бази даних забезпечують можливість регулярного резервного копіювання даних, що гарантує їх безпеку та можливість відновлення в разі втрати.
6. Аналітика та звітність: Бази даних можуть бути використані для аналізу даних та генерації звітів, що дозволяє отримувати цінні інсайти та зробити обґрунтовані рішення.

Плюси використання баз даних:

- Ефективне збереження та організація даних.
- Швидкий доступ до великого обсягу даних.
- Забезпечення цілісності та безпеки даних.
- Многокористувацький доступ та контроль прав доступу.
- Можливість виконувати складні операції пошуку та аналізу даних.
- Забезпечення резервного копіювання та відновлення даних.
- Підтримка аналітики та звітності.

Мінуси використання баз даних:

- Вартість розгортання та підтримки бази даних.
- Вимоги до обладнання та ресурсів для ефективної роботи з базою даних.
- Складність налаштування та управління базою даних.
- Ризик втрати даних в разі неправильного управління або непередбачуваних ситуацій.

Загалом, бази даних є важливим інструментом для організації та управління даними. Вони забезпечують ефективне збереження, швидкий

доступ та безпеку даних, що дозволяє використовувати їх для аналітики, прийняття рішень та розвитку бізнесу.

3.5 MySQL

MySQL - це система управління базами даних (СУБД), яка використовує мову структурованих запитань (SQL) для створення, управління та взаємодії з базами даних. Розроблена та підтримується компанією Oracle Corporation, MySQL володіє великою популярністю через свою швидкодію, простоту використання та безкоштовний та відкритий код (Open Source).

Основні характеристики та можливості MySQL:

1. Мова SQL: MySQL використовує мову SQL для взаємодії з базою даних. SQL дозволяє створювати, зчитувати, оновлювати та видаляти дані з бази даних, а також виконувати адміністративні завдання.
2. Типи даних: MySQL підтримує різноманітні типи даних, включаючи числа, рядки, дати та час, географічні дані, JSON і багато інших. Типи даних можуть бути цілими числами, числами з плаваючою комою, рядками, датами, часами, та іншими.
3. Індексація: Індексація дозволяє прискорити пошук та вибірку даних з таблиць. MySQL підтримує створення різних видів індексів, таких як PRIMARY KEY, UNIQUE, та INDEX.
4. Транзакції: MySQL визначає транзакції для гарантії атомарності, консистентності, ізоляції та долі (ACID properties) під час виконання групи SQL-операцій.
5. Безпека: MySQL надає систему автентифікації та авторизації, що дозволяє контролювати доступ користувачів до бази даних. Використовуються ролі та права доступу.

6. Функції та збережені процедури: MySQL дозволяє створювати функції та збережені процедури, що полегшує повторне використання SQL-коду та підтримує модульність.
7. Реплікація: MySQL підтримує реплікацію для створення копій бази даних для забезпечення високої доступності та надійності.
8. Мови програмування: MySQL інтегрується з багатьма мовами програмування, включаючи Python, Java, PHP та інші, що полегшує роботу розробників у різних середовищах.
9. Інструменти адміністрування: Основним інструментом для адміністрування MySQL є MySQL Shell та MySQL Workbench. Вони дозволяють виконувати адміністративні операції, виконувати SQL-запити та моніторити базу даних.
10. Збережені точки відновлення (Savepoints): MySQL підтримує конструкцію SAVEPOINT для створення збережених точок відновлення, що дозволяє визначати точки для можливості відновлення стану транзакції.

MySQL є надійною та добре документованою СУБД, яка використовується у широкому спектрі проектів та застосунків, включаючи веб-розробку, бізнес-застосунки, телекомунікації, фінанси та інші.

MySQL Server - це система управління базами даних (СУБД) типу відкритого програмного забезпечення, яка використовує мову SQL для створення, управління та взаємодії з базами даних. MySQL є однією з найпопулярніших СУБД у світі і широко використовується у веб-розробці, бізнес-застосунках та інших областях.

Основні характеристики MySQL Server:

1. Мова SQL: MySQL використовує мову SQL (Structured Query Language) для взаємодії з базою даних. SQL дозволяє створювати, змінювати та опитувати дані в базі.
2. Транзакції: MySQL підтримує транзакції для гарантування консистентності даних при виконанні групи SQL-операцій.

3. Безпека: В MySQL реалізована система автентифікації та авторизації, що дозволяє обмежувати доступ користувачів до бази даних.
4. Індексація та оптимізація запитів: MySQL надає можливості для створення індексів, які покращують швидкодію великих таблиць, і має механізми оптимізації запитів.
5. Резервне копіювання та відновлення: MySQL дозволяє виконувати резервне копіювання бази даних для забезпечення безпеки даних і їх відновлення у випадку аварії.
6. Широкий спектр типів даних: Підтримка різноманітних типів даних, включаючи числа, рядки, дати, час, географічні дані, JSON і багато інших.

MySQL Workbench - це інтегроване середовище розробки та адміністрування для MySQL, яке надає графічний інтерфейс для взаємодії з базами даних. Це потужний інструмент, який дозволяє розробникам та адміністраторам зручно працювати з MySQL Server.

Основні можливості MySQL Workbench:

1. Графічний дизайнер бази даних: MySQL Workbench надає зручний інтерфейс для створення та моделювання баз даних за допомогою графічного дизайнера.
2. Виконання SQL-запитів: Розробники можуть виконувати SQL-запити безпосередньо в середовищі MySQL Workbench і переглядати результати.
3. Адміністрування сервера: MySQL Workbench дозволяє адміністраторам управляти параметрами сервера, виконувати резервне копіювання, відновлення, моніторити роботу сервера та інші адміністративні завдання.
4. Моделювання та оптимізація запитів: За допомогою MySQL Workbench можна аналізувати та оптимізувати SQL-запити для поліпшення продуктивності бази даних.

5. Синхронізація та міграція: MySQL Workbench надає засоби для синхронізації баз даних та міграції даних між різними серверами MySQL.
6. Візуалізація виконання запитів: Можливість візуального відстеження виконання SQL-запитів та аналізу планів виконання.

MySQL Workbench і MySQL Server взаємодіють між собою, надаючи розробникам та адміністраторам повний набір інструментів для зручної роботи з базами даних MySQL.

3.6 Веб-розробка

Веб-розробка - це процес створення та побудови веб-сайтів або веб-додатків. Це включає розробку фронтенду (клієнтської частини), бекенду (серверної частини) та бази даних, які взаємодіють для створення функціональності та інтерфейсу веб-додатка.

Основні складові веб-розробки:

HTML (HyperText Markup Language): Це основна мова розмітки, яка використовується для створення структури та вмісту веб-сторінок.

CSS (Cascading Style Sheets): Використовується для оформлення та стилізації веб-сторінок, дозволяє задавати вигляд елементів, кольори, шрифти, розташування тощо.

1. JavaScript: Це мова програмування, яка додає інтерактивність до веб-сторінок. JavaScript використовується для динамічної зміни контенту, взаємодії з користувачем, асинхронного завантаження даних та багатьох інших функцій.
2. Бекенд: Це частина веб-додатка, яка відповідає за обробку логіки, збереження даних та взаємодію з базою даних. Для розробки бекенду використовуються мови програмування, такі як Python, PHP, Ruby, Java, C# та інші, а також фреймворки, які спрощують процес розробки.

3. Бази даних: Використовуються для збереження та організації даних веб-додатка. Популярні бази даних включають MySQL, PostgreSQL, MongoDB, SQLite та інші.

Використання веб-розробки:

1. Створення веб-сайтів: Веб-розробка використовується для створення статичних веб-сторінок, веб-сайтів-візиток, блогів та інших типів веб-сайтів.
2. Розробка веб-додатків: Веб-розробка дозволяє створювати складні веб-додатки, такі як соціальні мережі, електронні комерційні платформи, онлайн-сервіси, інструменти для спільної роботи та багато іншого.
3. Мобільна веб-розробка: Веб-розробка також може використовуватися для створення мобільних веб-додатків, які можуть запускатися у веб-браузері на мобільних пристроях.
4. Адаптивний дизайн: Застосування веб-розробки дозволяє створювати веб-сайти, які коректно відображаються на різних пристроях та екранах розміром, що підходить для мобільних пристроїв, планшетів та настільних комп'ютерів.
5. Покращення взаємодії з користувачем: Веб-розробка дозволяє додавати різноманітні елементи інтерактивності та взаємодії до веб-сайтів, такі як форми зворотного зв'язку, анімація, перетягування та багато іншого.

Веб-розробка є важливою галуззю, оскільки дозволяє створювати інтерактивні та цікаві веб-додатки, які надають значимість користувачам і допомагають досягти бізнес-цілей.

Висновок до розділу 3

У даному розділі наведені характеристики інструментів, що будуть використані під час розробки продукту. У наступному розділі буде розглядатися сам процес розробки.

РОЗДІЛ 4

ПРОГРАМНИЙ ПРОДУКТ

4.1 Розробка системи протидії шахрайству

4.1.1 Побудова системи, яка виявляє та реагує на підозрілу поведінку користувачів.

Побудова системи, яка виявляє та реагує на підозрілу поведінку користувачів, включає кілька етапів. Нижче наведено загальний опис цих етапів:

1. Збір даних: Система повинна мати можливість збирати різноманітні дані про користувачів та їх поведінку. Це можуть бути дані про активності на веб-сайті, історія транзакцій, вхідні дані від сенсорів або будь-які інші відомості, що можуть бути корисними для виявлення підозрілої діяльності.
2. Аналіз даних: Після збору даних необхідно провести їх аналіз для виявлення підозрілих патернів та аномалій. Для цього можуть використовуватися методи машинного навчання, статистичний аналіз, алгоритми класифікації та кластеризації.
3. Виявлення підозрілої поведінки: На основі аналізу даних система може встановлювати порогові значення або правила, за допомогою яких буде виявляти підозрілу поведінку користувачів. Це можуть бути, наприклад, незвичайні активності, надзвичайно великі або незвичайні транзакції, зміни звичайних патернів поведінки та інші ознаки, що вказують на потенційну шахрайську діяльність.
4. Реагування та захист: Якщо система виявляє підозрілу поведінку, вона повинна мати можливість вживати відповідних

заходів захисту. Це може включати блокування доступу, сповіщення адміністраторів, вимоги до додаткової аутентифікації, перевірку заборонених дій та інші заходи для запобігання шахрайству.

5. Моніторинг та оновлення: Система повинна постійно моніторити поведінку користувачів та оновлювати свої правила та алгоритми на основі нових даних та виявлених шаблонів шахрайства. Це допоможе забезпечити ефективність системи та зменшити ризики.
6. Звітність та аналітика: Система також може надавати звіти та аналітичні дані про виявлену підозрілу діяльність користувачів. Це допоможе адміністраторам та відповідальним особам аналізувати тенденції, виявляти слабкі місця та приймати відповідні заходи для зміцнення системи протидії шахрайству.

Загалом, побудова системи виявлення та реагування на підозрілу поведінку користувачів включає збір даних, їх аналіз, виявлення підозрілої діяльності, реагування та захист, моніторинг та оновлення, а також звітність та аналітику. Ці етапи допомагають забезпечити ефективність та безпеку системи протидії шахрайству.

4.1.2 Розробка модулів для сповіщення адміністраторів або застосування інших заходів безпеки при виявленні підозрілого користувача.

Розробка модулів для сповіщення адміністраторів або застосування інших заходів безпеки при виявленні підозрілого користувача є важливою частиною системи протидії шахрайству. Нижче наведено деякі підходи та можливі модулі, які можуть бути використані для цієї цілі:

1. Сповіщення адміністратора: Модуль може бути розроблений для надсилання автоматичних сповіщень адміністраторам або відповідальним особам, коли виявляється підозріла діяльність.

Це може бути електронна пошта, SMS-повідомлення, повідомлення у месенджерах або інші канали зв'язку, що дозволяють оперативно повідомляти про потенційну загрозу.

2. Блокування доступу: Якщо виявлено підозрілу діяльність, модуль може заблокувати доступ користувача до певних ресурсів або функцій системи. Це може запобігти подальшому поширенню шахрайства та зменшити можливі збитки.
3. Додаткова аутентифікація: Модуль може вимагати від користувача пройти додаткову процедуру аутентифікації, наприклад, ввести додатковий код або використати біометричні дані. Це допоможе перевірити, що користувач є справжнім і мінімізує ризик несанкціонованого доступу.
4. Запис активності: Модуль може записувати активності підозрілих користувачів для подальшого аналізу та розслідування. Це може допомогти виявити шаблони та тренди шахрайства для подальшого вдосконалення системи.
5. Резервне копіювання та відновлення: Модуль може забезпечувати автоматичне резервне копіювання важливих даних або налаштувань системи. Це допоможе забезпечити можливість відновлення системи в разі успішного атаки або інциденту.
6. Аналіз та реагування в реальному часі: Модуль може використовувати аналітичні алгоритми для миттєвого аналізу потоку даних та реагування на підозрілі дії в реальному часі. Це дозволить системі швидко реагувати на шахрайську поведінку та негайно вживати заходів безпеки.
7. Машинне навчання та штучний інтелект: Модуль може використовувати методи машинного навчання та штучного інтелекту для автоматичного виявлення підозрілої поведінки та прийняття рішень. Наприклад, використання класифікаторів,

нейронних мереж або алгоритмів кластеризації може допомогти автоматично виявляти аномалії та підозрілу діяльність.

Ці модулі допоможуть системі виявляти та реагувати на підозрілу поведінку користувачів швидко та ефективно. Важливо розробити їх з урахуванням специфіки вашого додатка або системи, а також врахувати правові та етичні аспекти використання таких модулів.

4.2 Тестування та оцінка

4.2.1 Проведення експериментів для оцінки ефективності розробленої системи.

Проведення експериментів для оцінки ефективності розробленої системи є важливим етапом, який допоможе вам зрозуміти, наскільки добре ваша система протидії шахрайству працює. Нижче наведено кілька кроків, які можна виконати для проведення таких експериментів:

1. Визначити метрики успішності: Спочатку необхідно визначити метрики, за якими буде вимірюватися ефективність системи. Це можуть бути такі метрики, як точність виявлення шахрайства, кількість ложних позитивів (неправильно визнаних дій як підозрілих), кількість ложних негативів (неправильно не визнаних підозрілих дій) тощо.
2. Вибрати тестовий набір даних: Підготувати тестовий набір даних, який включає як підозрілі, так і доброчесні дії користувачів. Це дозволить нам оцінити роботу системи на різних типах даних та в різних сценаріях.
3. Застосувати систему до тестових даних: Запустити систему на тестовому наборі даних і зафіксуйте її результати. За допомогою розроблених метрик успішності оцінити, наскільки добре система виявляє підозрілу поведінку та уникне ложних сигналів.

4. Виконати порівняльний аналіз: Порівняти результати нашої системи з існуючими системами або методами для боротьби з шахрайством. Це допоможе нам зрозуміти, наскільки наша система ефективна у порівнянні зі стандартами або вже наявними рішеннями.
5. Аналізувати результати та вдосконалюйте систему: Проаналізуйте результати експериментів, ідентифікуйте сильні та слабкі сторони системи. Використовуйте ці відомості для вдосконалення системи та впровадження поліпшень.
6. Повторити експерименти: Повторити експерименти на більш широкому наборі даних або в різних умовах. Це дозволить нам перевірити стійкість та загальну ефективність системи.

Важливо пам'ятати, що експерименти з оцінки ефективності системи повинні бути проведені з врахуванням правових та етичних аспектів, зокрема захисту приватності користувачів та використання реальних даних відповідно до вимог законодавства.

4.2.2 Використання реальних або симульованих даних для перевірки роботи системи протидії шахрайству.

Для перевірки роботи системи протидії шахрайству можна використовувати як реальні дані, так і симульовані дані. Кожен з цих підходів має свої переваги і обмеження. Розглянемо їх докладніше:

1. Реальні дані: Використання реальних даних дозволяє вам оцінити роботу системи на реальних сценаріях та в реальному середовищі. Ви можете зібрати дані про поведінку користувачів, транзакції, дії тощо з живого середовища. Це дозволить вам оцінити реальну ефективність системи та виявити підозрілі дії, які вже стали причиною шахрайства.

Однак використання реальних даних може мати деякі обмеження. Крім того, реальні дані можуть бути обмеженими в обсязі або мають

нерівномірний розподіл підозрілих дій, що може вплинути на точність оцінки системи.

2. Симульовані дані: Використання симульованих даних дозволяє вам контролювати умови тестування та створювати різні сценарії для оцінки системи. Ви можете створити синтетичні дані, які відображають різні типи поведінки користувачів та підозрілі дії. Це дає вам можливість проводити експерименти у контрольованому середовищі та оцінювати реакцію системи на різні сценарії.

Симульовані дані також мають свої обмеження. Вони можуть не повністю відображати реальну поведінку користувачів або недостатньо реалістичні. Тому важливо розроброзробляти симуляції, які максимально наближені до реальності.

В ідеалі, комбінація реальних та симульованих даних може забезпечити комплексну оцінку роботи системи протидії шахрайству. Реальні дані можна використовувати для перевірки системи на реальних сценаріях, а симульовані дані допоможуть оцінити реакцію системи на різні типи підозрілих дій. Такий підхід дозволяє отримати більш повне уявлення про ефективність системи.

Важливо пам'ятати, що незалежно від типу даних, які використовуються, експерименти повинні бути проведені з урахуванням етичних аспектів, таких як захист приватності користувачів та дотримання законодавства.

4.2.3 Оцінка показників ефективності, таких як точність виявлення підозрілої поведінки та швидкість реакції на потенційні загрози.

Оцінка показників ефективності системи протидії шахрайству включає ряд метрик, серед яких основними є точність виявлення підозрілої

поведінки та швидкість реакції на потенційні загрози. Розглянемо ці метрики докладніше:

1. Точність (Accuracy): Ця метрика визначає, наскільки точно система виявляє підозрілу поведінку. Вона обчислюється як відношення кількості правильно класифікованих підозрілих випадків до загальної кількості класифікованих випадків. Висока точність означає, що система майже правильно виявляє підозрілу поведінку.
2. Швидкість реакції (Response Time): Ця метрика вимірює час, який потрібний системі для реагування на потенційну загрозу після виявлення підозрілої поведінки. Швидкість реакції грає важливу роль у забезпеченні безпеки, оскільки дозволяє системі приймати невідкладні заходи для запобігання шахрайству.
3. Чутливість (Sensitivity): Ця метрика визначає, наскільки добре система виявляє підозрілу поведінку серед реальних випадків. Вона обчислюється як відношення кількості правильно виявлених підозрілих випадків до загальної кількості фактично підозрілих випадків. Висока чутливість означає, що система ефективно виявляє підозрілу поведінку.
4. Специфічність (Specificity): Ця метрика визначає, наскільки добре система відмічає недійсні або непідозрілі випадки як нешахрайські. Вона обчислюється як відношення кількості правильно відмічених нешахрайських випадків до загальної кількості фактично нешахрайських випадків. Висока специфічність означає, що система мінімізує помилкові спрацювання і не відмічає непідозрілі випадки як підозрілі.
5. F-мера (F-measure): Ця метрика комбінує точність і чутливість, надаючи узагальнену міру ефективності системи. Вона обчислюється як гармонічне середнє між точністю і чутливістю.

Висока F-мера означає, що система досягає збалансованої точності і чутливості виявлення підозрілої поведінки.

Оцінка показників ефективності проводиться шляхом порівняння результатів з існуючими системами та методами для боротьби з шахрайством. Порівняння може включати аналіз ефективності, швидкості та інших важливих метрик для визначення переваг та обмежень розробленої системи.

4.3 Робота програми

4.3.1 Зовнішній вигляд та функціонал програми

При запуску програми, користувача просять ввести свої дані для того, щоб зберегти за ним результати тесту.

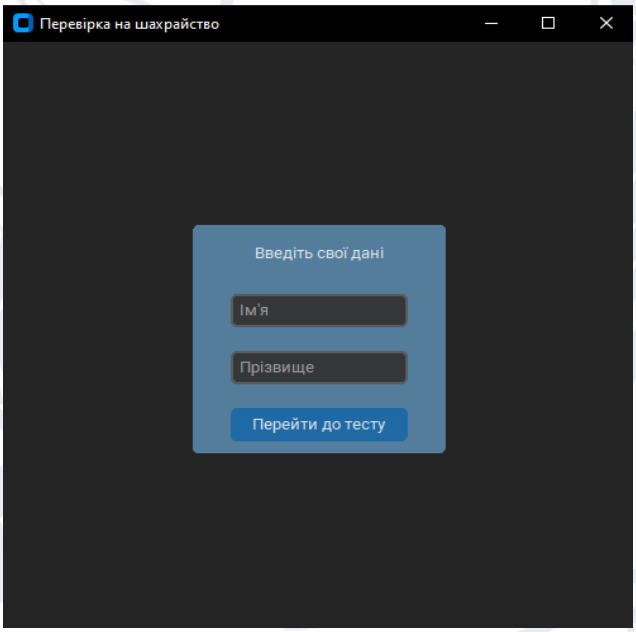

Рис. 4.3.1.1

Після запуску програми пропонується пройти тест, після проходження якого користувач може мати представлення того на скільки людина з протилежної сторони екрану являється шахраєм.

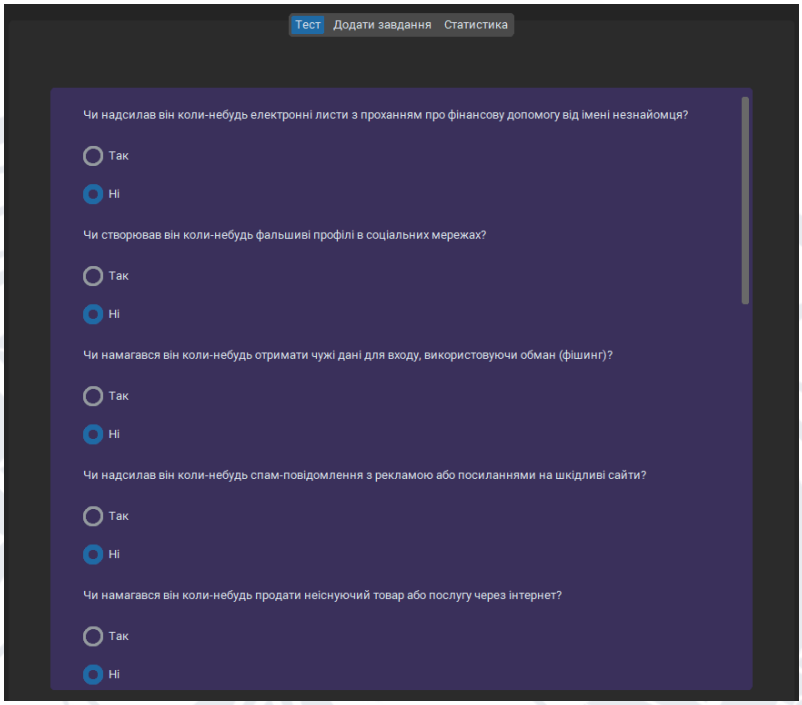

Рис. 4.3.1.2

В додатку є функція для адміниа, щоб додати питання для тесту.

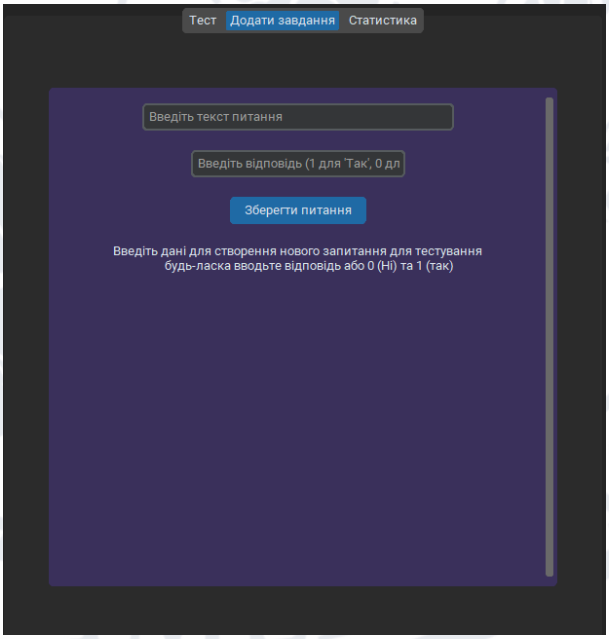

Рис. 4.3.1.3

Статистика злочинів шахраїв в соціальних мережах

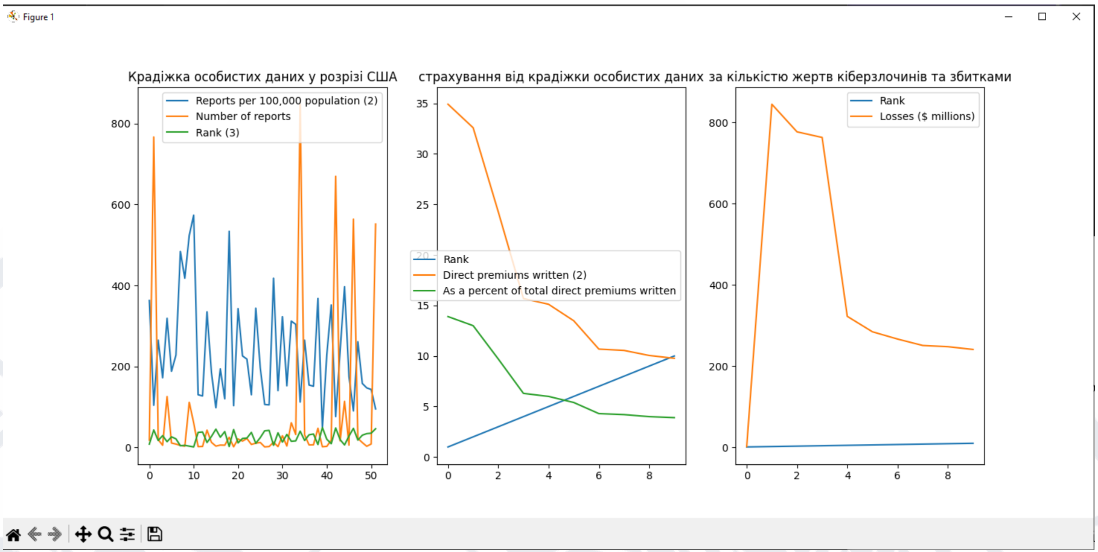

Рис. 4.3.1.4

Всі результати зберігаються, присутнє середнє значення випадків і відсоток після закінчення тесту.

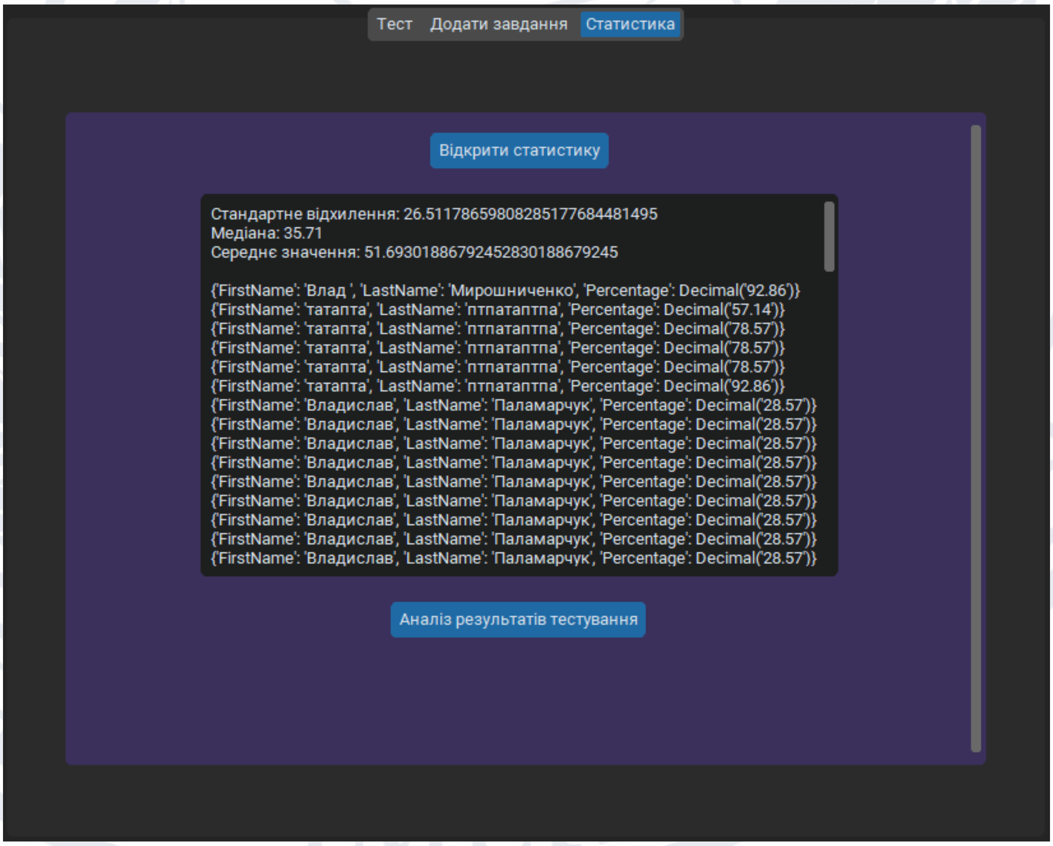

Рис. 4.3.1.5

Середній результат представлений в виді діаграми

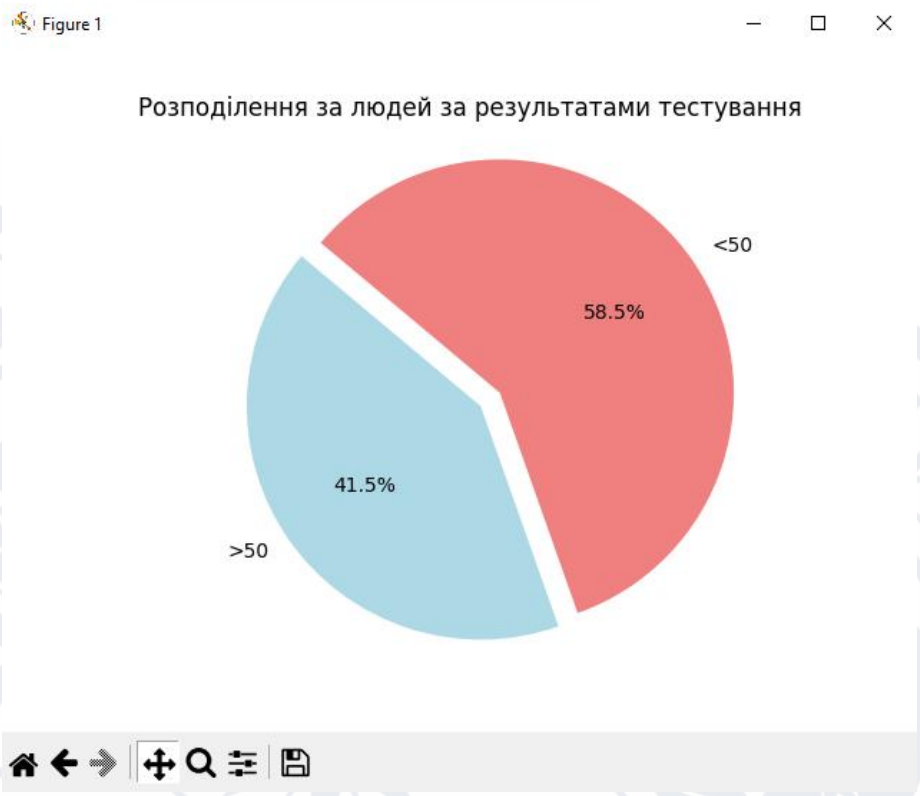

Рис. 4.3.1.6

Висновок до розділу 4

У даному розділі було розглянуто деякі етапи розробки додатку.

ВИСНОВКИ

Розроблена система боротьби з шахрайством є важливим і актуальним інструментом для захисту користувачів від шахрайських дій в мережі Інтернет. Шахрайство є серйозною проблемою, яка потребує ефективних та інноваційних підходів для запобігання його поширенню.

Система використовує різноманітні технології, включаючи машинне навчання, аналіз даних, виявлення аномалій та розробку алгоритмів для виявлення підозрілої поведінки користувачів. Це дозволяє системі ефективно ідентифікувати потенційні загрози та приймати відповідні заходи безпеки.

Розроблена система вимагає налагодження і оптимізації для досягнення максимальної ефективності. Використання реальних або симульованих даних для тестування та оцінки системи є важливим кроком у визначенні його потужності та обмежень.

Успішність розробленої системи може бути оцінена за допомогою різних метрик, таких як точність виявлення підозрілої поведінки, швидкість реакції на потенційні загрози, специфічність і чутливість системи тощо. Порівняння результатів з існуючими системами та методами також дасть можливість оцінити ефективність розробленої системи.

Розробка системи боротьби з шахрайством має юридичні аспекти, пов'язані зі збором, обробкою та використанням даних, а також захистом приватності користувачів. Урахування цих аспектів є важливим етапом у розробці політик та процедур для використання системи з дотриманням законодавства.

Оцінка ефективності системи та проведення експериментів з реальними або симульованими даними дає змогу зрозуміти, наскільки добре система працює в реальних умовах. Це допомагає виявити потенційні

недоліки і вдосконалити систему для покращення її функціональності та ефективності.

В цілому, розробка системи боротьби з шахрайством є складним завданням, яке вимагає поєднання технологій машинного навчання, аналітики даних, безпеки та юридичних аспектів. Ефективність системи може бути оцінена через проведення експериментів та порівняння з існуючими методами та системами боротьби з шахрайством.

Рекомендації для вдосконалення систем протидії шахрайству в соціальних мережах можуть включати різноманітні аспекти, спрямовані на забезпечення ефективності та відповідності нормам приватності та безпеки. Ось декілька рекомендацій:

1. Постійне оновлення алгоритмів виявлення:
- Регулярно вдосконалюйте алгоритми виявлення шахрайству, використовуючи нові технології та методи аналізу даних.
2. Використання штучного інтелекту та машинного навчання:
- Впроваджуйте розумні алгоритми машинного навчання та штучного інтелекту для виявлення нових типів шахрайства та підтримки системи в реальному часі.
3. Збільшення ступеня прозорості:
- Забезпечте користувачам чітку інформацію про те, як система виявлення шахрайства взаємодіє з їхніми даними та які заходи захисту приватності призначені.
4. Захист особистих даних:
- Максимально обмежуйте обсяг збору та збереження особистих даних, використовуйте сучасні методи шифрування та дотримуйтеся вимог щодо захисту конфіденційності.
5. Залучення користувачів у процес виявлення:
- Створюйте механізми для зворотного зв'язку від користувачів, щоб вони могли повідомляти про підозрілу активність та взаємодіяти з системою.

6. Партнерство з іншими соціальними мережами та службами:
- Укладайте партнерства з іншими платформами та організаціями для обміну інформацією про виявлені шахраї та ризиковані дії.
7. Ефективне навчання алгоритмів:
- Використовуйте дані про шахрайство для навчання алгоритмів, але зберігайте баланс між точністю та запобіганням зміщення.
8. Забезпечення відповідності з законодавством:
- Перевіряйте та оновлюйте систему відповідно до законодавства щодо захисту даних та приватності.
9. Етичні стандарти:
- Створюйте кодекс етики для системи протидії шахрайству, щоб забезпечити відповідальне використання та уникнути можливих етичних конфліктів.
10. Взаємодія з спільнотою:
- Відкривайте канали спілкування з користувачами та засновайте програми освіти для підвищення обізнаності щодо шахрайства та заходів боротьби з ним.

Ці рекомендації спрямовані на створення більш ефективних та етичних систем протидії шахрайству в соціальних мережах, зберігаючи при цьому високий рівень приватності та безпеки користувачів.

СПИСОК ЛІТЕРАТУРИ

1. Безпека інформаційних систем [Електронний ресурс] – Режим доступу до ресурсу: https://pidru4niki.com/74227/informatika/bezpeka_informatsiynih_sistem 11.09.2023
2. Кібербезпека [Електронний ресурс] – Режим доступу до ресурсу: https://dut.edu.ua/uploads/p_303_79299367.pdf 12.09.2023
3. Аналіз поведінки користувачів [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Аналіз_поведінки_користувачів 15.09.2023
4. Методи і техніки машинного навчання[Електронний ресурс] – Режим доступу до ресурсу: http://www-csd.univer.kharkov.ua/wp-content/uploads/2017/05/Metodi_mashinnogo_navchannya_2018_Ugryumov.pdf 20.09.2023
5. Виявлення аномалій і підозрілої поведінки [Електронний ресурс] – Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/46078/1/Keleberda_magistr.pdf 22.09.2023
6. Розробка систем інтелектуального аналізу [Електронний ресурс] – Режим доступу до ресурсу:http://www.tsatu.edu.ua/kn/course/intelektualnyj-analiz-danyh/ 25.09.2023
7. Системи керування базами даних [Електронний ресурс] – Режим доступу до ресурсу: https://miyklas.com.ua/p/informatica/9-klas/bazi-danikh-sistemi-keruvannia-bazami-danikh-361840/sistemi-keruvannia-bazami-danikh-352450/re-b0f14256-7ac2-4823-9f53-656061b85eaa 29.09.2023
8. Алгоритми класифікації та кластеризації [Електронний ресурс] – Режим доступу до ресурсу: http://csc.knu.ua/media/study/asp/mod_probl_inf_tech_sys_analysis_ivohin/lecture/lec11.pdf 01.10.2023

9. Системи прийняття рішень і обробки потокових даних [Електронний ресурс] – Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/48418/1/Systemy_i_metody_pidtrymky_pryiniattia_rishen.pdf 03.10.2023
10. Python – корисна річ чи черговий хайп? [Електронний ресурс] – Режим доступу до ресурсу: https://aws.amazon.com/ua/what-is/python/ 07.10.2023
11. Юридичні аспекти кібербезпеки та захисту персональних даних [Електронний ресурс] – Режим доступу до ресурсу: http://dspace.oduvs.edu.ua/bitstream/123456789/5139/1/12.pdf 10.10.2023
12. Приватність та етика обробки даних [Електронний ресурс] – Режим доступу до ресурсу: https://zmina.info/columns/zahyst-personalnyh-danyh-chomu-vazhlyvi-etychni-prynczypy-pid-chas-czyfrovizacziyi/ 12.10.2023
13. Оцінка ефективності систем захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: http://visnikkrnu.kdu.edu.ua/statti/2011-1-1(66)/16.pdf 15.10.2023
14. Технології моніьорингу та логування [Електронний ресурс] – Режим доступу до ресурсу: https://soft-den.com/monitoring-and-logging 18.10.2023
15. Віізуалізація даних [Електронний ресурс] – Режим доступу до ресурсу: https://www.ranktracker.com/uk/blog/what-is-data-visualization-and-how-to-use-it-for-seo/ 20.10.2023
16. Зелінська О.В., Потапова Н.А., Волонтир Л.О. Інформаційні системи та технології в галузі. Навчальний посібник. Вінниця: ВНАУ, 2020. 263 с. 22.10.2023
17. Бурєннікова Н.В., Зелінська О.В., Ушкаленко І.М., Бурєнніков Ю.Ю. Оптимізаційні методи та моделі. Навчальний посібник. Вінниця: ВНТУ, 2019. 114 с. 27.10.2023
18. Суханов А.О., Зелінська О.В. Використання сучасних інтелектуальних інформаційних технології. Комп'ютерні технології обробки даних: матеріали II Всеукраїнської науково-практичної конференції. Вінниця. ДонНУ імені Василя Стуса. 2021. С. 154-155. 01.11.2023

Додаток 2 до наказу
від «31» березня 2023 року
№119/05

ДЕКЛАРАЦІЯ

про дотримання академічної доброчесності

Я, _____
_____
____

Повністю вказується ПІБ та статус (посада для працівників, освітня (освітньо-наукова) програма – для здобувачів вищої освіти)

що нижче підписалась/підписався, розуміючи та підтримуючи загальновизнані засади справедливості, доброчесності та законності,

ЗОБОВ'ЯЗУЮСЬ:

дотримуватися принципів та правил академічної доброчесності, що визначені законодавством України, локальними нормативними актами Донецького національного університету імені Василя Стуса, положеннями, правилами, умовами, визначеними іншими суб'єктами, та не допускати їх порушення.

ПІДТВЕРДЖУЮ:

що мені відомі положення статті 42 Закону України «Про освіту»;

що у даній роботі не представляла/представляв чиїсь роботи повністю або частково як свої власні. Там, де я скористалася/скористався працею інших, я зробила/зробив відповідні посилання на джерела інформації;

що дана робота не передавалась іншим особам і подається вперше, не порушує авторських та суміжних прав закріплених статтями 21-25 Закону України «Про авторське право та суміжні права», а дані та інформація не отримувались в недозволений спосіб.

УСВІДОМЛЮЮ:

що ця робота може бути перевірена університетом на плагіат або інші порушення академічної доброчесності, в тому числі з використанням спеціалізованих сервісів;

що у разі порушення академічної доброчесності, до мене можуть бути застосовані процедури, передбачені законодавством України та Кодексом академічної доброчесності та корпоративної етики Донецького національного університету імені Василя Стуса, іншими локальними нормативними актами університету, та я можу бути притягнута/притягнутий до академічної відповідальності.

_____ _____

(дата) (підпис)