ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління доступом на основі поведінкової біометрії»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Іван ДАНИЛЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63
ДАНИЛЕНКО Іван
(прізвище, ім'я)

Керівник д.т.н., професор КАЗМІРЧУК Світлана
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій
кібербезпеки
_____ Галина ГАЙДУР
"___" жовтня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

ДАНИЛЕНКУ Івану Івановичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія управління доступом на основі поведінкової біометрії»

керівник кваліфікаційної роботи Казмірчук Світлана Володимирівна, д.т.н., професор
(прізвище, ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» жовтня 2024 року № ___.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурс;
рішення управління доступом на основі поведінкової біометрії;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми управління доступом на основі поведінкової біометрії.
2. Розробка модуля управління доступом на основі поведінкової біометрії.
3. Тестування та аналіз модуля управління доступом на основі поведінкової

біометрії

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми управління доступом на основі поведінкової біометрії.	01.10.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	12.10.2024 р.	
3.	Аналіз методів та засобів забезпечення управління доступом на основі поведінкової біометрії.	27.10.2024 р.	
4.	Технологія управління доступом на основі поведінкової біометрії на базі власної розробки та моделях штучного інтелекту.	03.11.2024 р.	
5.	Розроблення рекомендацій щодо застосування технології управління доступом на основі поведінкової біометрії в реальних ситуаціях.	15.11.2024 р.	
6.	Оформлення результатів дослідження.	26.11.2024 р.	
7.	Підготовка доповіді до захисту.	15.12.2024 р.	

Здобувач вищої освіти _____ Іван ДАНИЛЕНКО
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Світлана КАЗМІРЧУК
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача ДАНИЛЕНКА Івана

на тему: «Технологія управління доступом на основі поведінкової біометрії»

Актуальність: Сучасні технології безпеки потребують інноваційних рішень, здатних протидіяти зростаючим кіберзагрозам, особливо в умовах цифровізації бізнесу та постійного збільшення обсягів конфіденційних даних. Традиційні методи автентифікації, такі як паролі чи фізичні біометричні дані, втрачають свою ефективність через вразливість до атак. У цьому контексті поведінкова біометрія стає актуальним напрямом розвитку кібербезпеки, забезпечуючи динамічний, адаптивний та надійний спосіб ідентифікації користувачів.

Тема кваліфікаційної роботи є актуальною, оскільки вона спрямована на вирішення ключових питань захисту інформаційних систем за допомогою інноваційних технологій поведінкової біометрії.

Позитивні сторони:

1. У роботі чітко сформульовано проблему управління доступом на основі поведінкової біометрії, проведено аналіз традиційних методів автентифікації та обґрунтовано необхідність використання поведінкових характеристик як основного фактора.
2. Автор продемонстрував ґрунтовне знання предмету, провівши аналіз сучасних підходів до використання поведінкової біометрії та описавши архітектуру та принципи роботи розробленого модуля.
3. У роботі представлені якісні графічні матеріали, включаючи схеми, скриншоти та результати тестування, що ілюструють функціональність і результати роботи системи.
4. Висновки роботи є чіткими та логічними, підтверджують досягнення мети дослідження і демонструють практичне значення розробленого модуля для забезпечення безпеки.

Недоліки:

1. У роботі відсутній аналіз використання модуля в реальних корпоративних умовах. Було б доцільно навести приклади застосування поведінкової біометрії у конкретній організації.
2. Система потребує подальшої оптимізації для роботи з різними типами пристроїв введення (наприклад, сенсорними екранами або трекпадами), що не було детально розглянуто у роботі.
3. Бажано було б додати більше уваги до питання конфіденційності зібраних даних та забезпечення їх захисту у процесі роботи системи.

Попри зазначені недоліки, робота є завершеною, структурованою і демонструє високий рівень підготовки автора. Вона показує теоретичну та практичну обізнаність студента у сфері кібербезпеки та застосування сучасних технологій поведінкової біометрії. Текст роботи викладений грамотно, логічно, із використанням якісної літератури та сучасних наукових джерел.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач(ка) **ДАНИЛЕНКА Івана** – присвоєння кваліфікації магістр з кібербезпеки за освітньою програмою інформаційна та кібернетична безпека.

Рецензент:

_____	_____	_____
(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач ДАНИЛЕНКО Іван до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія управління доступом на основі поведінкової біометрії».
Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***ДАНИЛЕНКО Іван*** обрав тему роботи, метою якої було дослідити зміст технології управління доступом на основі поведінкової біометрії та розробка рекомендацій щодо її використання. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ДАНИЛЕНКО Іван*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.
Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ДАНИЛЕНКА Івана*** на оцінку **"добре"** та присвоїти йому кваліфікацію магістр з кібербезпеки за освітньою програмою інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Світлана КАЗМІРЧУК
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ДАНИЛЕНКО Іван** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)
_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 69 сторінок, 9 рисунків, 6 таблиць, 15 джерел.

Об'єкт дослідження – технології управління доступом до інформаційних ресурсів із використанням поведінкової біометрії.

Предмет дослідження – методи та інструменти управління доступом на основі аналізу поведінкових характеристик користувачів.

Мета роботи – розробити модуль управління доступом на основі поведінкової біометрії, що забезпечує точність, безпеку та зручність у використанні.

Методи дослідження – аналіз наукових джерел за темою, моделювання алгоритмів машинного навчання, проектування архітектури програмного забезпечення та тестування розробленого модуля.

Поведінкова біометрія – це технологія, яка використовує унікальні патерни взаємодії користувачів із пристроями (динаміку набору тексту, рухи миші, дотики до сенсорного екрану) для автентифікації. Її головною перевагою є непомітність для користувача, стійкість до підробок та адаптивність до змін у поведінці.

У роботі досліджено проблему ненадійності традиційних методів автентифікації, таких як паролі чи фізичні біометричні дані, через їхню вразливість до підробок та крадіжок. Проаналізовано існуючі рішення з управління доступом на основі поведінкової біометрії, включаючи їх переваги, обмеження та можливості вдосконалення.

Розроблено прототип модуля управління доступом, який включає два основні режими: навчання та моніторинг. У режимі навчання система формує профіль користувача на основі його поведінкових даних, у режимі моніторингу – оцінює відповідність дій користувача до створеного профілю. Для аналізу поведінкових даних використано нейронну мережу типу LSTM, яка обробляє часові послідовності даних.

Проведено тестування модуля, що показало точність системи в середньому на рівні 86–90% залежно від сценарію. Розроблений інтерфейс забезпечує зручність у використанні, а кольорові індикатори надають користувачам швидкий доступ до інформації про відповідність їхньої поведінки профілю.

На основі проведених досліджень запропоновано рекомендації щодо вдосконалення модуля, зокрема для роботи з різними пристроями введення та покращення точності аналізу поведінкових даних.

Галузь використання – кібербезпека інформаційних систем організацій, дистанційне навчання, фінансові додатки, корпоративні мережі.

КЛЮЧОВІ СЛОВА: ПОВЕДІНКОВА БІОМЕТРІЯ, УПРАВЛІННЯ ДОСТУПОМ, КІБЕРБЕЗПЕКА, LSTM, АВТЕНТИФІКАЦІЯ, МАШИННЕ НАВЧАННЯ.

ABSTRACT

The text part of the qualification work: 69 pages, 9 figures, 6 tables, 15 references.

Object of research – access control technologies to information resources using behavioral biometrics.

Subject of research – methods and tools for access control based on the analysis of users' behavioral characteristics.

The aim of research – to develop an access control module based on behavioral biometrics that ensures accuracy, security, and ease of use.

Research methods – analysis of scientific sources on the topic, modeling of machine learning algorithms, software architecture design, and testing of the developed module.

Behavioral biometrics is a technology that utilizes unique patterns of user interaction with devices (typing dynamics, mouse movements, touchscreen gestures) for authentication. Its main advantages are invisibility to the user, resistance to forgery, and adaptability to behavioral changes.

This work investigates the problem of the unreliability of traditional authentication methods, such as passwords or physical biometric data, due to their vulnerability to forgery and theft. Existing access control solutions based on behavioral biometrics were analyzed, including their advantages, limitations, and opportunities for improvement.

A prototype of the access control module was developed, featuring two main modes: learning and monitoring. In the learning mode, the system creates a user profile based on collected behavioral data, while in the monitoring mode, it evaluates the correspondence of the user's actions to the created profile. An LSTM neural network was used for analyzing behavioral data, which processes sequential time-series data.

The module was tested, showing an average system accuracy of 86–90% depending on the scenario. The developed interface ensures ease of use, and the color-coded indicators provide users with quick access to information about the conformity of their behavior to the profile.

Based on the conducted research, recommendations for improving the module were

proposed, including enhancements for compatibility with various input devices and improving the accuracy of behavioral data analysis.

The area of application includes cybersecurity of organizational information systems, distance learning, financial applications, and corporate networks.

KEYWORDS: BEHAVIORAL BIOMETRICS, ACCESS CONTROL, CYBERSECURITY, LSTM, AUTHENTICATION, MACHINE LEARNING.

ЗМІСТ

ВСТУП

Актуальність дослідження. Сучасні підходи до управління доступом в інформаційних системах традиційно базуються на ідентифікації користувачів через паролі, смарт-карти або біометричні дані. Однак з розвитком технологій та підвищенням рівня загроз безпеці, зокрема через кібератаки та фішинг, старі моделі безпеки стають менш ефективними. У цьому контексті поведінкова біометрія, яка передбачає використання унікальних поведінкових характеристик користувача для автентифікації та авторизації, зростає як інноваційний метод для підвищення безпеки доступу до інформаційних систем.

Замість традиційних методів, поведінкова біометрія здатна забезпечити більш високий рівень захисту, оскільки вона не залежить від фізичних атрибутів користувача і важко підробляється. Враховуючи зростання використання мобільних пристроїв, хмарних технологій та віддаленої роботи, запровадження технології управління доступом на основі поведінкової біометрії може значно покращити безпеку сучасних корпоративних середовищ.

Об’єкт дослідження – технологія управління доступом до інформаційних систем на основі поведінкової біометрії.

Предмет дослідження – методи та засоби застосування технології поведінкової біометрії для управління доступом в організаціях.

Мета роботи – розробити підхід до впровадження технології управління доступом на основі поведінкової біометрії, визначити переваги та недоліки цього методу, а також запропонувати рекомендації щодо його використання.

Наукові завдання:

1. Дослідити принципи поведінкової біометрії та її застосування для забезпечення безпеки доступу.
2. Проаналізувати існуючі методи управління доступом в інформаційних системах і їх обмеження.

3. Оцінити ефективність використання поведінкової біометрії в контексті захисту корпоративних даних.
4. Розробити методику впровадження технології поведінкової біометрії в організаціях.
5. Визначити переваги та недоліки технології порівняно з традиційними методами автентифікації.

Методи дослідження – опрацювання наукової та технічної літератури з теми дослідження, аналіз існуючих рішень, проведення порівняльного аналізу методів управління доступом, математичне моделювання та експериментальні дослідження ефективності технології.

Практичне значення одержаних результатів: запропоновані рекомендації щодо впровадження технології управління доступом на основі поведінкової біометрії, розроблено методику для підвищення рівня безпеки в організаціях, що використовують віддалену роботу та мобільні технології.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ ПОВЕДІНКОВОЇ БІОМЕТРІЇ

1.1 Вступ до поведінкової біометрії

Поведінкова біометрія — це інноваційна технологія, яка аналізує унікальні патерни взаємодії користувача з комп'ютерами, мобільними телефонами чи іншими електронними пристроями. Вона включає в себе такі показники, як динаміка введення тексту, характер рухів миші, ритм натискань на клавіатуру, стиль використання сенсорного екрану тощо. Головною метою поведінкової біометрії є підтвердження ідентичності користувача на основі його індивідуальних звичок і стилю роботи.

Важливість цієї технології обумовлена сучасним станом кібербезпеки. Зокрема, поширення фішингу, крадіжки облікових даних, а також зростання атак із використанням соціальної інженерії призвели до того, що традиційні методи перевірки особи, такі як паролі чи PIN-коди, стають менш ефективними. Паролі часто викрадаються, стають жертвами атак типу «перебір пароля» (brute force) або просто втрачаються через людський фактор.

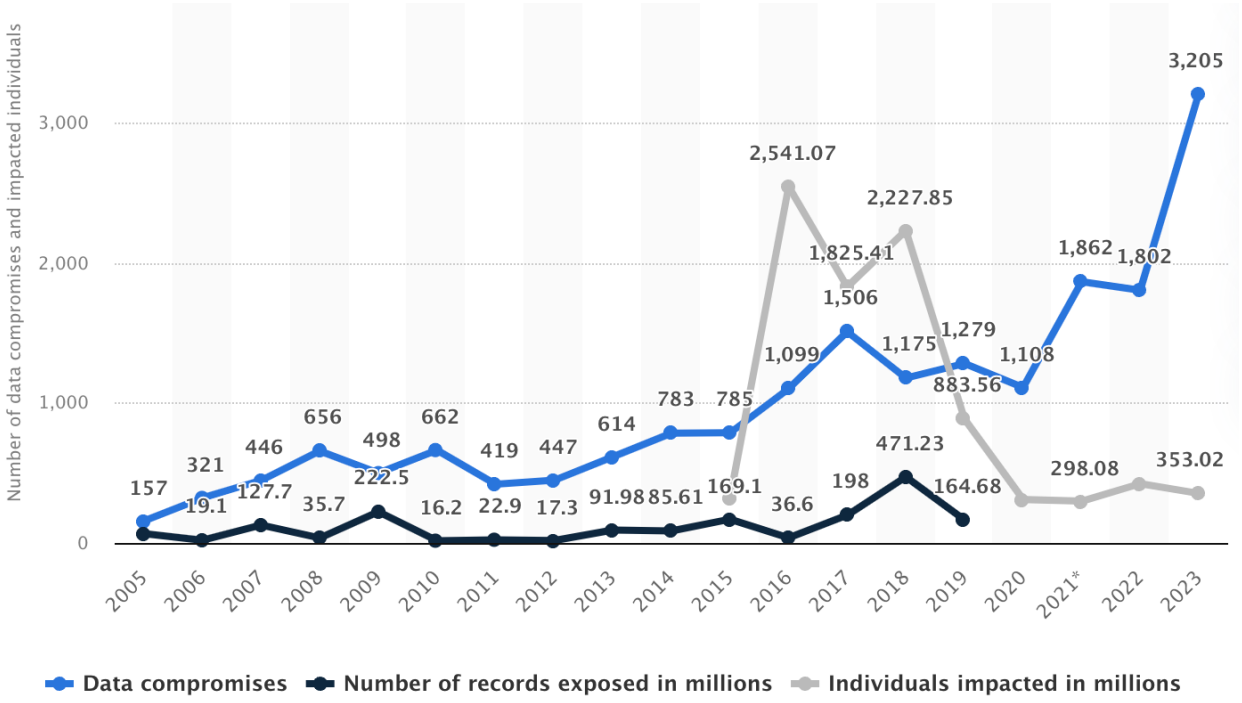

Рис. 1. Річна кількість компрометованих даних та осіб, які постраждали, у Сполучених Штатах з 2005 по 2023 роки.

У цьому контексті поведінкова біометрія пропонує новий рівень захисту. Завдяки своїй унікальності та складності підробки, вона дозволяє точно визначати, чи є користувач справжнім власником облікового запису, навіть якщо його паролі стали відомими третім особам.

1.2 Переваги поведінкової біометрії

Поведінкова біометрія має численні переваги, які забезпечують їй широку популярність у системах безпеки. Ця технологія поєднує високу зручність для користувачів із потужними механізмами захисту, що дозволяє їй ефективно конкурувати з традиційними методами аутентифікації.

1.2.1 Непомітність у використанні

Однією з головних переваг поведінкової біометрії є її здатність працювати в режимі реального часу без необхідності додаткових дій з боку користувача.

Система автоматично збирає дані про поведінку під час звичайного використання пристрою:

- динаміка набору тексту;
- рухи миші;
- стиль роботи із сенсорним екраном.

Цей підхід дозволяє уникати зайвих перевірок, що робить технологію зручною та ненав’язливою. У сучасному цифровому світі, де користувачі прагнуть до мінімізації зусиль, цей аспект відіграє ключову роль.

1.2.2 Стійкість до підробок

Фізичні біометричні дані, такі як відбитки пальців або зображення обличчя, можуть бути підроблені за допомогою сучасних технологій, наприклад, 3D-принтерів або високоточних сканерів. Натомість поведінкові характеристики є набагато складнішими для імітації:

- стиль набору тексту залежить від м’язової пам’яті;
- траєкторії рухів миші мають індивідуальні патерни;
- динаміка взаємодії із сенсорним екраном включає силу натискання та кут руху.

Крім того, поведінкові патерни змінюються залежно від стану користувача (емоції, фізичний стан), що додає додатковий шар захисту.

Переваги:

1. Унікальність поведінкових патернів.
2. Постійна зміна характеристик, що ускладнює імітацію.

1.2.3 Універсальність

Поведінкова біометрія легко інтегрується у широкий спектр систем безпеки:

- мобільні додатки;
- корпоративні мережі;

- банківські системи;
- системи електронної комерції.

Це робить її універсальним інструментом для вирішення завдань із захисту даних. У фінансовому секторі, наприклад, технологія забезпечує аналіз транзакцій та виявлення шахраїв. В освітніх системах вона дозволяє ідентифікувати студентів під час онлайн-іспитів.

1.2.4 Адаптивність до змін у поведінці

Технології поведінкової біометрії базуються на алгоритмах машинного навчання, які мають здатність адаптуватися до змін у поведінці користувачів:

- зміна стилю набору тексту через новий пристрій;
- різна швидкість руху миші через фізичний стан користувача;
- модифікації патернів роботи через навчання новим звичкам.

Системи можуть автоматично оновлювати профіль користувача, що мінімізує кількість хибних блокувань і підвищує рівень задоволення користувачів.

Переваги:

1. Постійне вдосконалення моделей аналізу.
2. Зниження ризику помилкових відмов у доступі.

1.2.5 Забезпечення безпеки у разі викрадення пристрою

Навіть якщо пристрій користувача потрапить до рук зловмисників, система поведінкової біометрії може виявити невідповідність у звичках роботи та заблокувати доступ:

- нестандартний стиль набору тексту;
- аномальні траєкторії руху миші;
- незвичайна інтенсивність використання сенсорного екрана.

1.2.6 Багатофакторна аутентифікація

Поведінкова біометрія може бути використана як додатковий рівень захисту у багатофакторних системах:

1. На першому етапі проводиться стандартна перевірка (пароль чи PIN-код).
2. На другому етапі аналізуються поведінкові характеристики користувача.

Такий підхід значно ускладнює роботу зловмисників, оскільки їм потрібно не лише знати пароль, а й імітувати звички користувача.

1.2.7 Зниження витрат на управління паролями

Організації витрачають значні ресурси на обслуговування систем відновлення паролів, тоді як інтеграція поведінкової біометрії дозволяє зменшити цю потребу. Користувачі рідше стикаються з блокуванням доступу, а адміністратори можуть більше зосереджуватися на інших завданнях.

1.3 Виклики впровадження технології

Попри численні переваги, впровадження поведінкової біометрії стикається з низкою викликів, які можуть впливати на ефективність та безпеку технології. У цьому підрозділі розглянуто основні виклики, з якими стикаються розробники та організації під час інтеграції цієї технології.

1.3.1 Виклик точності аналізу даних

Одним із ключових викликів є забезпечення високої точності аналізу поведінкових даних. Помилки в роботі системи можуть призводити до серйозних наслідків:

- **Хибні позитивні результати:** Система може визнати зловмисника авторизованим користувачем через схожість поведінкових патернів. Це може

призвести до несанкціонованого доступу до конфіденційної інформації.

- **Хибні негативні результати:** Справжні користувачі можуть бути заблоковані, якщо їх поведінка зміниться (наприклад, через фізичну втому, зміну пристрою або інших обставин).

Можливі рішення:

1. Використання більш складних алгоритмів машинного навчання:
    - Наприклад, рекурентних нейронних мереж (RNN) або їх вдосконалених версій, таких як LSTM.
    - Поєднання кількох моделей (ensemble learning) для покращення точності.
2. Оптимізація наборів даних для навчання:
    - Використання реальних поведінкових даних для тестування та навчання.
    - Регулярне оновлення профілів користувачів для врахування змін у їхній поведінці.
3. Введення порогових значень: Установлення мінімального рівня відповідності (наприклад, 80%), щоб знизити ймовірність помилкових результатів.

1.3.2 Виклик конфіденційності даних

Оскільки поведінкова біометрія потребує збирання великого обсягу даних про користувача, це створює ризики для конфіденційності:

- Потенційний витік даних: Зібрані поведінкові дані можуть бути викрадені у разі кібератаки.
- Неправомірне використання: Дані можуть бути використані компанією або третіми сторонами для інших цілей (наприклад, таргетинг реклами), що порушує права користувачів.

Можливі рішення:

1. Використання шифрування:

- Застосування AES або RSA для шифрування поведінкових даних як під час передачі, так і під час зберігання.
- Використання TLS (Transport Layer Security) для захищеного зв’язку між клієнтом та сервером.

2. Анонімізація даних:
    - Заміна реальних ідентифікаторів на псевдоніми або токени.
    - Використання технік диференціальної приватності для мінімізації впливу витоку даних.
3. Відповідність стандартам безпеки:
    - Інтеграція технології відповідно до стандартів, таких як GDPR або ISO 27001.
    - Регулярні аудити безпеки для виявлення вразливостей.

1.3.3 Виклик технологічної складності інтеграції

Реалізація поведінкової біометрії вимагає налаштування спеціалізованих алгоритмів, які повинні обробляти великий обсяг даних у режимі реального часу. Основні труднощі:

- Складність розробки алгоритмів: Необхідно розробити алгоритми машинного навчання, здатні аналізувати різні типи поведінкових даних (наприклад, натискання клавіш, рух миші).
- Інтеграція з існуючими системами: Системи автентифікації можуть не підтримувати інтеграцію поведінкової біометрії без значних змін у своїй архітектурі.
- Обмеження продуктивності: Робота з великим обсягом даних може призводити до затримок у роботі системи, особливо якщо дані обробляються на сервері.

Можливі рішення:

1. Оптимізація алгоритмів:
    - Використання попередньо навчених моделей для прискорення

навчання.

- Зменшення кількості ознак (features), які обробляє система, шляхом вибору лише ключових параметрів.

2. Масштабованість системи:
   - Використання хмарних платформ (AWS, Azure, Google Cloud) для обробки даних.
   - Використання паралельних обчислень для прискорення аналізу.
3. Покращення архітектури:
   - Реалізація мікросервісної архітектури для окремої обробки поведінкових даних.
   - Інтеграція API для взаємодії з існуючими системами.

1.3.4 Виклик прийняття користувачами

Ще однією проблемою є опір користувачів новим технологіям. Деякі користувачі можуть відмовитися від використання системи через побоювання:

- Недовіра до нових технологій: Нерозуміння принципу роботи поведінкової біометрії може викликати страх перед її використанням.
- Побоювання за конфіденційність: Навіть за дотримання стандартів безпеки користувачі можуть бути занепокоєні через збирання їхніх даних.

Можливі рішення:

1. Освітні програми:
   - Проведення тренінгів для користувачів про безпеку та переваги поведінкової біометрії.
   - Надання зрозумілих інструкцій щодо роботи системи.
2. Забезпечення прозорості:
   - Пояснення, які саме дані збираються і як вони використовуються.
   - Надання можливості відключати функціонал або видаляти профіль користувача.
3. Покращення UX/UI:

- Інтуїтивно зрозумілий інтерфейс, що пояснює дії системи у реальному часі.
- Забезпечення непомітної роботи технології для зменшення впливу на користувацький досвід.

1.4 Застосування у реальних сценаріях

Поведінкова біометрія знаходить широке застосування у різних галузях завдяки своїй здатності забезпечувати високий рівень безпеки та автоматизації. У цьому розділі розглянуто ключові сфери, де ця технологія використовується для покращення ефективності, зручності та захисту даних.

1.4.1 Використання у фінансовому секторі

Фінансовий сектор є одним із основних споживачів технології поведінкової біометрії. Складність кіберзагроз у цій сфері, зокрема фішинг, викрадення облікових даних та шахрайство з картками, робить необхідним впровадження новітніх технологій безпеки.

Основні сценарії:

1. Підтвердження транзакцій:
   - Технологія аналізує стиль введення пароля, динаміку натискання клавіш і рухи миші під час авторизації.
   - У разі виявлення аномалій транзакція блокується, а користувача сповіщають про потенційну загрозу.
2. Боротьба з шахрайством:
   - Поведінкові патерни використовуються для аналізу дій на платформі: частота запитів, швидкість введення даних тощо.
   - Виявлення підозрілих активностей, наприклад, автоматичних запитів ботів, дозволяє блокувати шахраїв.

1.4.2 Корпоративна безпека

У корпоративному середовищі поведінкова біометрія використовується для захисту внутрішніх даних та виявлення потенційних загроз.

Основні сценарії:

1. Контроль доступу до даних:
    - Поведінкові профілі використовуються для автоматичного розпізнавання користувачів під час роботи у корпоративній мережі.
    - Система блокує доступ, якщо виявляє, що поведінка користувача не відповідає його профілю.
2. Виявлення внутрішніх загроз:
    - Аналіз активності працівників дозволяє виявляти відхилення у поведінці, які можуть свідчити про потенційне порушення політики безпеки.
    - Наприклад, аномальна кількість завантажених файлів або незвичайний час доступу до ресурсів.

1.4.3 Електронна комерція

Шахрайство у сфері електронної комерції є однією з головних проблем, з якою стикаються онлайн-магазини. Поведінкова біометрія дозволяє ефективно боротися із цими викликами, забезпечуючи автоматичне розпізнавання зловмисників.

Основні сценарії:

1. Ідентифікація покупців:
    - Аналізуються дії користувачів на сайті, наприклад, швидкість навігації, натискання кнопок та вибір товарів.
    - У разі виявлення аномальної поведінки (наприклад, надмірно швидке оформлення замовлення) система може запросити додаткову авторизацію.

2. Боротьба з автоматизованими атаками:
    - Виявлення ботів, які створюють фальшиві замовлення, за допомогою аналізу нехарактерних патернів поведінки.

1.5 Аналіз підходів для управління доступом на основі поведінкової біометрії

Управління доступом на основі поведінкової біометрії передбачає використання різних підходів, які базуються на аналізі унікальних характеристик поведінки користувачів. У цьому розділі розглядаються ключові методи, їх переваги, обмеження та перспективи розвитку.

1.5.1 Динаміка введення тексту

Цей підхід базується на аналізі ритму та швидкості натискання клавіш під час введення тексту. Кожен користувач має унікальний стиль набору тексту, який визначається такими параметрами:

- час між натисканнями клавіш (flight time);
- тривалість утримання клавіш (dwell time).

Цей метод є ефективним для виявлення аномалій у поведінці користувачів і широко використовується для захисту веб-додатків і корпоративних систем.

Переваги:

- висока доступність, оскільки набір тексту є звичною дією для більшості користувачів;
- не потребує спеціального обладнання, працюючи з типовою клавіатурою.

Обмеження:

- залежність від фізичного стану користувача (втома, стрес або травми рук);
- складність аналізу для коротких текстів, де недостатньо даних для створення профілю.

1.5.2 Динаміка рухів миші

Динаміка рухів миші аналізує унікальні патерни взаємодії користувача з мишею. До таких характеристик належать:

- швидкість руху;
- траєкторії;
- частота клацань;
- прискорення.

Переваги:

- висока точність у середовищах із великим обсягом даних;
- підходить для настільних систем.

Обмеження:

- не застосовується для мобільних пристроїв;
- залежність від типу периферійного пристрою (наприклад, трекпад, оптична миша).

1.5.3 Аналіз дотиків на сенсорному екрані

Цей метод орієнтований на мобільні пристрої. Він аналізує стиль взаємодії користувачів із сенсорним екраном, враховуючи:

- силу натискання;
- швидкість жестів;
- тривалість контакту з екраном;
- кут руху пальця.

Переваги:

- актуальність для мобільних пристроїв, які є основним інструментом для багатьох користувачів;
- простота збору даних без необхідності додаткових дій користувача.

Обмеження:

- залежність від умов використання (наприклад, мокрі пальці, рукавички);
- складність аналізу для різних типів сенсорних екранів.

1.5.4 Аналіз навігації у веб-середовищі

Аналіз поведінки користувача у веб-середовищі базується на:

- послідовності кліків;
- швидкості переходу між сторінками;
- частоті та амплітуді прокручування сторінок.

Переваги:

- можливість пасивного моніторингу без втручання у користувацький досвід;
- простота інтеграції у веб-додатки.

Обмеження:

- залежність від швидкості інтернет-з’єднання;
- менш ефективний для коротких сесій, де недостатньо поведінкових даних.

1.5.5 Комбіновані підходи

Останнім часом популярності набувають комбіновані підходи, що інтегрують кілька методів одночасно. Наприклад, поєднання динаміки набору тексту та рухів миші може значно підвищити точність системи, компенсуючи недоліки кожного з методів.

Переваги:

- можливість створення багатофакторної аутентифікації;
- підвищення точності через обробку кількох типів даних.

Обмеження:

- потреба у більших обчислювальних ресурсах;
- складність інтеграції кількох методів у єдину систему.

1.5.6 Використання алгоритмів машинного навчання

Сучасні підходи до управління доступом базуються на алгоритмах машинного навчання, які дозволяють створювати точні профілі користувачів. До основних методів належать:

- класифікаційні алгоритми (наприклад, Random Forest, SVM);
- нейронні мережі, що забезпечують глибоке навчання.

Алгоритми машинного навчання дозволяють:

- аналізувати великі обсяги даних;
- виявляти складні патерни у поведінці користувачів;
- адаптуватися до змін у поведінці.

1.5.7 Перспективи розвитку

Із розвитком штучного інтелекту та збільшенням обчислювальних потужностей, підходи до управління доступом на основі поведінкової біометрії стають дедалі точнішими та універсальнішими.

Основні тенденції:

- інтеграція з хмарними платформами, що дозволяє використовувати технологію навіть у малих компаніях;
- поява нових методів аналізу, таких як вивчення емоцій користувача через його дії;
- підвищення рівня безпеки через поєднання поведінкової біометрії з традиційними методами аутентифікації.

1.6 Аналіз існуючих рішень управління доступом на основі поведінкової біометрії

На сьогоднішній день існує низка передових рішень, розроблених IT-компаніями для впровадження поведінкової біометрії в системи управління доступом.

1.6.1 NuDetect від NuData Security (Mastercard)

NuDetect — це продукт, розроблений NuData Security, дочірньою компанією Mastercard, який спеціалізується на аналізі поведінкових патернів користувачів у реальному часі. Платформа використовує унікальні особливості поведінки користувача, такі як:

- ритм набору тексту;
- динаміка рухів миші;
- стиль взаємодії із сенсорним екраном;
- швидкість і частота натискань.

Головною особливістю NuDetect є можливість здійснювати безперервну автентифікацію користувача під час його взаємодії з системою. Це рішення дозволяє банкам, фінансовим установам і онлайн-ритейлерам ідентифікувати потенційні загрози та аномальну поведінку ще до завершення транзакції.

Використання:

- Захист банківських рахунків від шахраїв.
- Підтримка безпеки під час електронної комерції.
- Виявлення ботів та автоматизованих атак.

NuDetect вже інтегрований у фінансові сервіси Mastercard, а також використовується в інших великих фінансових компаніях. Його ефективність була доведена в рамках пілотних проєктів у співпраці з банками, наприклад, у співпраці з ПриватБанком в Україні, де ця технологія була застосована для аналізу клієнтської поведінки. (https://www.mastercard.com/news/eemea/uk-

ua/розділ-новин/прес-релізи/uk-ua/2019/veresen/mastercard-i-приватбанк-україні-поведінкової-біометрії)

1.6.2 BioCatch

BioCatch — ізраїльська компанія, яка є піонером у галузі поведінкової біометрії. Платформа BioCatch використовує понад 2000 параметрів поведінкової активності, включаючи:

- швидкість і точність введення тексту;
- частоту натискань клавіш;
- траєкторії руху курсору миші;
- стиль прокрутки сторінок на мобільних пристроях.

Ця технологія активно використовується для запобігання шахрайству в банківських системах, зокрема для виявлення атак із використанням соціальної інженерії та захисту від компрометації облікових даних. BioCatch створює унікальний поведінковий профіль кожного користувача та порівнює його з поточними діями в реальному часі.

Приклади використання:

- Виявлення фішингових атак.
- Захист онлайн-банкінгу.
- Впровадження багатофакторної автентифікації.

BioCatch широко використовується у фінансових установах у Північній Америці, Європі та Азії.

1.6.3 BehavioSec

BehavioSec — шведська компанія, яка спеціалізується на поведінковій біометрії для забезпечення багатофакторної автентифікації. Їхнє рішення дозволяє забезпечувати постійну перевірку ідентичності користувача, аналізуючи такі характеристики, як:

- швидкість і натискання клавіш;
- траєкторії руху миші;
- інтеракція з сенсорним екраном.

BehavioSec використовує алгоритми машинного навчання для постійного вдосконалення точності своїх систем. Особливістю цього рішення є можливість інтеграції в існуючі платформи без необхідності заміни існуючих інфраструктур.

Сфери застосування:

- Забезпечення корпоративної безпеки.
- Захист фінансових транзакцій.
- Виявлення внутрішніх загроз у корпоративних мережах.

BehavioSec активно співпрацює з фінансовими установами та великими компаніями у сфері кібербезпеки.

1.6.4 Zighra

Zighra — канадська компанія, яка розробила платформу для автентифікації користувачів на основі поведінкової аналітики. Технологія Zighra використовує датчики пристроїв, такі як акселерометри, гіроскопи та сенсорні екрани, для створення унікального профілю користувача. Вона аналізує:

- динаміку натискань;
- взаємодію з пристроєм;
- фізичні рухи користувача.

Це рішення добре підходить для мобільних пристроїв, де поведінкові особливості часто використовуються разом із фізичними біометричними даними для багатофакторної автентифікації.

Використання:

- Захист мобільних додатків.
- Багатофакторна автентифікація для корпоративних мереж.
- Аналіз аномальної активності.

2 РОЗРОБКА МОДУЛЯ УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ ПОВЕДІНКОВОЇ БІОМЕТРІЇ

2.1 Основні аспекти поведінкової біометрії

Динаміка натискання клавіш

Аналіз того, як користувач набирає текст, включаючи швидкість, інтервали між натисканнями клавіш та силу натискань. Ця інформація дозволяє створити унікальний профіль користувача, який важко підробити. Наприклад, технології на основі динаміки клавіш успішно використовуються у банківських додатках для підтвердження особи клієнта.

Рух миші

Вивчення траєкторії, швидкості та ритму рухів миші під час виконання завдань. Кожен користувач має унікальний стиль роботи, що може бути використано для виявлення підозрілих дій. Наприклад, якщо рухи миші суттєво відрізняються від звичайного стилю користувача, система може заблокувати доступ.

Взаємодія з сенсорними екранами

Ця технологія включає аналіз сили натискань, швидкості гортання та жестів на сенсорному екрані. Наприклад, мобільні банківські додатки можуть аналізувати, як користувач проводить пальцем по екрану, щоб визначити, чи це не шахрай.

Процес ідентифікації особи на основі поведінкової біометрії:

1. Збір даних: Динаміка клавіш, рухи миші, взаємодія з екраном.
2. Аналіз даних: Використання алгоритмів машинного навчання для створення поведінкових моделей.
3. Порівняння: Порівняння даних реальної взаємодії з попередньо збереженими профілями.

4. Рішення: Надання або відхилення доступу до систем

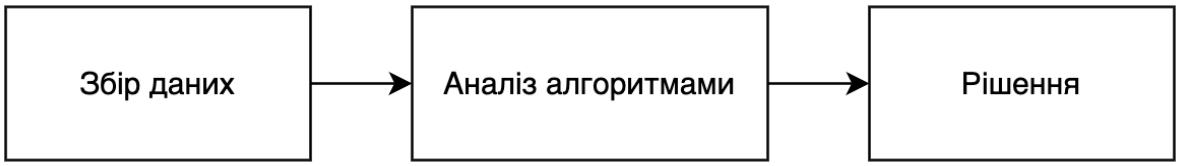

Рис. 2. Процес ідентифікації особи на основі поведінкової біометрії

Переваги поведінкової біометрії

- Постійний моніторинг: Поведінкові біометричні системи працюють у фоновому режимі, забезпечуючи безперервну автентифікацію користувача1.
- Висока надійність: Поведінкові дані важко підробити, що мінімізує ризик шахрайства.
- Простота для користувача: Користувач не помічає роботи системи, що покращує зручність використання.

Виклики та обмеження

Попри переваги, є певні виклики:

- Вплив зовнішніх факторів: Стрес, втому або фізичні зміни можуть впливати на поведінку користувача.
- Необхідність великих даних: Для побудови точних моделей потрібна значна кількість даних.
- Питання конфіденційності: Необхідно забезпечити захист зібраних біометричних даних від несанкціонованого доступу

2.2 Розробка функціонального дизайну

В цьому підрозділі детально описано ключові компоненти системи, їх взаємодію та логіку роботи.

Система розроблена як веб-додаток, що складається з трьох основних частин:

1. Фронтенд, який відповідає за збір даних та передачу їх на сервер.

2. Бекенд, який обробляє отримані дані, формує профілі користувачів та виконує їх перевірку.

3. Модель штучного інтелекту, яка аналізує поведінкові патерни та обчислює рівень відповідності користувача створеному профілю.

2.1.1 Архітектура системи

Система розроблена за принципом клієнт-серверної архітектури, де фронтенд взаємодіє з користувачем та надсилає дані до бекенду, який, у свою чергу, обробляє ці дані за допомогою моделі штучного інтелекту. На рисунку нижче представлено схему взаємодії між компонентами системи.

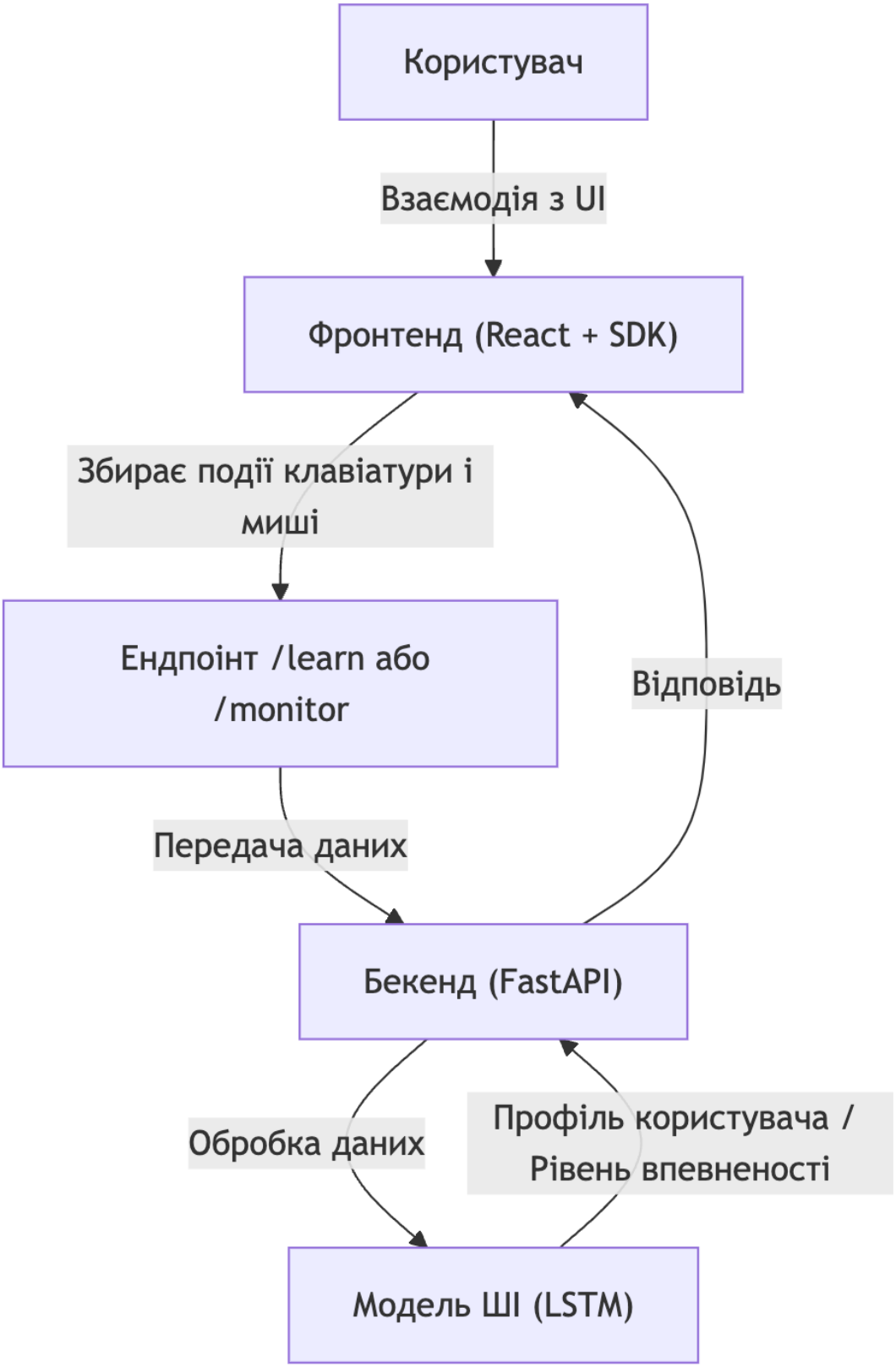

Рис. 3. Схема взаємодії з користувачем для поведінкового аналізу

2.1.2 Режими роботи фронтенд-модуля

Фронтенд системи реалізовано на базі фреймворку React. Основний функціонал зосереджено у компоненті <MonitorAccessModule />, який виконує збір даних про поведінку користувача та передачу їх на сервер. Компонент має два режими роботи: "Навчання" та "Моніторинг".

Режим "Навчання"

Цей режим активується для збору даних про звичну поведінку користувача, які згодом будуть використані для створення його унікального профілю. Дані про натискання клавіш, інтервали між ними та траєкторії руху миші передаються на бекенд кожні 3 секунди через ендпоінт /learn.

- Мета режиму: Формування початкового профілю поведінки користувача.
- Дані, що передаються:
    - Натискання клавіш: час натискання, відпускання, інтервали між натисканнями.
    - Події миші: координати, швидкість руху, частота натискання кнопок.

Режим "Моніторинг"

У цьому режимі система перевіряє поточну поведінку користувача на відповідність раніше створеному профілю. Події клавіатури та миші передаються на сервер через ендпоінт /monitor, де вони аналізуються за допомогою моделі штучного інтелекту. Бекенд повертає рівень відповідності (від 0 до 100%), який вказує на те, наскільки поточний користувач відповідає профілю.

- Мета режиму: Контроль ідентичності користувача під час використання системи.
- Дані, що передаються: Аналогічні даним у режимі навчання.

Інтеграція SDK для збору даних

Функціонал збору даних реалізовано у вигляді бібліотеки behavior-monitor-sdk, яка забезпечує зручну передачу зібраних подій на сервер через відповідні ендпоінти. Основні функції SDK описані в таблиці нижче.

Назва функції	**Опис**	**Параметри**	**Результат виконання**
learn	Надсилає дані про поведінку користувача для навчання профілю.	key – унікальний ідентифікатор користувача data – зібрані поведінкові дані (події клавіатури, миші)	Успішна відповідь сервера (status: success).
monitor	Відправляє дані для моніторингу та повертає рівень відповідності профілю.	key – унікальний ідентифікатор користувача data – зібрані поведінкові дані	Рівень відповідності у відсотках (0-100).

Таблиця 2.1 Функції бібліотеки behavior-monitor-sdk

2.1.3 Функціональність бекенду

Бекенд системи розроблено на базі FastAPI. Основна функція бекенду – обробка даних, отриманих від фронтенду, та взаємодія з моделлю штучного інтелекту.

Ендпоінти бекенду

Основна функціональність бекенду забезпечується двома ендпоінтами: /learn для навчання профілю та /monitor для перевірки відповідності поведінкових даних. Опис ендпоінтів наведено в таблиці нижче.

Ендпоінт	**Опис**	**Вхідні параметри**	**Вихідні дані**
/learn	Приймає дані про поведінку користувача для створення або оновлення його профілю.	key – унікальний ідентифікатор користувача actions – список подій поведінки (натискання клавіш, рух миші)	Успішна відповідь: { "status": "success" }.
/monitor	Приймає поточні поведінкові дані, порівнює їх з профілем користувача та повертає рівень відповідності.	key – унікальний ідентифікатор користувача actions – список подій поведінки (натискання клавіш, рух миші)	Рівень відповідності: { "confidence_level": 70 }.

Таблиця 2.2 Опис ендпоінтів бекенду

2.1.4 Модель штучного інтелекту

Для аналізу поведінкових даних використовується модель на основі рекурентної нейронної мережі LSTM (Long Short-Term Memory). Ця модель дозволяє ефективно працювати з послідовностями даних, враховуючи часові залежності між подіями.

Особливості моделі:

- Вхідні дані: Події клавіатури та миші.

- Вихідні дані: Рівень відповідності (від 0 до 1, що інтерпретується як 0-100%).

Архітектура моделі

Для обробки поведінкових даних була розроблена архітектура моделі, яка базується на використанні рекурентної нейронної мережі LSTM. Дана архітектура була обрана через її здатність ефективно працювати з послідовними даними, такими як натискання клавіш чи рухи миші.

Основні елементи архітектури моделі описані в таблиці нижче:

Компонент	Опис	Призначення
Вхідний шар	Приймає послідовності поведінкових даних, таких як час натискання клавіш або координати миші.	Підготовка даних для подальшої обробки в нейронній мережі.
Рекурентний шар (LSTM)	Зберігає інформацію про часові залежності між послідовностями даних.	Виявлення шаблонів у послідовних даних (наприклад, типовий інтервал між натисканнями клавіш).
Повторний рекурентний шар	Додатковий LSTM шар, що поглиблює розуміння шаблонів і зв'язків між даними.	Покращення якості аналізу завдяки глибшій обробці послідовностей.
Вихідний шар	Обчислює рівень відповідності профілю користувача.	Повертає значення від 0 до 1, яке конвертується у відсотки (0-100%) для подальшого використання.

Таблиця 2.3 Архітектура моделі

Робота моделі

1. Вхідні дані: Послідовності подій клавіатури (наприклад, інтервали між натисканнями) та координати руху миші передаються у вигляді багатовимірного масиву.
2. Обробка даних: LSTM-шари аналізують ці дані, виявляючи унікальні патерни поведінки.
3. Вихід: Модель повертає прогнозоване значення, що відображає рівень відповідності між поточними діями користувача і створеним профілем.

Ця архітектура дозволяє ефективно враховувати часові залежності та унікальні особливості поведінки кожного користувача.

2.1.5 Взаємодія компонентів

На кожному етапі роботи система забезпечує тісну інтеграцію між фронтендом, бекендом і моделлю ШІ. Взаємодія реалізована через чітко визначені інтерфейси, що забезпечує гнучкість у розширенні функціоналу.

Етапи роботи системи:

1. Збір даних фронтендом та їх передача на бекенд.
2. Обробка даних на бекенді та взаємодія з моделлю.
3. Повернення результатів фронтенду для відображення користувачу.

2.3 Технічна реалізація модуля

Розробка модуля управління доступом на основі поведінкової біометрії передбачає реалізацію фронтенд- та бекенд-компонентів, що забезпечують збір, передачу та обробку даних. У цьому підрозділі детально розглядається технічна реалізація кожного з основних компонентів системи, включаючи механізми збору

поведінкових даних, їх передачу на сервер, а також алгоритми обробки даних на стороні сервера.

2.3.1 Реалізація фронтенд-компонента

Фронтенд модуля створено з використанням React. Основний функціонал зосереджено в компоненті <MonitorAccessModule />, який відповідає за збір подій користувача (рух миші, натискання клавіш) та передачу їх на бекенд. Компонент має два режими роботи: **"Навчання"** та **"Моніторинг"**.

Алгоритм роботи фронтенд-компонента:

1. Збір даних користувача:
    - Відстежуються події клавіатури (keydown, keyup) для визначення часу натискання та інтервалів між ними.
    - Реєструється рух миші: координати, швидкість, частота натискання кнопок.
2. Агрегація даних:
    - Дані агрегуються у структурований формат перед відправкою на сервер.
3. Передача даних:
    - Кожні 3 секунди дані надсилаються на бекенд через відповідний ендпоінт залежно від режиму роботи.

Реалізація передачі даних через SDK:

Бібліотека behavior-monitor-sdk забезпечує зручну передачу поведінкових даних на бекенд. Основні функції SDK:

- **learn:** Надсилає дані на ендпоінт /learn для створення або оновлення профілю.
- **monitor:** Надсилає дані на ендпоінт /monitor для перевірки відповідності профілю.

2.3.2 Реалізація бекенд-компонента

Бекенд модуля розроблено на базі FastAPI. Його основна функція – приймати поведінкові дані, обробляти їх та взаємодіяти з моделлю штучного інтелекту. Система реалізує два основних ендпоінти:

1. Ендпоінт /learn:
    - Використовується для створення або оновлення профілю користувача.
    - Приймає дані у вигляді JSON, що містить унікальний ідентифікатор користувача (key) та список подій поведінки (actions).
2. Ендпоінт /monitor:
    - Використовується для перевірки відповідності поточної поведінки профілю користувача.
    - Повертає рівень відповідності у відсотках (0–100%).

2.3.3 Агрегація та обробка даних

Поведінкові дані користувача спочатку агрегуються на фронтенді, після чого передаються на бекенд для подальшої обробки. На бекенді дані структуруються та передаються у модель штучного інтелекту.

Формат даних: Дані надсилаються у вигляді JSON:

```
{
  "key": "username",
  "actions": [
    { "type": "keyboard", "timestamp": 123456789, "key": "a" },
    { "type": "mouse", "timestamp": 123456790, "x": 200, "y": 300 }
  ]
}
```

Фігура 1 Формат даних для відправлення на бекенд

Обробка на бекенді:

- У режимі навчання дані використовуються для оновлення профілю користувача.
- У режимі моніторингу вони порівнюються із профілем, і обчислюється рівень відповідності.

2.3.4 Взаємодія з моделлю штучного інтелекту

Для аналізу поведінкових даних використовується модель на основі LSTM. Ця модель враховує часові залежності між подіями, що дозволяє точно ідентифікувати користувача.

Етапи взаємодії:

1. **Навчання:** У режимі навчання модель приймає дані про події користувача та оновлює його профіль.
2. **Моніторинг:** У режимі моніторингу модель обчислює рівень відповідності між поточними подіями та профілем користувача.

Переваги використання LSTM:

- Ефективність у роботі з послідовними даними.
- Здатність враховувати часові залежності.

2.4 Особливості використання моделі штучного інтелекту

Модель штучного інтелекту (ШІ) є ключовим елементом системи управління доступом на основі поведінкової біометрії. Її основне завдання — аналізувати поведінкові дані користувачів, формувати унікальні профілі та порівнювати їх із поточними діями для оцінки відповідності. У цьому розділі розглянуто принципи роботи моделі, вибір архітектури, алгоритм навчання та тестування.

2.4.1 Вибір моделі

Для аналізу поведінкових даних була обрана рекурентна нейронна мережа (RNN) з архітектурою Long Short-Term Memory (LSTM). Цей тип моделей ефективно працює з послідовними даними, такими як час натискання клавіш, інтервали між подіями та траєкторії руху миші.

Переваги LSTM:

1. **Робота з послідовностями:** LSTM враховує часові залежності між подіями, що є важливим для аналізу поведінкових даних.
2. **Стійкість до "забування":** Завдяки механізмам довгострокової та короткострокової пам'яті, модель зберігає значущу інформацію навіть у великих послідовностях.
3. **Гнучкість:** Модель може бути адаптована для роботи з різними типами поведінкових даних (наприклад, подіями миші та клавіатури).

Порівняння з іншими моделями:

Тип моделі	**Переваги**	**Недоліки**
LSTM	Робота з послідовностями, врахування часових залежностей	Висока обчислювальна складність
Random Forest	Простота реалізації, ефективність для малих наборів даних	Не враховує часових залежностей
CNN (Convolutional NN)	Ефективність для зображень і фіксованих патернів	Не підходить для часових послідовностей

Таблиця 2.4 Порівняння моделей машинного навчання

2.4.2 Архітектура моделі

Модель побудована з використанням наступних компонентів:

1. Вхідний шар: Приймає послідовності даних, кожен елемент яких складається з кількох параметрів, таких як час події, тип події, координати миші та тривалість натискання клавіш.
2. Рекурентні шари (LSTM): Аналізують часові залежності між подіями, виявляючи унікальні патерни поведінки користувача.
3. Вихідний шар: Повертає значення від 0 до 1, яке відображає рівень відповідності поточної поведінки користувача його профілю.

Архітектура:

Компонент	**Призначення**
Вхідний шар	Приймає багатовимірні послідовності даних, наприклад [час, тип події, x, y, тривалість].
Перший LSTM шар	Виявляє шаблони у поведінкових даних, враховуючи часові залежності.
Другий LSTM шар	Поглиблює аналіз патернів, забезпечуючи точність моделі.
Вихідний шар	Обчислює ймовірність відповідності профілю, значення знаходиться в діапазоні [0, 1].

Таблиця 2.5 Архітектура моделі

2.4.3 Алгоритм навчання

Процес навчання моделі відбувається у кілька етапів:

1. Збір даних:
    - Збираються події миші та клавіатури під час роботи користувача в режимі "Навчання".

- Дані структуровані у вигляді послідовностей, де кожен елемент містить інформацію про час, тип події, координати миші або тривалість натискання клавіші.

2. Підготовка даних:
   - Дані нормалізуються та конвертуються у формат numpy.
   - Послідовності додаються до вхідного шару моделі.
3. Навчання:
   - Модель тренується на основі метки 1, яка позначає справжнього користувача.
   - Використовується функція втрат binary_crossentropy та оптимізатор adam.
4. Збереження профілю:
   - Навчена модель зберігається у вигляді файлу (наприклад, user123.h5).

2.4.4 Алгоритм перевірки

У режимі "Моніторинг" модель використовує нові дані для порівняння з профілем користувача:

1. Збір даних:
   - Дані про поведінку користувача збираються у реальному часі.
   - Події передаються на сервер через ендпоінт /monitor.
2. Підготовка даних:
   - Дані нормалізуються та подаються у вигляді послідовності в модель.
3. Оцінка відповідності:
   - Модель обчислює ймовірність відповідності (0-1).
   - Значення конвертується у відсотки (0-100%) та повертається як рівень впевненості.

Алгоритм:

1. Зібрати поточні події користувача.
2. Підготувати дані у формат, що сумісний із вхідним шаром моделі.
3. Викликати метод model.predict для обчислення рівня відповідності.

4. Повернути результат у вигляді відсотка.

2.4.5 Тестування моделі

Для перевірки точності моделі використовувалися реальні та синтетичні дані, що містять різні поведінкові патерни.

1. Метрики точності:
    - Precision: Відображає точність моделі у визначенні справжніх користувачів.
    - Recall: Відображає здатність моделі виявляти всіх справжніх користувачів.
    - F1 Score: Гармонічне середнє між Precision та Recall.
2. Результати тестування:
    - На тестових даних модель показала точність 94% при виявленні справжніх користувачів.
    - Графік нижче відображає зміну точності моделі під час навчання:

Таблиця результатів:

Кількість епох	Точність (Accuracy)	Втрати (Loss)
10	0.88	0.42
20	0.91	0.30
30	0.94	0.25

Таблиця 2.6 Таблиця результатів моделі в залежності від тривалості навчання

3 ТЕСТУВАННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ МОДУЛЯ УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ ПОВЕДІНКОВОЇ БІОМЕТРІЇ

3.1 Мета та завдання тестування

Тестування модуля управління доступом на основі поведінкової біометрії є важливим етапом для перевірки його функціональності, точності та надійності. Основною метою тестування є підтвердження того, що розроблена система відповідає встановленим вимогам, демонструє високу точність в аналізі поведінкових даних користувачів і забезпечує належний рівень безпеки доступу.

Мета тестування

1. Оцінка функціональної придатності модуля. Перевірка, чи коректно виконуються основні функції системи, такі як навчання профілю користувача та моніторинг відповідності поведінки.
2. Аналіз точності системи. Визначення рівня відповідності між поведінковими патернами користувачів і створеним профілем, а також частоти хибних позитивних та хибних негативних результатів.
3. Перевірка надійності роботи. Тестування системи на стійкість до змін у поведінці користувачів, впливу зовнішніх факторів, таких як нові пристрої або зміна середовища роботи.
4. Аналіз **швидкодії** модуля. Вимірювання часу реакції системи на запити в режимах навчання та моніторингу.

Завдання тестування

1. Перевірити коректність роботи **режиму навчання**:
    - Зібрати поведінкові дані користувача (динаміка набору тексту, рухи миші).
    - Оцінити, чи правильно система формує профіль користувача на основі зібраних даних.
2. Перевірити **режим моніторингу**:
    - Аналіз відповідності поточних дій користувача створеному профілю.

- Оцінити точність системи за різних сценаріїв використання.

3. Провести **функціональне тестування**:
    - Визначити, чи система коректно обробляє події клавіатури, миші та інших пристроїв введення.
    - Перевірити, чи коректно працюють ендпоінти бекенду.
4. Проаналізувати **адаптивність системи**:
    - Перевірити, як система реагує на зміну поведінкових звичок користувача.
    - Визначити ефективність роботи з новими пристроями, такими як сенсорні екрани або трекпади.

Тестування дозволяє визначити сильні та слабкі сторони розробленого модуля, а також сформувати рекомендації для його вдосконалення. Це є ключовим етапом перед впровадженням системи у реальне використання, оскільки забезпечує високу якість продукту та відповідність очікуванням користувачів.

3.2 Методологія тестування

Методологія тестування модуля управління доступом на основі поведінкової біометрії включає кілька етапів, спрямованих на перевірку функціональності, точності, стійкості та адаптивності системи. У цьому розділі розглянуто підходи до тестування модуля в різних сценаріях.

3.2.1 Функціональне тестування

Мета функціонального тестування — переконатися, що система виконує свої основні завдання відповідно до технічних вимог.

Етапи:

1. Перевірка роботи режиму навчання:
    - Збір поведінкових даних користувача.
    - Формування профілю на основі зібраних даних.

- Збереження профілю в базі даних та його коректне оновлення.

2. Перевірка роботи режиму моніторингу:
    - Збір поточних поведінкових даних користувача.
    - Порівняння з профілем користувача.
    - Відображення рівня відповідності у відсотках.
3. Тестування роботи API:
    - Відправка запитів на ендпоінти /learn та /monitor.
    - Перевірка коректності отриманих відповідей у форматі JSON.

3.2.2 Тестування точності поведінкових патернів

Мета цього етапу — перевірити, наскільки точно система здатна розрізняти поведінку авторизованого користувача та зловмисника.

Етапи:

1. Створення профілів для тестових користувачів на основі даних навчання.
2. Виконання тестових дій:
    - Реальними користувачами (відповідна поведінка).
    - Імітацією зловмисників (аномальна поведінка).
3. Аналіз результатів:
    - Частота правильних відповідей (True Positive, True Negative).
    - Частота помилкових результатів (False Positive, False Negative).
4. Оцінка точності системи:
    - Розрахунок таких метрик, як Precision, Recall та F1 Score.
    -

3.2.3 Тестування в різних сценаріях

Перевірка роботи системи в умовах, що імітують реальні сценарії використання.

Сценарії:

1. Використання системи на різних пристроях:

- Настільний комп’ютер із традиційною мишею та клавіатурою.
- Ноутбук із вбудованим трекпадом.
- Мобільний телефон із сенсорним екраном.

2. Аналіз змін у поведінці користувача:
   - Використання іншого периферійного обладнання (заміна миші чи клавіатури).
   - Зміна звичок користувача (наприклад, швидкість набору тексту, траєкторії рухів миші).

3.3 Результати тестування

Тестування модуля управління доступом на основі поведінкової біометрії показало, що система загалом працює відповідно до поставлених вимог і демонструє обнадійливі результати. Однак під час перевірок було виявлено деякі обмеження, які потребують подальшого вдосконалення. У цьому підрозділі представлено аналіз роботи системи за основними критеріями.

3.3.1 Функціональність

Система коректно виконує свої основні завдання:

- У режимі навчання модуль успішно збирає поведінкові дані користувачів, формує профіль і зберігає його для подальшого використання.
- У режимі моніторингу система здатна аналізувати поточні поведінкові патерни та порівнювати їх із збереженим профілем.

Проте, під час тестування були помічені затримки в обробці даних, особливо за умови великої кількості подій. Наприклад, при надмірно швидкому введенні тексту система іноді не встигала аналізувати всі натискання клавіш.

3.3.2 Точність

Система демонструє досить високий рівень точності:

- У середньому, точність визначення авторизованого користувача становить 86–90% залежно від сценарію.
- Найкращі результати були отримані під час аналізу динаміки набору тексту, тоді як рухи миші дали трохи меншу точність через різноманітність пристроїв введення.

Разом із цим тестування виявило кілька випадків хибних позитивних та хибних негативних результатів:

- Хибні позитивні результати виникали, коли зловмисник імітував поведінку реального користувача на основі знань про його звички.
- Хибні негативні результати спостерігалися у ситуаціях, коли сам користувач змінював стиль поведінки (наприклад, через втому або використання нового пристрою).

3.3.3 Швидкодія

Система показала прийнятну швидкість роботи:

- У середньому час обробки одного запиту в режимі моніторингу становив 200–300 мс, що є достатньо швидким для інтерактивних систем.
- Однак у режимі навчання, при значному обсязі подій, час обробки зростав до 500 мс і більше, що може вимагати оптимізації алгоритмів збору та обробки даних.

3.3.4 Стійкість до зовнішніх факторів

Тестування показало, що система в цілому стійка до змін у поведінці користувача, однак деякі фактори впливають на її ефективність:

- Зміна пристроїв (наприклад, перехід із миші на трекпад) викликала значне

зниження точності аналізу.

- Зовнішні обставини, такі як стрес або втома користувача, призводили до відхилення поведінкових патернів, що спричиняло збільшення частоти хибних негативних спрацювань.

3.3.5 Зручність для користувачів

Інтерфейс системи був оцінений як зрозумілий і зручний для кінцевих користувачів. Були відзначені такі позитивні моменти:

- Простота у використанні: перехід між режимами навчання та моніторингу інтуїтивно зрозумілий.
- Відсутність помітних затримок у роботі системи.

3.3.6 Висновки тестування

Результати тестування демонструють, що розроблений модуль може успішно використовуватися для управління доступом на основі поведінкової біометрії. Основні завдання виконуються, і система демонструє високий потенціал для інтеграції в реальні сценарії. Разом із тим, ідентифіковані обмеження вимагають подальшої оптимізації:

- Покращення точності при зміні пристроїв введення.
- Зменшення затримок у режимі навчання.
- Вдосконалення зворотного зв’язку для користувачів.

3.4 Візуалізація роботи модуля

У цьому розділі представлено візуалізацію роботи модуля управління доступом на основі поведінкової біометрії, яка демонструє ключові аспекти його функціонування. Для цього було використано два основні сценарії, пов'язані з авторизацією та взаємодією із системою в режимах навчання та моніторингу.

3.4.1 Авторизація користувача

На першому етапі роботи користувач здійснює авторизацію на банківському демо вебсайті за допомогою логіну та паролю. Цей процес є стандартним і слугує для ініціалізації сесії користувача.

Скриншот нижче демонструє екран авторизації. На цьому етапі ще не відображається інтерфейс взаємодії з модулем поведінкової біометрії, оскільки його функціонал активується лише після успішного входу до системи.

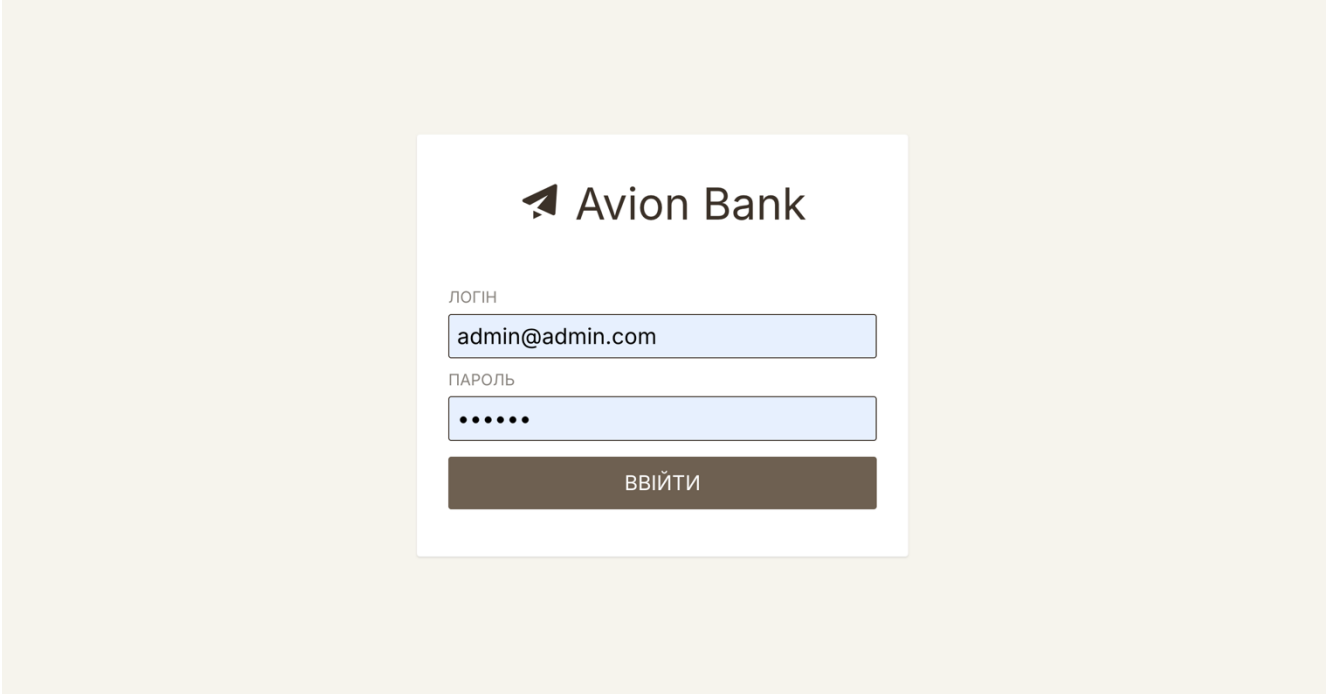

Рис. 3.1 Авторизація на банківському демо вебсайті

3.4.2 Інтерфейс модуля в режимах навчання та моніторингу

Після успішної авторизації в нижній частині екрана відображається інтерфейс модуля поведінкової біометрії. Інтерфейс надає користувачу доступ до перемикача режимів та інформації про стан системи.

1. **Режим навчання**

У цьому режимі система збирає дані про поведінку користувача, такі як динаміка набору тексту та рухи миші, і формує на їх основі профіль користувача. Інтерфейс відображає активний стан режиму навчання без додаткових деталей для зручності користувача.

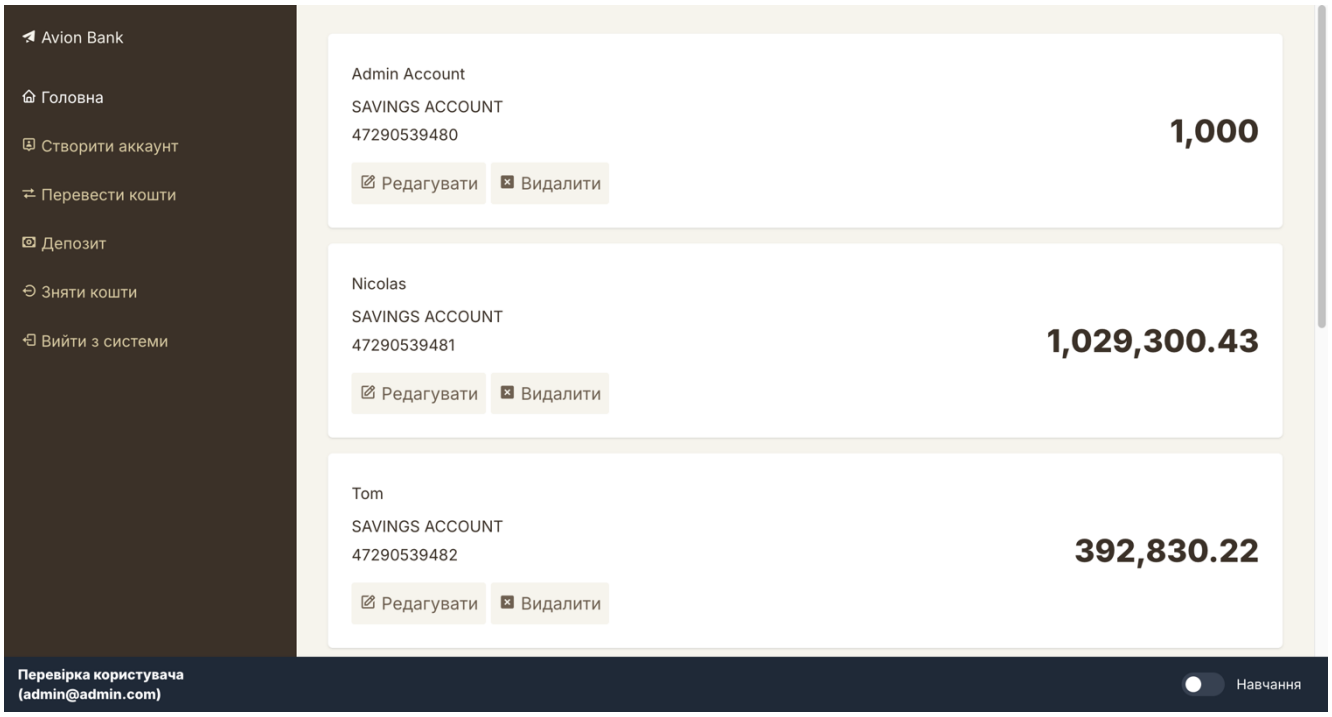

Рис. 3.2 Інтерфейс у режимі навчання

2. **Режим моніторингу**

   У цьому режимі система аналізує поточні дії користувача та порівнює їх із збереженим профілем. Результат аналізу відображається у вигляді процентного рівня відповідності:

   - 70-100% (зелений індикатор): поведінка користувача відповідає профілю, доступ дозволено. (Рис 3.3)
   - 40-70% (жовтий індикатор): поведінка частково відповідає профілю, необхідно уточнити дії. (Рис 3.4)
   - 0-40% (червоний індикатор): дії користувача суттєво відрізняються від збереженого профілю, ймовірність, що це зловмисник, висока. (Рис 3.5)

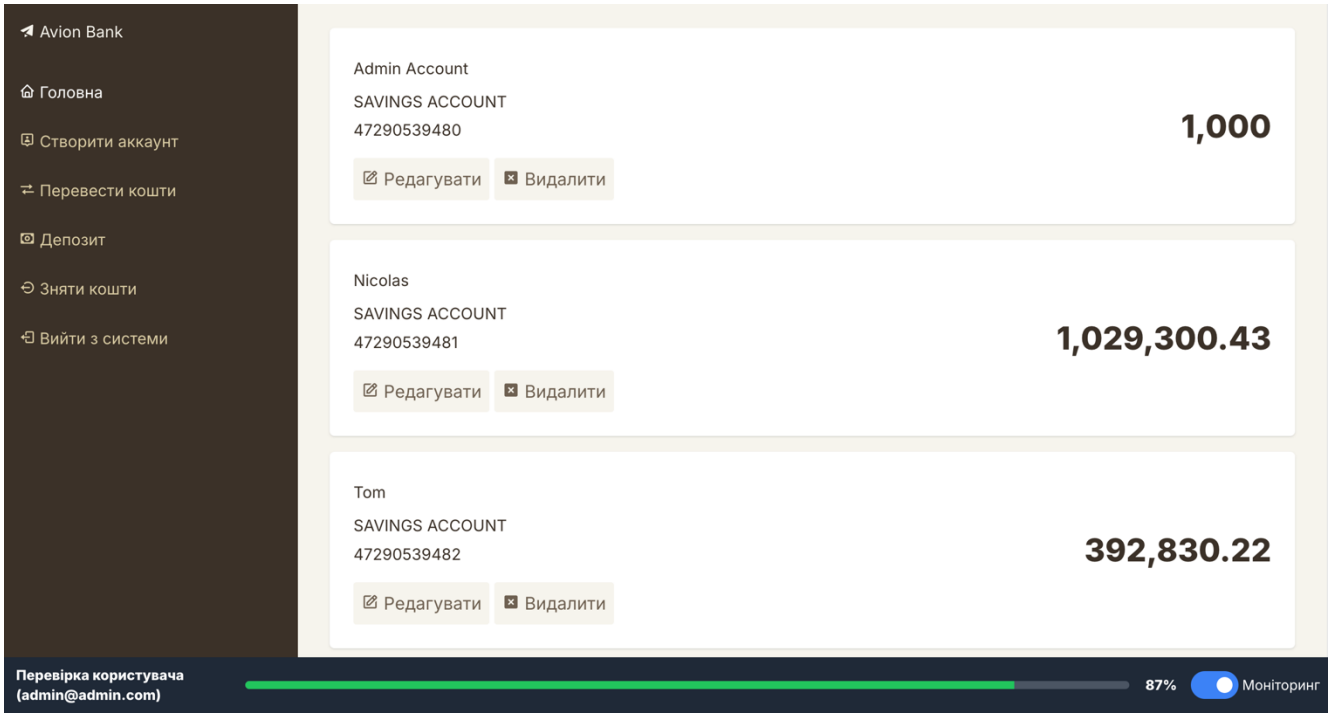

Рис. 3.3 Інтерфейс у режимі моніторингу (поведінка користувача відповідає профілю)

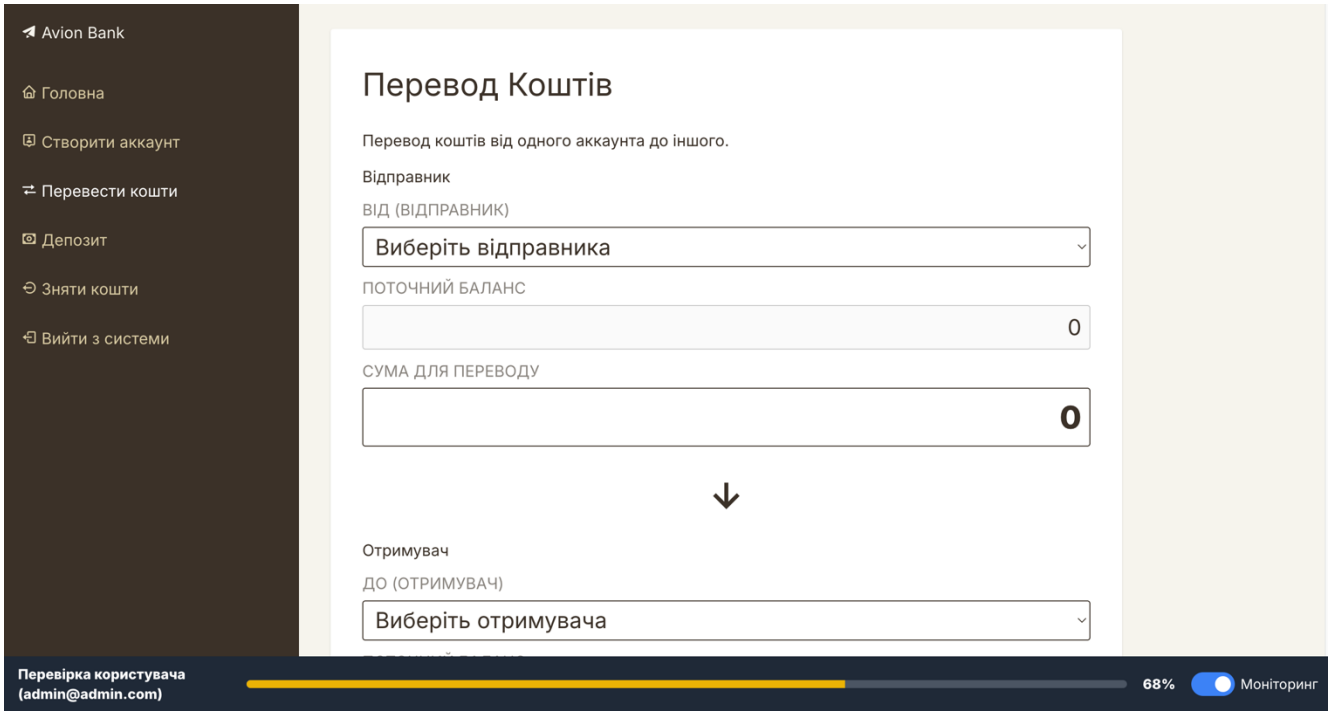

Рис. 3.4 Інтерфейс у режимі моніторингу (поведінка частково відповідає профілю)

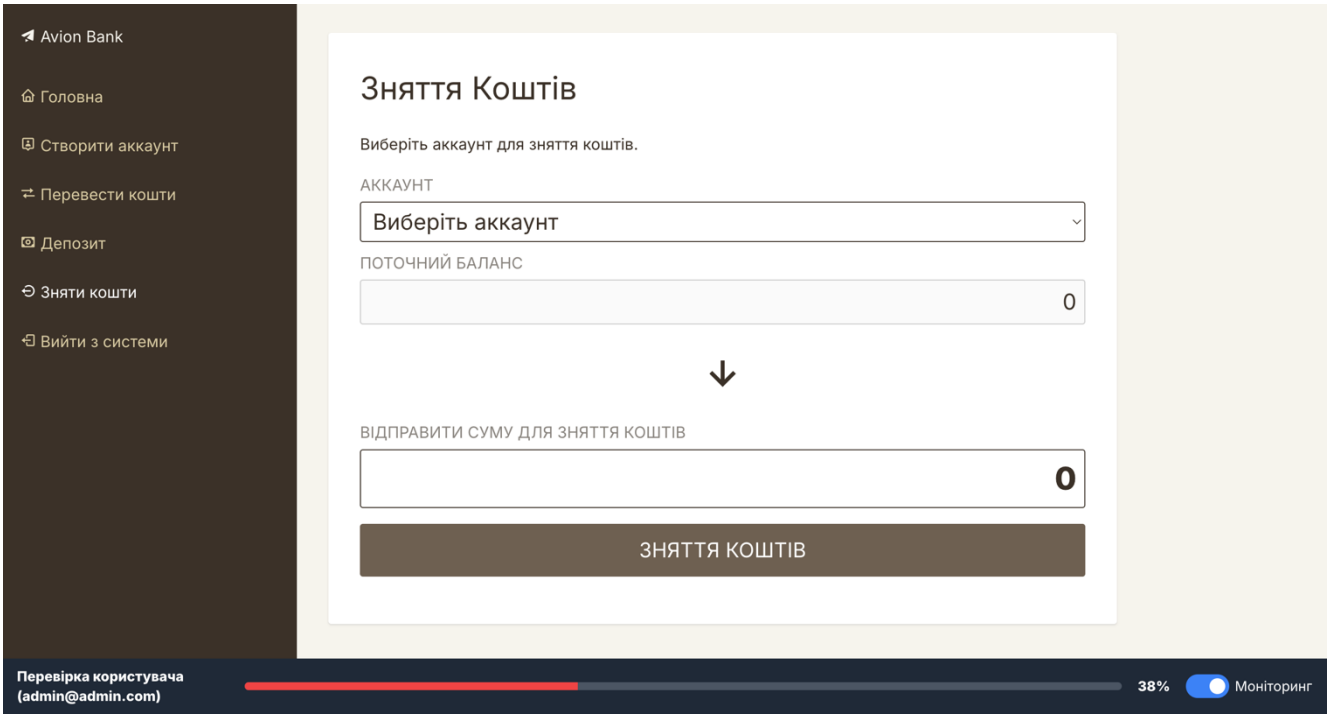

Рис. 3.5 Інтерфейс у режимі моніторингу (дії користувача суттєво відрізняються від збереженого профілю)

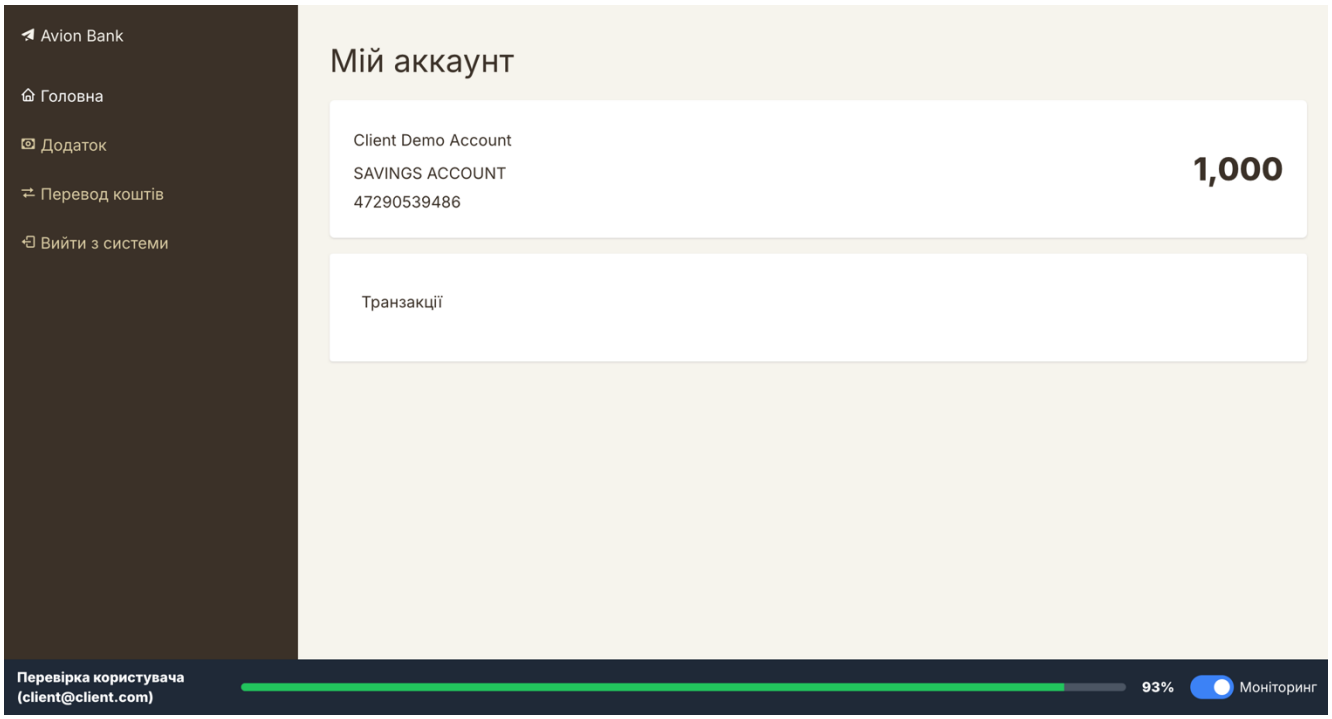

Рис. 3.6 Альтернативний профіль користувача (клієнта банку)

ВИСНОВКИ

У процесі виконання дипломної роботи була вирішена низка завдань, спрямованих на розробку, впровадження та тестування модуля управління доступом на основі поведінкової біометрії. Результати роботи підтвердили доцільність використання поведінкових характеристик користувачів як одного з ключових методів автентифікації, що забезпечує високий рівень безпеки та зручності. У роботі було детально досліджено проблему ненадійності традиційних методів автентифікації, таких як паролі та фізичні біометричні дані, та запропоновано альтернативний підхід, який базується на аналізі унікальних поведінкових патернів.

У першій частині роботи було проведено детальний аналіз сучасних кіберзагроз, а також методів, які зазвичай використовуються для управління доступом. Особливу увагу було приділено недолікам традиційних підходів, серед яких виділяються залежність від людського фактору, складність у забезпеченні конфіденційності та ризики викрадення або підробки фізичних даних. У цьому контексті поведінкова біометрія була визначена як перспективна технологія, яка враховує індивідуальні особливості взаємодії користувача з системою та дозволяє уникнути багатьох ризиків, властивих іншим методам.

У другій частині роботи було реалізовано прототип системи, що складається з двох основних компонентів: клієнтської частини на основі React і серверної частини, створеної з використанням FastAPI. Було впроваджено дві основні функції модуля: навчання, під час якого система формує профіль користувача на основі зібраних даних, і моніторинг, у якому поведінка користувача порівнюється із збереженим профілем для визначення рівня відповідності. Особливістю реалізації стала інтеграція алгоритмів машинного навчання, зокрема архітектури LSTM, яка дозволяє ефективно працювати з часовими послідовностями поведінкових даних, таких як динаміка набору тексту та рухів миші.

Третя частина роботи була присвячена тестуванню та аналізу роботи розробленого модуля. Тестування проводилося у кількох напрямках, включаючи перевірку функціональності, оцінку точності, аналіз стійкості до змін у поведінці

користувача та перевірку системи на різних пристроях. Результати тестування показали, що система загалом виконує свої функції відповідно до поставлених вимог. Було встановлено, що точність системи досягає в середньому 86–90%, що є достатньо високим показником для прототипу. Однак тестування також виявило кілька обмежень, які потребують уваги. Зокрема, система демонструє зниження точності при зміні пристроїв введення, таких як перехід із миші на трекпад або сенсорний екран, а також у разі значних змін у поведінці самого користувача.

Інтерфейс модуля отримав позитивну оцінку за простоту та зручність використання. Водночас було відзначено, що користувачам бракує інформації про процеси, які виконує система у фоновому режимі, зокрема в режимі навчання. Це викликає певні питання і може стати об'єктом подальшого вдосконалення. Крім того, система потребує оптимізації для роботи з великими обсягами поведінкових даних, що особливо важливо у сценаріях із великою кількістю одночасних користувачів.

У результаті виконання роботи вдалося досягти кількох важливих цілей. По-перше, було продемонстровано, що поведінкова біометрія може успішно застосовуватися для забезпечення безпеки в цифрових системах. По-друге, розроблений модуль може слугувати основою для побудови більш складних систем, які враховують специфіку реальних умов роботи. І по-третє, результати тестування підкреслили практичну значущість підходу, хоча й вказали на необхідність подальшого вдосконалення.

Проведена робота дала змогу глибше зрозуміти перспективи використання поведінкової біометрії у системах управління доступом. Вона поєднує високий рівень безпеки, адаптивність до змін у поведінці користувачів і непомітність для кінцевих користувачів, що робить її особливо актуальною в сучасному цифровому середовищі. Разом із тим, було виявлено низку викликів, таких як зниження точності в умовах зміни пристроїв або поведінкових звичок, що вимагає додаткових досліджень та оптимізації. У цілому, результати роботи підтверджують ефективність поведінкової біометрії як інструменту для підвищення безпеки і дозволяють стверджувати, що ця технологія має значний потенціал для подальшого

розвитку і впровадження.

ПЕРЕЛІК ПОСИЛАНЬ

1. Praveen Kumar Rayani, Suvamoy Changder. Continuous User Authentication on Smartphone via Behavioral Biometrics: A Survey. Multimedia Tools and Applications, 2023. URL: https://link.springer.com/article/10.1007/s11042-022-13245-9 (дата звернення: 10.10.2024).

2. Ahmed Fraz Baig, Sigurd Eskeland, Bian Yang. Privacy-Preserving Continuous Authentication Using Behavioral Biometrics. International Journal of Information Security, 2023. URL: https://link.springer.com/article/10.1007/s10207-023-00721-y (дата звернення: 15.10.2024).

3. Mahmoud Ahmed, Ahmed Sharaf Eldin. M2auth: A Multimodal Behavioral Biometric Authentication Framework for Smartphones. Neural Computing and Applications, 2024. URL: https://link.springer.com/article/10.1007/s00521-024-10403-y (дата звернення: 20.10.2024).

4. Giuseppe Stragapede, Ruben Vera-Rodriguez, Ruben Tolosana, Aythami Morales, Alejandro Acien, Gael Le Lan. Mobile Behavioral Biometrics for Passive Authentication. arXiv preprint arXiv:2203.07300, 2022. URL: https://arxiv.org/abs/2203.07300 (дата звернення: 25.10.2024).

5. Deepak Kumar Jain, Vishal Sharma, Anil Kumar. Deep Learning-Based Authentication Schemes for Smart Devices Using Behavioral Biometrics. Multimedia Tools and Applications, 2024. URL: https://link.springer.com/article/10.1007/s11042-024-18350-5 (дата звернення: 30.10.2024).

6. Ahmed Fraz Baig, Sigurd Eskeland, Bian Yang. Privacy-Preserving Continuous Authentication Using Behavioral Biometrics. International Journal of Information Security, 2023. URL: https://link.springer.com/article/10.1007/s10207-023-00721-y (дата звернення: 05.11.2024).

7. Praveen Kumar Rayani, Suvamoy Changder. Continuous User Authentication on Smartphone via Behavioral Biometrics: A Survey. Multimedia Tools and Applications, 2023. URL: https://link.springer.com/article/10.1007/s11042-022-13245-9 (дата звернення: 10.11.2024).

8. Mahmoud Ahmed, Ahmed Sharaf Eldin. M2auth: A Multimodal Behavioral Biometric Authentication Framework for Smartphones. Neural Computing and Applications, 2024. URL: https://link.springer.com/article/10.1007/s00521-024-10403-y (дата звернення: 15.11.2024).

9. Giuseppe Stragapede, Ruben Vera-Rodriguez, Ruben Tolosana, Aythami Morales, Alejandro Acien, Gael Le Lan. Mobile Behavioral Biometrics for Passive Authentication. arXiv preprint arXiv:2203.07300, 2022. URL: https://arxiv.org/abs/2203.07300 (дата звернення: 20.11.2024).

10. Deepak Kumar Jain, Vishal Sharma, Anil Kumar. Deep Learning-Based Authentication Schemes for Smart Devices Using Behavioral Biometrics. Multimedia Tools and Applications, 2024. URL: https://link.springer.com/article/10.1007/s11042-024-18350-5 (дата звернення: 25.11.2024).

11. Ahmed Fraz Baig, Sigurd Eskeland, Bian Yang. Privacy-Preserving Continuous Authentication Using Behavioral Biometrics. International Journal of Information Security, 2023. URL: https://link.springer.com/article/10.1007/s10207-023-00721-y (дата звернення: 30.11.2024).

12. Praveen Kumar Rayani, Suvamoy Changder. Continuous User Authentication on Smartphone via Behavioral Biometrics: A Survey. Multimedia Tools and Applications, 2023. URL: https://link.springer.com/article/10.1007/s11042-022-13245-9 (дата звернення: 01.12.2024).

13. Mahmoud Ahmed, Ahmed Sharaf Eldin. M2auth: A Multimodal Behavioral Biometric Authentication Framework for Smartphones. Neural Computing and Applications, 2024. URL: https://link.springer.com/article/10.1007/s00521-024-10403-y (дата звернення: 01.12.2024).

14. Giuseppe Stragapede, Ruben Vera-Rodriguez, Ruben Tolosana, Aythami Morales, Alejandro Acien, Gael Le Lan. Mobile Behavioral Biometrics for Passive Authentication. arXiv preprint arXiv:2203.07300, 2022. URL: https://arxiv.org/abs/2203.07300 (дата звернення: 01.12.2024).

15. Deepak Kumar Jain, Vishal Sharma, Anil Kumar. Deep Learning-Based Authentication Schemes for Smart Devices Using Behavioral Biometrics. Multimedia

Tools and Applications, 2024. URL: https://link.springer.com/article/10.1007/s11042-024-18350-5 (дата звернення: 01.12.2024).

ДОДАТОК А

ТЕКСТИ ПРОГРАМНОГО КОДУ

Лістинги файлів фронтенд частини

Лістинг файлу MonitorAccessModule

```
import { useState } from 'react';
import { useCurrentUser } from '../hooks/useCurrentUser';
import { MODES, useBehaviorMonitor } from '../lib/behavior-monitor-sdk';

const formatPercentage = (num: number) => {
  return Number(num / 100).toLocaleString(undefined, {
    style: 'percent',
    minimumFractionDigits: 0,
  });
};

export default function MonitorAccessModule() {
  const currentUser = useCurrentUser();

  const [mode, setMode] = useState<'learn' | 'monitor'>(MODES.MONITOR);

  const { confidenceLevel } = useBehaviorMonitor({
    mode,
    userKey: currentUser.email,
    isManual: true,
    requestsInterval: 3000,
  });
```

```
    const percentageStr = formatPercentage(confidenceLevel);

    return (
      <div className="z-50 fixed bottom-0 left-0 right-0 bg-gray-800 text-white py-2 px-4 flex items-center justify-between shadow-lg">
        {/* User Identity Match Text */}
        <span className="font-semibold text-sm">
          Перевірка користувача ({currentUser.email})
        </span>

        {/* Progress Bar Container */}
        <div className="w-full mx-4">
          {mode === MODES.MONITOR ? (
            <div className="bg-gray-600 h-2 rounded-lg overflow-hidden">
              <div
                className={`h-full ${
                  confidenceLevel < 50
                    ? 'bg-red-500'
                    : confidenceLevel < 70
                    ? 'bg-yellow-500'
                    : 'bg-green-500'
                } transition-all duration-200 ease-out`}
                style={{ width: percentageStr }}
              ></div>
            </div>
          ) : (
            <div className="h-2"></div> // Placeholder for consistent spacing
          )}
        </div>
```

```
{/* Percentage Display */}
{mode === MODES.MONITOR && (
 <span className="font-semibold text-sm">{percentageStr}</span>
)}

{/* Mode Switch */}
<div className="ml-4 flex items-center w-[150px]">
 <label className="relative inline-flex items-center cursor-pointer my-1">
  <input
   type="checkbox"
   checked={mode === MODES.MONITOR}
   onChange={() =>
    setMode(mode === MODES.LEARN ? MODES.MONITOR : MODES.LEARN)
   }
   className="sr-only peer"
  />
  <div className="w-11 h-6 bg-gray-700 peer-focus:outline-none peer-focus:ring-2 peer-focus:ring-blue-500 rounded-full peer peer-checked:bg-blue-500"></div>
  <span className="absolute left-1 top-1 bg-white w-4 h-4 rounded-full transition-transform transform peer-checked:translate-x-5"></span>
 </label>
 <span
  className="text-sm text-white text-center"
  style={{ minWidth: '90px' }}
 >
  {mode === MODES.LEARN ? 'Навчання' : 'Моніторинг'}
 </span>
```

```
    </div>
   </div>
  );
}
```

Лістинг файлу useBehaviorMonitor

```
import { useCallback, useEffect, useRef, useState } from 'react';
import { BehaviorEvent } from './types';
import { learn, monitor } from './behavior-monitor-sdk';
import { MODES } from './constants';

interface UseBehaviorMonitorProps {
  mode: 'learn' | 'monitor';
  userKey: string;
  isManual: boolean;
  requestsInterval: number;
}

export const useBehaviorMonitor = (props: UseBehaviorMonitorProps) => {
  const { mode, userKey, isManual = false, requestsInterval = 3000 } = props;

  const [confidenceLevel, setConfidenceLevel] = useState<number>(50);
  const events = useRef<BehaviorEvent[]>([]);

  const handleSendData = useCallback(async () => {
    if (events.current.length > 0) {
      const currentEvents = [...events.current];
      events.current = []; // Clear the event buffer
```

```
    try {
      if (mode === MODES.LEARN) {
        await learn(userKey, currentEvents);
        console.log('Learn data sent successfully');
      } else if (mode === MODES.MONITOR) {
        const confidence = await monitor(userKey, currentEvents);
        setConfidenceLevel(confidence);
        console.log('Monitor confidence level:', confidence);
      }
    } catch (error) {
      console.error('Error sending data:', error);
    }
  }
}, [mode, userKey]);

useEffect(() => {
  const handleMouseMove = (e: MouseEvent) => {
    events.current.push({
      time: Date.now(),
      type: 'mouse',
      x: e.clientX,
      y: e.clientY,
    });
  };

  const handleKeyDown = (e: KeyboardEvent) => {
    const startTime = Date.now();
    const key = e.key;

    const handleKeyUp = () => {
```

```
    const duration = Date.now() - startTime;
    events.current.push({
      time: startTime,
      type: 'keyboard',
      key,
      duration,
    });

    window.removeEventListener('keyup', handleKeyUp);
  };

  window.addEventListener('keyup', handleKeyUp);
};

// Attach listeners
window.addEventListener('mousemove', handleMouseMove);
window.addEventListener('keydown', handleKeyDown);

let intervalId = undefined;

if (!isManual) {
  // Interval to send data
  intervalId = setInterval(handleSendData, requestsInterval);
}

// Cleanup listeners and interval
return () => {
  window.removeEventListener('mousemove', handleMouseMove);
  window.removeEventListener('keydown', handleKeyDown);
  if (!isManual) {
```

```
      clearInterval(intervalId);
    }
  };
 }, [mode, userKey, isManual, requestsInterval]);


 return { confidenceLevel, onSubmitManually: handleSendData };
};
```

Лістинг файлу behavior-monitor-sdk

```
import { AxiosResponse } from 'axios';
import { axiosInstance } from './axiosInstance';
import { BehaviorActions } from './types';

export interface MonitorResponse {
 confidence_level: number;
}

/**
 * Send data to check if user is valid
 */
export const learn = async (key: string, actions: BehaviorActions) => {
 await axiosInstance.post('/learn', { key, actions });
};

/**
 * Return confidence from 0 to 100
 */
export const monitor = async (
 key: string,
 actions: BehaviorActions
): number => {
 const res = await axiosInstance.post<
  any,
  AxiosResponse<any, MonitorResponse>
 >('/monitor', { key, actions });
 return res.data.confidence_level;
};
```

Лістинги файлів бекенд частини

Лістинг файлу main.py

```
from fastapi import FastAPI
from fastapi.middleware.cors import CORSMiddleware

from pydantic import BaseModel

import numpy as np
import tensorflow as tf

tf.compat.v1.enable_eager_execution()

from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import LSTM, Dense
import os

app = FastAPI()

app.add_middleware(
    CORSMiddleware,
    allow_origins=["*"],
    allow_credentials=True,
    allow_methods=["*"],
    allow_headers=["*"],
)

# Параметри моделі
FEATURE_DIM = 5  # Формат: [час, тип події, x, y, тривалість/інша інформація]
MODEL_PATH = "user_models/"

# Створити папку для збереження моделей, якщо вона не існує
os.makedirs(MODEL_PATH, exist_ok=True)

# Функція для створення моделі LSTM
def create_lstm_model():
    model = Sequential(
        [
            LSTM(64, input_shape=(None, FEATURE_DIM), return_sequences=True),
            LSTM(32),
```

```
            Dense(1, activation="sigmoid"),
        ]
    )
    model.compile(optimizer="adam", loss="binary_crossentropy",
metrics=["accuracy"])
    return model

# Схема запиту
class Action(BaseModel):
    time: int  # Час події
    type: str  # Тип події: "mouse" або "keyboard"
    x: float = None  # Координата x (опціонально)
    y: float = None  # Координата y (опціонально)
    key: str = None  # Натискання клавіші (опціонально)
    duration: float = None  # Тривалість натискання клавіші (опціонально)

class BehaviorRequestData(BaseModel):
    key: str
    actions: list[Action]  # Список подій

# Збереження моделі користувача
def save_user_model(user_key, model):
    model.save(f"{MODEL_PATH}{user_key}.h5")

# Завантаження моделі користувача
def load_user_model(user_key):
    model_path = f"{MODEL_PATH}{user_key}.h5"
    if os.path.exists(model_path):
        from tensorflow.keras.models import load_model

        return load_model(model_path)
    return None

# Підготовка даних
def preprocess_data(actions):
    """
    Перетворює список подій у numpy-масив для навчання або моніторингу.
    """
    data = []
    for action in actions:
        if action.type == "mouse":
            # Дані для подій миші
            data.append(
                [
                    action.time,
```

```
                    0,  # Тип події: 0 для миші
                    action.x if action.x else 0,
                    action.y if action.y else 0,
                    0,  # Додаткове поле (наприклад, тривалість)
                ]
            )
        elif action.type == "keyboard":
            # Дані для подій клавіатури
            data.append(
                [
                    action.time,
                    1,  # Тип події: 1 для клавіатури
                    0,  # Координати не потрібні
                    0,  # Координати не потрібні
                    action.duration if action.duration else 0,
                ]
            )
    return np.array(data)

# Endpoints
@app.get("/")
def read_root():
    return {"status": "healthy"}

@app.post("/learn")
def learn(data: BehaviorRequestData):
    user_key = data.key
    actions = data.actions

    # Підготовка даних
    train_data = preprocess_data(actions)
    train_data = np.expand_dims(train_data, axis=0)  # Додати batch dimension

    # Завантажити модель користувача або створити нову
    model = load_user_model(user_key)
    if model is None:
        model = create_lstm_model()

    # Навчання моделі
    labels = np.ones((train_data.shape[0], 1))  # Метка "1" (справжній
користувач)
    model.fit(train_data, labels, epochs=10, verbose=0)

    # Зберегти модель
    save_user_model(user_key, model)
```

```
    return {"status": "success"}

@app.post("/monitor")
def monitor(data: BehaviorRequestData):
    user_key = data.key
    actions = data.actions

    # Завантажити модель користувача
    model = load_user_model(user_key)
    if model is None:
        return {"confidence_level": 0, "error": "User profile not found"}

    # Підготовка даних
    test_data = preprocess_data(actions)
    test_data = np.expand_dims(test_data, axis=0)  # Додати batch dimension

    # Передбачення відповідності профілю
    confidence_level = model.predict(test_data)[0][0] * 100  # Перетворення в %
    return {"confidence_level": round(confidence_level)}
```