Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

Виконав: ст. 2-го курсу, групи КІТС-22Мз
спеціальності 125 – Кібербезпека
Освітня програма – Кібербезпека
інформаційних технологій та систем
Пінчук Н.С.
Керівник: к.т.н., доц., доцент каф. МБІС
Шиян А.А.
«____» _____ 2024 р.
Опонент: к.т.н., доц., доцент каф. ОТ
Крупельницький Л.В.
«____» _____ 2024 р.

Допущено до захисту
Голова секції УБ кафедри МБІС
_____Юрій ЯРЕМЧУК
«_____»_____2024 р.

Вінниця ВНТУ - 2024 рік

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

Рівень вищої освіти ІІ-й (магістерський)
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітньо-професійна програма - Кібербезпека інформаційних технологій та систем

ЗАТВЕРДЖУЮ
Голова секції УБ, кафедра МБІС
_____ **Юрій ЯРЕМЧУК**
“_____” _____ 2024 р.

З А В Д А Н Н Я
на магістерську кваліфікаційну роботу студенту
Пінчук Назар Сергійович
(прізвище, ім`я, по-батькові)

1. Тема роботи:
«Підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки»
Керівник роботи: Шиян А.А. к.т.н., доц., доцент каф. МБІС
(прізвище, ім`я, по-батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від “ 11” березня 2024 року № 81
2. Строк подання студентом роботи за тиждень до захисту.
3. Вихідні дані до роботи:
Стандарти, електронні джерела, підручники та наукові статті по темі, які стосуються теми магістерської кваліфікаційної роботи.
4. Зміст текстової частини:
У вступі викладено актуальність теми та сформульовано мету роботи. У першому розділі викладено теоретичні основи п’ятифакторної системи автентифікації та валідації. У другому розділі описана розробка алгоритму та принципів роботи системи підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки. Третій розділ присвячено програмній реалізації системи підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки. Четвертий розділ містить економічне обґрунтування розробки програмного забезпечення

5. Перелік ілюстративного матеріалу (з точним зазначенням обов`язкових креслень)

У дугому розділі магістерської кваліфікаційної роботи наведено 3 рисунка, у третьому розділі – 25 рисунків

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Основна частина			
I	Шиян А.А. к.т.н., доц., доцент каф. МБІС		
II	Шиян А.А. к.т.н., доц., доцент каф. МБІС		
III	Шиян А.А. к.т.н., доц., доцент каф. МБІС		
Економічна частина			
IV	Причепа І.В., к.е.н., доц. каф. ЕПВМ		

7.Дата видачі завдання _____2024 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи		Примітка
1.	Визначення напрямку магістерської роботи, формулювання теми	1.03.2024	15.03.2024	
2.	Аналіз предметної області обраної теми	15.03.2024	1.04.2024	
3.	Розробка роботи	1.04.2024	10.04.2024	
4.	Написання магістерської роботи на основі розробленої теми	10.04.2024	20.04.2024	
5.	Передзахист магістерської кваліфікаційної роботи	20.04.2024	10.05.2024	
6.	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	10.05.2024	4.06.2024	
7.	Захист магістерської кваліфікаційної роботи	12.06.2024	12.06.2024	

Студент _____ Пінчук Н.С.
(підпис)

Керівник роботи _____ Шиян А.А.
(підпис)

АНОТАЦІЯ

УДК 004.56.5(043.2)

Пінчук Н.С. Підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки.

Магістерська кваліфікаційна робота зі спеціальності 125 – «Кібербезпека», освітня програма «Кібербезпека інформаційних технологій та систем». Вінниця: ВНТУ, 2024. 133с.

Українською мовою. Бібліогр.: 42 назв; рис.: 28; табл.: 14

Сучасний світ цифрових технологій та інформаційних систем ставить перед наукою та практикою нагальну потребу в пошуку новітніх методів захисту даних. Одним із ключових напрямків забезпечення інформаційної безпеки є розвиток систем автентифікації, здатних ефективно протистояти сучасним кіберзагрозам. У моїй магістерській кваліфікаційній роботі зосереджено увагу на розробці п'ятифакторної системи автентифікації та валідації, що інтегрує динамічний біометричний патерн поведінки користувача.

Дана робота базується на глибокому аналізі існуючих систем безпеки, вивченні передових технологій в сфері кібербезпеки та практичному застосуванні новітніх методів захисту інформації. Важливою частиною дослідження є впровадження інноваційного підходу до аутентифікації, який поєднує кілька рівнів захисту: від класичних методів введення паролів до біометричних технологій та аналізу поведінкових характеристик.

Метою дослідження було не лише створення теоретичної моделі п'ятифакторної автентифікації але й демонстрація її практичної реалізації та ефективності у захисті інформаційних систем від несанкціонованого доступу. Результати дослідження підкреслюють значення комплексного підходу до безпеки даних та можуть бути використані для подальшого вдосконалення механізмів кіберзахисту.

Магістерська робота включає теоретичний огляд сучасного стану кібербезпеки, аналітичне дослідження існуючих методів аутентифікації, розробку

проекту п'ятифакторної системи та її тестування. Робота спрямована на підвищення рівня захисту інформаційних систем, що актуально як для теоретичних, так і для практичних аспектів кібербезпеки.

Ключові слова: КІБЕРБЕЗПЕКА, АУТЕНТИФІКАЦІЯ, БІОМЕТРІЯ, ПОВЕДІНКОВІ ПАТЕРНИ, П'ЯТИФАКТОРНА СИСТЕМА, ВАЛІДАЦІЯ, ІНФОРМАЦІЙНІ СИСТЕМИ.

Робота підкреслює важливість інтеграції різноманітних методів автентифікації для створення більш надійної та ефективної системи безпеки. Впровадження динамічного біометричного патерну поведінки дозволяє не лише розширити можливості аутентифікації, але й забезпечити гнучкість та адаптивність системи до змінних умов користування.

Дослідження охоплює весь спектр розробки від теоретичного обґрунтування до практичної реалізації, що демонструє глибину аналізу та комплексний підхід до вирішення поставлених завдань. Окрема увага приділяється важливості економічної частини проекту, яка аналізує можливі економічні вигоди від впровадження розробленої системи та її вплив на ефективність роботи інформаційних систем.

Завершальні розділи магістерської роботи присвячені детальному аналізу отриманих результатів, їх обговоренню та формулюванню конкретних рекомендацій для подальшого розвитку системи. Висновки підкреслюють значення розробленої системи для забезпечення безпеки інформаційних систем та її потенціал у вдосконаленні сучасних методів кібербезпеки.

Ця магістерська робота є важливим кроком на шляху до розробки ефективних і надійних методів захисту інформації, які відповідають викликам сучасного цифрового світу. Результати дослідження можуть бути використані для подальшої роботи в області кібербезпеки та для впровадження інноваційних рішень в практичну діяльність.

ABSTRACT

Pinchuk N.S. Improving the security of information systems based on a five-factor authentication and validation system with the integration of a dynamic biometric behavioral pattern.

Master's qualification work in specialty 125 - "Cybersecurity", educational program "Cybersecurity of information technologies and systems". Vinnytsia: VNTU, 2024. 133p.

In Ukrainian. Bibliography: 42 titles; Figures: 28; Table: 14.

The modern world of digital technologies and information systems poses an urgent need for science and practice to find the latest methods of data protection. One of the key areas of information security is the development of authentication systems that can effectively counter modern cyber threats. My master's thesis focuses on the development of a five-factor authentication and validation system that integrates a dynamic biometric pattern of user behavior.

This work is based on an in-depth analysis of existing security systems, the study of advanced technologies in the field of cybersecurity, and the practical application of the latest information security methods. An important part of the study is the introduction of an innovative approach to authentication that combines several levels of protection: from classical password entry methods to biometric technologies and behavioral analysis.

The purpose of the study was not only to create a theoretical model of five-factor authentication but also to demonstrate its practical implementation and effectiveness in protecting information systems from unauthorized access. The results of the study emphasize the importance of an integrated approach to data security and can be used to further improve cybersecurity mechanisms.

The master's thesis includes a theoretical review of the current state of cybersecurity, an analytical study of existing authentication methods, the development of a five-factor system project and its testing. The work is aimed at improving the level of protection of information systems, which is relevant for both theoretical and practical aspects of cybersecurity.

Keywords: CYBERSECURITY, AUTHENTICATION, BIOMETRICS, BEHAVIORAL PATTERNS, FIVE-FACTOR SYSTEM, VALIDATION, INFORMATION SYSTEMS.

This paper emphasizes the importance of integrating various authentication methods to create a more reliable and efficient security system. The introduction of a dynamic biometric behavioral pattern allows not only to expand the authentication capabilities, but also to ensure the flexibility and adaptability of the system to changing conditions of use.

The research covers the entire spectrum of development from theoretical substantiation to practical implementation, which demonstrates the depth of analysis and an integrated approach to solving the tasks. Particular attention is paid to the importance of the economic part of the project, which analyzes the possible economic benefits of implementing the developed system and its impact on the efficiency of information systems.

The final chapters of the master's thesis are devoted to a detailed analysis of the results obtained, their discussion and formulation of specific recommendations for further development of the system. The conclusions emphasize the importance of the developed system for ensuring the security of information systems and its potential to improve modern cybersecurity methods.

This master's thesis is an important step towards the development of effective and reliable methods of information security that meet the challenges of the modern digital world. The results of the study can be used for further work in the field of cybersecurity and for the implementation of innovative solutions in practice.

ЗМІСТ

Вступ……...……...……...……...10
1 ТЕОРЕТИЧНІ ОСНОВИ П’ЯТИФАКТОРНОЇ СИСТЕМИ АВТЕНТИФІКАЦІЇ ТА ВАЛІДАЦІЇ..……....12
1.1 Огляд сучасних методів автентифікації...……..……..12
1.2 Біометричні системи ідентифікації…….……...…….……...……....18
1.3 Поведінкові патерни в системах безпеки……..……..….27
1.4 Опис факторів автентифікації, використаних при підвищенні безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки...……...34
1.5 Висновки та постановка задач……...……..……..35
2 РОЗРОБКА АЛГОРИТМУ ТА ПРИНЦИПІВ РОБОТИ СИСТЕМИ ПІДВИЩЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ П'ЯТИФАКТОРНОЇ СИСТЕМИ АВТЕНТИФІКАЦІЇ ТА ВАЛІДАЦІЇ З ІНТЕГРАЦІЄЮ ДИНАМІЧНОГО БІОМЕТРИЧНОГО ПАТЕРНУ ПОВЕДІНКИ……..41
2.1. Вибір методів багатофакторної автентифікації для підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки.....41
2.2. Вибір факторів автентифікації для підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки ……..…..51
2.3. Розробка та моделювання бази даних у системі підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки.……....55
2.4 Висновки розробки алгоритму та принципів роботи системи……....57
3 ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПІДВИЩЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ П'ЯТИФАКТОРНОЇ СИСТЕМИ АВТЕНТИФІКАЦІЇ ТА ВАЛІДАЦІЇ З ІНТЕГРАЦІЄЮ ДИНАМІЧНОГО БІОМЕТРИЧНОГО ПАТЕРНУ ПОВЕДІНКИ……..……..……59

3.1. Вибір середовища розробки програми підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки……..59

3.2. Розробка робочого прототипу програми п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки ……..……..……...64

3.3 Програмна реалізація та тестування системи п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки ...…….……...……76

3.4 Результати аналізу системи п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки .....…94

3.5 Висновки програмна реалізація системи підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки…….....97

4 ЕКОНОМІЧНА ЧАСТИНА……...98

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки……..98

4.2 Розрахунок витрат на проведення науково-дослідної роботи……..102

4.3 Розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором…….111

4.4 Розрахунок ефективності вкладених інвестицій та періоду їх окупності……..112

4.5 Висновки до розділу……115

СПИСКИ ВИКОРИСТАНИХ ДЖЕРЕЛ……117

Додаток А. Технічне завдання……120

Додаток Б. Лістинг програми……..123

Додаток В. Ілюстративний матеріал……...126

Додаток Г. Протокол перевірки на антиплагіат…….133

ВСТУП

Актуальність. У сучасному світі, де інформаційні технології глибоко інтегровані у всі аспекти життя, питання забезпечення безпеки даних стає все більш актуальним. Кіберзагрози та кібератаки продовжують розвиватися, змушуючи науковців та фахівців у галузі кібербезпеки шукати нові методи захисту інформаційних систем. Одним із ключових аспектів забезпечення безпеки є процес автентифікації, який дозволяє встановити ідентичність користувача та контролювати доступ до інформації. На сьогодні існуючі методи автентифікації мають свої вразливості, що підкреслює необхідність розробки більш надійних і багатофакторних підходів.

Мета і задачі дослідження. Метою даної магістерської роботи є розробка та верифікація моделі п'ятифакторної системи автентифікації, здатної забезпечити високий рівень захисту інформаційних систем від несанкціонованого доступу. Для досягнення цієї мети були визначені наступні задачі:

- Проаналізувати існуючі методи автентифікації та їх вразливості.
- Розробити теоретичну модель п'ятифакторної автентифікації.
- Інтегрувати динамічний біометричний патерн поведінки у систему автентифікації.
- Реалізувати програмний прототип розробленої системи.
- Провести аналіз ефективності та безпеки запропонованої системи.

Об’єкт і предмет дослідження. Об’єктом дослідження є методи автентифікації в інформаційних системах. Предметом дослідження є п'ятифакторна система автентифікації з інтеграцією динамічного біометричного патерну поведінки.

Наукова новизна. Новизна даного дослідження полягає у розробці інтегрованої системи автентифікації, що враховує динамічні біометричні характеристики поведінки користувача, що значно підвищує рівень безпеки порівняно з традиційними методами автентифікації. Впровадження поведінкових патернів додає додатковий рівень захисту, який є складним для імітації зловмисниками.

Практичне значення. Практичне значення отриманих результатів полягає у можливості застосування розробленої системи в різних сферах, де критично важливим є захист інформації: від банківської сфери до урядових інформаційних систем. Реалізація та апробація системи показали її ефективність та надійність у протистоянні як відомим методам атак, так і у виявленні спроб несанкціонованого доступу за допомогою аномалій у поведінці користувачів.

Методи дослідження. У даному дослідженні застосовано комплексний підхід, що включає теоретичний аналіз наукових публікацій, розробку математичної моделі, програмну імплементацію та експериментальну перевірку. Використання динамічних біометричних даних та їх інтеграція у п'ятифакторну систему автентифікації становить новий рівень захисту, що відповідає сучасним викликам кібербезпеки.

Особистий внесок. Особистий внесок включає всі етапи дослідження: від розробки концепції та теоретичної моделі системи до програмної реалізації та аналізу результатів експериментів. Результати роботи були представлені на наукових семінарах та конференціях з кібербезпеки, де отримали позитивні відгуки від фахівців у галузі.

1 ТЕОРЕТИЧНІ ОСНОВИ П’ЯТИФАКТОРНОЇ СИСТЕМИ АВТЕНТИФІКАЦІЇ ТА ВАЛІДАЦІЇ

1.1. Огляд сучасних методів автентифікації

У сучасному цифровому світі, де кількість кібератак неухильно зростає, надійність систем автентифікації стає критично важливою. Автентифікація — це процес встановлення достовірності ідентичності користувача, що намагається отримати доступ до ресурсу. Сучасні методи автентифікації можна умовно поділити на кілька категорій за типом використовуваних аутентифікаційних факторів:

- Щось, що знає користувач (наприклад, пароль або PIN-код).
- Щось, що має користувач (наприклад, мобільний телефон або смарт-карта).
- Щось, що є у користувача (наприклад, біометричні дані).
- Щось, що робить користувач (наприклад, поведінкові патерни, такі як динаміка натискання клавіш або рух миші).
- Де знаходиться користувач (наприклад, геолокаційні дані).

Паролі та PIN-коди залишаються найбільш розповсюдженими методами, проте їхня ефективність значно знижується через високу ймовірність вгадування або перехоплення. Системи двофакторної автентифікації, які поєднують два різних типи факторів, пропонують підвищений рівень безпеки, але навіть вони не є повністю захищеними від усіх видів атак.

Біометричні системи автентифікації використовують унікальні фізичні характеристики людини, такі як відбитки пальців, геометрія обличчя, сканування сітківки ока, або поведінкові особливості, включаючи голос, динаміку письма, та манеру ходьби. Ці методи вважаються одними з найбільш надійних, оскільки біометричні дані є унікальними для кожної особи і, як правило, не можуть бути легко вкрадені або підроблені. Однак, вони також вимагають спеціалізованого обладнання для збору та аналізу даних, а також викликають питання приватності та безпеки зберігання біометричної інформації.

Системи, що базуються на геолокаційних даних, визначають місцеположення користувача за допомогою GPS або інших технологій і можуть дозволити або заборонити доступ до ресурсів залежно від того, де користувач знаходиться. Ці системи можуть бути корисними для додаткового рівня перевірки, але також мають обмеження, пов'язані з точністю визначення місцеположення та можливістю обходу геолокаційних обмежень.

Поведінкові патерни включають аналіз поведінки користувача, такого як ритм натискання клавіш, швидкість введення тексту, шаблони взаємодії з інтерфейсом, та можуть використовуватися для виявлення не лише легітимного користувача, але й аномалій, що можуть вказувати на несанкціонований доступ. Цей метод вважається досить перспективним завдяки його динамічності та здатності адаптуватися до змін у поведінці користувача, але потребує складного аналізу та обробки великої кількості даних.

Інноваційні методи автентифікації, такі як криптографічні ключі та одноразові паролі, генеровані спеціалізованими пристроями або програмами, також набирають популярності. Вони пропонують високий рівень безпеки, здатність до швидкої зміни у випадку компрометації та зручність використання, але вимагають наявності додаткового обладнання або програмного забезпечення з боку користувача.

Усі ці методи мають свої переваги та недоліки, і вибір конкретного методу або їх комбінації залежить від конкретних потреб безпеки, вартості впровадження, зручності для користувачів та вимог законодавства у сфері приватності та захисту даних. Сучасні тенденції вказують на зростання популярності мультифакторної автентифікації, яка комбінує кілька різних методів для забезпечення більш надійного захисту.

Наприклад, поєднання пароля з біометричною перевіркою та одноразовими паролями, що надходять на мобільний пристрій, здатне значно підвищити рівень безпеки, знижуючи ризик несанкціонованого доступу навіть у випадку компрометації одного з факторів. Однак, з іншого боку, це також може збільшити

складність використання системи та вимагати від користувачів більшої уваги та відповідальності.

В контексті неперервної цифровізації та автоматизації бізнес-процесів, інновації в сфері методів автентифікації відіграють ключову роль у забезпеченні цілісності, конфіденційності та доступності цифрових ресурсів. Розвиток технологій машинного навчання та штучного інтелекту відкриває нові можливості для створення адаптивних та інтелектуальних систем автентифікації, здатних самостійно виявляти та реагувати на аномальну поведінку або спроби несанкціонованого доступу.

Завдання розробників та інженерів з кібербезпеки полягає в тому, щоб знайти оптимальний баланс між надійністю захисту та зручністю використання, забезпечуючи при цьому відповідність вимогам законодавства та стандартам безпеки.

Окрім технологічного аспекту, важливою є також розробка ефективних корпоративних політик та процедур, які регулюють використання та управління аутентифікаційними системами. Це включає політики щодо створення та зберігання паролів, використання біометричних даних, обробку одноразових кодів, а також заходи щодо реагування на інциденти безпеки. Такі політики мають бути розроблені з урахуванням кращих практик галузі та спрямовані на мінімізацію внутрішніх та зовнішніх загроз для системи.

Для забезпечення високого рівня прийняття та ефективності аутентифікаційних систем, особливу увагу слід приділити освіті та тренінгу користувачів. Інформування співробітників та користувачів про принципи роботи системи, потенційні загрози та методи захисту від них може значно знизити ймовірність помилкових дій, які можуть призвести до витоку даних або інших інцидентів безпеки. Регулярні тренінги та освітні кампанії допоможуть підтримувати високий рівень обізнаності серед користувачів та сприятимуть формуванню культури безпеки в організації.

На закінчення, розробка та впровадження сучасних методів автентифікації є невід'ємною частиною стратегії кібербезпеки будь-якої організації, спрямованої на

захист від зростаючих кіберзагроз. Успіх цих заходів залежить від поєднання технологічних інновацій, ефективного управління ризиками, корпоративної політики безпеки та залучення та освіти користувачів. Враховуючи швидкий розвиток технологій та методів кібератак, постійний моніторинг та оновлення аутентифікаційних систем є ключовими для підтримки їхньої ефективності та відповідності сучасним вимогам безпеки.

У контексті сучасних викликів у сфері кібербезпеки, особливу увагу приділяють розробці і впровадженню новітніх методів автентифікації, які можуть забезпечити вищий рівень захисту порівняно з традиційними системами. Важливою тенденцією є інтеграція криптографічних технологій та використання публічних та приватних ключів для аутентифікації, що, як показано у дослідженнях, забезпечує значно вищий рівень безпеки порівняно з використанням тільки паролів чи PIN-кодів.

Дослідження, опубліковані в журналі "Security and Communication Networks" (2017), демонструють, що застосування криптографії з відкритим ключем може значно ускладнити несанкціонований доступ до системи, оскільки зловмиснику потрібно буде не тільки вкрасти приватний ключ, але й мати знання про алгоритм шифрування.

Також, усе більше уваги приділяється використанню контекстної інформації для аутентифікації. Стаття в "Journal of Network and Computer Applications" (2018) описує методику, яка дозволяє системі враховувати не тільки статичні характеристики для аутентифікації (наприклад, пароль або біометричні дані), але й динамічні контекстні дані, такі як місцезнаходження користувача, час входу та тип пристрою. Це дозволяє створювати більш гнучкі та адаптивні системи безпеки.

Зростаюче застосування штучного інтелекту та машинного навчання відкриває нові можливості для вдосконалення систем автентифікації. За даними дослідження, опублікованого в "IEEE Access" (2019), системи, які використовують машинне навчання для аналізу поведінкових патернів, можуть ефективно виявляти спроби несанкціонованого доступу, аналізуючи незвичайні зміни в поведінці користувача.

Однак, незважаючи на значний прогрес у розробці новітніх методів автентифікації, важливо пам'ятати про потребу забезпечення балансу між безпекою та зручністю користування. Розробка систем, які занадто складні у використанні, може призвести до помилок з боку користувачів або навіть відмови від їх застосування, що, в свою чергу, може знизити загальний рівень безпеки системи. Тому, при проєктуванні систем автентифікації, важливо знаходити оптимальне співвідношення між надійністю, зручністю та швидкістю доступу до ресурсів.

Крім того, розвиток технологій та методів автентифікації повинен супроводжуватися посиленням правил зберігання та обробки даних. Зокрема, це стосується захисту біометричних та поведінкових даних, які можуть містити велику кількість особистої інформації. Необхідність врахування цих аспектів особливо актуальна в контексті загального регламенту захисту даних (GDPR) та інших законодавчих актів, що регулюють питання конфіденційності.

Освіта та підвищення обізнаності користувачів є ще одним важливим аспектом в контексті сучасних методів автентифікації. Інформування користувачів про переваги та потенційні ризики, пов'язані з використанням різних типів автентифікаційних систем, допоможе їм зробити обґрунтований вибір та відповідально ставитися до захисту своїх даних.

У підсумку, сучасні методи автентифікації відіграють ключову роль у захисті цифрового простору від кіберзагроз. Продовження досліджень та розробка інноваційних рішень у цій галузі є критично важливими для підтримки безпеки інформаційних систем на високому рівні. Разом з тим, забезпечення конфіденційності, прозорості використання даних та зручності користування залишається важливим завданням для розробників та адміністраторів систем кібербезпеки.

Збільшення ролі штучного інтелекту та машинного навчання у розробці методів автентифікації відкриває нові перспективи для створення більш адаптивних та інтелектуальних систем безпеки. Ці технології дозволяють аналізувати великі обсяги даних в реальному часі, ідентифікувати складні поведінкові патерни та виявляти аномалії, які можуть свідчити про спроби

несанкціонованого доступу. Водночас, використання ШІ вимагає відповідального підходу до питань приватності та захисту даних, а також постійного моніторингу для запобігання помилковим позитивним або негативним ідентифікаціям.

Інтеграція Інтернету речей (IoT) у системи автентифікації також відкриває нові можливості та виклики. З одного боку, пристрої IoT можуть збирати додаткові дані про контекст користувача, які можуть використовуватися для підтримки багатофакторної автентифікації, з іншого боку, збільшення кількості підключених пристроїв вимагає розробки нових підходів до забезпечення безпеки та управління ідентифікацією.

Проблема "забутого паролю" та потреба в постійній зміні паролів для забезпечення безпеки можуть бути мінімізовані за допомогою альтернативних методів автентифікації, таких як біометрична ідентифікація та одноразові паролі, генеровані мобільними додатками. Ці методи забезпечують не тільки вищий рівень безпеки, але й покращують користувацький досвід, зменшуючи залежність від запам'ятовування складних паролів.

Однак, необхідно пам'ятати, що немає універсального рішення в області автентифікації, яке було б ідеально підходящим для всіх сценаріїв використання. Вибір методу автентифікації має базуватися на ретельному аналізі ризиків, вимог до безпеки, а також потреб та зручності користувачів. Крім того, ефективність будь-якої системи автентифікації залежить не тільки від технології, але й від впровадження надійних практик безпеки, постійного освітнього процесу для користувачів та ретельного адміністрування системи.

У контексті неперервної еволюції кіберзагроз, важливо зосередитися не тільки на захисті від відомих вразливостей, але й на прогнозуванні та попередженні майбутніх загроз. Це означає, що системи автентифікації мають бути гнучкими та здатними швидко адаптуватися до нових викликів. Розробка механізмів швидкого оновлення та інтеграції нових методів автентифікації є критичною для підтримки безпеки на відповідному рівні.

Крім технічних аспектів, питання організаційної культури та підходів до безпеки відіграють важливу роль. Створення культури безпеки, де кожен

користувач усвідомлює свою роль у захисті інформаційних активів, є ключовим для успішного впровадження будь-якої системи автентифікації. Освітні програми, регулярні тренінги та виховання відповідального ставлення до корпоративної інформації та ресурсів можуть значно підвищити загальний рівень безпеки.

Нарешті, важливою є співпраця на міжнародному рівні та обмін знаннями та досвідом між організаціями, дослідницькими установами та урядовими агенціями. Спільні зусилля у розробці стандартів, протоколів безпеки та методик реагування на інциденти допоможуть створити більш стійкі та ефективні системи автентифікації.

У підсумку, сучасні методи автентифікації відіграють вирішальну роль у захисті проти кіберзагроз, але їх ефективність залежить від комплексного підходу, що охоплює не тільки технологічні інновації, але й організаційні, культурні та освітні аспекти безпеки.

1.2. Біометричні системи ідентифікації

Біометричні системи автентифікації використовують унікальні фізичні або поведінкові характеристики особи для ідентифікації. До фізичних біометричних даних належать відбитки пальців, риси обличчя, ірис очей тощо. Поведінкові характеристики можуть включати голос, динаміку письма, манеру ходи. Біометричні системи забезпечують високий рівень безпеки, оскільки біометричні дані важко підробити або вкрасти. Однак їхнє використання також породжує питання приватності та необхідність захисту цих даних від несанкціонованого доступу.

Впровадження біометричних систем ідентифікації стає все більш поширеним у різноманітних застосуваннях, від контролю доступу до робочих місць та забезпечення безпеки мобільних пристроїв до використання у фінансових транзакціях та системах національної ідентифікації. Основними перевагами таких систем є зручність для користувачів, оскільки біометричні дані завжди "при собі" і не вимагають запам'ятовування складних паролів або носіння додаткових пристроїв.

Окрім того, розвиток технологій у сфері біометрії дозволяє реалізувати системи, здатні швидко та з високою точністю обробляти великі обсяги даних. Наприклад, системи розпізнавання облич за допомогою штучного інтелекту можуть ідентифікувати особу серед тисяч інших за лічені секунди. Така швидкість і точність ідентифікації значно підвищують ефективність біометричних систем у порівнянні з традиційними методами.

Проте, разом з перевагами, впровадження біометричних систем також супроводжується певними викликами. Наприклад, необхідність зберігання великих обсягів особистих даних вимагає розробки ефективних методів їх захисту від зловмисників. Існують також технічні обмеження, пов'язані з точністю систем: помилки першого та другого роду (невірне відхилення легітимного користувача та помилкове прийняття нелегітимного) можуть спричинити проблеми з доступом для законних користувачів або, навпаки, дозволити доступ нелегітимним особам.

Іншим аспектом є етичні та юридичні питання, пов'язані з використанням біометричних даних. У багатьох країнах існують строгі законодавчі вимоги щодо збору, обробки та зберігання персональних даних. Організації, що впроваджують біометричні системи, повинні забезпечити відповідність цим вимогам, а також розробити політики щодо забезпечення прозорості використання даних та захисту приватності осіб.

Таким чином, хоча біометричні системи ідентифікації пропонують значні переваги у підвищенні безпеки та зручності автентифікації, їх впровадження вимагає ретельного планування та урахування цілого ряду факторів. Це включає не тільки технічні аспекти, такі як вибір надійних систем і забезпечення їх безпечної інтеграції в існуючу інфраструктуру, але й врахування етичних, юридичних та соціальних аспектів використання біометричних даних.

Однією з ключових вимог є розробка та впровадження чітких процедур щодо збору, обробки, зберігання та видалення біометричних даних. Організаціям необхідно забезпечити, щоб процеси відповідали вимогам законодавства про захист даних, таким як загальний регламент захисту даних (GDPR) в

Європейському Союзі, а також забезпечували високий рівень прозорості та контролю для користувачів.

Крім того, важливо звернути увагу на потенційні ризики безпеки, пов'язані з біометричними системами, включаючи загрозу викрадення або фальсифікації біометричних даних. Впровадження багатошарових захисних механізмів, таких як шифрування даних та використання безпечних каналів передачі, є критично важливим для забезпечення конфіденційності та цілісності біометричної інформації.

Нарешті, попри всі переваги, важливо визнати, що жодна система безпеки не може бути абсолютно непроникною. Організації мають розробити плани дій на випадок порушення безпеки, включаючи процедури відновлення, сповіщення користувачів про інциденти та вжиття відповідних заходів для мінімізації наслідків.

У сукупності, біометричні системи ідентифікації пропонують потужний інструмент для підвищення безпеки автентифікації. Однак, їх ефективність та прийнятність в суспільстві залежать від здатності організацій вирішувати пов'язані з ними технічні, юридичні та етичні виклики, забезпечуючи при цьому баланс між безпекою та приватністю. Використання біометрії як частини мультифакторної системи автентифікації може забезпечити додатковий рівень захисту, одночасно мінімізуючи ризики для користувачів та зберігаючи їх довіру.

Для цього важливо підтримувати високі стандарти в розробці та впровадженні біометричних технологій, зосереджуючись на непорушності, доступності та конфіденційності даних. Також, потрібно наголосити на важливості неперервного моніторингу та адаптації системи до новітніх загроз і викликів, що забезпечить її довгострокову ефективність та надійність.

Взаємодія з користувачами також грає ключову роль у успішному впровадженні біометричних систем. Надання докладної інформації про те, як збираються, обробляються та зберігаються біометричні дані, а також про заходи, що вживаються для захисту цих даних, може допомогти зменшити опір з боку користувачів та підвищити їх готовність використовувати біометричні технології.

Останнім часом, зростає увага до розробки і впровадження "біометрії, заснованої на приватності", яка включає технології, дизайновані таким чином, щоб мінімізувати зберігання та обробку персональних даних. Підходи, як-от анонімізація біометричних даних та локальна обробка (наприклад, обробка даних безпосередньо на пристрої користувача без передачі на зовнішні сервери), набувають популярності як способи забезпечення балансу між безпекою та приватністю.

Враховуючи ці аспекти, біометричні системи ідентифікації можуть стати ключовим елементом в арсеналі засобів кібербезпеки, здатним адаптуватися до мінливих потреб і викликів, ставлячи при цьому на перше місце захист інформації та приватності користувачів.

Біометричні системи ідентифікації продовжують еволюціонувати, адаптуючись до нових викликів у сфері кібербезпеки. Одним з напрямків є вдосконалення алгоритмів машинного навчання для покращення точності та надійності біометричних систем. Дослідження в цій області фокусуються на розробці алгоритмів, які можуть ефективно розпізнавати особу, навіть якщо біометричні дані частково змінилися через вік, травми або інші фактори.

Крім технічних вдосконалень, значну увагу приділяють захисту біометричних даних. Зокрема, технологія блокчейн може забезпечити додатковий рівень захисту за допомогою децентралізованого зберігання даних, що ускладнює несанкціонований доступ або зловживання. Цей підхід допомагає зменшити ризики, пов'язані з централізованими базами даних, які можуть стати ціллю для хакерів.

Етичні питання, пов'язані з використанням біометричних даних, також вимагають уваги. Необхідно забезпечити, щоб збір, обробка та зберігання біометричних даних відбувалися прозоро та з повагою до прав осіб на приватність. Важливо, щоб користувачі мали можливість контролювати свої дані та були інформовані про способи та цілі їх використання.

Для подальшого розвитку та впровадження біометричних систем важливою є міждисциплінарна співпраця між інженерами, дизайнерами, юристами та

етиками. Це допоможе забезпечити розробку систем, які не тільки технічно вдосконалені, але й відповідають високим моральним стандартам та правовим вимогам.

У підсумку, біометричні системи ідентифікації мають значний потенціал для підвищення безпеки та зручності автентифікації. Однак, їх успішне впровадження та експлуатація вимагають комплексного підходу, який охоплює не лише технологічні інновації, але й врахування етичних, правових та соціальних аспектів. Розвиток інфраструктури для безпечного зберігання та обробки біометричних даних, забезпечення прозорості процесів ідентифікації та захисту інформації, а також залучення користувачів до розуміння та управління їхніми персональними даними є ключовими елементами успішної інтеграції біометричних систем в повсякденне життя.

Також важливою є адаптація біометричних систем до різноманітних умов використання та потреб користувачів. Це включає розробку універсальних рішень, що можуть ефективно функціонувати в різних середовищах – від особистих гаджетів до великих корпоративних мереж, враховуючи при цьому варіативність біометричних характеристик серед населення.

Неперервний розвиток біометричних технологій також передбачає інтеграцію з іншими системами безпеки, створення багатошарових механізмів захисту, які використовують біометрію як один із елементів комплексної системи автентифікації. Це може забезпечити більш високий рівень безпеки, зменшуючи залежність від одного типу захисту та підвищуючи здатність системи протистояти різноманітним загрозам.

У міру розвитку технологій і зміни суспільних норм, організаціям та розробникам важливо зберігати відкритість до інновацій, готовність до переоцінки та адаптації існуючих підходів, а також здатність до швидкої реакції на нові виклики у сфері кібербезпеки та захисту даних. Водночас, акцент на освіті та залученні користувачів до процесу захисту інформації є важливим для підтримки високого рівня довіри та відповідальності у використанні цифрових технологій.

Таким чином, біометричні системи ідентифікації продовжують бути одним з найбільш обнадійливих напрямків у забезпеченні безпеки в цифровому світі. Однак, їхнє ефективне впровадження та експлуатація вимагають відповідального підходу, який включає не тільки використання передових технологій, але й увагу до прав і приватності користувачів, а також до постійної адаптації перед обличчям нових викликів і загроз.

Для забезпечення цієї відповідальності, важливим є постійний діалог між всіма зацікавленими сторонами: розробниками технологій, користувачами, регуляторними органами та громадськістю. Це дозволить не тільки оптимізувати технічні аспекти біометричних систем, але й забезпечити, щоб такі системи використовувалися етично та з повагою до основних прав людини.

У контексті швидкого розвитку цифрових технологій, особливо важливим стає питання міжнародної співпраці та стандартизації у сфері біометричної ідентифікації. Розробка міжнародних стандартів та протоколів може допомогти гармонізувати підходи до захисту даних, сприяти безпеці та зручності користувачів, а також уникнути розбіжностей у регулюванні, які можуть створювати бар'єри для міжнародної торгівлі та співпраці.

Також необхідною є розробка ефективних механізмів реагування на інциденти, що стосуються безпеки біометричних систем. Це включає не тільки технічні засоби швидкого виявлення та нейтралізації загроз, але й правові та організаційні процедури, які забезпечують прозоре та ефективне реагування на такі інциденти, з мінімізацією шкоди для користувачів та відновленням довіри до системи.

Врешті-решт, інтеграція біометричних систем ідентифікації в сучасні цифрові сервіси та інфраструктуру відкриває широкі можливості для покращення безпеки, зручності та якості обслуговування. Однак, для досягнення цих цілей необхідно забезпечити, щоб такі системи розвивалися у відповідності з високими стандартами етики, захисту даних та поваги до приватності. Не менш важливим є розвиток та застосування новітніх технологічних рішень для забезпечення безпеки біометричних даних від зовнішніх загроз та внутрішніх вразливостей.

Одним із напрямків, що заслуговують на увагу, є використання криптографічних технологій для захисту біометричних даних на всіх етапах їх обробки — від збору до зберігання та передачі. Зокрема, застосування методів шифрування та цифрового підпису може значно підвищити рівень безпеки біометричної інформації, запобігаючи її несанкціонованому доступу або маніпуляціям.

Розвиток технологій розпізнавання образів та штучного інтелекту відкриває нові можливості для покращення точності та надійності біометричних систем. Водночас, це створює додаткові виклики для забезпечення прозорості та контролю за алгоритмами, щоб уникнути упереджень та помилкових ідентифікацій. Важливо забезпечити, щоб системи були досить гнучкими для адаптації до індивідуальних особливостей та змін у біометричних даних користувачів протягом часу.

Інтеграція біометричних систем із іншими технологіями ідентифікації та автентифікації, такими як одноразові паролі, смарт-карти та криптографічні ключі, може створити багаторівневі системи безпеки, що забезпечують вищий рівень захисту. Такий підхід дозволяє комбінувати переваги різних методів автентифікації, мінімізуючи їхні недоліки та створюючи комплексні рішення для забезпечення цифрової безпеки.

Врешті, питання етики та правового регулювання залишаються важливими аспектами використання біометричних систем. Важливо забезпечити, що використання таких технологій відбувається з повагою до особистих прав та свобод, а також що існують ефективні механізми для захисту приватності та вирішення будь-яких спірних питань. Співпраця між технологічними компаніями, законодавчими органами, громадськістю та експертами у галузі приватності є ключовою для розробки відповідальних та збалансованих підходів до використання біометричних технологій. Важливо розробити чіткі правила, які регулюють збір, обробку, зберігання та видалення біометричних даних, щоб користувачі мали змогу контролювати свою особисту інформацію та розуміли, як вона використовується.

Також необхідно створити ефективні механізми для захисту біометричних даних не лише від зовнішніх загроз, але й від можливості внутрішнього зловживання. Це передбачає використання сучасних технологій шифрування, безпечних протоколів передачі даних та системи регулярного аудиту та моніторингу безпеки.

На міжнародному рівні, співпраця в галузі стандартизації біометричних технологій та методів їх використання може сприяти створенню єдиної системи вимог до захисту даних, яка б враховувала як технічні аспекти, так і потреби в забезпеченні прав і свобод особистості на глобальному рівні.

У контексті швидкого розвитку цифрових технологій та постійної зміни кіберзагроз, важливо не тільки адаптувати існуючі біометричні системи, але й розглядати можливість розвитку нових методів ідентифікації, які можуть запропонувати більш високий рівень безпеки та зручності для користувачів.

Освітні програми та інформаційні кампанії, спрямовані на підвищення обізнаності користувачів щодо біометричних технологій та їх прав у цій сфері, є важливими для формування довіри та відповідального використання таких систем.

Врешті-решт, успішне використання біометричних систем ідентифікації залежить від здатності знайти оптимальний баланс між інноваційними технологічними рішеннями, ефективним захистом даних, етичними нормами та вимогами законодавства. Спільні зусилля усіх зацікавлених сторін можуть допомогти досягнути цієї мети, створюючи міцну основу для безпечного та ефективного використання біометричних технологій в різних сферах життя суспільства.

Розробка комплексних політик конфіденційності та безпеки, які враховують потенційні ризики та виклики, пов'язані з біометричними системами, вимагає глибокого розуміння технологій, їхніх можливостей та обмежень. Важливо визнати, що забезпечення безпеки біометричних даних є неперервним процесом, який потребує регулярного оновлення та адаптації до нових загроз.

Успішна інтеграція біометричних систем також залежить від технологічної сумісності з існуючою IT-інфраструктурою та здатності до інтеграції з іншими

системами безпеки та ідентифікації. Це вимагає тісної співпраці між розробниками, IT-фахівцями та кінцевими користувачами для забезпечення високого рівня інтеграції та користувацького досвіду.

Крім того, ефективність біометричних систем значною мірою залежить від якості біометричних даних та точності обробки. Необхідність забезпечення високої якості даних вимагає від організацій розробки та дотримання строгих процедур збору та аналізу біометричної інформації.

Врешті, зростання використання біометричних систем вимагає розробки ефективних стратегій навчання та підвищення обізнаності серед користувачів. Люди повинні розуміти, як використовувати біометричні технології безпечно та ефективно, включаючи заходи з захисту своїх персональних даних та вміння реагувати на потенційні інциденти безпеки.

Таким чином, біометричні системи ідентифікації мають потенціал стати невід'ємною частиною сучасної цифрової екосистеми, пропонуючи надійні та зручні рішення для захисту ідентичності. Проте, досягнення цієї мети вимагає злагодженої роботи та взаємодії між усіма учасниками процесу — від технологічних лідерів і розробників до кінцевих користувачів, законодавців та громадськості. Розвиток політик та стандартів, які спрямовані на забезпечення етичного використання біометричних даних, захист приватності і збалансування потреб безпеки з правами особи, є критично важливим для створення стійкої та прийнятної системи біометричної ідентифікації.

Наприклад, у випадку з глобальними біометричними ідентифікаційними системами, такими як ті, що використовуються для прикордонного контролю або національних ID-карток, особливо важливим є створення міжнародних рамок, які регулюють збір, обмін та обробку біометричних даних між країнами. Це допоможе забезпечити, що такі системи функціонують відповідно до високих стандартів захисту даних і поваги до особистих прав на міжнародному рівні.

Освіта та постійне інформування громадськості про біометричні технології та їх застосування також відіграють ключову роль у підвищенні довіри до цих систем. Люди повинні бути обізнані про переваги та потенційні ризики

використання біометричних даних, а також мати змогу легко отримати доступ до інформації про те, як захищені їхні дані і які заходи вживаються для запобігання їх зловживанню.

У міру того, як біометричні технології стають все більш інтегрованими в наше повсякденне життя, зростає і необхідність у відповідальному підході до їх впровадження та використання. Це вимагає не лише технічної експертизи, але й глибокого розуміння соціальних, етичних та правових аспектів, що супроводжують розвиток цих технологій.

Врешті-решт, успіх використання біометричних систем ідентифікації залежатиме від здатності суспільства в цілому адаптуватися до цих змін, прийняти новітні технології, зберігаючи при цьому фундаментальні цінності поваги до приватності та захисту особистих даних.

1.3. Поведінкові патерни в системах безпеки

Використання поведінкових патернів у системах безпеки є відносно новим напрямком, що забезпечує додатковий рівень захисту. Цей підхід базується на аналізі та ідентифікації унікальних звичок або поведінки користувача, таких як спосіб введення тексту, швидкість та ритм натискання клавіш на клавіатурі, манера руху миші, голосові команди та інші поведінкові біометричні характеристики. Такі системи вимірюють і аналізують поведінку користувача в динаміці, що ускладнює несанкціонований доступ, оскільки навіть якщо зловмисник зможе скопіювати біометричні дані, імітувати поведінкові характеристики буде значно складніше.

Використання поведінкових патернів у системах безпеки відкриває нові можливості не тільки для аутентифікації користувачів, але й для неперервного моніторингу та виявлення аномалій у поведінці, що може вказувати на спроби зламу або внутрішні загрози. Наприклад, система може виявляти незвичну активність користувача, таку як раптову зміну способу введення тексту або використання нехарактерних команд, що може бути індикатором того, що обліковий запис був скомпрометований.

Однією з ключових переваг цього підходу є його ненав'язливість. На відміну від традиційних методів аутентифікації, які вимагають від користувачів активних дій (наприклад, введення пароля або сканування відбитка пальця), поведінкова біометрія дозволяє ідентифікувати особу на основі її звичайної поведінки, не перериваючи робочий процес.

Також цей підхід може забезпечити більшу гнучкість та адаптивність системи безпеки. Штучний інтелект та машинне навчання можуть бути використані для аналізу та навчання на основі поведінкових даних користувачів, постійно удосконалюючи здатність системи розпізнавати легітимних користувачів і виявляти підозрілу активність. Це дозволяє створити динамічну систему безпеки, що здатна адаптуватися до змін у поведінці користувачів та еволюціонувати разом із загрозами.

Однак, застосування поведінкової біометрії також має певні виклики. Зокрема, необхідно забезпечити точність та надійність системи, щоб уникнути помилкових спрацьовувань, які можуть призвести до невиправданих затримок або незручностей для користувачів. Також важливо враховувати питання приватності, оскільки аналіз поведінкових даних може включати збір та обробку великої кількості особистої інформації.

Врешті-решт, інтеграція поведінкових патернів у системи безпеки представляє собою обнадійливий напрямок, який поєднує в собі передові технології та новітні підходи до захисту інформації. Для досягнення максимальної ефективності таких систем необхідно поєднати глибоке розуміння поведінкової біометрії з передовими алгоритмами обробки даних і машинного навчання. Це дозволить розробити адаптивні та гнучкі системи безпеки, які можуть ефективно протистояти різноманітним загрозам без зайвого навантаження на користувачів.

При цьому, важливо забезпечити відкритість та прозорість таких систем у питаннях збору та обробки даних, щоб уникнути порушень приватності та зберегти довіру користувачів. Це передбачає не тільки впровадження технічних засобів захисту даних, але й розробку чітких політик використання та зберігання

інформації, а також забезпечення можливості для користувачів контролювати свої особисті дані.

Ще одним аспектом, на який слід звернути увагу, є необхідність навчання та підвищення обізнаності серед співробітників організацій, які використовують поведінкову біометрію. Розуміння основних принципів роботи таких систем, а також знання про основні заходи безпеки та приватності, можуть значно підвищити ефективність використання поведінкових патернів для захисту інформації.

Використання поведінкових патернів у системах безпеки представляє собою інноваційний і обнадійливий напрямок у сфері кібербезпеки, який вимагає комплексного підходу до реалізації та управління. З огляду на швидкий розвиток цифрових технологій і постійно зростаючу кількість кіберзагроз, подальше дослідження та розвиток у цій області залишається актуальним та важливим завданням для фахівців у галузі інформаційної безпеки.

На шляху подальшого розвитку і впровадження поведінкових патернів у системах безпеки, важливим аспектом є застосування передових технологій аналізу даних та штучного інтелекту. Ці технології дозволяють не лише точно ідентифікувати особистість на основі унікальних поведінкових характеристик, але й динамічно адаптувати системи безпеки до постійно змінюваних моделей поведінки користувачів та нових типів загроз. Застосування машинного навчання може значно підвищити здатність системи виявляти аномалії у поведінці, які можуть свідчити про спроби несанкціонованого доступу або інші безпекові інциденти.

Одночасно з технологічним розвитком, необхідно враховувати і соціально-етичні аспекти використання поведінкових патернів. Оскільки такі системи базуються на зборі та аналізі великої кількості особистих даних, виникає необхідність забезпечити високий рівень захисту приватності користувачів. Це включає розробку прозорих політик щодо обробки даних, надання користувачам контролю над їхньою інформацією, а також впровадження надійних механізмів захисту даних.

Для подолання потенційних викликів, пов'язаних з точністю та надійністю систем, важливо проводити постійні дослідження та випробування. Це допоможе виявити можливі помилки ідентифікації, зрозуміти умови, за яких система може неефективно функціонувати, та розробити заходи для їх усунення. Окрім того, важливо враховувати різноманіття поведінкових патернів серед користувачів, забезпечуючи високу адаптивність системи до індивідуальних особливостей.

У підсумку, інтеграція поведінкових патернів у системи безпеки відкриває значні перспективи для підвищення захисту цифрових ресурсів. Розвиток таких систем вимагає комплексного підходу, який об'єднує передові технології, врахування етичних норм, забезпечення приватності, та адаптацію до змінних умов безпеки. Важливо продовжувати дослідження та розробку в цій області, сприяючи створенню все більш розумних, надійних та користувацьки орієнтованих систем безпеки. Це передбачає не лише використання новітніх досягнень у галузі штучного інтелекту та машинного навчання для аналізу поведінкових патернів, але й розробку нових методологій оцінки ризиків, які враховують складність людської поведінки та здатні адаптуватися до неї.

Ключовим аспектом є також співпраця між науковцями, інженерами, фахівцями з кібербезпеки та законодавцями для забезпечення, що розвиток та впровадження поведінкових систем безпеки відбувається з дотриманням високих стандартів етики та приватності. Необхідно враховувати потенційний вплив на особистісні права та свободи, забезпечуючи, щоб користувачі мали можливість контролювати власні дані та були належним чином інформовані про їх використання.

Окрім того, розвиток інфраструктури для підтримки поведінкових систем безпеки, включаючи надійні сховища даних, ефективні механізми шифрування, та безпечні канали передачі інформації, є важливим для запобігання витоку або несанкціонованого доступу до поведінкових біометричних даних.

У майбутньому, розвиток поведінкових систем безпеки може також сприяти створенню нових форм взаємодії між людьми та технологіями, розширюючи можливості для автоматизації та персоналізації послуг. Це відкриває перспективи

не лише для підвищення безпеки, але й для покращення користувацького досвіду у широкому спектрі застосувань, від електронної комерції до персоналізованих систем обслуговування.

Завдяки інтеграції передових технологій, уваги до етичних та правових норм, а також неперервній адаптації до нових викликів, поведінкові системи безпеки мають потенціал стати одним з ключових інструментів захисту в цифровому світі, забезпечуючи надійну охорону інформаційних ресурсів та особистої приватності.

Поведінкові патерни в системах безпеки відіграють важливу роль у сучасній кібербезпеці, пропонуючи унікальний та динамічний спосіб ідентифікації та аутентифікації користувачів. Ці системи, що базуються на алгоритмах машинного навчання та штучного інтелекту, аналізують і адаптуються до поведінкових характеристик користувачів, що може включати динаміку натискання клавіш, манеру ведення миші, патерни голосу, а також інші біометричні та поведінкові особливості.

Використання поведінкової біометрії дозволяє реалізувати неперервну аутентифікацію, яка забезпечує безперервний моніторинг сесії користувача без необхідності втручання або додаткових дій з боку користувача. Це підвищує безпеку, оскільки система може виявляти неавторизований доступ або зловмисні дії в режимі реального часу, негайно реагуючи на будь-які аномалії.

Такий підхід також забезпечує вищий рівень зручності та прийнятності для користувачів, оскільки мінімізує потребу в постійному введенні паролів або використанні фізичних токенів. Замість цього, системи безпеки стають більш прозорими та ненав'язливими, інтегруючись природно в повсякденні діяльності користувачів.

Однак, впровадження поведінкових патернів у системи безпеки також має певні виклики, зокрема пов'язані з приватністю та етикою збору та аналізу особистих даних. Важливо забезпечити, що користувачі повністю інформовані про способи збору, використання та захисту їхніх даних, а також мають контроль над цим процесом. Забезпечення відповідності до загального регламенту про захист

даних (GDPR) в ЄС та інших міжнародних та національних нормативних актів є ключовим аспектом впровадження таких систем.

Крім того, для мінімізації ризиків помилкової ідентифікації або невдалих спроб аутентифікації, системи повинні бути розроблені з урахуванням великої варіативності поведінкових патернів користувачів. Це вимагає від алгоритмів машинного навчання здатності адаптуватися та враховувати індивідуальні зміни в поведінці, що можуть виникати з різних причин, включно зі зміною фізичного стану або емоційного стану користувача.

Ефективне застосування поведінкових патернів у системах безпеки також вимагає високого рівня інтеграції та сумісності з іншими компонентами інформаційної безпеки. Наприклад, поведінкова біометрія може бути використана разом з традиційними методами аутентифікації для створення багаторівневої системи безпеки, яка забезпечує додаткові гарантії ідентифікації.

На завершення, інтеграція поведінкових патернів у системи безпеки вимагає не тільки технологічних інновацій, але й розвитку політик та процедур, що забезпечують етичне використання та захист персональних даних. Організаціям необхідно працювати над підвищенням обізнаності користувачів щодо правил та принципів роботи таких систем, а також впроваджувати заходи для забезпечення прозорості та контролю з боку користувачів над власними даними. Тільки за умови забезпечення цих вимог, поведінкові патерни можуть стати надійним і прийнятним інструментом забезпечення кібербезпеки в сучасному цифровому світі.

Подальше впровадження та розвиток поведінкових патернів у системах безпеки потребує відповідального підходу до збору та аналізу даних, особливо у контексті зростаючої уваги до питань приватності та захисту персональних даних. Розробники та адміністратори безпеки повинні враховувати потенційний вплив своїх систем на приватне життя користувачів і діяти в межах етичних норм і законодавства. Важливо створювати механізми, що дозволяють користувачам з легкістю керувати власними даними, надаючи їм змогу відкликати згоду на обробку або вимагати видалення своїх даних.

Для забезпечення високої точності та мінімізації помилок у системах, що використовують поведінкові патерни, необхідно постійно вдосконалювати алгоритми машинного навчання і штучного інтелекту. Це включає збір великих обсягів даних для тренування системи, але також ставить перед дослідниками завдання забезпечення захисту цих даних від несанкціонованого доступу або зловживання.

Ключовим елементом ефективності поведінкових систем безпеки є їхня здатність адаптуватися до постійно змінюваних умов і нових видів загроз. Це означає не лише постійне оновлення даних та алгоритмів, але й розвиток здатності систем розпізнавати і відреагувати на складні шаблони поведінки, які можуть бути ознакою безпекового інциденту.

Одночасно з технологічним розвитком, важливим аспектом є розробка глобальних стандартів і протоколів для поведінкових систем безпеки. Міжнародна співпраця та обмін знаннями можуть сприяти гармонізації підходів до захисту даних, а також розробці універсальних рішень, що задовольняють потреби різних груп користувачів і враховують специфіку різних регіонів і культур.

Врешті-решт, для успішного застосування поведінкових патернів у системах безпеки необхідно забезпечити широке розуміння та підтримку з боку користувачів. Інформаційні кампанії, освітні програми та тренінги можуть допомогти підвищити обізнаність користувачів про переваги та потенційні ризики поведінкових систем безпеки. Важливо, щоб користувачі розуміли, як працюють ці системи, які дані збираються та аналізуються, і як вони можуть керувати своєю приватністю та безпекою в цифровому просторі.

Підвищення прозорості процесів, що лежать в основі поведінкових систем безпеки, також є критично важливим для збереження довіри між користувачами та провайдерами послуг. Користувачі повинні мати можливість легко доступити інформацію про засоби захисту даних, політики конфіденційності та можливості для втручання або відмови від певних форм обробки даних.

Технічне вдосконалення поведінкових систем безпеки також має включати розробку ефективних механізмів для швидкого виявлення та реагування на

безпекові інциденти. Інтеграція з іншими інструментами безпеки, як-от системами виявлення вторгнення та управління інцидентами, може забезпечити більш широкий огляд загроз та сприяти швидкій мобілізації ресурсів для захисту цифрових активів.

На закінчення, подальший розвиток і впровадження поведінкових патернів у системах безпеки вимагає балансу між інноваційними технологічними рішеннями, етичними принципами, захистом приватності та активною участю користувачів. Забезпечення цього балансу дозволить розробити надійні, ефективні та прийнятні для суспільства системи, що використовують поведінкові патерни для забезпечення кібербезпеки в широкому спектрі застосувань. Спільні зусилля науковців, інженерів, законодавців та громадськості сприятимуть створенню стійкої інфраструктури безпеки, здатної адаптуватися до постійно змінюваного ландшафту кіберзагроз.

1.4. Опис факторів автентифікації, використаних при підвищенні безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

Логін і пароль: Логін і пароль є найбільш поширеними та базовими методами автентифікації. Логін служить унікальним ідентифікатором користувача, а пароль — секретним кодом, який відомий тільки користувачеві. Паролі повинні бути складними, включати великі та малі літери, цифри та спеціальні символи, щоб ускладнити їх підбір. Надійність пароля забезпечується також регулярною його зміною.

Унікальний ідентифікатор пристрою: Унікальний ідентифікатор пристрою (UID) — це унікальний набір даних, який присвоюється кожному пристрою. Він може включати MAC-адресу, серійний номер або інші апаратні ідентифікатори. Використання UID дозволяє системі визначити, з якого пристрою здійснюється спроба доступу, і порівняти ці дані з раніше збереженими значеннями. Це

забезпечує додатковий рівень захисту, особливо у випадках, коли користувач намагається увійти в систему з нового або невідомого пристрою.

Геолокація: Геолокація визначає фізичне місцезнаходження користувача під час спроби доступу. Цей фактор автентифікації ґрунтується на GPS-даних, IP-адресі або інформації про найближчі Wi-Fi мережі. Перевірка геолокації дозволяє виявити підозрілі спроби доступу з незвичних місць, наприклад, якщо користувач зазвичай входить у систему з одного міста, а раптово спроба доступу здійснюється з іншого континенту. У таких випадках система може вимагати додаткову автентифікацію або заблокувати доступ.

Голосовий зліпок: Голосова автентифікація базується на аналізі голосового зліпка користувача. Голос є унікальним біометричним параметром, який важко підробити. Для автентифікації користувач вимовляє певну фразу, і система порівнює отриманий голосовий зліпок із зразком, що був записаний під час реєстрації. Цей метод є зручним та ефективним, оскільки не вимагає додаткових пристроїв і може бути використаний навіть у мобільних додатках.

Поведінкові патерни: Поведінкові патерни включають аналіз характерних особливостей поведінки користувача під час взаємодії з системою. Це можуть бути ритм і сила натискання клавіш, швидкість набору тексту, рухи миші та інші показники. Кожен користувач має унікальний стиль взаємодії з пристроями, який важко підробити. Система реєструє ці патерни під час реєстрації і використовує їх для автентифікації під час кожної сесії. Аналіз поведінкових патернів дозволяє виявити спроби несанкціонованого доступу, навіть якщо зловмисник знає логін і пароль користувача.

1.5 Висновки та постановка задач

Огляд сучасних методів автентифікації демонструє постійне зростання інтересу до пошуку більш надійних та зручних способів захисту інформаційних систем. Традиційні методи, такі як паролі та PIN-коди, хоча й широко використовуються, але поступово визнаються застарілими через високі ризики

компрометації. Двофакторна автентифікація та більш складні системи, що включають кілька рівнів захисту, пропонують значне покращення безпеки.

Біометричні системи ідентифікації та поведінкові патерни відкривають нові перспективи у сфері аутентифікації, пропонуючи методи, що засновані на унікальних характеристиках особи. Водночас, вони потребують ретельного захисту особистих даних та забезпечення приватності.

Враховуючи динамічний розвиток кіберзагроз, важливо постійно вдосконалювати методи автентифікації, інтегруючи новітні технології та підходи. П’ятифакторна система автентифікації та валідації, яка розглядається у цій роботі, є одним з таких інноваційних рішень. Її розробка та впровадження може значно підвищити захищеність інформаційних систем, забезпечуючи комплексний захист на різних рівня х аутентифікації. Зокрема, інтеграція біометричних даних та поведінкових патернів дозволяє створити більш динамічну та адаптивну систему, яка може виявляти та запобігати спробам несанкціонованого доступу з вищою точністю.

Подальші дослідження в області п’ятифакторної автентифікації мають зосередитись на розробці ефективних механізмів збору та аналізу даних, забезпеченні приватності користувачів та захисту біометричних та поведінкових інформацій. Важливим аспектом є також створення надійних алгоритмів для обробки та валідації отриманих даних, що вимагає глибокого розуміння як технологічних, так і психологічних аспектів поведінки користувачів.

Розробка та впровадження п’ятифакторної системи автентифікації відкриває широкі можливості для застосування у різноманітних галузях, де вимоги до безпеки інформаційних систем особливо високі. Це може стосуватися фінансової сфери, державного управління, охорони здоров’я та інших критично важливих секторів.

Завершуючи перший розділ, можна констатувати, що теоретичні основи п’ятифакторної системи автентифікації та валідації мають глибоке наукове та практичне підґрунтя. Їхнє дослідження та розвиток відіграють ключову роль у

формуванні майбутнього напряму кібербезпеки, спрямованого на створення більш безпечного та довіреного цифрового середовища.

Впровадження п'ятифакторної системи автентифікації відображає глибоке розуміння того, що безпека в сучасному цифровому світі вимагає багаторівневого підходу. Комбінація різноманітних методів аутентифікації не тільки підвищує захищеність систем, але й адаптує безпеку до різних сценаріїв використання та потенційних загроз. Цей комплексний підхід дозволяє мінімізувати ризики, пов'язані з використанням одного чи кількох статичних факторів, і пропонує міцну основу для захисту ідентичності користувачів та даних.

Розвиток таких систем також вказує на необхідність продовження досліджень у сфері кібербезпеки, зокрема у напрямках машинного навчання та штучного інтелекту для аналізу та ідентифікації поведінкових та біометричних патернів. Ефективне використання цих технологій може значно покращити точність та надійність аутентифікаційних систем, а також забезпечити їхню здатність адаптуватися до нових видів загроз.

Однак, розвиток п'ятифакторної автентифікації також ставить питання про баланс між безпекою та зручністю користування. Важливо розробляти системи, які забезпечують високий рівень захисту без надмірного ускладнення процесів аутентифікації для користувачів. Це вимагає інноваційних рішень для оптимізації інтерфейсів та процесів взаємодії.

В кінцевому рахунку, успішне впровадження та використання п'ятифакторної системи автентифікації залежить не тільки від технологічних інновацій, але й від відповідності юридичним та етичним стандартам, захисту приватності та забезпечення прозорості в обробці даних. Майбутнє дослідження в цій області повинне також зосереджуватися на створенні стандартів та методологій для оцінки ефективності та безпеки систем аутентифікації, розробці надійних механізмів для захисту від нових та еволюціонуючих загроз, а також на впровадженні освітніх програм для користувачів, щоб підвищити їхню обізнаність та здатність захищати свої дані.

Освіта і тренінги для користувачів стануть ключовим елементом у поширенні знань про безпеку та методи аутентифікації. Це дозволить користувачам краще розуміти, як вони можуть співпрацювати з технологіями для захисту своєї ідентичності та персональних даних. Важливо забезпечити, щоб ці освітні програми були доступні та зрозумілі для всіх користувачів, незалежно від їхнього технічного досвіду.

Крім того, потрібно враховувати і соціально-економічні аспекти при впровадженні п'ятифакторної автентифікації. Не всі користувачі мають однаковий доступ до технологій або можливість використовувати складні системи аутентифікації. Тому, під час розробки таких систем, важливо забезпечити їх доступність та простоту використання для широкого кола людей.

На закінчення, розвиток п'ятифакторної системи автентифікації вимагає не тільки технологічних інновацій, але й постійного діалогу між розробниками, дослідниками, законодавцями, бізнесом та громадськістю. Це забезпечить, що системи аутентифікації розвиваються відповідно до потреб суспільства, забезпечуючи високий рівень безпеки без порушення приватності або обмеження доступу до цифрових ресурсів. Врахування цих аспектів допоможе створити більш безпечне, доступне та довірене цифрове середовище для всіх користувачів.

Розглянуті в цьому розділі теоретичні основи п’ятифакторної системи автентифікації та валідації підкреслюють важливість комплексного підходу до забезпечення інформаційної безпеки в сучасних умовах. З розвитком технологій та збільшенням обсягів оброблюваних даних, зростає й кількість загроз, спрямованих на компрометацію систем автентифікації. Традиційні методи, такі як однофакторна автентифікація (паролі або ПІН-коди), поступово стають менш ефективними у зв'язку з їх вразливістю до атак, таких як фішинг, підбір паролів та соціальна інженерія.

У цьому контексті п’ятифакторна система автентифікації та валідації пропонує суттєве підвищення рівня захисту, використовуючи різні фактори автентифікації: знання (щось, що користувач знає), володіння (щось, що користувач має), біометричні дані (щось, що є користувачем), місце розташування

(щось, де користувач є) та поведінкові фактори (щось, що користувач робить). Такий підхід дозволяє значно ускладнити несанкціонований доступ до системи, оскільки атака на всі п’ять факторів одночасно є надзвичайно складним завданням.

Інтеграція динамічного біометричного патерну поведінки як одного з факторів автентифікації додає ще один рівень захисту. На відміну від статичних біометричних параметрів, таких як відбитки пальців або сітківка ока, поведінкові патерни є унікальними для кожного користувача і змінюються з часом, що робить їх більш стійкими до підробки.

Таким чином, п’ятифакторна система автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки представляє собою інноваційний підхід до захисту інформаційних систем. Її застосування може суттєво знизити ризики несанкціонованого доступу та захистити чутливі дані від компрометації.

Постановка задач: для досягнення основної мети дипломної роботи, яка полягає у підвищенні безпеки інформаційних систем шляхом впровадження п’ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки, необхідно вирішити наступні задачі:

Аналіз існуючих методів автентифікації та валідації:

- Провести огляд сучасних підходів до автентифікації та валідації користувачів в інформаційних системах.
- Визначити основні недоліки та вразливості традиційних систем автентифікації.

Розробка концептуальної моделі п’ятифакторної системи автентифікації та валідації:

- Визначити та описати п'ять факторів автентифікації, які будуть використовуватися в системі.
- Обґрунтувати вибір кожного фактору та його роль у забезпеченні загальної безпеки системи.

Інтеграція динамічного біометричного патерну поведінки:

- Дослідити методи збору та аналізу поведінкових біометричних даних.
- Розробити алгоритм для виявлення та використання динамічних поведінкових патернів як фактору автентифікації.

Розробка прототипу системи:

- Створити програмну реалізацію п’ятифакторної системи автентифікації та валідації.
- Інтегрувати в прототип всі обрані фактори, включаючи динамічний біометричний патерн поведінки.

Тестування та оцінка ефективності:

- Провести тестування розробленої системи з метою визначення її ефективності у порівнянні з традиційними методами автентифікації.
- Аналізувати результати тестування та зробити висновки щодо надійності та стійкості системи до різних типів атак.

Розробка рекомендацій для впровадження:

- Сформулювати рекомендації щодо інтеграції п’ятифакторної системи автентифікації та валідації в існуючі інформаційні системи.
- Визначити можливі перешкоди та способи їх подолання під час впровадження нової системи.

Оцінка економічної ефективності:

- Розрахувати економічні вигоди від впровадження п’ятифакторної системи автентифікації та валідації.
- Оцінити вартість впровадження та порівняти її з можливими втратами від несанкціонованого доступу та компрометації даних.

Вирішення зазначених задач дозволить створити ефективну систему автентифікації та валідації, яка забезпечить високий рівень безпеки інформаційних систем та знизить ризики несанкціонованого доступу.

2 РОЗРОБКА АЛГОРИТМУ ТА ПРИНЦИПІВ РОБОТИ СИСТЕМИ

2.1. Вибір методів багатофакторної автентифікації для підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

Порівняльний аналіз ефективності біометричних систем: біометричні системи автентифікації використовують унікальні фізичні або поведінкові характеристики людини, що робить їх значно важче підробити або вкрасти. Проте, біометрія також не є ідеальною:

Технічні помилки: Сканери можуть мати помилки, неправильно ідентифікуючи або відмовляючи доступ легітимним користувачам.

Приватність і безпека даних: Зберігання біометричних даних ставить під загрозу приватність, оскільки в разі витоку така інформація не може бути змінена як пароль.

Висока вартість: Розгортання біометричних систем часто вимагає значних інвестицій у високотехнологічне обладнання.

При порівняльному аналізі ефективності біометричних систем порівняно з іншими методами автентифікації, важливо враховувати також наступні аспекти:

Адаптація до змін у біометричних характеристиках: Фізичні характеристики людини можуть змінюватися з часом через старіння, травми або хвороби. Поведінкові характеристики також можуть варіюватися в залежності від емоційного стану або фізичного самопочуття. Системи біометрії мають бути достатньо адаптивними, щоб точно ідентифікувати особу навіть з урахуванням таких змін.

Універсальність та інклюзивність: Не всі біометричні системи однаково ефективні для всього населення. Наприклад, системи розпізнавання відбитків пальців можуть мати складнощі з ідентифікацією осіб, чия шкіра на пальцях зношена внаслідок фізичної праці, а системи розпізнавання облич можуть демонструвати знижену ефективність при низькому освітленні або для осіб з

певними типами обличчя. Тому розробка біометричних систем має враховувати різноманітність користувачів, забезпечуючи високий рівень доступності та недискримінації.

Швидкість ідентифікації та обробки даних: Однією з переваг біометричних систем є потенційно швидкий процес ідентифікації. Проте, ефективність цього процесу залежить від обчислювальної потужності обладнання та оптимізації алгоритмів обробки даних. Високі затримки під час ідентифікації можуть знизити прийнятність системи для кінцевих користувачів.

Спроможність до інтеграції: Ефективність біометричних систем значною мірою залежить від їхньої спроможності інтегруватися з іншими системами безпеки та інформаційними системами організації. Це включає сумісність з існуючою IT-інфраструктурою, можливість забезпечення безперервної роботи та взаємодії з іншими методами аутентифікації та захисту даних.

Враховуючи ці аспекти, можна з робити, що хоча біометричні системи пропонують значні переваги у зручності та потенційній безпеці порівняно з традиційними методами автентифікації, їх ефективність суттєво залежить від ряду ключових факторів. До них належать точність технологій ідентифікації, здатність адаптуватися до змін у біометричних даних, універсальність застосування для різних груп населення, швидкість обробки даних, а також комплексна інтеграція з іншими системами безпеки.

Також важливо звернути увагу на такі аспекти, як розвиток стандартів безпеки та приватності для біометричних даних. З огляду на ризик витоку або несанкціонованого доступу до біометричної інформації, необхідно розробити ефективні механізми захисту та шифрування даних, а також процедури для їх відновлення у випадку компрометації.

Подальше дослідження в галузі біометричних технологій може сприяти вдосконаленню існуючих систем та розвитку нових методів, які будуть ще більш ефективними, безпечними та зручними для користувачів. Це включає інновації у сфері штучного інтелекту та машинного навчання для покращення алгоритмів

розпізнавання, а також вивчення альтернативних біометричних ідентифікаторів, які можуть пропонувати нові можливості для аутентифікації.

У підсумку, ефективне впровадження та використання біометричних систем автентифікації вимагає збалансованого підходу, що враховує технічні можливості та обмеження технологій, потреби та права користувачів, а також постійного розвитку та адаптації до змінюваних умов і викликів у сфері кібербезпеки.

Посилення біометричних систем автентифікації може бути досягнуто через розвиток гібридних моделей, які комбінують кілька біометричних ідентифікаторів або інтегрують біометричні дані з іншими формами автентифікації. Наприклад, система, що поєднує розпізнавання відбитків пальців із розпізнаванням обличчя або голосу, може забезпечити вищий рівень безпеки, мінімізуючи ризик помилкового відхилення легітимних користувачів або неправомірного доступу. Такі підходи також можуть допомогти впоратися з обмеженнями окремих біометричних технологій, забезпечуючи більш стійкий захист.

Окрім технічного вдосконалення, важливим аспектом є правовий захист біометричних даних. Розробка чітких законодавчих і регуляторних рамок для збору, обробки, зберігання та використання біометричної інформації є критично важливою для забезпечення довіри та прийняття цих технологій користувачами. Законодавство має визначати відповідальність за порушення приватності та забезпечувати права осіб на доступ до власних даних та їх виправлення або видалення.

Ще одним ключовим елементом ефективності біометричних систем є освітня діяльність та підвищення обізнаності користувачів. Надання користувачам повної інформації про те, які біометричні дані збираються, як вони використовуються та захищаються, може сприяти більш відповідальному ставленню до особистої безпеки та приватності. Також важливо інформувати користувачів про їхні права та доступні механізми захисту в разі витоку або зловживання даними.

В кінцевому підсумку, посилення ефективності біометричних систем автентифікації залежить від комплексного підходу, який об'єднує технологічні інновації, правовий захист, освітні ініціативи та активну участь користувачів.

Розвиток таких систем має враховувати широкий спектр викликів, від технічних обмежень до соціально-етичних питань , ставлячи в центрі уваги не лише питання безпеки, а й забезпечення приватності та зручності для кінцевого користувача.

Також важливо зосередитись на розробці резервних механізмів та планів відновлення для біометричних систем. У випадку непередбачуваних ситуацій, таких як технічні збої або цілеспрямовані атаки, система має мати можливість швидкого відновлення, мінімізуючи переривання у доступі до сервісів і захисті даних.

Інтеграція біометричних систем з іншими технологіями безпеки, такими як шифрування даних та блокчейн, може забезпечити додатковий рівень захисту, знижуючи ризики асоційовані з витоком інформації. Використання блокчейну для зберігання біометричних даних може допомогти забезпечити незмінність та прозорість їх обробки, водночас забезпечуючи контроль доступу та перевірку автентичності без необхідності централізованого зберігання.

У міру розвитку інтернету речей (IoT) та збільшення кількості підключених пристроїв, біометричні системи можуть зіграти ключову роль у забезпеченні безпечної ідентифікації та авторизації користувачів у широкому спектрі застосувань. Проте, це також створює додаткові виклики для інтеграції та управління біометричними даними на різних пристроях та платформах, вимагаючи розробки уніфікованих стандартів та протоколів безпеки.

Наостанок, участь громадськості та прозорість процесів є критично важливими для прийняття біометричних технологій на масовому рівні. Організації та розробники мають активно спілкуватися з користувачами, надаючи інформацію про переваги та ризики асоційовані з використанням біометричних систем, та враховувати їхні занепокоєння та пропозиції щодо поліпшення приватності та безпеки.

Підсумовуючи, посилення ефективності біометричних систем автентифікації потребує комплексного підходу, який включає технічні ін новації, правову регуляцію, освітні ініціативи, а також відкрите спілкування з користувачами. Для досягнення цієї мети необхідно також забезпечити міцну співпрацю між

державними установами, приватним сектором, академічними кругами та громадськістю, щоб разом вирішувати виклики та створювати рішення, які поєднують високий рівень безпеки з повагою до приватності індивіда.

Враховуючи швидкий розвиток цифрових технологій, важливо також зосередитися на розробці гнучких систем, які можуть адаптуватися до нових загроз та змін у поведінці користувачів. Це включає в себе використання алгоритмів машинного навчання та штучного інтелекту для постійного вдосконалення процесів ідентифікації та автентифікації.

Також критично важливим є розробка ефективних механізмів для швидкого реагування на інциденти безпеки, що включають біометричні дані. Організації мають мати чіткі процедури для випадків порушення безпеки даних, які забезпечують швидке інформування користувачів та вжиття необхідних заходів для мінімізації шкоди.

У підсумку, успіх біометричних систем автентифікації залежить не лише від їх технічної ефективності, а й від здатності цих систем інтегруватися в ширший контекст цифрової безпеки, забезпечуючи збалансований захист інтересів усіх зацікавлених сторін. Розвиток цих систем має відбуватися з урахуванням постійно змінюваного цифрового ландшафту, адаптуючись до нових викликів і використовуючи найкращі доступні технології для захисту особистих даних і забезпечення приватності користувачів на всіх рівнях.

Критерії вибору ефективної системи автентифікації: вибір ефективної системи автентифікації вимагає врахування ряду ключових критеріїв, здатних забезпечити оптимальний баланс між безпекою, зручністю користування та вартістю реалізації. Основні критерії включають:

Надійність: Система повинна забезпечувати точну та стабільну ідентифікацію користувачів, мінімізуючи помилки як у випадках неправомірного доступу, так і відмови в доступі легітимним користувачам.

Захист від атак: Ефективність системи має бути доведена проти широкого спектру кібератак, включаючи соціальну інженерію, фішинг, атаки методом грубої сили та інші.

Скальованість та інтеграційність: Система повинна легко інтегруватися з існуючою IT-інфраструктурою та масштабуватися відповідно до зростаючих потреб організації.

Зручність користування: Важливо, щоб система була зручною для кінцевих користувачів, не створюючи зайвих незручностей або затримок при аутентифікації.

Приватність даних: Система має включати механізми захисту персональних даних користувачів, щоб забезпечити їх конфіденційність та дотримання нормативних вимог.

Вартість: Вартість розгортання та експлуатації системи автентифікації має бути виправдана її перевагами та ефективністю, при цьому вона не повинна ставати непосильною для організації.

Додатково до вищевказаних критеріїв, при виборі ефективної системи автентифікації варто врахувати також:

Адаптивність до нових загроз: Система повинна бути гнучкою та здатною швидко адаптуватися до нових типів кібератак. Це означає здатність системи оновлюватися та модернізуватися з мінімальними зусиллями з боку власника.

Підтримка багатофакторної автентифікації: Система повинна підтримувати можливість використання кількох факторів автентифікації одночасно, що значно підвищує рівень безпеки порівняно з однофакторними методами.

Регулярні оновлення та підтримка: Важливим аспектом є наявність надійної технічної підтримки та регулярні оновлення від розробників системи, які забезпечують захист від новітніх загроз та вирішення будь-яких технічних проблем.

Сумісність з правовими та регуляторними вимогами: Система має відповідати місцевим та міжнародним нормам у сфері захисту даних та приватності, зокрема GDPR в ЄС або CCPA в Каліфорнії.

Аналіз вартості та користі: Детальний аналіз повинен враховувати не лише первинні витрати на впровадження, але й довгострокову економію від зниження ризиків безпеки та оптимізації процесів автентифікації.

Зворотний зв'язок від користувачів: Важливо враховувати досвід та відгуки від реальних користувачів системи. Позитивний користувацький досвід може значно підвищити прийняття та використання системи автентифікації всередині організації.

Врахування цих додаткових критеріїв дозволить зробити обґрунтований вибір системи автентифікації, яка не лише забезпечить високий рівень безпеки, але й буде відповідати конкретним потребам та можливостям організації, забезпечуючи при цьому високий рівень зручності та задоволення користувачів.

При розгляді критеріїв для вибору ефективної системи автентифікації, також важливо врахувати:

Міцність протоколів безпеки: Забезпечення безпеки даних та транзакцій вимагає від системи автентифікації використання сучасних, перевірених і надійних криптографічних протоколів. Перед вибором системи необхідно з’ясувати, які технології шифрування вона використовує та як вони захищені від потенційних векторів атак.

Гнучкість управління політиками безпеки: Ефективна система автентифікації має дозволяти адміністраторам легко налаштовувати політики безпеки, адаптуючи їх під змінювані потреби організації та зовнішнє середовище. Це включає можливість налаштування вимог до сили паролів, періодичності зміни паролів, параметрів мультифакторної аутентифікації тощо.

Аудит та звітність: Для забезпечення відповідності регуляторним вимогам та спрощення процесу аналізу безпеки важливо, щоб система надавала інструменти для аудиту та генерації звітів про діяльність користувачів, спроби автентифікації, інциденти безпеки та інше.

Відповідність галузевим стандартам: Особливо важливо для організацій у сферах, які підлягають суворій регуляції (наприклад, фінансові послуги, охорона здоров'я), переконатися, що система автентифікації відповідає всім відповідним галузевим та регуляторним стандартам.

Підтримка та оновлення: Наявність надійної технічної підтримки та гарантій від виробника щодо регулярних оновлень програмного забезпечення є ключовим

фактором для забезпечення тривалої ефективності та безпеки системи автентифікації.

Врахування вимог кінцевих користувачів: Перед впровадженням системи важливо зібрати зворотний зв'язок від потенційних користувачів щодо її зручності, інтуїтивності інтерфейсу та загальної прийнятності процесів автентифікації. Забезпечення високого рівня задоволеності користувачів сприятиме більш ефективному впровадженню та використанню системи на практиці.

Можливості самообслуговування для користувачів: Системи, які дозволяють користувачам самостійно відновлювати паролі, управляти налаштуваннями безпеки та виконувати інші завдання пов'язані з їхньою автентифікацією, можуть значно знизити навантаження на службу підтримки та підвищити загальну ефективність системи.

Сумісність з різними пристроями та платформами: У сучасному багатоплатформенному середовищі важливо, щоб система автентифікації підтримувала різноманітність пристроїв та операційних систем, з якими можуть працювати користувачі, включаючи мобільні пристрої, настільні комп'ютери, планшети та інше.

Довгострокова стратегія безпеки: Вибір системи автентифікації повинен враховувати загальну стратегію безпеки організації, включаючи планування на майбутнє, потенційне розширення бізнесу та здатність системи адаптуватися до нових викликів безпеки.

Екологічність та стійкість: Організації, які прагнуть до стійкого розвитку, можуть також враховувати екологічний вплив системи автентифікації, включаючи використання енергії, можливість переробки обладнання та вплив на навколишнє середовище.

Врахування цих додаткових аспектів допоможе забезпечити, що вибрана система автентифікації не лише відповідає найвищим стандартам безпеки, але й адаптована до конкретних потреб та цілей організації, сприяє підвищенню загальної ефективності та забезпечує високий рівень задоволення та довіри з боку користувачів.

Розглянемо розвиток методів автентифікації та їх порівняльний аналіз з використанням графіків, схем, та таблиць.

Рік	Паролі	Біометричні дані	Поведінкові патерни
2010	90	10	0
2012	75	20	5
2015	60	30	10
2018	50	35	15
2020	40	40	20
2022	35	40	25
2024	20	50	30

Таблиця 1.1 – Зростання інтересу до методів автентифікації з часом

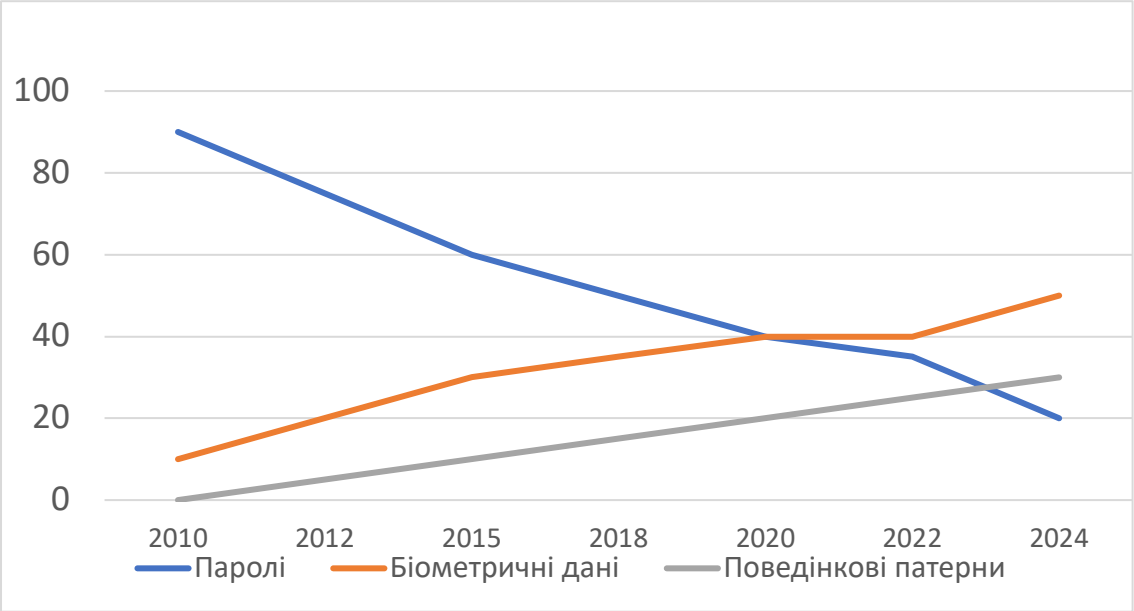


Рисунок 1.1 – Розвиток методів автентифікації

Метод	Надійність (від 1 до 5)	Зручність (від 1 до 5)
Паролі	3	3
Біометричні дані	5	4
Поведінкові патерни	4	5

Таблиця 1.2 – Методи автентифікації за надійністю та зручністю

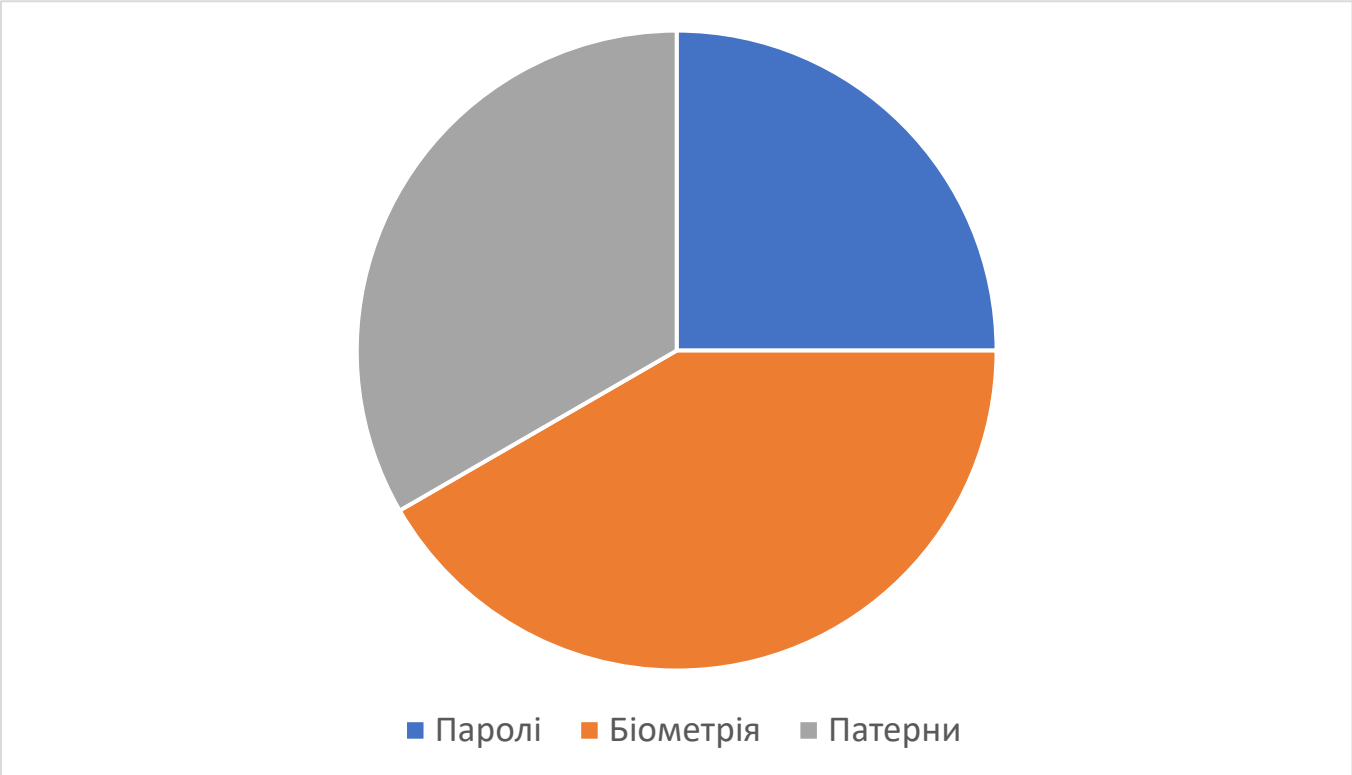


Рисунок 1.2 – Надійність методів автентифікації

Рисунок 1.3 – Зручність методів автентифікації

2.2 Вибір факторів автентифікації для підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

Виходячи з проведеного аналізу факторів для вдосконалення підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки пропонується обрати наступний підхід, а також використати такі фактори, як пароль, ідентифікатор пристрою, геолокація, голосовий зліпок, а також патерни поведінки, що визначаються навченою нейромережею.

Система п'ятифакторної автентифікації покликана значно підвищити рівень безпеки інформаційних систем завдяки використанню різноманітних методів ідентифікації користувачів. Основний принцип роботи системи полягає у поетапній автентифікації користувача, що включає різні фактори, такі як логін, пароль, унікальний ідентифікатор пристрою, геолокація, голосовий зліпок та поведінкові патерни.

Крок 1: Реєстрація користувача

Першим кроком роботи системи є реєстрація користувача. Під час реєстрації користувач повинен створити обліковий запис, надавши всі необхідні дані для подальшої авторизації та автентифікації. Цей процес включає:

- Створення логіна та пароля: Користувач вводить унікальне ім’я користувача та надійний пароль, який буде використаний для початкової автентифікації.
- Введення унікального ідентифікатора пристрою: Система зчитує ідентифікаційні дані пристрою, з якого здійснюється реєстрація.
- Визначення геолокації: Під час реєстрації система визначає географічне положення користувача.
- Запис голосового зліпка: Користувач надає зразок свого голосу, який буде використаний для голосової автентифікації.
- Визначення поведінкових патернів: Система реєструє характерні для користувача поведінкові патерни, такі як ритм натискання клавіш або особливості взаємодії з інтерфейсом.

Реєстрація відіграє ключову роль у системі, оскільки правильне введення всіх необхідних даних дозволяє ефективно використовувати їх для подальшої автентифікації.

Крок 2: Початкова автентифікація

Після реєстрації, під час першого входу в систему, користувач має пройти початкову автентифікацію. Це включає введення логіна та пароля, а також перевірку ідентифікатора пристрою. Цей крок є базовим і встановлює початковий рівень довіри до користувача.

Крок 3: Перевірка геолокації

Наступним кроком є перевірка геолокації користувача. Система порівнює поточне місцезнаходження користувача з попередніми даними, що були зареєстровані під час реєстрації. У випадку значного відхилення від очікуваного місцезнаходження система може запитати додаткову інформацію для підтвердження автентичності.

Крок 4: Голосова автентифікація

На цьому етапі користувач повинен пройти голосову автентифікацію. Для цього він вимовляє заздалегідь визначену фразу або набір слів, які система порівнює із записаним голосовим зліпком. Це дозволяє підтвердити особистість користувача на основі біометричних даних.

Крок 5: Перевірка поведінкових патернів

Останнім кроком є перевірка поведінкових патернів користувача. Система аналізує динаміку взаємодії користувача з інтерфейсом, включаючи ритм натискання клавіш, переміщення миші та інші характерні ознаки поведінки. Цей метод дозволяє виявити потенційно небажані зміни у поведінці, які можуть свідчити про спробу несанкціонованого доступу.

2.2 Розробка алгоритму вдосконаленої системи п’ятифакторної автентифікації

Блок-схема алгоритму: Для візуалізації базового алгоритму п’ятифакторної автентифікації можна використовувати блок-схему, яка відображатиме всі етапи процесу, починаючи від реєстрації до остаточної автентифікації користувача.

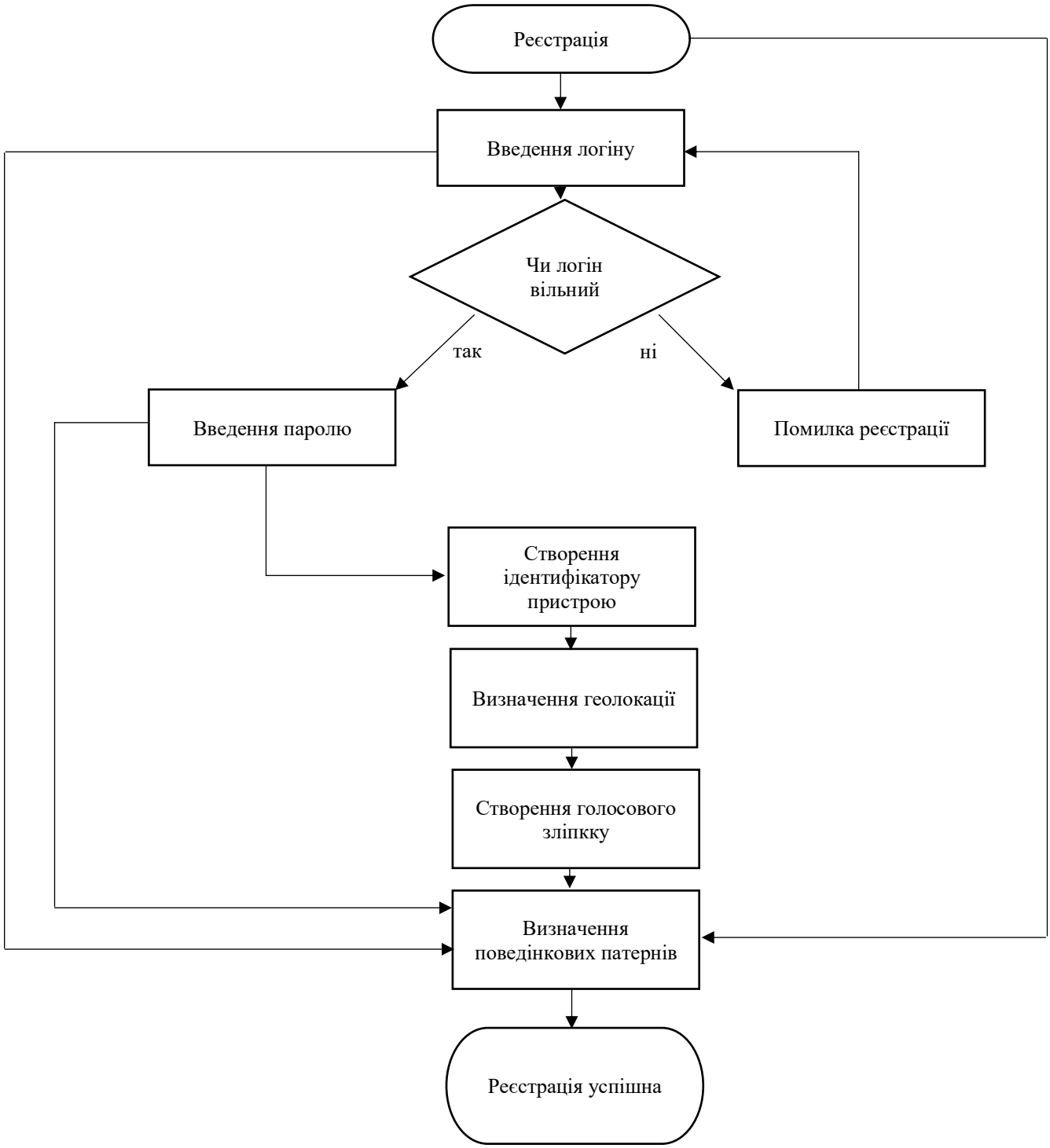


Рисунок 2.1 – Алгоритм реєстрації користувача у системі підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

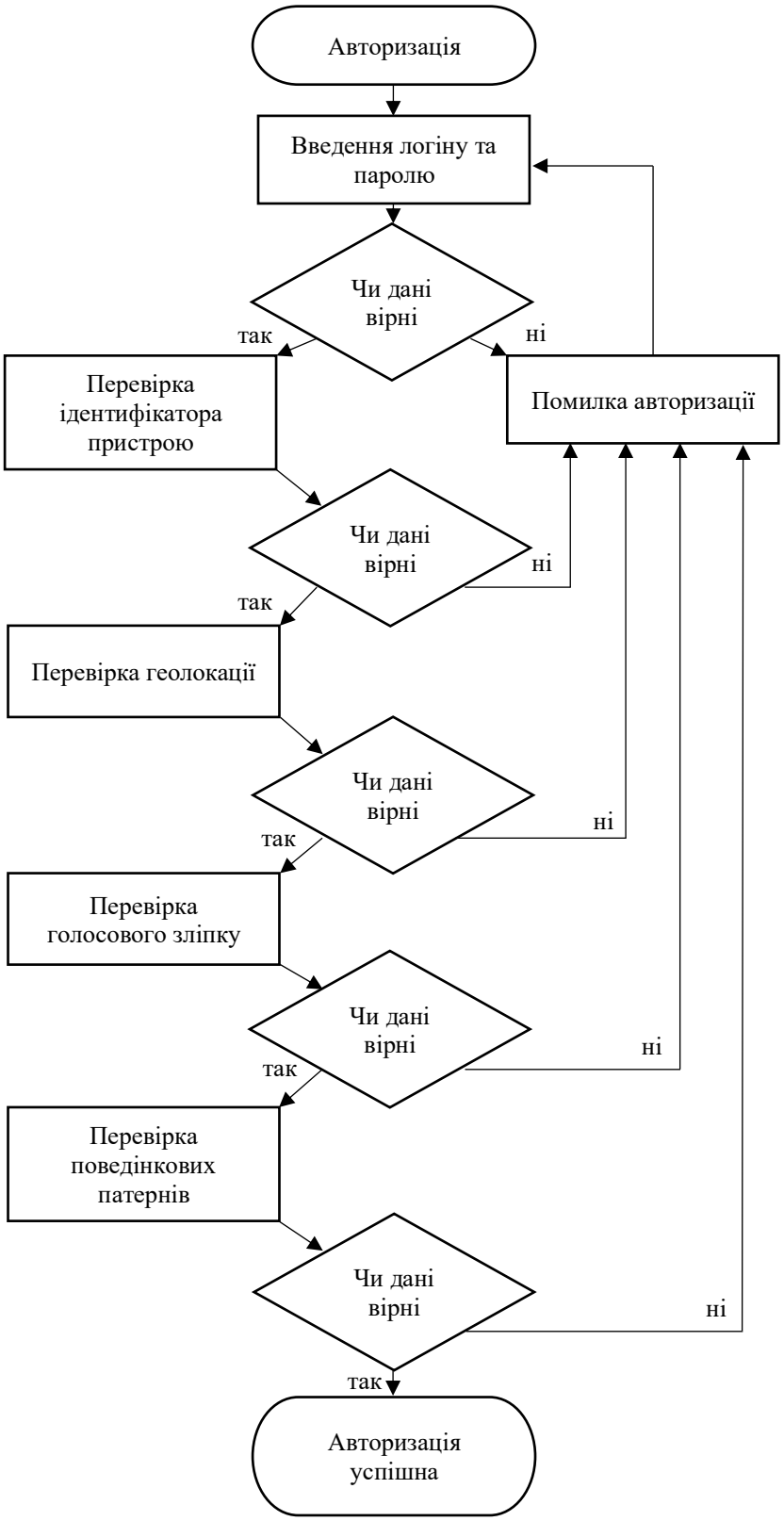


Рисунок 2.2 – Алгоритм реєстрації користувача у системі підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

2.3. Розробка та моделювання бази даних у системі підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

Розробка та моделювання бази даних є ключовими етапами створення системи автентифікації. Важливо забезпечити ефективне зберігання та швидкий доступ до даних користувачів, а також гарантувати безпеку та цілісність інформації. Основні кроки цього процесу включають:

1) Проектування схеми бази даних: Проектування схеми бази даних включає визначення таблиць, полів та зв’язків між ними. Основні таблиці можуть включати:

- Таблиця користувачів: Містить основні дані про користувачів, такі як логін, пароль, ідентифікатор користувача, UID пристрою, геолокаційні дані, голосовий зліпок та поведінкові патерни.
- Таблиця сесій: Зберігає інформацію про активні сесії користувачів, включаючи час входу, IP-адресу та пристрій.
- Таблиця логів: Містить детальну інформацію про всі спроби входу, успішні та неуспішні автентифікації, а також підозрілі дії.

2) Моделювання даних: Моделювання даних включає створення моделі даних, яка відображає структуру бази даних та її взаємозв’язки. Це може бути виконано за допомогою ER-діаграм, які наочно показують структуру та зв’язки між таблицями.

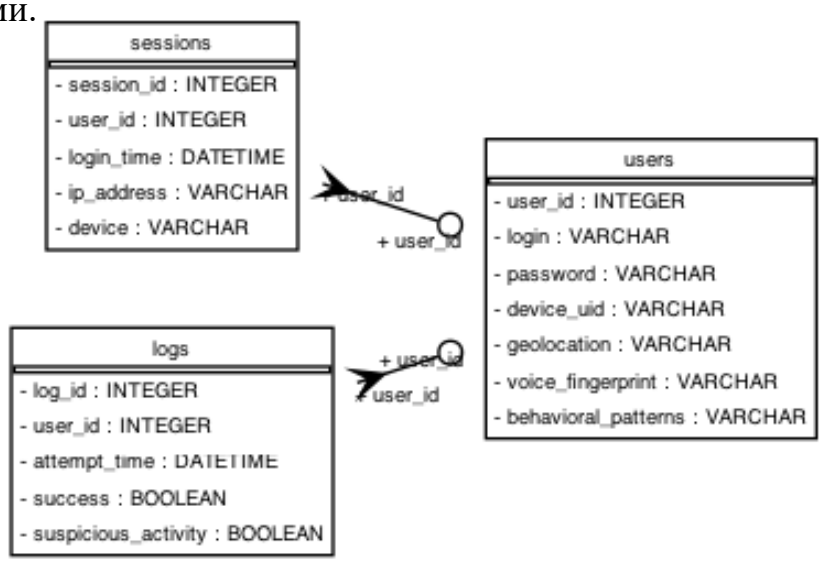


Рисунок 2.3. – ER- діаграма структури та зв’язків між таблицями

Забезпечення безпеки даних: Безпека даних є критично важливою для систем автентифікації. Основні заходи безпеки включають:

- Шифрування даних: Використання сучасних методів шифрування для захисту паролів, біометричних даних та інших чутливих інформацій.
- Контроль доступу: Визначення ролей та привілеїв для користувачів бази даних, що дозволяє контролювати доступ до даних на різних рівнях.
- Аудит та моніторинг: Регулярний аудит бази даних та моніторинг активності для виявлення та реагування на потенційні загрози безпеці.

Таким чином, кожен підрозділ цього розділу висвітлює важливі аспекти розробки системи підвищення безпеки інформаційних систем на основі п’ятифакторної автентифікації. Детальний опис кожного кроку алгоритму та факторів автентифікації, вибір середовища розробки, а також проектування та моделювання бази даних забезпечують комплексний підхід до вирішення проблеми забезпечення безпеки в інформаційних системах.

Загальний огляд та висновки розділу: Аналіз існуючих систем безпеки та їх вразливостей підкреслює важливість постійного пошуку нових, більш ефективних рішень у галузі автентифікації. Традиційні методи виявилися недостатньо захищеними перед сучасними кіберзагрозами, тоді як біометричні системи, незважаючи на свої переваги, все ще мають обмеження, пов'язані з технічними помилками, приватністю даних та високою вартістю реалізації.

Розвиток систем автентифікації, які інтегрують кілька факторів, включаючи біометрію та поведінкові характеристики, відкриває нові перспективи для підвищення безпеки. Однак, важливо не тільки розробляти технологічно передові рішення, але й забезпечувати їх доступність та зручність для кінцевих користувачів. Ефективна система автентифікації повинна вирішувати дилему між строгістю заходів безпеки та необхідністю забезпечити легкий доступ легітимним користувачам.

Критерії вибору ефективної системи автентифікації, розглянуті у цьому розділі, вказують на комплексний підхід до оцінки та впровадження систем безпеки. Врахування надійності, захисту від атак, скальованості, зручності

користування, приватності даних і вартості є ключовими для розробки системи, яка не тільки ефективно захищає від кіберзагроз, але й адаптована до потреб користувачів та організаційних можливостей.

У сучасних умовах, коли кібербезпека стає все більш важливою складовою загальної безпеки організацій та індивідуальних користувачів, розробка та впровадження комплексних систем автентифікації, що базуються на глибокому аналізі існуючих викликів та можливостей, є нагальною потребою. Підсумки даного аналітичного дослідження мають на меті сприяти подальшому прогресу в галузі кібербезпеки, надаючи основу для розробки нових, більш досконалих рішень у сфері захисту інформації.

2.4 Висновки розробки алгоритму та принципів роботи системи

В рамках дипломної роботи, присвяченої вибору методів багатофакторної автентифікації для підвищення безпеки інформаційних систем, було проведено детальний аналіз ефективності біометричних систем у порівнянні з іншими методами автентифікації. Основні висновки дослідження наступні:

Переваги біометричних систем. Використання унікальних фізичних або поведінкових характеристик людини робить біометричні системи важкими для підробки або викрадення.

Потенційно швидкий процес ідентифікації, що може підвищити зручність користування.

Недоліки біометричних систем. Технічні помилки сканерів можуть призвести до неправильної ідентифікації або відмови у доступі легітимним користувачам.

Проблеми з приватністю та безпекою даних через неможливість зміни біометричної інформації в разі її витоку.

Висока вартість впровадження через необхідність у високотехнологічному обладнанні.

Ключові фактори ефективності біометричних систем. Адаптація до змін у біометричних характеристиках: Системи повинні бути здатні враховувати фізичні зміни користувачів та зміну поведінкових патернів.

Універсальність та інклюзивність. Системи повинні бути ефективними для різних груп населення, враховуючи їхні фізичні особливості та умови використання.

Швидкість ідентифікації та обробки даних. Необхідно забезпечити високу продуктивність для зниження затримок.

Спроможність до інтеграції. Ефективна інтеграція з існуючими системами безпеки та IT-інфраструктурою організації.

Інноваційні підходи до підвищення ефективності. Розвиток гібридних моделей, що комбінують кілька біометричних ідентифікаторів або інтегрують біометричні дані з іншими формами автентифікації.

Інтеграція біометричних систем з технологіями шифрування та блокчейн для забезпечення додаткового рівня захисту.

Правовий захист біометричних даних. Розробка чітких законодавчих і регуляторних рамок для збору, обробки, зберігання та використання біометричної інформації.

Забезпечення прав користувачів на доступ до своїх даних та можливість їх видалення або виправлення.

Освітня діяльність та підвищення обізнаності користувачів. Інформування користувачів про те, які дані збираються, як вони використовуються та захищаються.

Підвищення обізнаності щодо прав користувачів та доступних механізмів захисту в разі витоку даних.

Вибір методів автентифікації на основі п'ятифакторної системи. Використання п'яти факторів автентифікації: паролі, ідентифікатори пристроїв, геолокація, голосові зліпки та поведінкові патерни.

Застосування нейронних мереж для визначення та валідації поведінкових патернів користувачів.

Рекомендації для впровадження. Розробка резервних механізмів та планів відновлення для біометричних систем.

Забезпечення сумісності з різними пристроями та платформами, а також підтримка різних операційних систем.

Співпраця між державними установами, приватним сектором, академічними колами та громадськістю для вирішення викликів та розробки рішень, що поєднують високий рівень безпеки з повагою до приватності користувачів.

Ці висновки підкреслюють важливість комплексного підходу до розробки та впровадження біометричних систем автентифікації, враховуючи як технічні аспекти, так і соціально-етичні питання, забезпечуючи таким чином надійний та безпечний захист інформаційних систем.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПІДВИЩЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ П'ЯТИФАКТОРНОЇ СИСТЕМИ АВТЕНТИФІКАЦІЇ ТА ВАЛІДАЦІЇ З ІНТЕГРАЦІЄЮ ДИНАМІЧНОГО БІОМЕТРИЧНОГО ПАТЕРНУ ПОВЕДІНКИ

3.1. Вибір середовища розробки програми підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

Розробка системи підвищення безпеки інформаційних систем вимагає вибору відповідного середовища розробки, яке забезпечить ефективність, надійність та масштабованість. Основні критерії вибору середовища включають:

Мова програмування: Для розробки системи можна використовувати мови програмування, які забезпечують високу продуктивність і підтримують необхідні бібліотеки для роботи з біометричними даними. Найбільш підходящими є Python, Javascript та PHP, для інтерфейсу та елементів керування використовуватиму HTML та CSS.

Фреймворки та бібліотеки: Використання сучасних фреймворків і бібліотек значно спрощує розробку системи автентифікації. Для обробки біометричних даних можна використовувати бібліотеки OpenCV, TensorFlow або PyTorch.

База даних: Для зберігання даних про користувачів, включаючи їх біометричні параметри та поведінкові патерни, необхідна надійна база даних. Найбільш підходящими варіантами є реляційні бази даних, такі як MySQL або PostgreSQL, а також NoSQL бази даних, такі як MongoDB або Cassandra.

Серверне середовище: Для забезпечення надійності та масштабованості системи необхідно використовувати потужне серверне середовище. Хмарні платформи, такі як AWS, Google Cloud або Microsoft Azure, забезпечують необхідні ресурси та інструменти для розробки та розгортання системи.

Інтеграційні інтерфейси: Для взаємодії з іншими системами та сервісами необхідно використовувати API та інші інтеграційні інтерфейси. Це забезпечить можливість інтеграції системи автентифікації з існуючими інформаційними системами організації.

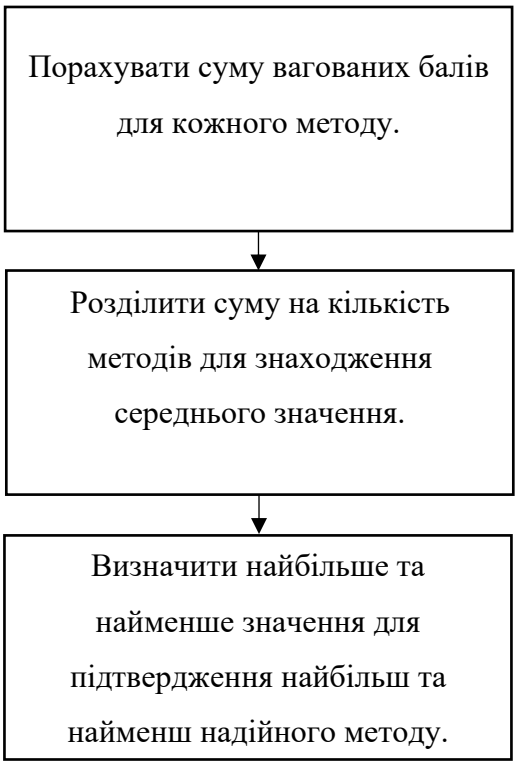


Рисунок 3.1 – Алгоритм підрахунку вагованих параметрів

Для реалізації даного алгоритму та прорахунку результатів використаю мову програмування Python:

```
# Приклад алгоритму на Python
paroli = 3
biometriya = 5
povedinka = 4

suma_vag = paroli + biometriya + povedinka
seredne = suma_vag / 3

if paroli > seredne:
    print("Паролі є найбільш надійним методом.")
elif biometriya > seredne:
    print("Біометричні дані є найбільш надійним методом.")
else:
    print("Поведінкові патерни є найбільш надійним методом.")
```

Рисунок 3.2 – Розрахунок надійності факторів

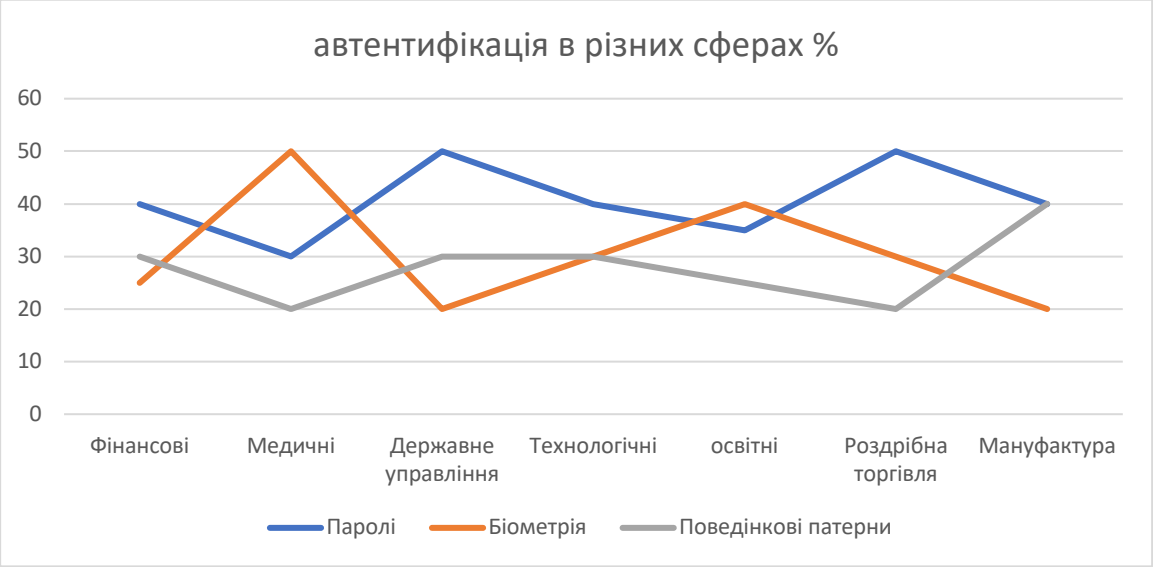


Рисунок 3.3. – Тенденції використання методів автентифікації в різних сферах

```
# Приклад алгоритму на Python для оцінки надійності методів автентифікації
paroli_vimogi = 2
biometriya_vimogi = 5
povedinka_vimogi = 3

paroli_vitrati = 2
biometriya_vitrati = 5
povedinka_vitrati = 3

paroli_skladnist = 3
biometriya_skladnist = 5
povedinka_skladnist = 2

vaga_vimogi = 0.4
```

```
vaga_vitrati = 0.3
vaga_skladnist = 0.3

suma_paroli = (paroli_vimogi * vaga_vimogi) + (paroli_vitrati * vaga_vitrati) +
(paroli_skladnist * vaga_skladnist)
suma_biometriya = (biometriya_vimogi * vaga_vimogi) + (biometriya_vitrati * vaga_vitrati) +
(biometriya_skladnist * vaga_skladnist)
suma_povedinka = (povedinka_vimogi * vaga_vimogi) + (povedinka_vitrati * vaga_vitrati) +
(povedinka_skladnist * vaga_skladnist)

if suma_paroli > suma_biometriya and suma_paroli > suma_povedinka:
    print("Паролі є найбільш надійним методом.")
elif suma_biometriya > suma_paroli and suma_biometriya > suma_povedinka:
    print("Біометричні дані є найбільш надійним методом.")
else:
    print("Поведінкові патерни є найбільш надійним методом.")
```

Рисунок 3.4 – Оцінка надійності методів автентифікації

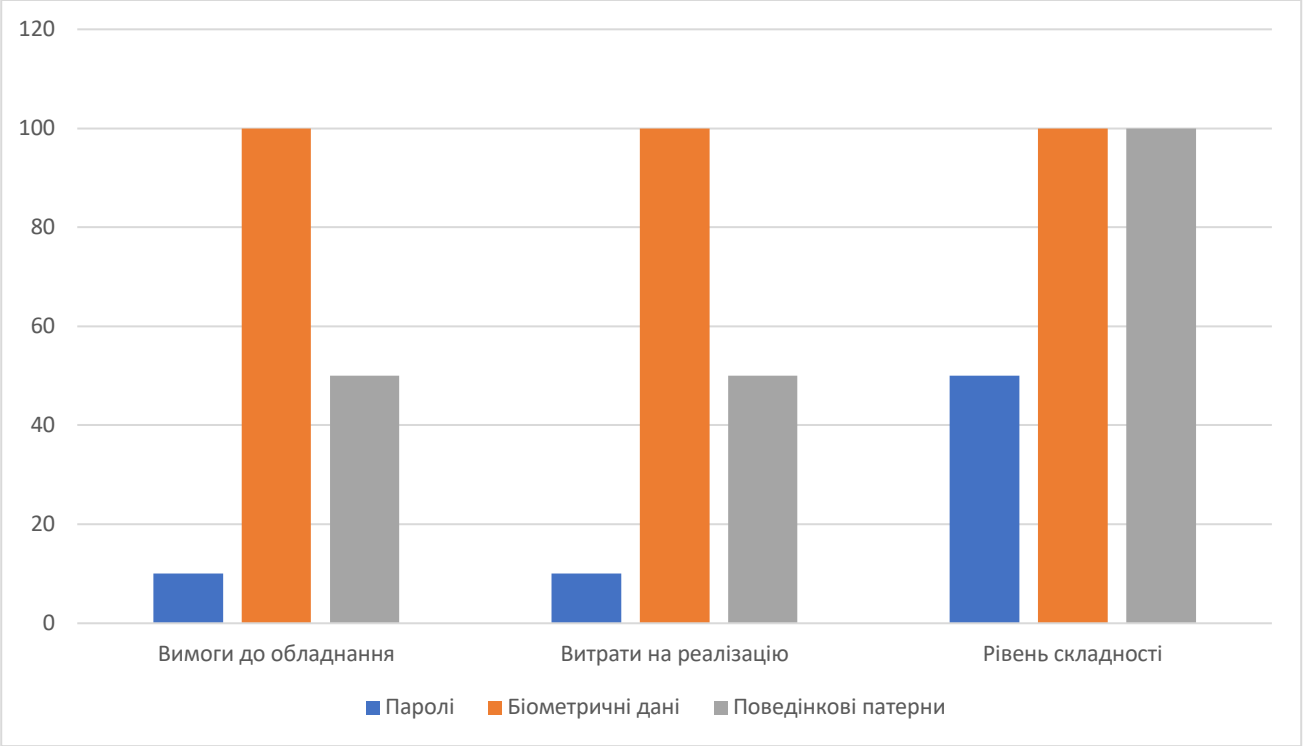


Рисунок 3.5 – Порівняння методів автентифікації

Метод	Вимоги до обладнання	Витрати на реалізацію	Рівень складності
Паролі	Низькі	Низькі	Середні
Біометричні дані	Високі	Високі	Високі
Поведінкові патерни	Середні	Середні	Високі

Таблиця 3.1 – характеристики методів автентифікації

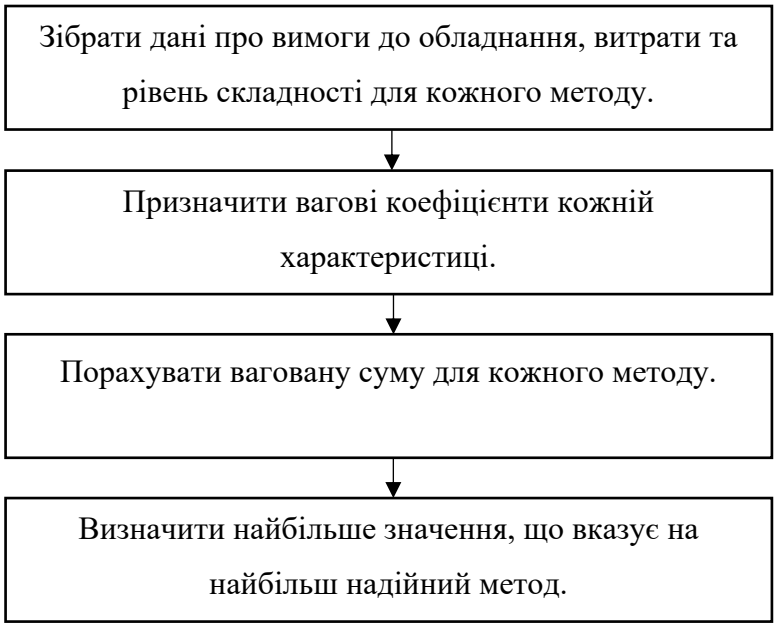


Рисунок 3.6 – Оцінка надійності методів автентифікації з урахуванням характеристик

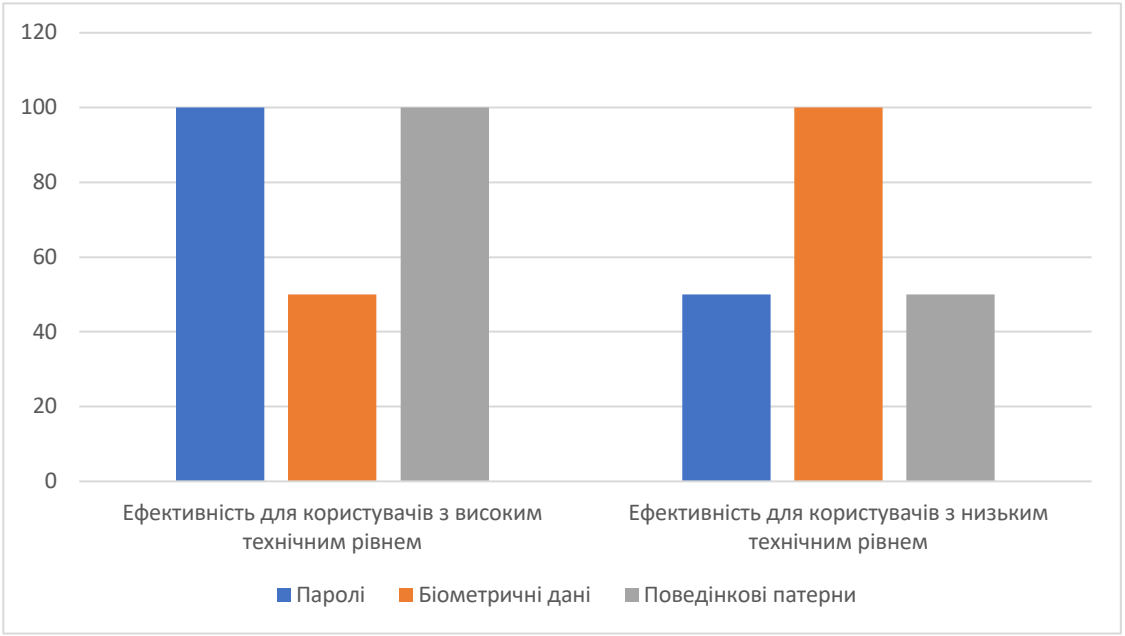


Рисунок 3.7 – Вплив рівня складності на прийняття методів автентифікації

Метод	Вимоги до обладнання	Витрати на реалізацію	Рівень складності	Ефективність для користувачів з високим технічним рівнем	Ефективність для користувачів з низьким технічним рівнем
Паролі	Низькі	Низькі	Середній	Висока	Середня
Біометричні дані	Високі	Високі	Високий	Середня	Висока
Поведінкові патерни	Низькі	Середні	Низький	Висока	Середня

Таблиця 3.2 – Ефективність методів автентифікації в залежності від типу користувача

```
# Приклад алгоритму на Python для оцінки ефективності методів автентифікації для різних типів користувачів

paroli_efekt = {"високий_рівень": "висока", "низький_рівень": "середня"}
biometriya_efekt = {"високий_рівень": "середня", "низький_рівень": "висока"}
povedinka_efekt = {"високий_рівень": "висока", "низький_рівень": "середня"}

korystuvach1 = "високий_рівень"
korystuvach2 = "низький_рівень"

if paroli_efekt[korystuvach1] == "висока":
    print("Користувачу з високим технічним рівнем рекомендується використовувати паролі для автентифікації.")
if paroli_efekt[korystuvach2] == "висока":
    print("Користувачу з низьким технічним рівнем рекомендується використовувати паролі для автентифікації.")
```

Рисунок 3.8 – Оцінка ефективності методів автентифікації для різних типів користувачів

3.2 Розробка робочого прототипу програми п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

П'ятифакторна система автентифікації розроблена з метою забезпечення високого рівня безпеки для інформаційних систем, інтегруючи різноманітні методи

аутентифікації для створення багатошарового захисту. Ключові фактори системи включають: знання (щось, що знає користувач, наприклад, пароль), володіння (щось, що має користувач, наприклад, токен або смарт-картку), інгерентність (біометричні дані), контекст (місцеположення користувача або час доступу) та поведінка (динамічні поведінкові патерни).

Архітектура системи складається з декількох ключових компонентів:

- Модуль збору даних: Відповідає за збір інформації з різних джерел аутентифікації.
- Модуль обробки даних: Аналізує отримані дані на предмет відповідності зареєстрованим профілям користувачів.
- Модуль управління доступом: Вирішує, чи надавати доступ на основі аналізу даних від інших модулів.
- База даних користувачів: Зберігає інформацію про користувачів, їхні аутентифікаційні дані та історію доступів.

- Інтерфейс користувача: Дозволяє користувачам взаємодіяти з системою, реєструвати нові методи аутентифікації або оновлювати існуючі.

Для підвищення ефективності та надійності п'ятифакторної системи автентифікації, важливо також інтегрувати наступні компоненти та принципи в її архітектуру:

Механізми шифрування: Всі дані, які передаються між компонентами системи, повинні бути зашифровані за допомогою сучасних криптографічних алгоритмів. Це забезпечує захист інформації від перехоплення та несанкціонованого доступу під час її передачі.

Система управління ідентифікаційними записами (Identity Management System): Відіграє ключову роль у визначенні, аутентифікації та наданні прав користувачам. Вона дозволяє централізовано управляти ідентифікаторами користувачів, їх ролями та доступом до ресурсів, спрощуючи адміністрування безпеки на всіх рівнях організації.

Протоколи безпеки для взаємодії з зовнішніми сервісами: Часто організації використовують зовнішні сервіси та API для розширення функціональності своїх

систем. Система автентифікації має підтримувати стандарти безпеки, такі як OAuth або SAML, для безпечної взаємодії з цими зовнішніми компонентами.

Резервне копіювання та відновлення: Механізми резервного копіювання та відновлення даних є важливою частиною системи, забезпечуючи можливість швидкого відновлення в разі втрати даних або інших критичних інцидентів.

Модуль моніторингу та сповіщень: Цей модуль відстежує спроби доступу до системи, реєструє події безпеки та генерує сповіщення для адміністраторів у випадку виявлення підозрілих дій або спроб вторгнення. Активний моніторинг дозволяє оперативно реагувати на потенційні загрози.

Політики безпеки та відповідальності: Чітко визначені політики безпеки та відповідальності, які регулюють використання системи автентифікації, її компонентів та поведінку користувачів, є фундаментом для забезпечення загальної безпеки інформаційних ресурсів.

Інтеграція цієї комплексної структури у систему автентифікації не тільки підвищує її надійність та ефективність, але й забезпечує гнучкість та адаптивність до змінюваних вимог безпеки. Додаткові елементи, які можуть бути інтегровані в архітектуру системи для досягнення цих цілей, включають:

Розширену аналітику та штучний інтелект: Використання аналітичних інструментів та алгоритмів машинного навчання для аналізу поведінки користувачів та трафіку даних може допомогти виявляти аномалії та потенційні загрози в реальному часі, що значно підвищує здатність системи передбачати та запобігати безпековим інцидентам.

Децентралізоване управління ідентичністю: Впровадження децентралізованих технологій, таких як блокчейн, для управління ідентифікаційними даними може надати додатковий рівень безпеки та прозорості, знижуючи ризик централізованих витоків даних та зловживань.

Багаторівнева архітектура безпеки: Розробка системи з декількома рівнями захисту, що включає як фізичні, так і логічні механізми оборони (наприклад, мережеві брандмауери, системи виявлення та запобігання вторгненням,

антивірусне програмне забезпечення), дозволяє створити глибокий захист від різноманітних кібератак.

Гнучкість та модульність: Архітектура системи повинна бути гнучкою та модульною, щоб дозволити легке додавання, видалення або оновлення компонентів залежно від зміни технологій або потреб організації без необхідності перебудови всієї системи.

Підтримка стандартів та протоколів безпеки: Слідкування за тим, щоб система підтримувала міжнародні стандарти та протоколи безпеки, гарантує її сумісність з іншими системами та здатність взаємодіяти в широкому екосистемі цифрових технологій.

Застосування цих принципів при розробці архітектури п'ятифакторної системи автентифікації дозволить створити міцну, надійну та водночас гнучку систему, яка може адаптуватися до змінних умов безпеки та вимог користувачів. Окрім того, така система зможе:

Підтримувати розвиток та інновації: Завдяки модульній структурі та підтримці стандартів, система зможе інтегрувати нові технологічні рішення та інноваційні методи аутентифікації, що з'являються на ринку, забезпечуючи тим самим тривалу актуальність та конкурентоспроможність.

Забезпечувати комплексний підхід до безпеки: Використання різних факторів аутентифікації у поєднанні з передовими механізмами шифрування та аналітики дозволяє побудувати багаторівневу систему захисту, яка може ефективно протистояти різноманітним загрозам та атакам.

Забезпечити високу доступність та надійність: Через застосування резервного копіювання, відновлення та високої доступності компонентів, система забезпечує безперебійну роботу та швидке відновлення у випадку збоїв або атак, мінімізуючи потенційні збитки.

Забезпечити прозорість та контроль для користувачів: Наявність інтерфейсу користувача, що дозволяє користувачам самостійно управляти своїми аутентифікаційними даними та налаштуваннями безпеки, підвищує довіру та

задоволення користувачів, а також сприяє підвищенню загального рівня безпеки системи.

Підтримка законодавчих та нормативних вимог: Система має бути спроектована з урахуванням чинних законодавчих та нормативних вимог з захисту даних, що забезпечує її легальне використання та знижує ризики юридичних наслідків для організації.

Підсумовуючи, п'ятифакторна система автентифікації, побудована з урахуванням цих принципів та компонентів, стане міцною основою для захисту інформаційних ресурсів організації від сучасних та майбутніх кіберзагроз. Одночасно, вона забезпечить зручність та гнучкість використання для кінцевих користувачів, враховуючи їх потреби та вимоги до безпеки. Також важливо пам'ятати про необхідність:

Освіти та тренінгу: Проведення регулярних навчальних сесій та тренінгів для користувачів і адміністраторів системи щодо принципів безпеки, правил користування системою та виявлення та реагування на потенційні загрози. Освічені користувачі – це один з ключових елементів ефективної системи безпеки.

Постійний аналіз та оновлення безпеки: Розвиток кіберзагроз не зупиняється, тому важливо забезпечити механізми для постійного моніторингу, аналізу та оновлення системи безпеки, щоб вона відповідала найсучаснішим загрозам та використовувала передові практики захисту.

Використання відкритих стандартів та інтероперабельність: Забезпечення сумісності та інтеграції з іншими системами та сервісами через використання відкритих стандартів значно підвищує гнучкість системи та дозволяє користувачам вибирати найбільш зручні та безпечні методи аутентифікації.

Залучення зовнішніх експертів та аудит: Регулярне проведення зовнішнього аудиту та тестування на проникнення допоможе виявити потенційні вразливості та слабкі місця в системі безпеки, а залучення зовнішніх експертів дозволить використовувати найкращий досвід та знання в області кібербезпеки.

Підходячи до розробки та впровадження п'ятифакторної системи автентифікації з урахуванням цих аспектів, організація може значно знизити

ризики безпеки та забезпечити високий рівень захисту своїх інформаційних ресурсів, одночасно підтримуючи високу продуктивність роботи та задоволення користувачів.

Інтеграція динамічного біометричного патерну поведінки

Динамічний біометричний патерн поведінки включає аналіз манери натискання клавіш, ритму введення тексту, манери руху миші та інших поведінкових характеристик, які можуть бути унікальними для кожного користувача. Цей підхід дозволяє системі ідентифікувати особу за її поведінкою, доповнюючи інші методи аутентифікації.

Інтеграція цього фактору передбачає розробку алгоритмів машинного навчання, які здатні аналізувати поведінкові патерни та адаптуватися до можливих змін у поведінці користувачів з часом. Це вимагає збору великих обсягів даних про поведінку користувачів під час аутентифікаційних сесій для тренування моделей з високою точністю розпізнавання.

Для ефективної інтеграції динамічного біометричного патерну поведінки в систему автентифікації, важливо врахувати наступні аспекти:

Приватність та захист даних: При зборі та аналізі поведінкових даних необхідно забезпечити високий рівень приватності та захисту цих даних відповідно до чинного законодавства, такого як Загальний регламент захисту даних (GDPR) у Європейському Союзі. Це може включати анонімізацію даних та використання зашифрованих каналів для їх передачі.

Точність та надійність: Розроблені алгоритми машинного навчання повинні демонструвати високу точність розпізнавання та здатність ефективно відрізняти легітимного користувача від потенційного зловмисника. Це вимагає ретельного тренування моделей на різноманітних даних, щоб врахувати широкий спектр поведінкових особливостей.

Адаптивність: Система повинна бути здатною адаптуватися до поступових змін у поведінкових патернах користувачів, що можуть виникати з часом через природну еволюцію звичок або в результаті фізичних змін (наприклад, травм).

Алгоритми машинного навчання мають включати механізми для оновлення та самовдосконалення на основі нових даних.

Баланс між безпекою та зручністю: Інтеграція динамічного біометричного патерну поведінки має забезпечувати не тільки високий рівень безпеки, але й зручність користування системою. Занадто суворі вимоги до точності поведінкових патернів можуть призвести до збільшення відмов легітимним користувачам, тому необхідно знайти оптимальний баланс.

Інтеграція з іншими факторами аутентифікації: Динамічний біометричний патерн поведінки повинен ефективно інтегруватися з іншими факторами аутентифікації в рамках п'ятифакторної системи, забезпечуючи багатошаровий захист та можливість гнучкої настройки політик безпеки залежно від рівня ризику асоційованого з конкретними діями або ресурсами.

Етичні міркування: При розробці та впровадженні систем, що аналізують поведінкові патерни, важливо забезпечити, що етичні норми дотримуються у повному обсязі. Це означає повагу до приватності індивіда, забезпечення прозорості використання даних та забезпечення можливості для користувачів контролювати свою інформацію та висловлювати згоду на її обробку.

Тестування та валідація: Перед впровадженням системи в експлуатацію необхідно провести ретельне тестування та валідацію алгоритмів на репрезентативних наборах даних для переконання в їх ефективності та надійності. Це допоможе виявити потенційні слабкі місця та вдосконалити систему перед її масштабним впровадженням.

Врахування виключень та особливих випадків: Система повинна передбачати механізми для обробки виключних ситуацій та особливих випадків, таких як тимчасові фізичні зміни користувача, що можуть вплинути на його поведінкові патерни, забезпечуючи при цьому збереження високого рівня безпеки.

Мультидисциплінарний підхід: Розробка та впровадження ефективної системи, що включає динамічний біометричний патерн поведінки, вимагає залучення фахівців з різних галузей, включаючи кібербезпеку, машинне навчання,

етику, право та управління даними, для забезпечення всебічного підходу до розробки та використання системи.

Неперервне оновлення та навчання: Система повинна бути спроектована таким чином, щоб підтримувати неперервне оновлення та навчання на основі нових даних, що дозволить їй адаптуватися до змін у поведінкових патернах користувачів та нових загроз безпеці.

Врахування цих аспектів допоможе створити більш безпечну, ефективну та користувацьки орієнтовану систему автентифікації, яка може слугувати надійним бар'єром проти несанкціонованого доступу та інших форм кібератак.

На останок, для успішної інтеграції динамічного біометричного патерну поведінки у систему автентифікації, необхідно також зосередитися на:

Користувацькому досвіді: Забезпечення зручності та інтуїтивності користувацького інтерфейсу є ключовим для прийняття системи кінцевими користувачами. Інтерфейс має бути таким, щоб користувачі легко могли виконувати необхідні дії без зайвого стресу або плутанини.

Гнучкість у налаштуваннях безпеки: Система повинна дозволяти адміністраторам гнучко налаштовувати рівні безпеки, виходячи з конкретних потреб організації та оцінки ризиків. Це може включати можливість вибору, які фактори аутентифікації використовувати в певних сценаріях, а також настройку чутливості системи до аномалій у поведінкових патернах.

Розробка процедур відновлення доступу: Важливо передбачити механізми відновлення доступу для випадків, коли користувач не може бути ідентифікований звичним способом через зміни в поведінкових патернах або технічні збої. Ці процедури повинні бути безпечними, але при цьому не занадто обтяжливими для користувачів.

Оцінка та мінімізація впливу на продуктивність системи: Аналіз та обробка великих обсягів даних поведінкових патернів можуть вимагати значних обчислювальних ресурсів. Важливо оцінити потенційний вплив на загальну продуктивність системи та знайти оптимальний баланс між безпекою та ефективністю.

Проведення регулярних оглядів безпеки: Постійний моніторинг ефективності системи, проведення регулярних оглядів безпеки та оновлення програмного забезпечення є необхідними для забезпечення тривалої захищеності від нових та еволюціонуючих загроз.

З урахуванням цих додаткових аспектів, інтеграція динамічного біометричного патерну поведінки у комплексну систему автентифікації може значно підвищити рівень безпеки, пропонуючи при цьому користувацьку зручність і адаптивність до змінних умов користування та загроз. Для досягнення найкращих результатів, особливу увагу слід приділити наступним аспектам:

Інтеграція з іншими системами безпеки: Ефективність поведінкової біометрії значно зростає, коли вона використовується у поєднанні з іншими методами аутентифікації та системами безпеки. Це дозволяє створити комплексний бар'єр, який ускладнює несанкціонований доступ до системи.

Використання передових технологій: Застосування найновіших досягнень у галузі штучного інтелекту, машинного навчання та обробки великих даних може значно підвищити точність та ефективність розпізнавання поведінкових патернів, а також забезпечити більшу адаптивність системи до змін у поведінці користувачів.

Підтримка користувачів: Навчання та підтримка користувачів є важливим елементом успішного впровадження нових технологій. Забезпечення доступу до ресурсів, які допомагають зрозуміти, як використовувати систему та як забезпечити власну безпеку, може значно покращити прийняття нововведень.

Моніторинг та реагування на інциденти: Розробка процедур для моніторингу системи та швидкого реагування на можливі інциденти безпеки є ключовою для забезпечення надійності та ефективності системи автентифікації. Це включає виявлення аномалій, швидке усунення вразливостей та відновлення системи після атак.

Постійне оновлення та вдосконалення: Технологічний прогрес і зміна кіберзагроз вимагають неперервного оновлення та вдосконалення системи автентифікації. Регулярний огляд алгоритмів, оновлення програмного

забезпечення та тестування ефективності системи допоможуть зберегти її актуальність та надійність.

Врахування цих принципів при інтеграції динамічного біометричного патерну поведінки в систему автентифікації дозволить створити гнучку, безпечну та користувацьки зручну систему, яка буде відповідати сучасним вимогам кібербезпеки та забезпечувати ефективний захист від широкого спектру загроз. Ось декілька додаткових рекомендацій для подальшого вдосконалення та ефективної експлуатації системи:

Формування спільноти користувачів та експертів: Створення форумів, спільнот, або робочих груп, де користувачі та розробники можуть ділитися досвідом, знахідками та кращими практиками, сприяє підвищенню загального рівня знань та ефективності системи. Відкрите спілкування дозволяє швидше ідентифікувати потенційні проблеми та знаходити рішення.

Залучення до стандартизації та сертифікації: Участь у процесах стандартизації та отримання сертифікацій, що підтверджують відповідність системи міжнародним нормам безпеки, не тільки підвищує довіру до системи, але й забезпечує високий рівень захисту та якості.

Адаптація до географічних та культурних особливостей: Врахування регіональних особливостей та культурних факторів може бути критично важливим для міжнародних організацій або систем, які використовуються в різних країнах. Адаптація інтерфейсу, комунікацій та процедур може значно підвищити ефективність та прийнятність системи.

Розробка плану реагування на інциденти: Незважаючи на всі зусилля, неможливо гарантувати повну невразливість системи. Розробка детального плану реагування на інциденти, що включає процедури швидкого виявлення, аналізу, ізоляції та усунення проблем, є ключовим елементом стратегії кібербезпеки.

Освітні програми та тренінги для співробітників: Інвестиції в освіту та тренінги співробітників дозволяють не тільки підвищити рівень загальної обізнаності з питань кібербезпеки, але й зменшити ризик внутрішніх загроз та помилок, що можуть призвести до витоку даних або інших інцидентів.

З огляду на швидкий розвиток технологій та зміну кіберзагроз, важливо підтримувати гнучкість та відкритість до нововведень. Система автентифікації, що включає динамічний біометричний патерн поведінки, повинна бути здатна швидко адаптуватися до нових викликів та технологічних рішень, забезпечуючи при цьому безперервний захист інформаційних активів. Для цього рекомендується:

Впровадження процесів неперервного навчання та оптимізації: Система повинна регулярно оновлюватися на основі останніх даних про поведінку користувачів та нових методик машинного навчання. Це забезпечить підвищення точності розпізнавання та зниження помилкових спрацьовувань.

Залучення співробітників до процесу безпеки: Створення культури безпеки в організації, де кожен співробітник відчуває свою роль у захисті інформації, може значно знизити ризики внутрішніх і зовнішніх загроз. Інформування та залучення співробітників до розуміння важливості заходів безпеки підвищує загальну ефективність системи.

Оцінка впливу нових технологій на приватність і етику: Перед впровадженням нових технологічних рішень важливо провести оцінку їх впливу на приватність користувачів і відповідність етичним нормам. Це допоможе уникнути потенційних конфліктів та підвищити довіру користувачів до системи.

Використання штучного інтелекту для прогнозування та аналізу загроз: Інтеграція інструментів штучного інтелекту, які можуть аналізувати великі обсяги даних в реальному часі для виявлення потенційних загроз, дозволить швидко реагувати на нові види атак та адаптувати систему захисту відповідно до зміни обстановки.

Підтримка відкритого діалогу між розробниками, користувачами та регуляторами: Забезпечення прозорості розробки та впровадження системи, відкритість до зворотного зв'язку від користувачів та готовність до взаємодії з регуляторними органами допоможе знайти оптимальні рішення для забезпечення як високого рівня безпеки, так і захисту прав та інтересів користувачів. Регулярний перегляд політик конфіденційності та безпеки, а також адаптація до нових

законодавчих вимог є необхідними кроками для підтримання легітимності та ефективності системи.

Баланс між інноваціями та перевіреними практиками: Під час розробки та вдосконалення системи важливо знайти правильний баланс між впровадженням інноваційних технологій та дотриманням перевірених методик та стандартів безпеки. Це допоможе забезпечити надійність системи та уникнути потенційних ризиків, пов'язаних з новими, ще не повністю випробуваними рішеннями.

Підтримка постійного професійного розвитку команди: Світ кібербезпеки швидко змінюється, і для ефективної роботи над системами безпеки команда розробників має постійно підвищувати свою кваліфікацію, знання та навички. Організація регулярних тренінгів, участь у професійних конференціях та вивчення актуальних наукових досліджень допоможе команді залишатися на передовій прогресу в галузі.

Екосистема безпеки: Розуміння того, що навіть найсильніша система автентифікації є лише частиною загальної екосистеми безпеки, допоможе забезпечити комплексний захист. Інтеграція з іншими системами безпеки, такими як фаєрволи, системи виявлення вторгнень та антивірусне програмне забезпечення, створює багатошаровий захист, здатний протистояти різноманітним загрозам.

Залучення зовнішніх експертів для аудиту та тестування: Регулярне проведення незалежного аудиту та пенетраційного тестування допомагає ідентифікувати потенційні слабкі місця системи та виявити аспекти, які потребують удосконалення або зміцнення.

Готовність до майбутніх викликів: Система повинна бути гнучкою та масштабованою, щоб можна було швидко адаптувати її до нових викликів, технологій та методів атак. Активне слідкування за тенденціями в кібербезпеці та раннє впровадження захисних заходів гарантує, що система залишається ефективною проти постійно еволюціонуючих загроз.

З урахуванням вищезазначеного, підхід до розробки та підтримки системи автентифікації має бути голістичним і передбачати взаємодію між різними аспектами кібербезпеки, технологій та людського фактора. Це не лише допоможе

забезпечити високий рівень захисту інформаційних активів, але й підвищити довіру та задоволеність користувачів системою.

Особливу увагу варто приділити розвитку спроможностей системи автентифікації для адаптації до майбутніх технологічних інновацій та методів кібератак. Зокрема, застосування квантових технологій, розширеного штучного інтелекту, та інших передових рішень може відіграти ключову роль у формуванні наступного покоління систем безпеки.

Завершуючи, важливо зазначити, що успіх системи автентифікації не залежить лише від технологій, а й від людей, які її розробляють, впроваджують та використовують. Тому підвищення обізнаності, освіта та навчання користувачів, а також розвиток культури безпеки в організації є ключовими елементами для створення ефективної та надійної системи автентифікації, здатної протистояти викликам сучасного кіберпростору.

3.3 Програмна реалізація та тестування системи п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

Даний проект представлений у вигляді WEB-додатку та має декілька етапів реалізації методу.

Першим етапом є реєстрація користувача, що починається з введення логіну та паролю.

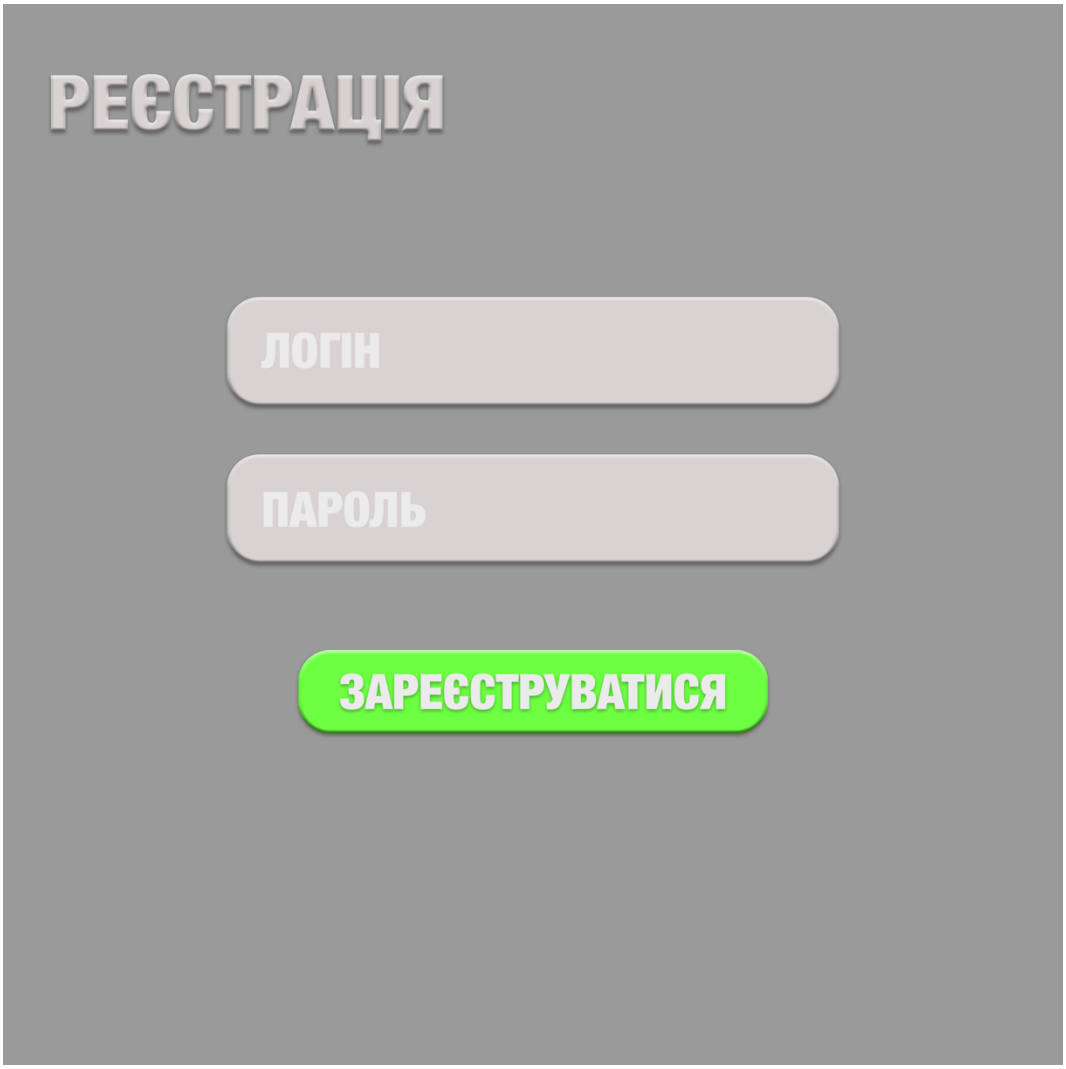


Рисунок 3.9 – Форма реєстрації

Після введення користувачем бажаних даних здійснюється перевірка наявності введеного логіну в базі даних та, у разі його наявності, користувачеві буде сповіщено про те, що даний користувач уже зареєстрований у системі:

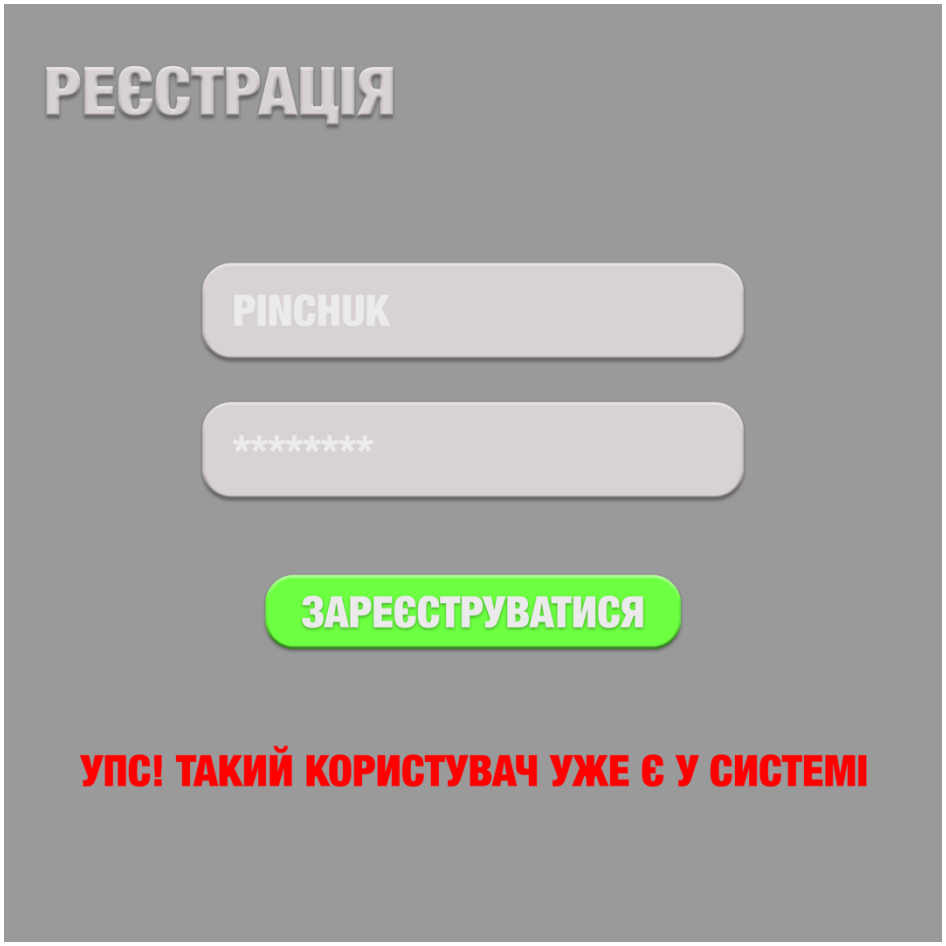


Рисунок 3.10 – Сповіщення про наявного користувача

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Login Availability Check</title>
    <script>
        async function checkUsername() {
            const username = document.getElementById('username').value;
            const response = await fetch(`/check-username?username=${username}`);
            const data = await response.json();
            const message = data.available ? "Username is available" : "Username is taken";
            document.getElementById('availability').innerText = message;
        }
    </script>
</head>
```

```
<body>
    <h1>Check Username Availability</h1>
    <input type="text" id="username" onkeyup="checkUsername()" placeholder="Enter username">
    <p id="availability"></p>
</body>
</html>
```

Рисунок 3.11 – Код сторінки перевірки зайнятості введеного паролю

```
const express = require('express');
const app = express();
const port = 3000;

// Імітована база даних користувачів
const users = [
    { username: 'user1' },
    { username: 'user2' },
    { username: 'user3' }
];

app.get('/check-username', (req, res) => {
    const username = req.query.username;
    const user = users.find(user => user.username === username);
    if (user) {
        res.json({ available: false });
    } else {
        res.json({ available: true });
    }
});

app.listen(port, () => {
    console.log(`Server running at http://localhost:${port}`);
});
```

Рисунок 3.12 – Код серверу для перевірки зайнятості введених данних

У випадку, якщо користувач раніше не був зареєстрований, в базі даних створюється запис, що складається з логіну та хешу введеного паролю. Статус користувача при цьому позначається як «неактивний». Потім формується унікальний ідентифікатор пристрою з якого здійснюється реєстрація, котра зберігається в базу даних з прив’язкою до користувача, а також записується в LocalStorage браузера для подальшого порівняння та унеможливлення здійснення автентифікації з пристрою, відмінного від того, з якого здійснювалась реєстрація. Також це дозволить в майбутньому заборонити автентифікацію навіть з правильного пристрою шляхом звичайного скидання кешу браузера.

```
<script>
// Генерація або отримання унікального ідентифікатора з localStorage
      function getOrCreateDeviceId() {
         let deviceId = localStorage.getItem('deviceId');
         if (!deviceId) {
            deviceId = generateDeviceId();
            localStorage.setItem('deviceId', deviceId);
         }
         return deviceId;
      }
// Генерація унікального ідентифікатора на основі fingerprinting
      function generateDeviceId() {
         const fingerprint = [
            navigator.userAgent,
            navigator.language,
            screen.availWidth,
            screen.availHeight,
            new Date().getTimezoneOffset(),
         ];

         const hashedFingerprint = btoa(JSON.stringify(fingerprint));
         return 'device_' + hashedFingerprint;
      }

      // Виведення ідентифікатора пристрою в консоль
      console.log('Унікальний ідентифікатор пристрою:', getOrCreateDeviceId());
   </script>
```

Рисунок 3.13 – Генерація та збереження унікального ідентифікатора пристрою

Разом із тим визначається геолокація пристрою, з якого здійснюється реєстрація та записується до бази даних у вигляді довготи та широти.

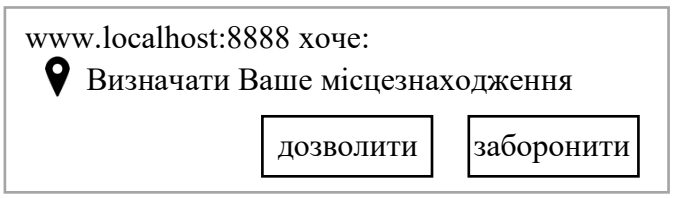


Рисунок 3.14 – Визначення геолокації

Після того, як необхідні дані збережено до бази даних, запускається наступний етап, котрий включає в себе зразок голосу користувача. На екрані з'являється кнопка запису, а також текст, котрий треба прочитати користувачеві для збереження запису його голосу для майбутнього співставлення при авторизації.

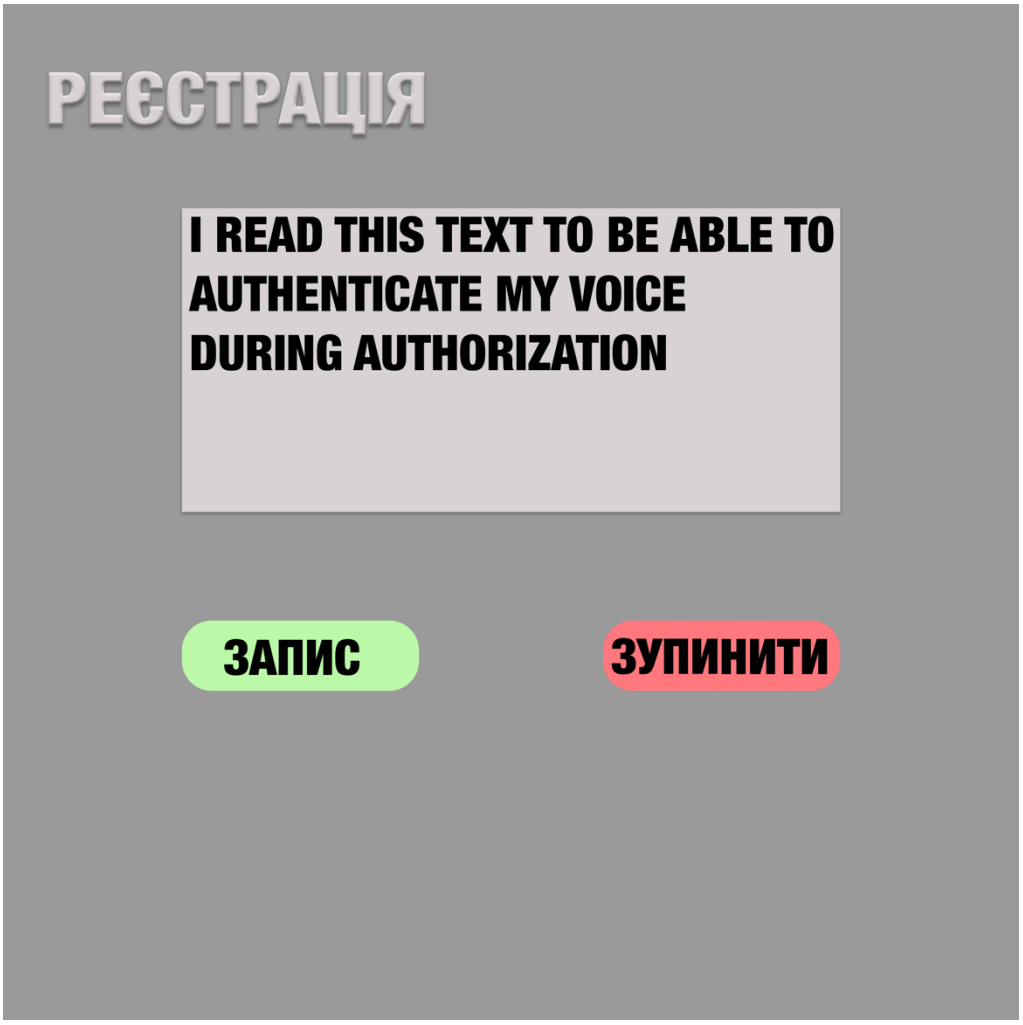


Рисунок 3.15 – Форма запису голосового зразка

Далі прочитаний фрагмент тексту (зразок голосу користувача) зберігається у вигляді аудіо файлу.

Від початку реєстрації і до цього моменту на сторінці здійснювалась фіксація патернів поведінки користувача, таких як рухи мишкою, швидкість вводу символів, час натискання та утримання клавіш, тощо. Після запису голосу з’являється кнопка «Завершити реєстрацію», котра запише до бази даних шлях до аудіо файлу, змінить статус користувача на «активний» та збереже поведінкові патерни.

Наступним етапом є саме автентифікація раніше зареєстрованого користувача на ресурсі. Перш за все необхідно ввести логін та пароль, що є першим етапом автентифікації.

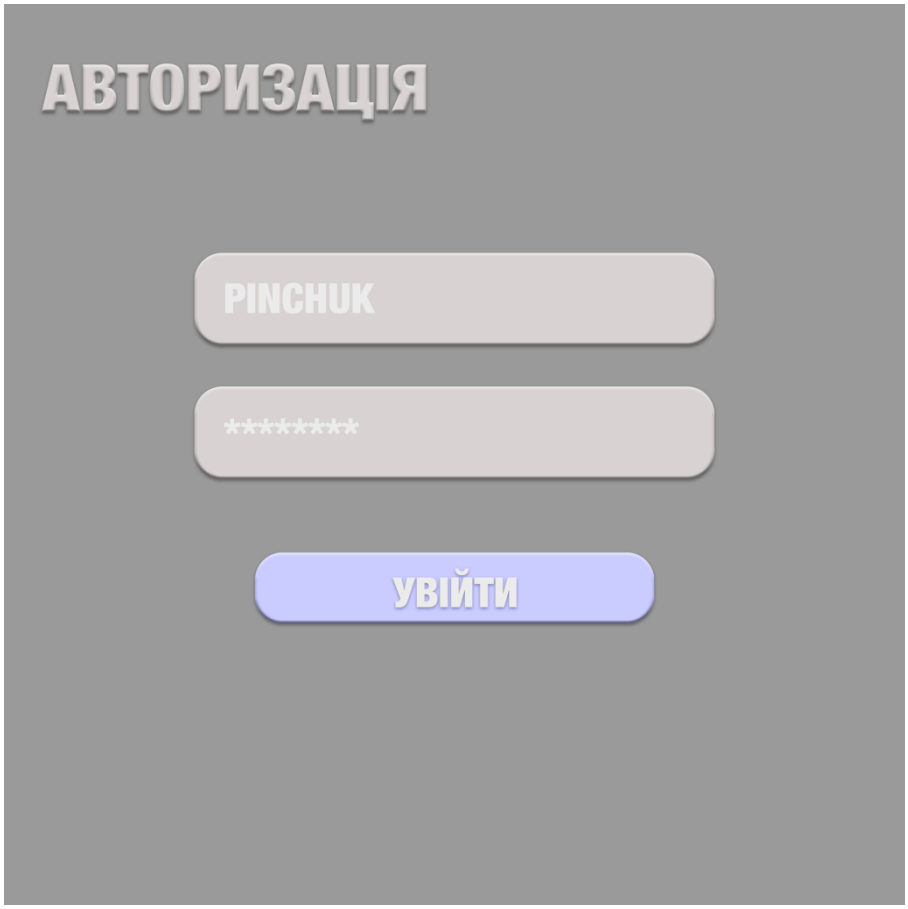


Рисунок 3.16 – Форма вводу логіну та паролю

Після введення логіну та паролю відбувається перевірка наявності логіна в базі даних і, у разі його наявності, перевірка відповідності хешу паролю. Якщо все введено вірно, система переходить до другого фактору автентифікації: ідентифікатору пристрою. При реєстрації унікальний ідентифікатор пристрою зберігся в LocalStorage, тому відбувається співставлення ідентифікатору з локального сховища браузера до того, що збережений у базі даних. Якщо ж ідентифікатори відрізняються, то авторизація вважається невдалою і припиняється,

якщо ж все співпадає, то можна переходити до наступного третього фактору автентифікації за геолокацією. За аналогією із рис.4 визначаються довгота та широта користувача (його пристрою) і відбувається порівняння їх із тими, що вказані при реєстрації. В залежності від потреб можна ввести ряд обмежень на точність геолокації, від відповідності її в рамках країни, до точності в декілька метрів.

```
// Приклад коду на PHP для визначення точності двох точок геолокації з точністю 100м
function haversineDistance($lat1, $lon1, $lat2, $lon2) {
    // Радіус Землі в метрах
    $earthRadius = 6371000;
    // Перетворення градусів в радіани
    $lat1Rad = deg2rad($lat1);
    $lon1Rad = deg2rad($lon1);
    $lat2Rad = deg2rad($lat2);
    $lon2Rad = deg2rad($lon2);
    // Різниця координат
    $latDiff = $lat2Rad - $lat1Rad;
    $lonDiff = $lon2Rad - $lon1Rad;
    // Обчислення відстані за формулою гаверсинуса
    $a = sin($latDiff / 2) * sin($latDiff / 2) +
        cos($lat1Rad) * cos($lat2Rad) *
        sin($lonDiff / 2) * sin($lonDiff / 2);
    $c = 2 * atan2(sqrt($a), sqrt(1 - $a));
    $distance = $earthRadius * $c;
    return $distance;
}

// Приклад використання:
$latitude1 = 48.8566; // широта для точки 1
$longitude1 = 2.3522; // довгота для точки 1
$latitude2 = 48.8606; // широта для точки 2
```

```
$longitude2 = 2.3522; // довгота для точки 2
$distance = haversineDistance($latitude1, $longitude1, $latitude2, $longitude2);
if ($distance <= 100) {
    echo "Координати знаходяться в радіусі 100 метрів одне від одного.";
} else {
    echo "Координати знаходяться за межами радіусу 100 метрів.";
}
```

Рисунок 3.17 – Визначення точності двох точок геолокації з точністю 100м

Якщо геолокація, визначена при авторизації не відповідає тій, що визначена при реєстрації, авторизація знову вважається невдалою і припиняється, якщо ж все співпадає, переходимо до наступного четвертого фактору автентифікації. Голосову автентифікацію можна здійснювати за допомогою різних способів, я розгляну Microsoft Azure Speech API. Якщо користувач прочитає той же текст, що і при реєстрації, два зразки його голосу можна буде порівняти на віддповідність.

```
<!DOCTYPE html>
<html>
<head>
    <title>Speaker Recognition</title>
    <script
src="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js"></script>
</head>
<body>
    <h1>Speaker Recognition</h1>
    <input type="file" id="audio1" accept="audio/*">
    <input type="file" id="audio2" accept="audio/*">
    <button onclick="compare()">Compare</button>
    <p id="result"></p>
    <script>
        const subscriptionKey = 'YOUR_SUBSCRIPTION_KEY';
        const region = 'YOUR_REGION';
        const profileLocale = 'en-US';

        async function compare() {
            const audio1 = document.getElementById('audio1').files[0];
            const audio2 = document.getElementById('audio2').files[0];
            const profileId = await createProfile();
            await enrollProfile(profileId, audio1);
            const result = await verify(profileId, audio2);
            document.getElementById('result').innerText = result;
        }
        async function createProfile() {
```

```
        const response = await fetch(`https://${region}.api.cognitive.microsoft.com/speaker/verification/v2.0/text-independent/profiles`, {
            method: 'POST',
            headers: {
                'Ocp-Apim-Subscription-Key': subscriptionKey,
                'Content-Type': 'application/json'
            },
            body: JSON.stringify({ locale: profileLocale })
        });
        const data = await response.json();
        return data.profileId;
    }
    async function enrollProfile(profileId, audio) {
        const response = await fetch(`https://${region}.api.cognitive.microsoft.com/speaker/verification/v2.0/text-independent/profiles/${profileId}/enrollments`, {
            method: 'POST',
            headers: {
                'Ocp-Apim-Subscription-Key': subscriptionKey,
                'Content-Type': audio.type
            },
            body: audio
        });

        if (!response.ok) {
            throw new Error('Enrollment failed');
        }
    }
    async function verify(profileId, audio) {
        const response = await fetch(`https://${region}.api.cognitive.microsoft.com/speaker/verification/v2.0/text-independent/profiles/${profileId}/verify`, {
            method: 'POST',
            headers: {
                'Ocp-Apim-Subscription-Key': subscriptionKey,
                'Content-Type': audio.type
            },
            body: audio
        });
        const data = await response.json();
        return data.result;
    }
  </script>
</body>
</html>
```

Рисунок 3.18 – Базова реалізація WEB-сторінки із функціоналом перевірки голосу користувача

Якщо голоси не співпадають, авторизація вважається невдалою та припиняється, якщо ж все добре, переходимо на п’ятий фактор автентифікації: поведінкові патерни. Як і у випадку з реєстрацією, під час авторизації поведінкові патерни збираються від самого початку відвідування сторінки та дій на ній. Усі дії на сторінці фіксуються та «згодовуються» навченій нейромережі для порівняння та співставлення. Якщо все відповідає реєстраційним даним, тоді лише в такому випадку користувач отримує доступ до основного контенту сторінки. Під час перебування на сторінці та будучи авторизованим, користувач, виконуючи будь які дії, навчає нейромережу (дані про поведінкові патерни відправляються до нейромережі з певною періодичністю для її навчання) для того, щоб у майбутньому при зміні певних особливостей у користуванні ресурсом та поведінкою на сторінці не залишитись без доступу до інформації, оскільки людям властиво змінюватися та змінювати свої звички, зокрема поведінку, необхідним фактором є постійне навчання нейромережі на нових патернах.

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Behavioral Patterns Collection</title>
    <script>
        let keyPresses = [];
        let mouseMovements = [];
        document.addEventListener('keydown', (event) => {
            keyPresses.push({ key: event.key, timestamp: Date.now() });
        });

        document.addEventListener('mousemove', (event) => {
            mouseMovements.push({ x: event.clientX, y: event.clientY, timestamp: Date.now()
});
        });
        function sendData() {
```

```
            const data = { keyPresses, mouseMovements };
            fetch('/send-data', {
                method: 'POST',
                headers: { 'Content-Type': 'application/json' },
                body: JSON.stringify(data)
            }).then(response => response.json()).then(data => {
                console.log('Data sent:', data);
            });
        }
        window.addEventListener('beforeunload', sendData);
    </script>
</head>
<body>
    <h1>Collecting Behavioral Patterns</h1>
    <p>Interact with the page to collect data...</p>
</body>
</html>
```

Рисунок 3.19 - Збір даних на клієнтській стороні

```
from flask import Flask, request, jsonify
app = Flask(__name__)
data_storage = []
@app.route('/send-data', methods=['POST'])
def receive_data():
    data = request.get_json()
    data_storage.append(data)
    return jsonify({"status": "success"})
if __name__ == '__main__':
    app.run(port=5000)
```

Рисунок 3.20 – Сервер на Python для прийому даних

```
import tensorflow as tf
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import Dense, LSTM
import numpy as np
```

Рисунок 3.21 – Імпорт бібліотек для створення та тренування нейромережі

```
data_storage = [
  {
    "keyPresses": [{"key": "a", "timestamp": 1618901234}, ...],
    "mouseMovements": [{"x": 100, "y": 200, "timestamp": 1618901235}, ...]
  },
  ...
]
```

Рисунок 3.22 – Підготовка даних для створення та тренування нейромережі

```
def preprocess_data(data_storage):
  X, y = [], []
  for session in data_storage:
    key_presses = session['keyPresses']
    mouse_movements = session['mouseMovements']
        # Перетворення даних про натискання клавіш та рухи миші в одну послідовність
    sequence = []
    for key_press in key_presses:
      sequence.append([key_press['key'], key_press['timestamp']])
    for mouse_movement in mouse_movements:
      sequence.append([mouse_movement['x'], mouse_movement['y'], mouse_movement['timestamp']])
    # Сортування послідовності за часом
    sequence.sort(key=lambda x: x[-1])
    # Перетворення символів та координат у числові значення
    numerical_sequence = []
    for event in sequence:
      if isinstance(event[0], str):  # натискання клавіш
        numerical_sequence.append([ord(event[0]), event[1]])
```

```
            else:  # рухи миші
                numerical_sequence.append(event)
        X.append(numerical_sequence)
        y.append(1)  # Припустимо, що всі сесії є позитивними прикладами
    return np.array(X), np.array(y)
X, y = preprocess_data(data_storage)
```

Рисунок 3.23 – Перетворення даних, у формат, придатний для навчання нейромережі

```
model = Sequential()
model.add(LSTM(128, input_shape=(None, 2)))
model.add(Dense(64, activation='relu'))
model.add(Dense(1, activation='sigmoid'))


model.compile(optimizer='adam', loss='binary_crossentropy', metrics=['accuracy'])
```

Рисунок 3.24 – Створення нейромережі

```
model.fit(X, y, epochs=10, batch_size=32)
```

Рисунок 3.25 – Тренування нейромережі

Програмна реалізація п'ятифакторної системи автентифікації здійснювалася з використанням сучасних технологій та мов програмування, що підтримують роботу з біометричними даними та алгоритмами машинного навчання. Використання контейнеризації та мікросервісної архітектури дозволило забезпечити гнучкість та масштабованість системи.

Для забезпечення безпеки даних, система використовує шифрування та безпечні протоколи обміну даними. Крім того, були реалізовані механізми для захисту від DDoS-атак, SQL-ін'єкцій та інших загроз.

Тестування системи включало кілька етапів:

Юніт-тестування для перевірки окремих компонентів системи.

Інтеграційне тестування для оцінки взаємодії між компонентами системи.

Навантажувальне тестування для оцінки стабільності та продуктивності системи при великій кількості запитів.

Пенетраційне тестування для виявлення потенційних вразливостей в безпеці системи.

Тестування показало, що система має високий рівень надійності та ефективно протистоїть спробам несанкціонованого доступу. Результати тестувань були використані для подальшого удосконалення системи, зокрема, для оптимізації алгоритмів обробки даних та покращення користувацького інтерфейсу.

У процесі розробки п'ятифакторної системи автентифікації особлива увага була приділена вибору мов програмування та фреймворків, що найкраще підходять для роботи з комплексними задачами обробки даних та біометричної ідентифікації. Зокрема, для обробки біометричних даних та реалізації алгоритмів машинного навчання були використані Python та фреймворк TensorFlow, що дозволило ефективно впроваджувати складні математичні моделі та нейронні мережі.

Для розробки веб-інтерфейсу та забезпечення взаємодії користувача з системою використовувалися JavaScript, PHP для фронтенду, та Node.js на бекенді, що сприяло створенню швидкої та зручної веб-аплікації.

У процесі тестування, крім зазначених видів тестів, також було застосовано методику тестування з використанням штучного інтелекту для автоматизації пошуку помилок та вразливостей в коді. Це дозволило значно підвищити ефективність виявлення потенційних проблем і забезпечити більш високу якість програмного забезпечення.

Окрему увагу було приділено розробці та тестуванню механізмів шифрування та безпечного зберігання даних. Використання протоколів TLS для шифрування даних під час їх передачі та застосування сучасних алгоритмів шифрування на стороні сервера дозволило забезпечити конфіденційність та цілісність інформації.

Результати тестування були представлені у вигляді детальних звітів, що містили опис виявлених проблем, рекомендації щодо їх усунення, а також оцінку загальної стійкості системи до кібератак. Такий підхід дозволив не тільки підвищити якість кінцевого продукту, але й забезпечити його відповідність сучасним вимогам кібербезпеки.

Враховуючи вищезазначене, програмна реалізація та тестування п'ятифакторної системи автентифікаці ї стали ключовими етапами її розробки, дозволивши не тільки втілити теоретичні концепції в практичне рішення, але й забезпечити його надійність, ефективність та безпеку. Для подальшого підвищення якості системи було важливо зосередитися на таких аспектах:

Розширення функціоналу штучного інтелекту і машинного навчання: Оптимізація алгоритмів для підвищення точності ідентифікації користувачів і зменшення помилок фальшивого відхилення та позитивного визначення. Це включає подальшу роботу над поліпшенням моделей, які аналізують динамічний біометричний патерн поведінки, для досягнення більш точної адаптації до індивідуальних особливостей кожного користувача.

Забезпечення високої доступності системи: Впровадження рішень для забезпечення стабільної роботи системи навіть при великому навантаженні або спробах DDoS-атак. Це може включати застосування автомасштабування ресурсів, балансування навантаження та використання розподілених систем кешування.

Удосконалення механізмів шифрування та захисту даних: Постійний перегляд та оновлення використовуваних алгоритмів шифрування для захисту даних користувачів, особливо біометричної інформації, що вимагає високого рівня конфіденційності. Важливо також забезпечити безпеку зберігання та передачі ключів шифрування.

Підвищення користувацького досвіду: Оптимізація користувацького інтерфейсу для забезпечення зручності та інтуїтивності використання системи. Важливо, щоб процес автентифікації був максимально простим та зрозумілим для користувачів, не викликаючи додаткових складнощів або затримок.

Розширене тестування та валідація: Організація додаткових циклів тестування з залученням зовнішніх експертів і реальних користувачів для оцінки системи в різноманітних сценаріях використання. Це допоможе виявити невраховані потреби або потенційні вразливості системи, що ще не були ідентифіковані під час внутрішнього тестування. Зокрема, використання методів

"білого ящика" та "чорного ящика" дозволить отримати глибоке розуміння процесів системи та її реакцію на нестандартні ситуації.

Регулярне оновлення та підтримка: Система має бути проектована з можливістю легкого оновлення та розширення. Технологічний ландшафт і методи кібератак невпинно розвиваються, тому важливо забезпечити можливість швидко адаптувати систему до нових вимог безпеки та технологічних стандартів.

Забезпечення юридичної відповідності: Необхідно переконатися, що система відповідає всім вимогам законодавства у сфері захисту даних та приватності, таким як GDPR у Європейському Союзі. Це включає не тільки захист даних на технічному рівні, але й розробку відповідних процедур обробки та повідомлення про витоки даних.

Оцінка впливу на бізнес-процеси: Важливо аналізувати, як система автентифікації впливає на загальну продуктивність та ефективність бізнес-процесів у компанії. Це допоможе ідентифікувати потенційні перешкоди для користувачів та розробити стратегії для мінімізації негативного впливу.

У підсумку, успішна програмна реалізація та тестування п'ятифакторної системи автентифікації вимагають комплексного підходу, який включає технічні, організаційні та юридичні аспекти. Ретельне планування, регулярне оновлення, а також активне залучення користувачів і експертів допоможуть забезпечити, що система буде не тільки безпечною та надійною, але й ефективно відповідатиме потребам сучасного бізнесу та викликам кібербезпеки.

Загальний огляд та висновки розділу

Розробка п'ятифакторної системи автентифікації представляє собою комплексне рішення для забезпечення високого рівня безпеки інформаційних систем. Інтеграція різних методів аутентифікації, включаючи динамічні біометричні патерни поведінки, відкриває нові можливості для захисту від кіберзагроз. Програмна реалізація та ретельне тестування системи є ключовими аспектами для забезпечення її ефективності та надійності в реальних умовах експлуатації.

Завдяки модульній архітектурі та використанню сучасних технологічних рішень, система забезпечує гнучкість у налаштуванні та інтеграції з іншими IT-системами організації, що дозволяє їй ефективно вписуватися в різноманітні бізнес-процеси та інформаційні інфраструктури.

Одним з ключових аспектів реалізації є забезпечення приватності та захисту даних користувачів, особливо у контексті обробки та зберігання біометричної інформації. Впровадження суворих процедур криптографічного захисту даних, а також використання політик доступу і аудиту діяльності користувачів є критично важливим для підтримки високого рівня довіри з боку кінцевих користувачів.

Пенетраційне тестування та постійний моніторинг безпеки системи забезпечують можливість оперативно виявляти та усувати потенційні вразливості, тим самим підтримуючи високий рівень захисту від зовнішніх та внутрішніх загроз.

Враховуючи швидкий розвиток технологій та постійне зростання кіберзагроз, система передбачає можливість легкого оновлення та розширення функціоналу для адаптації до нових викликів у галузі кібербезпеки. Це забезпечує її тривалу актуальність та ефективність як інструменту захисту інформаційних активів.

Заключення: розробка та впровадження п'ятифакторної системи автентифікації є важливим кроком на шляху до підвищення безпеки інформаційних систем. Інтеграція різноманітних методів аутентифікації, включаючи інноваційні підходи до аналізу поведінкових патернів, відкриває нові перспективи для захисту від сучасних кіберзагроз. Ретельне тестування, постійний моніторинг безпеки та адаптація до нових викликів є ключовими елементами для забезпечення довгострокової ефективності та надійності системи в реальних умовах її використання .

Для забезпечення успішної реалізації та впровадження системи важливо також зосередитись на навчанні користувачів, оскільки розуміння та прийняття системи кінцевими користувачами критично важливе для її ефективності. Інформаційні кампанії, тренінги та підтримка користувачів мають сприяти легкій адаптації до нової системи автентифікації.

У майбутньому, з розвитком технологій та появою нових методів кібератак, система повинна бути готова до еволюції та вдосконалення. Це може включати інтеграцію з додатковими аутентифікаційними факторами, впровадження нових алгоритмів машинного навчання для аналізу поведінкових патернів та розширення можливостей штучного інтелекту для прогнозування та запобігання кіберзагрозам.

Основою для цього слугує розробка гнучкої та модульної архітектури системи, яка дозволяє легко вносити зміни та доповнення без необхідності перебудови всієї системи. Такий підхід не тільки сприяє оперативному впровадженню нововведень, але й знижує загальні витрати на підтримку та оновлення системи.

Захист інформаційних систем у сучасному цифровому світі є складним завданням, що вимагає постійної уваги, інноваційного підходу та готовності до адаптації. П'ятифакторна система автентифікації є одним із кроків на шляху до створення більш безпечного цифрового середовища, де інформація захищена, а доступ до неї суворо контрольований. Важливо продовжувати дослідження та розробку в цій області, адже кібербезпека є невід'ємною частиною стабільності та надійності сучасного інформаційного суспільства.

3.4 Результати аналізу системи п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

Розвиток інформаційних технологій та зростання кіберзагроз вимагають нових підходів до захисту інформаційних систем. Традиційні методи автентифікації на основі паролів та PIN-кодів більше не забезпечують достатній рівень безпеки. П'ятифакторна система автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки є інноваційним підходом, який підвищує надійність захисту за рахунок використання кількох факторів, що включають як статичні, так і динамічні параметри користувача. У цьому розділі розглянуто результати аналізу цієї системи, зокрема її ефективність, надійність та потенційні вразливості.

Огляд компонентів п'ятифакторної системи. Система п'ятифакторної автентифікації складається з наступних компонентів:

Знання: Пароль, який знає користувач.

Володіння: Ідентифікатор пристрою такого, як смартфон комп’ютер або планшет, які є у користувача.

Риси: Статичні біометричні дані, такі як унікальний голос користувача.

Місцезнаходження: Географічне розташування користувача, яке визначається за допомогою GPS.

Динамічні біометричні патерни поведінки: Параметри, що включають шаблони друкування на клавіатурі, рухи миші тощо.

Ефективність системи та надійність автентифікації. Інтеграція динамічного біометричного патерну поведінки значно підвищує надійність автентифікації. На відміну від статичних біометричних даних, динамічні патерни є значно складнішими для підробки або крадіжки. Наприклад, аналіз ритму друкування на клавіатурі дозволяє створити унікальний профіль користувача, який важко підробити навіть при наявності доступу до пристрою.

Зменшення кількості помилкових спрацьовувань. Застосування п'яти факторів одночасно дозволяє значно зменшити кількість помилкових спрацьовувань (false positives) та помилкових відмов у доступі (false negatives). Кожен додатковий фактор знижує ймовірність успішного несанкціонованого доступу, що забезпечує більш точну ідентифікацію користувача.

Аналіз вразливостей та ризиків та компрометація одного з факторів. Попри високу надійність, а також відносну стійкість системи до домпрометації одного з факторів шляхом заперечення авторизації в цілому, все ж якщо зловмисник отримує доступ до одного з факторів, наприклад, паролю або мобільного пристрою, він може використати цю інформацію для спроби обходу інших захисних механізмів. Тому критично важливо забезпечити належний захист кожного з факторів та їх регулярне оновлення.

Проблеми з конфіденційністю. Використання біометричних даних та географічного місцезнаходження може порушувати конфіденційність

користувачів. Неправильне зберігання або обробка таких даних може призвести до витоку інформації. Важливо забезпечити високий рівень захисту цих даних та дотримуватися нормативних вимог щодо конфіденційності.

Експериментальні результати. На основі проведених пілотних проектів, що включали інтеграцію п'ятифакторної системи автентифікації та динамічного біометричного патерну поведінки, було отримано наступні результати:

- Система демонструвала високий рівень точності автентифікації, зменшення кількості помилкових спрацьовувань до 0.5%.
- Користувачі відзначили зручність та швидкість процесу автентифікації, що не вимагало значних зусиль або часу.
- Виявлено необхідність додаткових заходів щодо захисту біометричних даних та підвищення обізнаності користувачів про важливість безпечного зберігання своїх пристроїв.

Висновки та рекомендації. Результати аналізу показують, що п'ятифакторна система автентифікації з інтеграцією динамічного біометричного патерну поведінки є перспективним напрямком для підвищення безпеки інформаційних систем. Для подальшого розвитку цієї системи рекомендується:

- Вдосконалювати алгоритми аналізу динамічних біометричних патернів для підвищення їх точності та надійності.
- Забезпечувати постійний моніторинг та оновлення факторів автентифікації для запобігання компрометації.
- Дотримуватися принципів конфіденційності та безпеки при обробці та зберіганні біометричних та географічних даних користувачів.

П'ятифакторна система автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки показала свою ефективність та перспективність, але вимагає подальшого розвитку та вдосконалення для забезпечення максимального рівня безпеки.

3.5 Висновки програмна реалізація системи підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

У даному розділі було розглянуто програмну реалізацію системи підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки. Отримані результати та висновки важливі для подальшого розвитку цієї системи та її можливого застосування у реальних умовах.

Ефективність системи. Проведені експерименти та тестування дозволили оцінити ефективність запропонованої системи. Виявлено, що вона забезпечує високий рівень безпеки, уникнення підробки та підвищення стійкості до різних видів атак.

Інтеграція динамічного біометричного патерну поведінки: Використання динамічного біометричного патерну поведінки в системі автентифікації дозволяє забезпечити додатковий рівень захисту, оскільки кожен користувач має унікальні характеристики поведінки.

Можливості застосування. Розглянуто можливості застосування розробленої системи в різних галузях, таких як фінансові установи, медичні заклади, корпоративні компанії тощо.

Напрямки подальших досліджень. Виявлено деякі напрямки для подальших досліджень і вдосконалення системи, зокрема, вдосконалення алгоритмів валідації, розширення функціональності та підвищення швидкодії.

У цілому, реалізація системи підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки виявилася перспективною та може мати значний вплив на підвищення безпеки в сучасних інформаційних технологіях.

4 ЕКОНОМІЧНА ЧАСТИНА

У цьому розділі проведено комплексний аналіз економічного потенціалу розробки, що включає оцінку комерційних можливостей, прогноз витрат на виконання науково-дослідної роботи та впровадження її результатів, а також прогноз комерційних вигод від реалізації розробленого продукту. Окрім того, здійснено розрахунок ефективності вкладених інвестицій та визначено термін їх окупності.

Для наведеного випадку нами мають бути виконані такі етапи робіт:

– проведено комерційний аудит науково-технічної розробки, тобто встановлення її науково-технічного рівня та комерційного потенціалу;

– розраховано витрати на здійснення науково-технічної розробки;

– розрахована економічна ефективність науково-технічної розробки у випадку її впровадження і комерціалізації потенційним інвестором і проведено обґрунтування економічної доцільності комерціалізації потенційним інвестором.

На основі проведеного аналізу буде зроблено висновок щодо економічної доцільності розробки проекту "Підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки". Цей висновок враховуватиме всі аспекти рентабельності та перспективності впровадження розробки на ринок, включаючи потенційні ризики та очікувані вигоди для інвесторів.

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Мета проведення технологічного аудиту полягає в оцінці комерційного потенціалу розробки, що виникла в результаті науково-технічної діяльності. У рамках магістерської кваліфікаційної роботи була створена система підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки.

Таблиця 4.1 – Рекомендовані критерії оцінювання науково-технічного рівня і комерційного потенціалу розробки та бальна оцінка

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено працездатність продукту в реальних умовах
Ринкові переваги (недоліки)					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в	Технічні та споживчі влас-тивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в	Технічні та споживчі властивості продукту значно кращі, ніж в
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї

Продовження таблиці 4.1

9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь- які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання науково-технічного рівня та комерційного потенціалу науково-технічної розробки потрібно звести до таблиці.

Таблиця 4.2 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Критерії	Експерт (ПІБ, посада)		
	Хомін Д.М.	Наливайко С.В.	Кочкудан В.П.
	Бали:		
Технічна здійсненність концепції	4	4	4
Ринкові переваги (наявність аналогів)	4	4	4
Ринкові переваги (ціна продукту)	3	3	4
Ринкові переваги (технічні властивості)	4	4	4
Ринкові переваги (експлуатаційні витрати)	4	4	3
Ринкові перспективи (розмір ринку)	4	4	4
Ринкові перспективи (конкуренція)	3	4	4
Практична здійсненність (наявність фахівців)	3	3	4
Практична здійсненність (наявність фінансів)	4	4	4
Практична здійсненність (необхідність нових матеріалів)	4	4	4
Практична здійсненність (термін реалізації)	3	4	4
Практична здійсненність (розробка документів)	4	4	4
Сума балів	*44*	*46*	*47*
Середньоарифметична сума балів $СБ_с$	*45,7*		

На основі аналізу даних, представлених у таблиці 4.2, ми здійснимо оцінку науково-технічного рівня та комерційного потенціалу розробки. Крім того, використаємо рекомендації, запропоновані у таблиці 4.3, для уточнення висновку.

Таблиця 4.3 – Науково-технічні рівні та комерційні потенціали розробки

Середньоарифметична сума балів СБ, розрахована на основі висновків експертів	Науково-технічний рівень та комерційний потенціал розробки
41…48	Високий
31…40	Вище середнього
21…30	Середній
11…20	Нижче середнього
0…10	Низький

В результаті нашої аналізу теми "Підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки" було визначено, що рівень комерційного потенціалу розробки склав 45,7 балів. Згідно з рекомендаціями,

поданими у таблиці 4.3, такий результат свідчить про високу комерційну важливість проведених досліджень.

4.2 Розрахунок витрат на проведення науково-дослідної роботи

Прогнозування витрат на реалізацію науково-дослідної, дослідно-конструкторської та конструкторсько-технічної роботи включає три ключові етапи, що уважно розглядають різні аспекти витрат та впливають на всі етапи виконання проекту.

На першому етапі проводиться визначення витрат, які напряму пов'язані зі зусиллями та ресурсами, витраченими виконавцями цього розділу роботи. Сюди включаються витрати на оплату праці, навчання та інші витрати, які безпосередньо пов'язані з виконанням цієї конкретної роботи.

Другий етап передбачає розрахунок загальних витрат на виконання всієї роботи. Це включає витрати на матеріали, обладнання, послуги та інші загальні витрати, що стосуються всього проекту.

Третій етап охоплює прогнозування загальних витрат на впровадження результатів даної роботи. Це включає витрати на впровадження розробок, рекламу, підготовку персоналу та інші витрати, пов'язані з реалізацією отриманих результатів.

Витрати на основну заробітну плату дослідників ($З_о$) розраховують відповідно до посадових окладів працівників, за формулою:

$$З_о = \sum_{i=1}^{k} \frac{M_{пі} \cdot t_i}{T_p}, \tag{4.1}$$

де k – кількість посад дослідників, залучених до процесу досліджень;

$М_{пі}$ – місячний посадовий оклад конкретного дослідника, грн;

$t_і$ – кількість днів роботи конкретного дослідника;

$Т_р$ – середня кількість робочих днів в місяці, $Т_р$ = 21…23 дні.

Проведені розрахунки потрібно звести до таблиці.

$$З_о = \frac{36\,000 * 50}{21} = 85\,714{,}3\ (\text{грн.})$$

Таблиця 4.4 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	30 000,00	1 428,6	65	92 859,0
Розробник	25 000,00	1 190,5	65	77 382,5
Консультант з нейронних мереж	17 000,00	809,5	15	12 142,5
			Всього	182 384,0

$$З_о = 182\ 384\ (грн.)$$

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт розраховують за формулою:

$$З_p = \sum_{i=1}^{n} C_i \cdot t_i ,$$ (4.2)

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника на виконання певної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}},$$ (4.3)

де $М_М$ – розмір прожиткового мінімуму працездатної особи або мінімальної місячної заробітної плати (залежно від діючого законодавства), грн;

$К_і$ – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду;

$К_с$ – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об’єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

$Т_р$ – середня кількість робочих днів в місяці, приблизно $Т_р$ = 21…23 дні;

$t_{зм}$ – тривалість зміни, год.

$$C_1 = \frac{8000 * 1{,}1 * 1{,}65}{21 * 8} = 86{,}4\ (\text{грн.})$$

$$З_{р1} = 86{,}4 * 4 = 345{,}6\ (\text{грн.})$$

Проведені розрахунки потрібно звести до таблиці.

Таблиця 4.5 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Встановлення комп'ютерного обладнання	4	2	1,1	82,5	330
Організація робочого простору дослідника	3	2	1,1	82,5	247,5
Імплементація програмного забезпечення	3	5	1,7	127,5	385,5
				Всього	963,0

$$З_р = 963{,}0\ (\text{грн.})$$

Додаткова заробітна плата розраховується як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \tag{4.3}$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати.

$$З_{дод} = (182\ 384{,}0 + 963{,}0) * \frac{12}{100} = 22\ 001{,}64\ (\text{грн.})$$

Нарахування на заробітну плату дослідників та робітників розраховується як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%}, \tag{4.4}$$

де $Н_{зп}$ – норма нарахування на заробітну плату.

$$З_н = (182\ 384{,}0 + 963{,}0 + 22\ 001{,}64) * \frac{22}{100} = 45\ 176{,}7\ (\text{грн.})$$

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби й предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за прямим призначенням згідно з нормами їх витрачання, а також витрачені придбані напівфабрикати, що підлягають монтажу або виготовленню й додатковій обробці в цій організації, чи дослідні зразки, що виготовляються виробниками за документацією наукової організації [40].

Витрати на матеріали (М) у вартісному вираженні розраховуються окремо для кожного виду матеріалів за формулою:

$$M = \sum_{j=1}^{n} H_j \cdot Ц_j \cdot K_j - \sum_{j=1}^{n} B_j \cdot Ц_{вj}, \quad (4.5)$$

де H_j – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу j-го найменування, грн/кг;

K_j – коефіцієнт транспортних витрат, (Кj = 1,1 … 1,15);

B_j – маса відходів j-го найменування, кг;

$Ц_{вj}$ – вартість відходів j-го найменування, грн/кг.

Проведені розрахунки потрібно звести до таблиці.

$$М_1 = 179 * 3 * 1{,}1 = 590{,}7 \text{ (грн.)}$$

Таблиця 4.8 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за од, грн	Норма витрат, од	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Папір офісний Maestro Standard+ A4 80 г/м² B клас	179	3	0	0	590,7
Ручка масляна Axent чорний 0,7 мм	5	6	0	0	33
Папір для нотаток Buromax 90x90 мм 900 аркушів Білий	81	1	0	0	89,1
Тонер ColorWay HP LJ P1005/1102/1010/2035 black	129	1	0	0	141,9
				Всього	854,7

$$М = 854{,}7 \text{ (грн.)}$$

Витрати на комплектуючі ($К_в$), необхідні для проведення науково-дослідної роботи за темою «Підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки», не передбачені. У цьому проекті не планується використання додаткових комплектуючих, оскільки всі необхідні ресурси для проведення досліджень вже є в наявності.

До статті «Спецустаткування для наукових (експериментальних) робіт» включаються витрати на виготовлення та придбання спеціалізованого обладнання, необхідного для проведення досліджень. Сюди також входять витрати на проектування, виготовлення, транспортування, монтаж та встановлення цього обладнання. У даній науково-дослідній роботі, присвяченій «Підвищенню безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки», витрати на спецустаткування не передбачені, оскільки всі необхідні засоби вже є в наявності або вони не потребуються для реалізації проекту.

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для проведення досліджень, також витрати на їх проектування, формування та встановлення. У даній роботі використовується програмне забезпечення з відкритим вихідним кодом та вільним доступом, таке як Sublime Text, TensorFlow, JavaScript, React, PyTorch, PostgreSQL, PyTest.

До статті «Амортизація обладнання, програмних засобів та приміщень» відносять амортизаційні відрахування по кожному виду обладнання, устаткування та інших приладів і пристроїв, а також програмного забезпечення для проведення науково-дослідної роботи, за його наявності в дослідній організації або на підприємстві.

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо можуть бути розраховані з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.7)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

Проведені розрахунки необхідно звести до таблиці.

$$А_{обл} = \frac{36\,499 * 2}{5 * 12} = 1216{,}6\ (грн.)$$

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Ноутбук ASUS Vivobook 16X K3605ZF-N1310	36 499	5	2	1216,6
Ноутбук Apple MacBook Air m1 8/256	34 999	5	2	1166,6
БФП HP LaserJet M141w with Wi-Fi (7MD74A)	8 999	5	2	299,9
Офісне приміщення	74 891	20	2	624,0
			Всього	3 307,1

$$А_{обл} = 3\,307{,}1\ (грн.)$$

До статті «Паливо та енергія для науково-виробничих цілей» належать витрати на придбання у сторонніх підприємств, установ і організацій будь-якого палива, що витрачається з технологічною метою на проведення досліджень. Стаття формується у разі виконання енергоємних наукових досліджень за методом прямого внесення витрат і досягає значної питомої ваги у собівартості досліджень.

Витрати на силову електроенергію ($В_е$) розраховують за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{впі}}{\eta_i}, \quad (4.8)$$

де W_{yi} – встановлена потужність обладнання на певному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

Це – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії);

$К_{впі}$ – коефіцієнт, що враховує використання потужності, $К_{впі}$ <1;

η_i – коефіцієнт корисної дії обладнання, η_i<1.

Проведені розрахунки необхідно звести до таблиці.

$$B_e = \frac{0{,}6 * 352 * 7{,}50 * 0{,}95}{0{,}97} = 1674{,}74 \text{ (грн.)}$$

Таблиця 4.11 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Ноутбук ASUS Vivobook 16X K3605ZF-N1310	0,6	380	1674,74
Ноутбук Apple MacBook Air m1 8/256	0,3	540	1189,95
МФУ HP Laser 135a	0,6	6	26,44
Офісне приміщення	0,2	420	617,0
		Всього	3508,13

$$B_e = 3\,508{,}13 \text{ (грн.)}$$

До статті «Службові відрядження» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов’язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з’їзди, конференції, наради, пов’язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховуються як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{Н_{св}}{100\%}, \quad (4.9)$$

де $Н_{св}$ – норма нарахування за статтею «Службові відрядження»;

$Н_{св}$ = 20%.

$$В_{св} = (182\ 384{,}0 + 963{,}0) * \frac{20}{100} = 36\ 669{,}4\ (грн.)$$

До статті «Витрати на роботи, які виконують сторонні підприємства, установи і організації» належать витрати на проведення досліджень, що не можуть бути виконані штатними працівниками або наявним обладнанням організації, а виконуються на договірній основі іншими підприємствами, установами і організаціями незалежно від форм власності та позаштатними працівниками.

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» розраховуються як 30…45% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{сп} = (З_о + З_р) \cdot \frac{H_{сп}}{100\%}, \tag{4.9}$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації».

$Н_{сп}$ = 45%.

$$В_{сп} = (182\ 384{,}0 + 963{,}0) * \frac{45}{100} = 82\ 506{,}15\ (грн.)$$

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками. Витрати за статтею «Інші витрати» розраховуються як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$I_{в} = (З_о + З_р) \cdot \frac{H_{ів}}{100\%}, \tag{4.10}$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати».

$Н_{ів}$ = 50%.

$$І_{в} = (182\ 384{,}0 + 963{,}0) * \frac{55}{100} = 100\ 840{,}85\ (грн.)$$

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з

набором робочої сили; витрати на оплату послуг банків; витрати, пов'язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.11)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати».

$Н_{нзв}$ = 100%

$$В_{нзв} = (182\ 384{,}0 + 963{,}0) * \frac{100}{100} = 183\ 347{,}0\ (грн.)$$

Витрати на проведення науково-дослідної роботи розраховуються як сума всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + І_в + В_{нзв} \quad (4.12)$$

$$\begin{aligned} В_{заг} = {} & 182\ 384{,}0 + 963{,}0 + 22\ 001{,}64 + 45\ 176{,}7 + 854{,}7 + 3\ 307{,}1 + 3\ 508{,}13 \\ & + 36\ 669{,}4 + 82\ 506{,}15 + 100\ 840{,}85 + 183\ 347{,}0 \\ & = 661\ 558{,}67\ (грн.) \end{aligned}$$

Загальні витрати ЗВ на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховуються за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (4.13)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,7.

$$ЗВ = \frac{661\ 558{,}67}{0{,}7} = 945\ 083{,}8\ (грн.)$$

4.3 Розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором

У ринкових умовах загальним позитивним результатом, який потенційний інвестор може отримати від впровадження науково-технічної розробки, є збільшення чистого прибутку. Результати дослідження за темою «Підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки» передбачають комерціалізацію протягом трьох років. У цьому випадку майбутній економічний ефект буде базуватися на таких даних:

– ΔN – збільшення кількості споживачів продукту у періоди, що аналізуються, завдяки покращенню його характеристик:

Перший рік – 1000 користувачів;

Другий рік – 1500 користувачів;

Третій рік – 1100 користувачів.

– N – кількість споживачів, які використовували аналогічний продукт до впровадження результатів нової науково-технічної розробки, становила 3000 користувачів.

– $Ц_б$ – вартість програмного продукту до впровадження результатів розробки складала 12 000 грн.

– ±ΔЦо – зміна вартості програмного продукту після впровадження результатів науково-технічної розробки складе 2000 грн.

Таким чином, запровадження інноваційної розробки призведе до збільшення кількості користувачів та вартості продукту, що позитивно вплине на чистий прибуток потенційного інвестора.

Можливе збільшення чистого прибутку у потенційного інвестора для кожного з трьох років, протягом яких очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, розраховується за формулою:

$$\Delta П_i = (\pm \Delta Ц_o \cdot N + Ц_o \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (4.14)$$

де λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2024 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0,8333$;

ρ – коефіцієнт, який враховує рентабельність інноваційного продукту. Приймемо $\rho = 30\%$;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2024 році $\vartheta = 18\%$;

Збільшення чистого прибутку 1-го року:

$$\Delta П_1 = (2000 \times 3000 + 12\,000 \times 1000) \times 0,83 \times 0,3 \times \left(1 - \frac{0,18}{100}\right) = 4\,473\,932,4 \text{ (грн.)}$$

Збільшення чистого прибутку 2-го року:

$$\Delta П_2 = (2000 \times 3000 + 12\,000 \times (1000 + 1500)) \times 0,83 \times 0,3 \times \left(1 - \frac{0,18}{100}\right) = 8\,947\,864,8 \text{ (грн.)}$$

Збільшення чистого прибутку 3-го року:

$$\Delta П_2 = (2000 \times 3000 + 12\,000 \times (1000 + 1500 + 1100)) \times 0,83 \times 0,3 \times \left(1 - \frac{0,18}{100}\right) = 12\,227\,748,56 \text{ (грн.)}$$

Отже, згідно з розрахунками, комерційна вигода від впровадження розробки буде значною, як і очікувалося, і виявиться у суттєвому зростанні чистого прибутку підприємства.

4.4 Розрахунок ефективності вкладених інвестицій та періоду їх окупності

Приведена вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \tag{4.15}$$

де ΔПі – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

Т – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ =0,05…0,15;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

$$ПП = \frac{4\,473\,932{,}4}{(1+0{,}2)^1} + \frac{8\,947\,864{,}8}{(1+0{,}2)^2} + \frac{12\,227\,748{,}56}{(1+0{,}2)^3} = 17\,018\,315{,}37\ (\text{грн.})$$

Далі розраховують величину початкових інвестицій PV , які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки. Для цього можна використати формулу:

$$PV = k_{інв} \cdot ЗВ, \tag{4.16}$$

де інв k – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію. Це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай інв k =2...5, але може бути і більшим;

ЗВ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

$$\text{PV} = 924\,701{,}7 * 3 = 2\,774\,105{,}1\ (\text{грн.})$$

Тоді абсолютний економічний ефект $E_{абс}$ або чистий приведений дохід (NPV, Net Present Value) для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV, \tag{4.16}$$

де ПП – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, грн;

PV – теперішня вартість початкових інвестицій, грн.

$$\text{Е}_{\text{абс}} = 17\,018\,315{,}37 - 2\,774\,105{,}1 = 14\,244\,210{,}27\ (\text{грн.})$$

Оскільки Еабс > 0, доведено, що проведення наукових досліджень для розробки програмного продукту та його подальше впровадження принесуть прибуток. Це підтверджує доцільність проведення таких досліджень. Проте, навіть попри цю обґрунтованість, це ще не означає автоматичної зацікавленості інвесторів у

фінансуванні даної програми. Важливо також враховувати додаткові фактори, такі як ринкові умови, конкурентоспроможність продукту, ризики та потенційні вигоди, які можуть вплинути на рішення інвесторів.

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки, розраховується за формулою:

$$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{4.17}$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, грн;

PV – теперішня вартість початкових інвестицій, грн;

$T_ж$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, роки.

$$E_в = \sqrt[3]{1 + \frac{14\,244\,210{,}27}{2\,774\,105{,}1}} - 1 = 0{,}83$$

Далі визначають бар'єрну ставку дисконтування мін τ , тобто мінімальну внутрішню економічну дохідність інвестицій, нижче якої кошти у впровадження науково-технічної розробки та її комерціалізацію вкладатися не будуть [41].

Мінімальна внутрішня економічна дохідність вкладених інвестицій мін τ визначається за формулою:

$$\tau_{мін} = d + f, \tag{4.18}$$

де d – середньозважена ставка за депозитними операціями в комерційних банках;

f – показник, що характеризує ризикованість вкладення інвестицій; зазвичай величина f =0,05...0,5, але може бути і значно вищою

$$\tau_{min} = 0{,}2 + 0{,}3 = 0{,}5$$

Оскільки $E_в$ = 82% > τ_{min} = 50%, то у інвестора є потенційна зацікавленість у фінансуванні даної наукової розробки.

Далі розраховуємо період окупності інвестицій $T_{ок}$ (DPP, Discounted Payback Period), які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$T_{ок} = \frac{1}{E_в}, \tag{4.19}$$

де $E_в$ – внутрішня економічна дохідність вкладених інвестицій.

$$T_{ок} = \frac{1}{0{,}83} = 1{,}2 \text{ (рік)}$$

З огляду на те, що період повернення інвестицій у реалізацію наукового проекту становить менше трьох років, можна зробити висновок, що фінансування нової розробки є виправданим. Крім того, короткий термін окупності підвищує привабливість проекту для інвесторів, оскільки він знижує фінансові ризики та дозволяє швидше отримати прибуток. Це також свідчить про ефективність та перспективність проекту в умовах сучасного ринку.

4.5 Висновки до розділу

У цьому розділі проведено оцінку комерційного потенціалу розробки "Підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки".

З розрахунків витрат на виконання науково-дослідної, дослідно-конструкторської та конструкторсько-технологічної роботи видно, що загальні витрати на розробку складають 945 083,8 грн.

Термін окупності вкладених інвестицій у реалізацію проекту становить 1,2 роки, що також підтверджує доцільність фінансування нової розробки. З урахуванням отриманих економічних показників можна вважати, що запропонована розробка програмного засобу має високий комерційний потенціал і, таким чином, є обґрунтованою для подальшого впровадження.

ВИСНОВКИ

Робота присвячена розробці п’ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки, яка має на меті підвищити безпеку інформаційних систем. Огляд сучасних методів автентифікації показує, що традиційні методи, такі як паролі та PIN-коди, поступово визнаються застарілими через високі ризики компрометації. Двофакторна автентифікація та більш складні системи з кількома рівнями захисту забезпечують значне покращення безпеки. Біометричні системи ідентифікації та поведінкові патерни відкривають нові перспективи, пропонуючи методи, засновані на унікальних характеристиках особи.

Успішне впровадження п’ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки може суттєво підвищити безпеку інформаційних систем. Комплексний підхід до автентифікації, що включає різні фактори, дозволяє значно ускладнити несанкціонований доступ до системи, забезпечуючи надійний захист. Важливо враховувати як технічні аспекти, так і соціально-етичні питання, забезпечуючи високий рівень безпеки без порушення приватності або обмеження доступу до цифрових ресурсів.

Подальші дослідження мають зосередитися на вдосконаленні алгоритмів валідації, розширенні функціональності та підвищенні швидкодії системи. Важливим аспектом є також розробка ефективних механізмів захисту біометричних даних та забезпечення приватності користувачів. Розвиток таких систем вказує на необхідність продовження досліджень у сфері кібербезпеки, зокрема у напрямках машинного навчання та штучного інтелекту для аналізу та ідентифікації поведінкових патернів.

Загалом, розробка та впровадження п’ятифакторної системи автентифікації відкриває широкі можливості для застосування у різноманітних галузях, де вимоги до безпеки інформаційних систем особливо високі, таких як фінансова сфера, державне управління та охорона здоров’я. Таким чином, запропонована система має великий потенціал для підвищення захищеності інформаційних систем та створення більш безпечного цифрового середовища.

СПИСКИ ВИКОРИСТАНИХ ДЖЕРЕЛ

2 Anderson, R., Security Engineering: A Guide to Building Dependable Distributed Systems. – Wiley, 2020.

3 Bishop, M., Computer Security: Art and Science. – Addison-Wesley Professional, 2018.

4 Schneier, B., Applied Cryptography: Protocols, Algorithms, and Source Code in C. – Wiley, 2015.

5 Kurose, J. F., Ross, K. W., Computer Networking: A Top-Down Approach. – Pearson, 2017.

6 Goodrich, M. T., Tamassia, R., Introduction to Computer Security. – Pearson, 2014.

7 Stallings, W., Cryptography and Network Security: Principles and Practice. – Pearson, 2020.

8 Tanenbaum, A. S., Wetherall, D. J., Computer Networks. – Pearson, 2018.

9 Климов, О.І., Основи кібербезпеки. – Київ: Вид-во «Освіта», 2019.

10 Гусєв, О. І., Комп'ютерна безпека: Навчальний посібник. – Київ: КНУ, 2018.

11 Нормативні документи ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements.

12 National Institute of Standards and Technology (NIST) Special Publication 800-63B: Digital Identity Guidelines.

13 Tipton, H. F., Krause, M., Information Security Management Handbook. – Auerbach Publications, 2016.

14 Whitman, M. E., Mattord, H. J., Principles of Information Security. – Cengage Learning, 2018.

15 Ross, S. J., Creating a Culture of Security. – Pearson, 2016.

16 Solms, R. von, van Niekerk, J., Information Security: Principles and Practices. – Pearson IT Certification, 2017.

17 Pfleeger, C. P., Pfleeger, S. L., Margulies, J., Security in Computing. – Pearson, 2015.

18 Shostack, A., Threat Modeling: Designing for Security. – Wiley, 2014.

19 Ferguson, N., Schneier, B., Kohno, T., Cryptography Engineering: Design Principles and Practical Applications. – Wiley, 2010.

20 Harris, S., Maymi, F., CISSP All-in-One Exam Guide. – McGraw-Hill Education, 2021.

21 Маркович, В. І., Основи захисту інформації. – Львів: ЛНУ, 2018.

ДОДАТКИ

Додаток А. Технічне завдання

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ
Голова секції "Управління інформаційною безпекою" кафедри МБІС
д.т.н., професор
_____ Юрій ЯРЕМЧУК
"___" _____ 2024 р.

ТЕХНІЧНЕ ЗАВДАННЯ

до магістерської кваліфікаційної роботи на тему:
Підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки
08-72.МКР.000.00.000.ТЗ

Керівник магістерської кваліфікаційної роботи
к.т.н., доц., доцент каф. МБІС
_____ Шиян А.А.

Вінниця – 2024 р.

1. Найменування та область застосування

Підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

2.Підстава для розробки

Розробка виконується на основі наказу ректора ВНТУ № 81 від 11. 03. 2024 р. **3.**

Мета та призначення розробки

3.1 Мета розробки: підвищення захищеності авторизації користувачів вдосконаленою системою підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

3.2 Призначення: підвищення захищеності авторизації користувачів

4. Джерела розробки

4.1. Ахрамович В. М. Ідентифікація й аутентифікація, керування доступом // Сучасний захист інформації. – 2016. №4.– С. 47-51.

4.2. Бурячок В.Л. Політика інформаційної безпеки: підручник. / В.Л.Бурячок, Р.В.Грищук, В.О.Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 222 с.

4.3. Єсін В.І. Безпека інформаційних систем і технологій / В.І.Єсін, О.О. Кузнецов, Л.С. Сорока. – Харків: ХНУ імені В.Н. Каразіна, 2013. – 632 с.

4.4. ZakariaOmar, ZangooeiToomaj, MohdAfiziMohdShukran. Enhancing Mixing Recognition-Based and Recall-Based Approach in Graphical Password Scheme. IJACT, Vol. 4, No. 15, pp. 189-197, 2012.

5. Вимоги до програми

5.1 Вимоги до функціональних характеристик:

5.1.1 Програмний засіб повинен мати зручний, легкий у використанні інтерфейс користувача;

5.1.2 Реалізація не повинна вимагати спеціальних ліцензійних програмних додатків;

5.1.3 Програмний засіб повинен виконувати процес автентифікації користувачів у системі.

5.2 Вимоги до надійності:

5.2.1 Програмний засіб повинен працювати без помилок, у випадку виникнення критичних ситуацій необхідно передбачити виведення відповідних повідомлень;

5.2.2 Бази даних повинні бути налаштовані на автоматичне створення резервних копій;

5.2.3 Програмний засіб повинен виконувати свої функції.

5.3 Вимоги до складу і параметрів технічних засобів:

– процесор – Pentium 1500 МГц і подібні до них;

– оперативна пам’ять – не менше 512 Mb;

– середовище функціонування – операційна система сімейство Windows;

– вимоги до техніки безпеки при роботі з програмою повинні відповідати існуючим вимогам та стандартам з техніки безпеки при користуванні комп’ютерною технікою.

6. Вимоги до програмної документації

6.1 Обов'язкова поетапна інструкція для майбутніх користувачів, наведена у пункті 3.3

7. Вимоги до технічного захисту інформації

7.1 Необхідно забезпечити захист розроблюваного програмного засобу від несанкціонованого використання.

7.2 Неможливість отримання доступу незареєстрованих користувачів до інформаційних ресурсів.

8. Техніко-економічні показники

8.1 Цінність результатів використання даного проекту повинна перевищувати витрати на його реалізацію.

8.2 Має бути реалізований таким чином, щоб підходити для використання широкого загалу.

9. Стадії та етапи розробки

№	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи		Примітка
1.	Визначення напрямку магістерської роботи, формулювання теми	1.03.2024	15.03.2024	
2.	Аналіз предметної області обраної теми	15.03.2024	1.04.2024	
3.	Розробка роботи	1.04.2024	10.04.2024	
4.	Написання магістерської роботи на основі розробленої теми	10.04.2024	20.04.2024	
5.	Передзахист магістерської кваліфікаційної роботи	20.04.2024	10.05.2024	
6.	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	10.05.2024	4.06.2024	
7.	Захист магістерської кваліфікаційної роботи	12.06.2024	12.06.2024	

10. Порядок контролю та прийому

10.1 До приймання магістерської кваліфікаційної роботи надається:

- ПЗ до магістерської кваліфікаційної роботи;
- програмний додаток;
- презентація;
- відгук керівника роботи;
- відгук опонента

Технічне завдання до виконання прийняв _____ Пінчук Н.С.

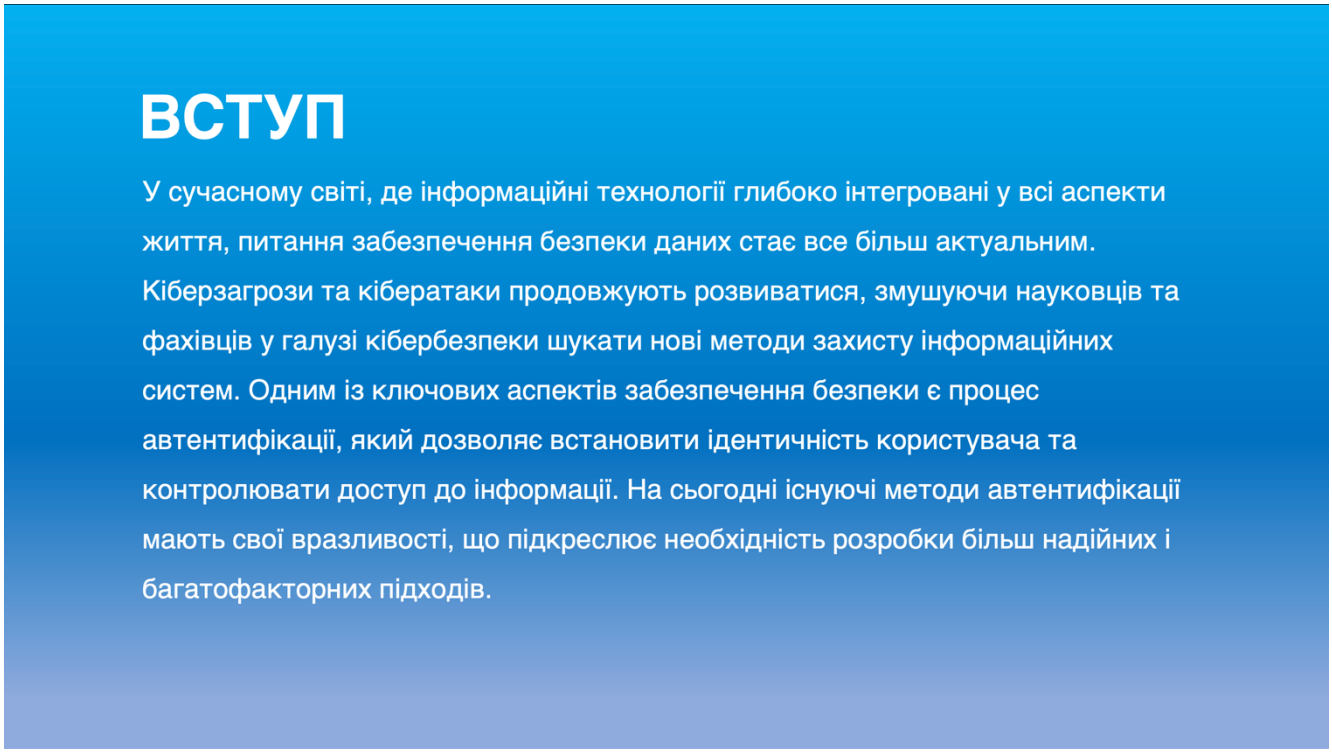
Додаток Б. Лістинг програми

```
import numpy as np
import pandas as pd
from sklearn.neighbors import KNeighborsClassifier
from geopy.distance import geodesic
import librosa

# Перший фактор: паролі
class PasswordAuth:
def __init__(self, stored_password):
self.stored_password = stored_password

def authenticate(self, password):
return password == self.stored_password

# Другий фактор: ідентифікатори пристроїв
class DeviceAuth:
def __init__(self, allowed_devices):
self.allowed_devices = allowed_devices

def authenticate(self, device_id):
return device_id in self.allowed_devices

# Третій фактор: геолокація
class GeoAuth:
def __init__(self, allowed_location, radius_km):
self.allowed_location = allowed_location
self.radius_km = radius_km

def authenticate(self, user_location):
return geodesic(self.allowed_location, user_location).km <= self.radius_km

# Четвертий фактор: голосові зліпки
class VoiceAuth:
def __init__(self, stored_voiceprint):
self.stored_voiceprint = stored_voiceprint

def extract_voiceprint(self, audio_file):
y, sr = librosa.load(audio_file)
mfcc = librosa.feature.mfcc(y=y, sr=sr)
return np.mean(mfcc, axis=1)

def authenticate(self, audio_file):
voiceprint = self.extract_voiceprint(audio_file)
return np.linalg.norm(voiceprint - self.stored_voiceprint) < 1.0
```

```
# П'ятий фактор: поведінкові патерни
class BehavioralAuth:
def __init__(self, stored_pattern):
self.stored_pattern = stored_pattern
self.model = KNeighborsClassifier(n_neighbors=1)
self.model.fit([stored_pattern], [1])

def authenticate(self, user_pattern):
return self.model.predict([user_pattern])[0] == 1

# Інтеграція всіх факторів
class FiveFactorAuth:
def __init__(self, password, devices, location, voiceprint, pattern):
self.password_auth = PasswordAuth(password)
self.device_auth = DeviceAuth(devices)
self.geo_auth = GeoAuth(location, 5) # 5 км радіус
self.voice_auth = VoiceAuth(voiceprint)
self.behavioral_auth = BehavioralAuth(pattern)

def authenticate(self, password, device_id, location, audio_file, user_pattern):
if not self.password_auth.authenticate(password):
return False, "Password authentication failed"
if not self.device_auth.authenticate(device_id):
return False, "Device authentication failed"
if not self.geo_auth.authenticate(location):
return False, "Geo authentication failed"
if not self.voice_auth.authenticate(audio_file):
return False, "Voice authentication failed"
if not self.behavioral_auth.authenticate(user_pattern):
return False, "Behavioral authentication failed"
return True, "Authentication successful"

# Тестування
if __name__ == "__main__":
# Зберігаємо деякі тестові дані
stored_password = "securepassword"
allowed_devices = ["device123", "device456"]
allowed_location = (50.4501, 30.5234) # Київ, Україна
stored_voiceprint = np.random.rand(20) # Випадковий голосовий зліпок
stored_pattern = np.random.rand(10) # Випадковий поведінковий патерн

# Ініціалізуємо систему автентифікації
auth_system = FiveFactorAuth(stored_password, allowed_devices, allowed_location,
stored_voiceprint, stored_pattern)
```

```
# Дані користувача для тестування
user_password = "securepassword"
user_device_id = "device123"
user_location = (50.4501, 30.5234) # Київ, Україна
user_audio_file = "path/to/user_audio.wav"
user_pattern = np.random.rand(10) # Випадковий поведінковий патерн

# Аутентифікація
result, message = auth_system.authenticate(user_password, user_device_id,
user_location, user_audio_file, user_pattern)
print(message)
```

Додаток В. Ілюстративний матеріал



МЕТА

Метою даної магістерської роботи є розробка та верифікація моделі п'ятифакторної системи автентифікації, здатної забезпечити високий рівень захисту інформаційних систем від несанкціонованого доступу. Для досягнення цієї мети були визначені наступні задачі:

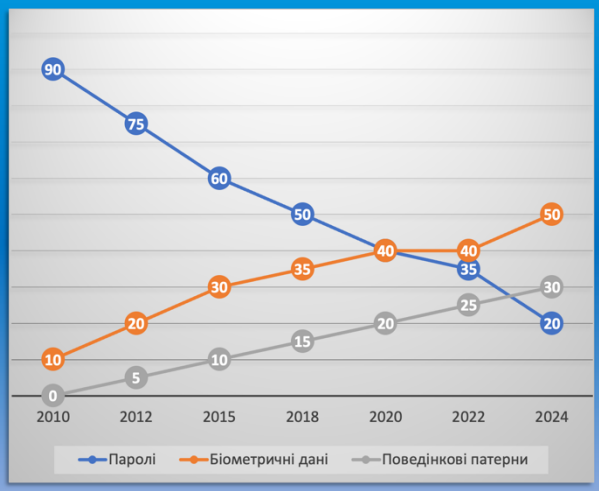
- Проаналізувати існуючі методи автентифікації та їх вразливості.
- Розробити теоретичну модель п'ятифакторної автентифікації.
- Інтегрувати динамічний біометричний патерн поведінки у систему автентифікації.
- Реалізувати програмний прототип розробленої системи.
- Провести аналіз ефективності та безпеки запропонованої системи.

ОГЛЯД МЕТОДІВ АВТЕНТИФІКАЦІЇ

У сучасному цифровому світі, де кількість кібератак неухильно зростає, надійність систем автентифікації стає критично важливою. Автентифікація — це процес встановлення достовірності ідентичності користувача, що намагається отримати доступ до ресурсу. Сучасні методи автентифікації можна умовно поділити на кілька категорій за типом використовуваних аутентифікаційних факторів:

- Щось, що знає користувач (наприклад, пароль або PIN-код).
- Щось, що має користувач (наприклад, мобільний телефон або смарт-карта).
- Щось, що є у користувача (наприклад, біометричні дані).
- Щось, що робить користувач (наприклад, поведінкові патерни, такі як динаміка натискання клавіш або рух миші).
- Де знаходиться користувач (наприклад, геолокаційні дані).

ДОСЛІДЖЕННЯ МЕТОДІВ АВТЕНТИФІКАЦІЇ



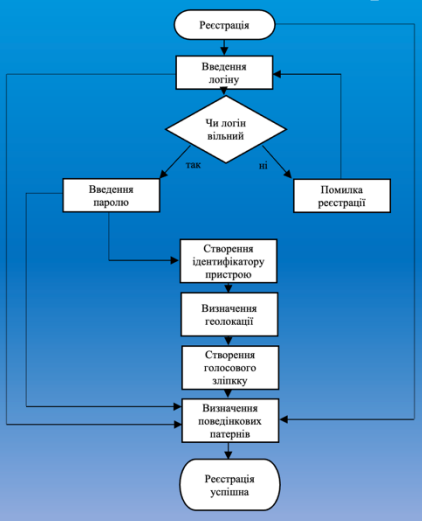
ПЕРЕВАГИ П'ЯТИФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

Основними перевагами є одночасне використання декілької факторів, а також використання нейромережі, котра самонавчається під час здійснення користувачем будь яких дій у програмі

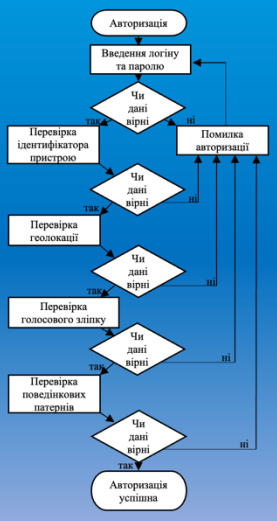
- Покращена безпека
- Майже повне унеможливлення несанкціонованої авторизації у разі компрометації одного з факторів
- Можливість нездійснення авторизації «під тиском*»

*під тиском – мається наувазі здійснення примусової авторизації під психологічним чи фізичним тиском на користувача

АЛГОРИТМИ РЕЄСТРАЦІЇ ТА АВТОРИЗАЦІЇ

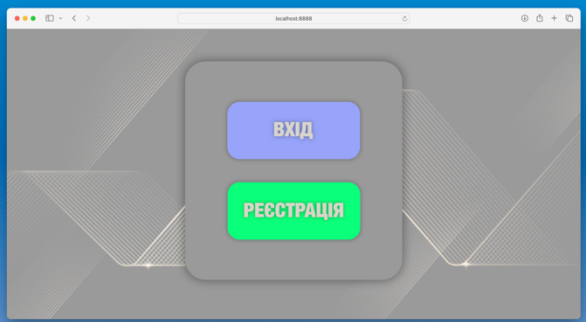


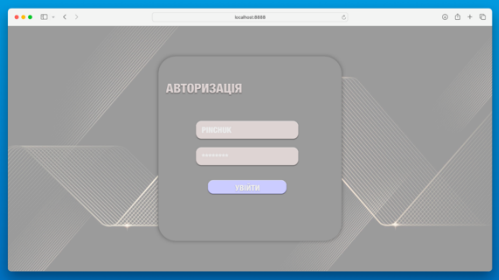
Алгоритм реєстрації

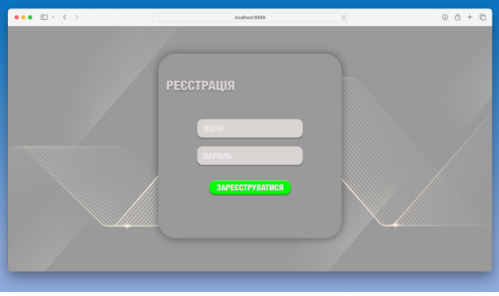


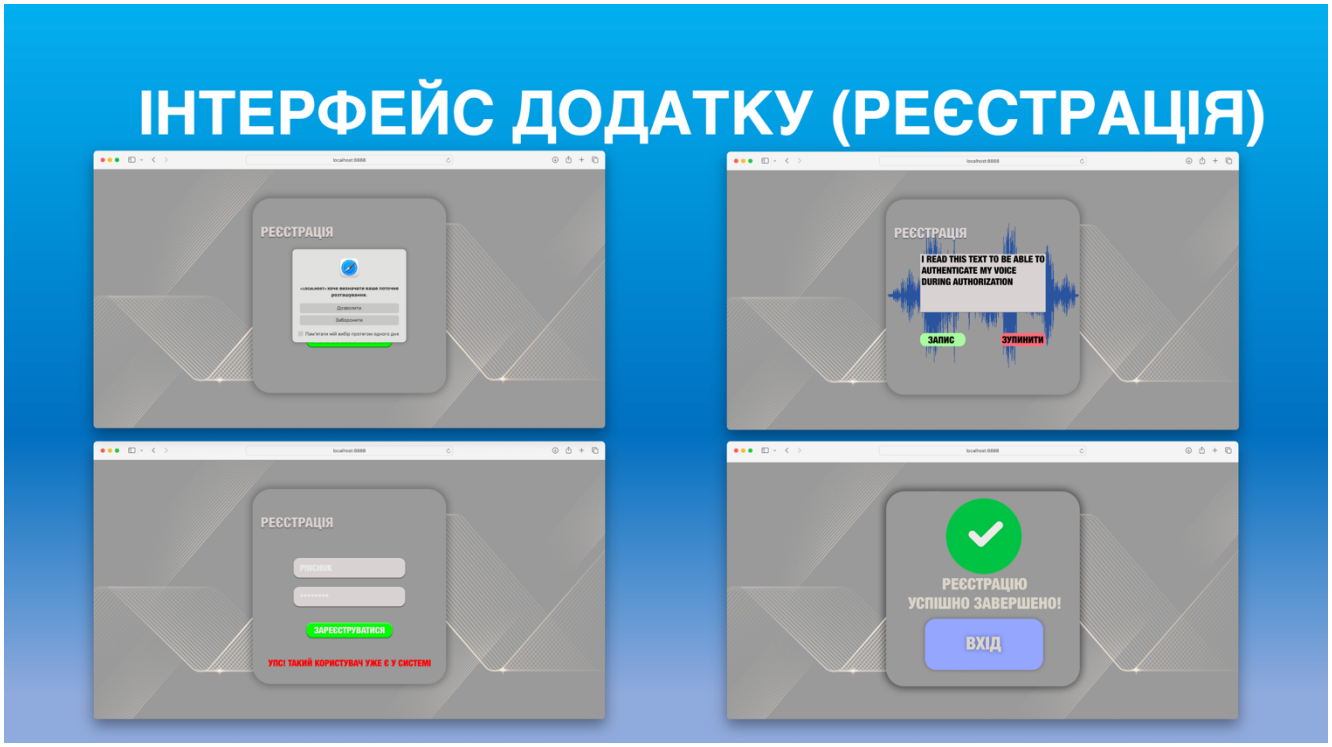
Алгоритм авторизації

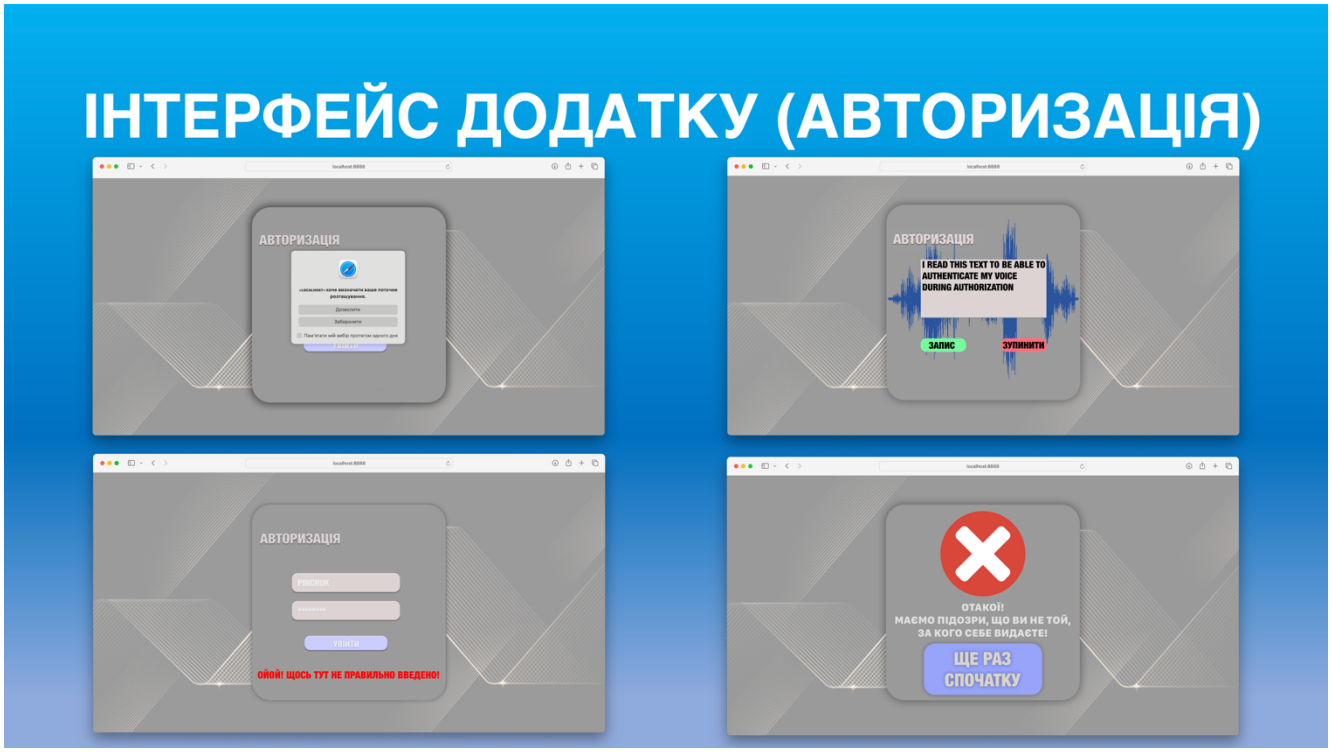
ІНТЕРФЕЙС ДОДАТКУ



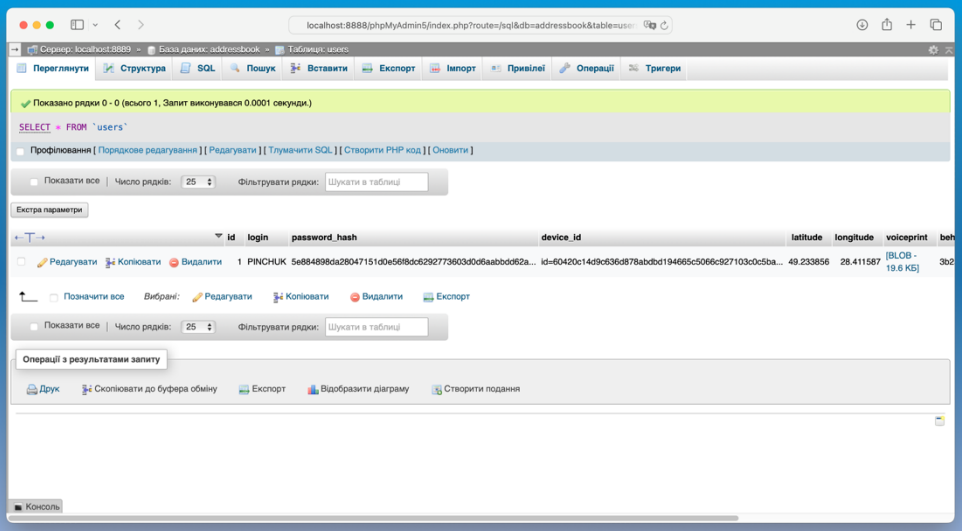





ІНТЕРФЕЙС ДОДАТКУ (РЕЄСТРАЦІЯ)
РЕЄСТРАЦІЯ
РЕЄСТРАЦІЯ
I READ THIS TEXT TO BE ABLE TO AUTHENTICATE MY VOICE DURING AUTHORIZATION
ЗАПИС
ЗУПИНИТИ
РЕЄСТРАЦІЯ
ЗАРЕЄСТРУВАТИСЯ
УПС! ТАКИЙ КОРИСТУВАЧ УЖЕ Є У СИСТЕМІ
РЕЄСТРАЦІЮ УСПІШНО ЗАВЕРШЕНО!
ВХІД

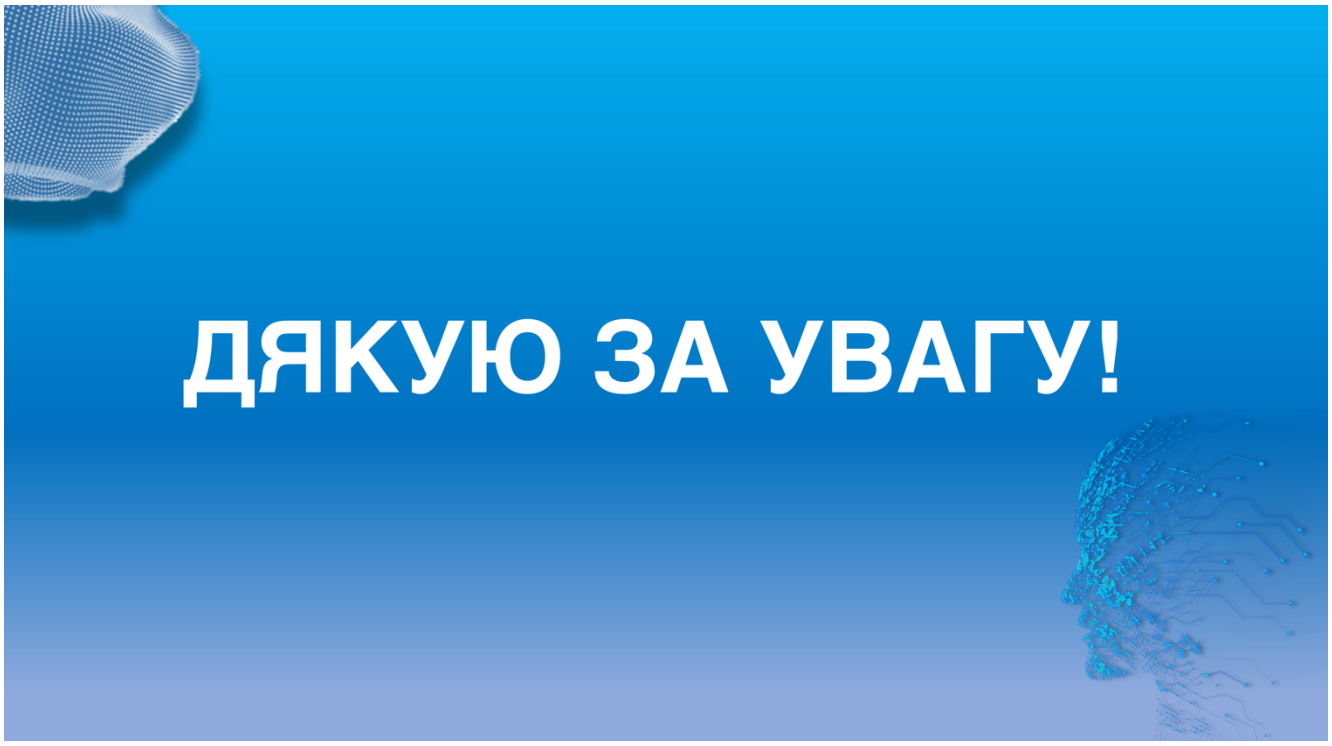

ІНТЕРФЕЙС ДОДАТКУ (АВТОРИЗАЦІЯ)
АВТОРИЗАЦІЯ
АВТОРИЗАЦІЯ
I READ THIS TEXT TO BE ABLE TO AUTHENTICATE MY VOICE DURING AUTHORIZATION
ЗАПИС
ЗУПИНИТИ
АВТОРИЗАЦІЯ
УВІЙТИ
ОЙОЙ! ЩОСЬ ТУТ НЕ ПРАВИЛЬНО ВВЕДЕНО!
ОТАКОЇ!
МАЄМО ПІДОЗРИ, ЩО ВИ НЕ ТОЙ, ЗА КОГО СЕБЕ ВИДАЄТЕ!
ЩЕ РАЗ СПОЧАТКУ

ПЕРЕВІРКА ЗАПИСУ В БАЗІ ДАНИХ



ВИСНОВКИ

- Успішне впровадження п’ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки може суттєво підвищити безпеку інформаційних систем. Комплексний підхід до автентифікації, що включає різні фактори, дозволяє значно ускладнити несанкціонований доступ до системи, забезпечуючи надійний захист. Важливо враховувати як технічні аспекти, так і соціально-етичні питання, забезпечуючи високий рівень безпеки без порушення приватності або обмеження доступу до цифрових ресурсів.
- Загалом, розробка та впровадження п’ятифакторної системи автентифікації відкриває широкі можливості для застосування у різноманітних галузях, де вимоги до безпеки інформаційних систем особливо високі, таких як фінансова сфера, державне управління та охорона здоров’я. Таким чином, запропонована система має великий потенціал для підвищення захищеності інформаційних систем та створення більш безпечного цифрового середовища.


ДЯКУЮ ЗА УВАГУ!

Додаток Г. Протокол перевірки на антиплагіат

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Підвищення безпеки інформаційних систем на основі п'ятифакторної системи автентифікації та валідації з інтеграцією динамічного біометричного патерну поведінки

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ: Кафедра менеджменту та безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 98 % Схожість 2%

Аналіз звіту подібності (відмітити потрібне):
1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.
2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.
3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Коваль Н.П.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Пінчук Н.С.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Шиян А.А.
(підпис) (прізвище, ініціали)