Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

БАКАЛАВРСЬКА ДИПЛОМНА РОБОТА НА ТЕМУ:

«Засіб багатофакторної автентифікації користувачів»

Виконав: студент 4 курсу групи 1БС-19б
спеціальності 125 Кібербезпека
_____ Качай Р.В.
Керівник: к. т. н., доцент каф. ЗІ
_____ Дудатьєв А.В.
«19» червня 2023 р.
Рецензент: к. т. н. доц. каф. ПЗ
_____ Хошаба О.М.
«19» червня 2023 р.

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____ Лужецький В. А.
«19» червня 2023 р.

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти І (бакалаврський)
Галузь знань – 12 Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітньо–професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ

Зав. кафедри ЗІ, д. т. н., проф.

_____В. А. Лужецький

20 березня 2023 року

ЗАВДАННЯ

НА БАКАЛАВРСЬКУ ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Качай Роман Володимирович

1. Тема роботи: «Засіб багатофакторної автентифікеації корирстувачів» керівник роботи: Дудатьєв Андрій Веніамінович, к.т.н., доц. каф. ЗІ.

Затверджені наказом ректора ВНТУ від 20 березня 2023р. №67

2. Строк подання студентом роботи 19 червня 2023 р.

3. Вхідні дані до роботи:

Користувацькі паролі

Ідентифікатори користувачів

Фактор знання

Алгоритми для здійснення порівняння біометричних даних та розрахунку співпадінь

4. Перелік ілюстративного матеріалу: Архітектура системи біометричної автентифікації, структурна парольної автентифікації, концептуальна схема узагальненої біометричної системи, алгоритм роботи програмного засобу

Інтерфейс програмного засобу

5. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Дудатьєв А.В., к. т. н., доц. каф. ЗІ	20.03.23	16.06.23
2	Дудатьєв А.В., к. т. н., доц. каф. ЗІ	20.03.23	16.06.23
3	Дудатьєв А.В., к. т. н., доц. каф. ЗІ	20.03.23	16.06.23

6. Дата видачі завдання 20 березня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів Бакалаврської дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	20.03.23 – 26.03.23	
2	Аналіз літературних джерел за напрямком бакалаврської дипломної Роботи	27.03.23 – 09.04.23	
3	Розробка рішень	10.04.23 – 23.04.23	
4	Модельвання автентифікації	24.04.23 – 24.05.23	
5	Аналіз виконання ТЗ, висновки	25.05.23 – 31.05.23	
6	Оформлення пояснювальної записки	01.06.23 – 15.06.23	
7	Попередній захист та доопрацювання БДР	16.06.23 – 19.06.23	
8	Представлення БДР до захисту	20.06.23 – 23.06.23	
9	Захист БДР	20.06.23 – 23.06.23	

Студент _____ Роман КАЧАЙ

Керівник роботи _____ Андрій ДУДАТЬЄВ

АНОТАЦІЯ

Дипломна робота складається зі вступу, двох розділів, загальних висновків до кожного розділу, списку використаних джерел, додатків і 10 рисунків, 1 таблиці. Список використаних джерел містить 8 найменувань. Загальний обсяг роботи 72 сторінки.

Метою дипломної роботи є розробка система багатофакторної автентифікації та розмежування доступу до інформаційної системи.В роботі також був проведений аналіз та порівняння існуючих методів автентифікації, систем багатофакторної автентифікації та розмежування доступу.

Також було продемонстровано веб-додаток з багатофакторною автентифікацією. Завдяки роботі було коротко поясненно як відбувається автентифікація в інформаційних системах. Було показано вихідні коди всіх алгоритмів щоб користувач міг використовувати будь-яку частину коду так само, як і будь-який компонент програмного забезпечення.

ABSTRACT

The thesis consists of an introduction, two chapters, general conclusions to each chapter, a list of used sources, appendices and 10 figures, one tables. The list of used sources contains 8 items. The total volume of work is 72 pages.

The aim of the thesis is to develop a system of multifactor authentication and demarcation of access to the information system.The paper also analyzed and compared existing authentication methods, multifactor authentication systems and access demarcation.

A web application with multi-factor authentication was also demonstrated. Thanks to the work, it was briefly explained how authentication occurs in information systems. The source codes of all algorithms were shown so that the user could use any part of the code in the same way as any software component.

ЗМІСТ

ВСТУП

У сучасному цифровому світі, де інформація є великою цінністю, забезпечення безпеки особистих даних та конфіденційності стає все більш актуальним завданням. Одним із важливих аспектів забезпечення безпеки є автентифікація користувачів, тобто процес перевірки ідентифікаційних даних, що підтверджують правомірний доступ до системи або послуги.

У цій бакалаврській роботі ми дослідимо різні аспекти багатофакторної автентифікації користувачів. Ми розглянемо різні типи факторів, які можна використовувати в процесі автентифікації, такі як паролі, фізичні пристрої, біометричні дані та інші. Також будуть розглянуті сучасні методи та алгоритми, що застосовуються для забезпечення безпеки в багатофакторній автентифікації.

Метою цієї роботи є дослідження, аналіз та оцінка ефективності багатофакторних систем автентифікації з метою визначення їх переваг, недоліків та можливостей впровадження. Результати цього дослідження допоможуть розширити наше розуміння процесу автентифікації користувачів та сприятимуть вдосконаленню систем безпеки у цифровому середовищі.

Структура роботи наступна: у першому розділі будуть розглянуті основні концепції та принципи багатофакторної автентифікації, у другому розділі - аналіз існуючих методів та алгоритмів, у третьому розділі - опис проведених експериментів та результатів, а у заключному розділі - висновки та рекомендації щодо використання багатофакторної автентифікації у різних сферах.

В результаті цієї роботи ми сподіваємося зрозуміти переваги та обмеження багатофакторної автентифікації, а також надати практичні рекомендації щодо використання цього засобу в реальних ситуаціях. Наша робота внесе вагомий внесок у поліпшення безпеки та захисту інформації в цифровому світі.

1 Аналітичний огляд багатофакторної автентифікації

1.1 Огляд існуючих методів автентифікації

У сфері інформаційних технологій використовуються різні методи автентифікації.

- Однобічна аутентифікація передбачає, що клієнт системи самостійно підтверджує свою ідентичність для доступу до інформації.
- У двобічній аутентифікації, крім клієнта, сама система також перевіряє свою автентичність, наприклад, банк може запитувати додаткові дані для підтвердження ідентичності.
- Трибічна аутентифікація використовує нотаріальну службу аутентифікації, щоб переконатися в достовірності кожного партнера в обміні інформацією.

Методи автентифікації можна також умовно поділити на однофакторні і двофакторні. Однофакторні методи включають логічні (паролі, ключові фрази, які вводяться з клавіатури) і ідентифікаційні (фізичні об'єкти, такі як карти, дискети, магнітні картки, штрих-кодові карти і т.д.). Цей принцип ідентифікації ґрунтується на використанні певного предмета або ключа, що перебуває в ексклюзивному володінні користувача, наприклад, електронні ключі.

У сучасному світі широко поширені різні типи пристроїв для автентифікації, зокрема різноманітні карти. Карти можуть бути безконтактними, що дає зручність використання в комп'ютерних системах та системах доступу до приміщень.

Апаратна ідентифікація надає різні методи та засоби для захисту доступу до ресурсів і ідентифікації користувачів. Смарт-карти, такі як банківські картки, є одним з найнадійніших способів ідентифікації. Вони мають захищену пам'ять і можуть використовуватися для доступу до різних

систем. Існують також дешевші альтернативи, такі як магнітні карти або картки зі штрих-кодом, але вони менш стійкі до злому.

Токени - це ще один тип ключів, які можна використовувати для апаратної ідентифікації. Вони підключаються безпосередньо до порту комп'ютера, такого як USB або LPT, і мають власну захищену пам'ять. Токени забезпечують високий рівень надійності, оскільки ключі зберігаються в захищеній пам'яті, які хакерам важко підібрати. Крім того, вони мають різні захисні механізми і можуть виконувати додаткові функції завдяки вбудованому мікропроцесору.

Однак, апаратна ідентифікація також має свої недоліки. Один з них - висока ціна. Вартість електронних ключів і програмного забезпечення для роботи з ними може бути значною. Крім того, для впровадження системи майнової ідентифікації потрібні вкладення, оскільки кожного користувача треба забезпечити персональними токенами. Крім того, деякі типи ключів можуть зношуватися або бути загублені користувачами з часом.

Біометрія може використовувати такі параметри, як відбитки пальців, райдужна оболонка ока, голос, обличчя або геометрія долоні.

За допомогою біометричних методів, ідентифікація може бути здійснена швидко та з високим рівнем точності. Біометричні дані скануються або зчитуються з користувача, перетворюються на цифровий формат та порівнюються з збереженими в базі даних даними для підтвердження особи. Цей процес дозволяє встановити впевненість у тому, що особа, яка намагається отримати доступ, є правомірним користувачем.

Однак, використання біометрії також має свої виклики. Перш за все, для використання біометричних методів ідентифікації потрібне належне обладнання, таке як сканер відбитків пальців або камера високої роздільної здатності. Крім того, зберігання і обробка біометричних даних потребує великої уваги до приватності і безпеки, оскільки ці дані є особистими і чутливими. Для успішної реалізації біометричних систем також потрібні

відповідні процедури адміністрування та управління, щоб забезпечити їх ефективну роботу.

Отже, якщо мова йде про апаратну ідентифікацію, вибір методу залежить від конкретних потреб і вимог системи безпеки. Комбінація різних методів, таких як пароль і біометрія, може забезпечити більший рівень безпеки та надійності.

Звичайні методи апаратної ідентифікації, які можуть використовуватись разом з біометрією, включають:

1. Паролі: Пароль є одним з найпоширеніших методів ідентифікації. Він базується на знанні конфіденційної інформації, такої як слово або фраза, яку вводить користувач для підтвердження своєї особи. Використання паролів разом з біометричними методами може забезпечити подвійний рівень захисту.
2. Карти доступу: Карти доступу, які можуть бути зчитуваними за допомогою картрідера або близькості, є ще одним методом апаратної ідентифікації. Карти можуть містити інформацію, яка ідентифікує користувача, наприклад, унікальний номер або код.
3. Ключі аутентифікації: Ключі аутентифікації є фізичними пристроями, які містять криптографічні ключі для ідентифікації користувача. Це можуть бути USB-ключі, смарт-карти або інші пристрої, які забезпечують безпеку та аутентифікацію.
4. Токени безпеки: Токени безпеки - це електронні пристрої, які генерують одноразові паролі або коди для аутентифікації користувача. Ці токени можуть бути фізичними пристроями або мобільними додатками, які забезпечують додатковий рівень безпеки.

Комбінування різних методів апаратної ідентифікації дозволяє створити мультифакторну аутентифікацію, що забезпечує більший рівень безпеки. Наприклад, в системі може використовуватись біометрія (наприклад, сканування відбитка пальця або розпізнавання обличчя) разом з паролем або карткою доступу. Комбінування декількох методів знижує

ймовірність несанкціонованого доступу і покращує загальний рівень безпеки системи.

Звичайні методи апаратної ідентифікації можуть бути комбіновані з різними видами біометричних технологій. Деякі з них включають:

1. Відбиток пальця: Це один з найбільш поширених біометричних методів ідентифікації. Система сканує унікальні характеристики відбитка пальця, такі як довжина і форма ліній та валиків, і порівнює їх зі збереженими шаблонами, щоб підтвердити особу.
2. Розпізнавання обличчя: Цей метод використовує аналіз особливих рис обличчя, таких як форма очей, ніса, губ та розташування їх елементів. Алгоритми порівнюють ці риси з збереженими шаблонами для ідентифікації особи.
3. Розпізнавання ірису: Ірис ока також має унікальні характеристики, такі як узори, прожилки та колір. Технологія розпізнавання ірису зчитує ці характеристики за допомогою спеціальної камери і порівнює їх з шаблонами для ідентифікації особи.
4. Розпізнавання голосу: Цей метод базується на унікальних фізичних характеристиках голосу, таких як тембр, інтонація та акцент. Аналізуючи ці характеристики, система може ідентифікувати особу за їх голосом.
5. Розпізнавання DNA: Цей метод використовує унікальні генетичні характеристики особи, отримані зі зразків ДНК. Він зазвичай використовується у високоуровневих системах безпеки або у криміналістичних дослідженнях для точної ідентифікації особи.

Ці біометричні методи можуть бути використані окремо або комбіновані для підвищення рівня безпеки ідентифікації в системах контролю доступу, банківських системах, мобільних пристроях та інших сферах. Важливо враховувати, що збереження біометричних даних вимагає особливої уваги до приватності та захисту, оскільки ці дані є особистими і унікальними для кожної особи. [1]

1.2 Переваги та недоліки багатофакторної автентифікації

Багатофакторна автентифікація — це розширена перевірка належності акаунта користувачеві, що включає більше одного фактора. Під факторами мають на увазі:

- фактор знання — інформація, відома суб'єкту — ПІН-код, пароль, контрольне слово, відповідь на секретне запитання;
- фактор володіння — річ, що належить користувачеві — телефон, телефон, планшет, ПК, токен безпеки, смарт-картка;
- фактор властивості — біологічні характеристики суб'єкта – відбиток пальця або долоні, райдужка ока, голос, обличчя.

Часто багатофакторну автентифікацію (MFA) використовують у значенні двофакторної (2FA), що не буде помилкою.

Переваги багатофакторної автентифікації зводяться до кібербезпеки, це:

- додатковий захист від несанкціонованого доступу до конфіденційної чи корпоративної інформації;
- безпечне проведення банківських операцій;
- впевненість у збереженні даних на серверах.

До недоліків MFA складність використання непідготовленими користувачами. Багато хто просто не розуміє, навіщо використовувати багатофакторну автентифікацію (до цього питання ми ще повернемося трохи нижче). Тому, на жаль, на цей час поширеність цього методу безпеки становить 10%.

Принцип роботи багатофакторної автентифікації полягає в тому, що при авторизації користувача в операційній системі або в будь-якому обліковому записі, служба запитує підтвердження особи за допомогою додаткових факторів, які має користувач.

Приклади багатофакторної автентифікації:

- підтвердження особи за допомогою одноразового пароля (OTP), який може бути відправлений службою користувачеві декількома способами: через SMS, пошту, програму або токен;
- дії на додатковому пристрої: натискання кнопки підтвердження, введення шифру, промовляння фрази, підключення USB-ключа, сканування відбитка пальця.

Різні майданчики підтримують різноманітні типи багатофакторної аутентифікації. Зазвичай, авторизувавшись в обліковому записі, їх можна вибрати та налаштувати у вкладці «Безпека».[2]

Багатофакторна автентифікація, яка також називається 2-факторна автентифікація, пропонує користувачеві багато переваг. Ось деякі з найважливіших переваг двофакторної автентифікації:

- Підвищена безпека: Двофакторна автентифікація надає додатковий рівень безпеки, оскільки зловмиснику буде складніше отримати доступ до облікового запису без наявності другого фактора, який необхідно підтвердити. Навіть якщо зловмиснику вдасться зламати пароль, він все ще потребуватиме другого фактора для отримання доступу.
- Захист від фішингу: Багатофакторна автентифікація допомагає запобігти атакам фішингу, оскільки навіть якщо користувачі випадково введуть свої дані на підробленому сайті або відповідатимуть на шахрайський електронний лист, зловмиснику все одно буде потрібен другий фактор, який він не зможе отримати.
- Зручність: Двофакторна автентифікація може бути зручнішою, ніж просте введення пароля. Замість запам'ятовування складних паролів, користувач може використовувати фізичні пристрої (такі як смартфони або ключові картки) або біометричні дані (такі як відбитки пальців або сканування обличчя) для швидкого та безпечного входу.
- Гнучкість: Багатофакторна автентифікація може бути налаштована залежно від потреб користувача. Вона може включати різні фактори, такі як пароль, SMS-підтвердження, одноразові коди, біометричні дані або

апаратні токени. Користувачі можуть вибрати метод, який найбільше відповідає їхнім вподобанням та вимогам безпеки.

- Сумісність з різними пристроями: Багатофакторна автентифікація може бути використана на різних пристроях, включаючи комп'ютери, смартфони, планшети та інші мобільні пристрої. Це робить її універсальним і зручним методом для забезпечення безпеки на різних платформах.

Загалом, багатофакторна автентифікація є ефективним інструментом для підвищення безпеки в Інтернеті та захисту від несанкціонованого доступу до особистої інформації та облікових записів.

1.3 Моделі багатофакторної автентифікації

Моделі багатофакторної автентифікації включають різні підходи та протоколи, що дозволяють використовувати кілька факторів для підтвердження ідентичності користувача. Ось кілька популярних моделей багатофакторної автентифікації:

Модель на основі знань: В цій моделі користувачі надають інформацію, що є унікальною для них, наприклад, пароль або пін-код. Цей фактор, відомий тільки користувачу, є їх основним засобом ідентифікації.

Модель на основі володіння: Ця модель використовує фізичний об'єкт, який володіє користувач, наприклад, смартфон або токен. Цей фактор підтверджує ідентичність через фізичне володіння або доступ до пристрою.

Модель на основі біометрії: У цій моделі використовуються біометричні характеристики, такі як відбиток пальця, розпізнавання обличчя або сканування радужки ока. Ці унікальні фізичні характеристики використовуються для ідентифікації користувача.

Модель на основі місцезнаходження: В цій моделі використовується географічне місцезнаходження користувача. Ідентифікація здійснюється на

основі даних про місцезнаходження, наприклад, за допомогою GPS або IP-адреси.

Модель на основі місцезнаходження використовує інформацію про географічне положення користувача для автентифікації та ідентифікації. Вона базується на уявленні, що місцезнаходження може слугувати унікальним ідентифікатором або додатковим фактором для підтвердження особи.

Модель на основі часу: Ця модель використовує часові параметри для ідентифікації користувача. Наприклад, використання одноразових паролів, які діють лише протягом обмеженого періоду.

Модель на основі часу використовує інформацію про час для автентифікації, ідентифікації та контролю доступу користувачів. Час може слугувати важливим фактором для підтвердження особи або встановлення часових обмежень для доступу до систем та ресурсів.

Математична модель багатофакторної автентифікації може бути представлена у вигляді системи математичних рівнянь, алгоритмів та протоколів, які використовуються для ідентифікації та аутентифікації користувачів. Вона базується на математичних концепціях, таких як криптографія, теорія імовірностей та статистика.

Математична модель багатофакторної автентифікації може включати наступні елементи:

Функції хешування: Вони використовуються для перетворення вхідних даних (наприклад, пароля) в хеш-значення. Це дозволяє зберігати та порівнювати хеші замість самого пароля.

Криптографічні протоколи: Ці протоколи використовуються для обміну даними та забезпечення безпеки комунікації між користувачем і автентифікаційним сервером. Наприклад, SSL/TLS протоколи забезпечують шифрування та аутентифікацію даних.

Математичні моделі ризику: Ці моделі використовуються для оцінки ризику аутентифікації на основі різних факторів, таких як пароль,

біометричні дані, місцезнаходження тощо. Вони можуть враховувати ймовірності вторгнень або спроб шахрайства.

Моделі машинного навчання: В деяких випадках моделі машинного навчання можуть бути використані для виявлення аномальних або підозрілих поведінкових зразків, що можуть свідчити про несанкціонований доступ.

Ці елементи допомагають створити математичну модель, яка визначає правила та процедури для перевірки та підтвердження ідентичності користувачів.Головна перевага парольної аутентифікації – простота й звичність. Паролі давно вбудовані в операційні системи й інші сервіси. При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте, по сукупності характеристик їх варто визнати найслабшим засобом перевірки дійсності.Щоб пароль був запам'ятовуваним, його найчастіше роблять простим (ім'я подруги, назва спортивної команди й т.п.). Однак простий пароль неважко вгадати, особливо якщо знати пристрасті даного користувача. Іноді паролі із самого початку не зберігаються в таємниці, тому що мають стандартні значення, зазначені в документації, і далеко не завжди після установки системи виробляється їхня зміна.

Уведення пароля можна підглянути. Іноді для підглядання використовуються навіть оптичні прилади.Паролі нерідко повідомляють колегам, щоб ті могли, наприклад, підмінити на якийсь час власника пароля. Теоретично в подібних випадках більш правильно залучити засоби керувань доступом, але на практиці так ніхто не робить: а таємниця, яку знають двоє, це вже не таємниця.

Пароль можна вгадати "методом грубої сили", використовуючи, скажемо, словник. Якщо файл паролів зашифрований, але доступний для читання, його можна скачати до себе на комп'ютер і спробувати підібрати пароль, запрограмувавши повний перебір (передбачається, що алгоритм шифрування відомий).

Проте, важливі заходи дозволяють значно підвищити надійність парольного захисту:

- накладення технічних обмежень (пароль повинен бути не занадто коротким, він повинен містити букви, цифри, знаки пунктуації й т.п.);
- керування терміном дії паролів: їхня періодична зміна;
- обмеження доступу до файлу паролів;
- обмеження числа невдалих спроб входу в систему, це утруднить застосування "методу грубої сили"):
- навчання користувачів;
- використання програмних генераторів паролів (така програма, грунтуючись на нескладних правилах, може породжувати тільки благозвучні й, отже, запам'ятовувані паролі).

Перераховані заходи доцільно застосовувати завжди, навіть якщо поряд з паролями використовуються інші методи аутентифікації. Розглянуті вище паролі можна назвати багаторазовими: їхнє розкриття дозволяє зловмисникові діяти від імені легального користувача.[4]

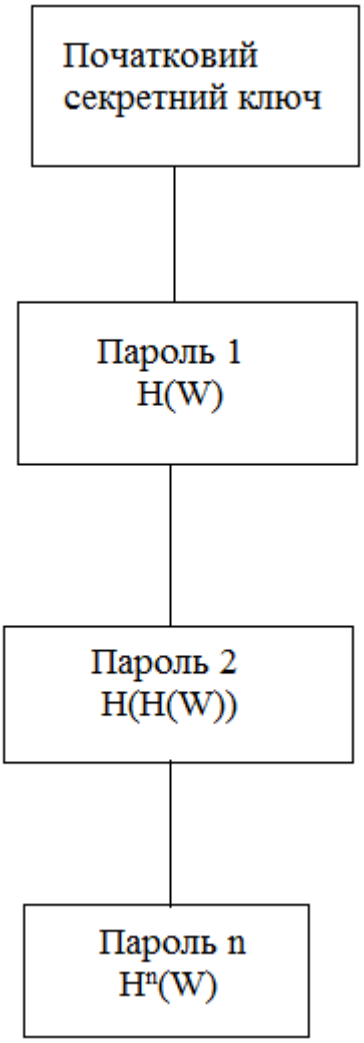


Рисунок 1.1 – Структура парольної автентифікації

«Hey Google» або «Hey Siri» — це прості команди, які можна використовувати для взаємодії з голосовим помічником телефона. Саме вони і представляють системи розпізнавання голосу, які реагують лише на конкретні голосові команди.Під час налаштування телефона потрібно лише вимовити кілька речень вголос, щоб дозволити алгоритму вивчати ваші голосові особливості. Чим більше ви розмовляєте з віртуальним помічником, таким як Google, Siri або Alexa, тим краще він розпізнає ваш голос.[5] В біометричних стандартах термін «біометрична ідентифікація» визначається як процес порівняння поданих біометричних даних з усіма шаблонами в базі даних (схема «один до декількох») з метою визначення відповідності та, якщо відповідність визначено, ідентифікації відповідної особи.

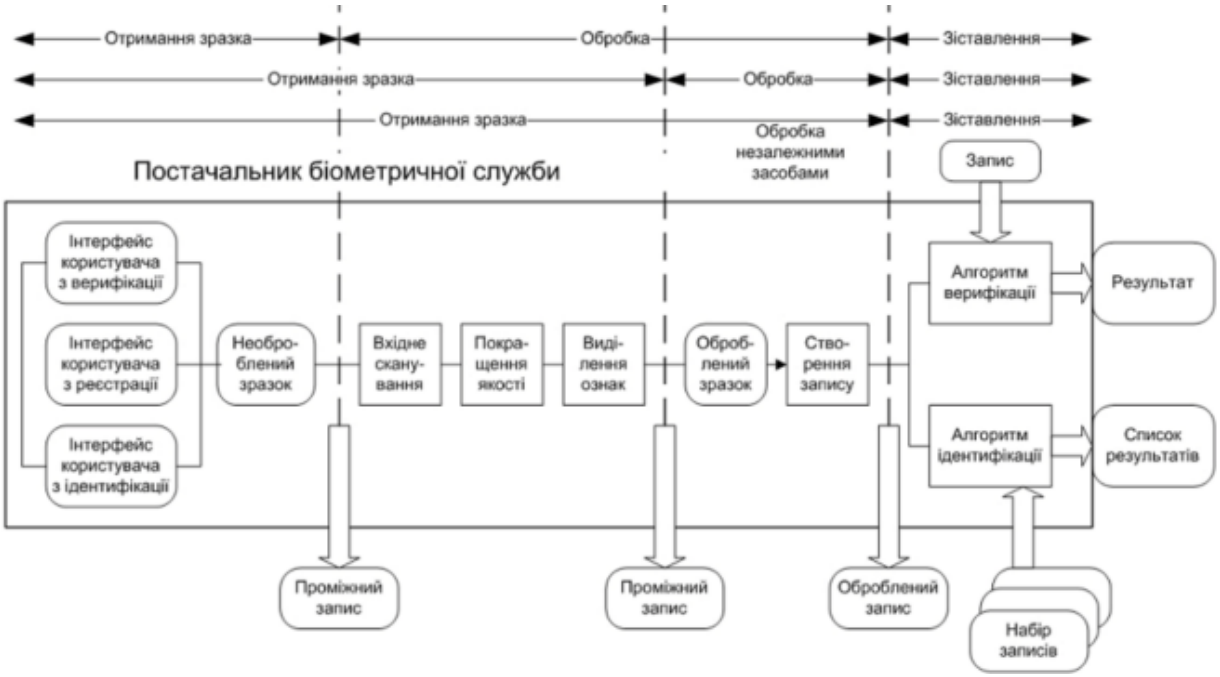


Рисунок 1.2 – Архітектурна реалізація базової моделі біометричної системи

Інформаційні потоки в узагальненій біометричній системі та її структурні компоненти подані на рисунку 1.3.

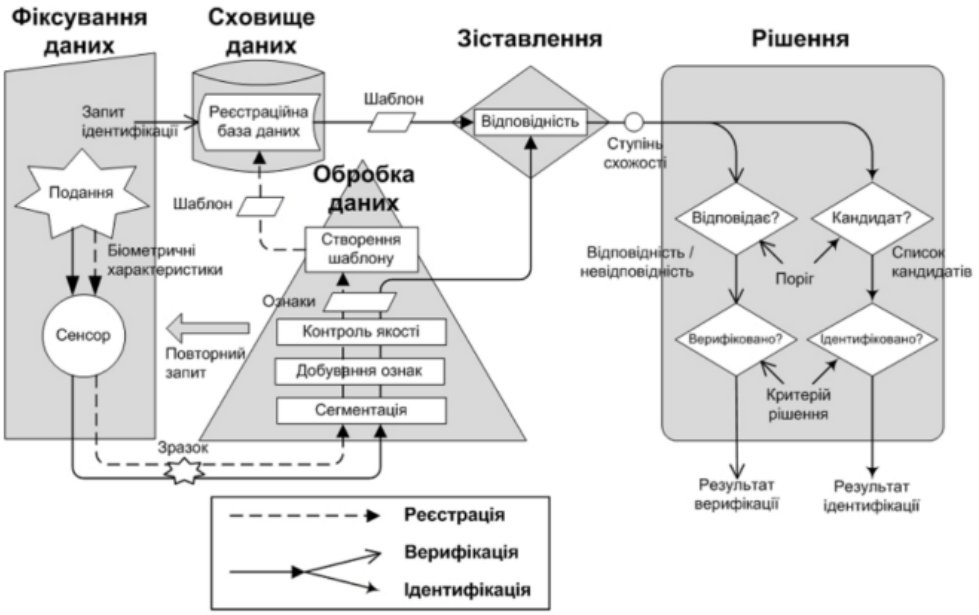


Рисунок 1.3 – Концептуальна схема узагальненої біометричної системи [6]

Таблиця 1.1 – Порівняльна таблиця методів багатофакторної автентифікації

Метод	Опис	Переваги	Недоліки
Пароль	Використання секретного коду або фрази	- Легко запам'ятати та використовувати - Низька вартість - Широко підтримується в багатьох системах	- Можливість вгадування або підбору паролю - Ризик витоку пароля - Вразливість до соціальної інженерії
Біометрія	Використання унікальних фізіологічних чи поведінкових характеристик користувача	- Висока точність - Важко підробити або підмінити - Висока специфічність	- Залежність від обладнання та інфраструктури - Можливість помилок та відхилень - Проблеми з приватністю
Фізичні токени	Використання фізичних пристроїв (токенів)	- Висока безпека - Можливість використання у віддалених сценаріях - Зручність використання	- Ризик втрати або крадіжки токену - Вартість розгортання та підтримки - Можливість фізичного пошкодження

1.4 Висновки до розділу

Однофакторна автентифікація, яка базується на одному факторі, зазвичай на знанні пароля, є найпоширенішим методом. Вона проста у використанні, але має деякі недоліки, такі як ризик компрометації паролів та залежність від сили паролів.

Багатофакторна автентифікація (MFA) є більш безпечним рішенням, оскільки вона використовує комбінацію двох або більше факторів (знання, володіння, власність) для перевірки ідентичності користувача. Вона підвищує безпеку, ускладнює несанкціонований доступ та зменшує ризик соціально-інженерних атак.

Фактори автентифікації можуть бути комбіновані для отримання більшого рівня безпеки. Це може включати пароль (знання), одноразовий код на мобільний телефон (володіння) або біометричні дані (власність). Багатофакторна автентифікація надає гнучкість та зручність користувачам.

Застосування багатофакторної автентифікації є особливо важливим для захисту цінних даних, облікових записів та систем, особливо в умовах зростаючих кіберзагроз.

Організації повинні уважно розглядати переваги та недоліки різних методів автентифікації, а також контекст і особливості своєї системи, для вибору найбільш підходящого підходу. Безпека повинна бути постійним пріоритетом, і використання багатофакторної автентифікації може значно підвищити рівень захисту систем та даних.

2 МОДЕЛІ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

Багатофакторна автентифікація включає в себе використання різних типів факторів для підтвердження особистості користувача. Це може включати комбінацію знання конфіденційної інформації (наприклад, пароля), володіння фізичними пристроями (такими як смартфони або ключові карти), використання біометричних даних (наприклад, відбитків пальців або розпізнавання обличчя), а також введення часово-залежних кодів або виконання певних дій для підтвердження особистості.

Коли користувач намагається отримати доступ до системи або ресурсів, йому потрібно надати вірну інформацію або виконати вірну послідовність дій для кожного з цих факторів. Такий підхід забезпечує більшу безпеку, оскільки зловмиснику складніше отримати доступ до системи, навіть якщо він знайомий з одним з факторів, так як йому потрібно мати доступ до кількох факторів одночасно.

Фактори знання

Фактор знання в багатофакторній автентифікації включає в себе використання конфіденційної інформації, яку лише користувач повинен знати. Це може бути пароль, пін-код, відповідь на секретне запитання або будь-яка інша інформація, яка використовується для перевірки особистості користувача.

Фактор знання вимагає, щоб користувач ввів вірну інформацію під час процесу автентифікації. Ця інформація зазвичай встановлюється власником облікового запису на початковому етапі налаштування багатофакторної автентифікації. Використання фактора знання додає додатковий шар безпеки, оскільки зловмиснику буде важко вгадати або підібрати правильну інформацію.

Однак варто зазначити, що використання лише фактора знання може мати свої обмеження, оскільки паролі часто можуть бути викрадені або вгадані. Тому рекомендується поєднувати фактор знання з іншими

факторами, такими як фактор володіння фізичними пристроями або фактор біометричних даних, для створення більш надійної системи автентифікації.

Фактори володіння

Фактори володіння в багатофакторній автентифікації включають в себе використання фізичних пристроїв або об'єктів, які потрібно мати володіти для підтвердження своєї ідентичності. Основна ідея полягає в тому, що користувач повинен мати фізичний об'єкт, який є унікальним для нього і не доступним для інших осіб.

Основні приклади факторів володіння включають:

1. Мобільні пристрої: Користувач може мати доступ до свого облікового запису або отримувати коди підтвердження на своєму мобільному телефоні або планшеті. Це може бути здійснено за допомогою SMS-повідомлень, мобільних додатків аутентифікації або спеціальних апаратних пристроїв, таких як USB-ключі або NFC-токени.
2. Апаратні ключі: Це фізичні пристрої, зазвичай у формі USB-ключів або смарт-карт, які зберігають криптографічні ключі та виконують процес автентифікації. Вони підтверджують особистість користувача шляхом взаємодії з комп'ютером або мобільним пристроєм.
3. Біометричні дані: Це включає в себе використання унікальних фізичних характеристик користувача, таких як відбиток пальця, розпізнавання обличчя, сканування раковини ока або голосове впізнавання. Біометричні дані використовуються для ідентифікації особи і забезпечення доступу до облікового запису або системи.

Використання факторів володіння разом з фактором знання створює більш надійну систему автентифікації. Комбінація різних факторів дозволяє підвищити безпеку, оскільки зловмиснику буде значно складніше отримати доступ до облікового запису, навіть якщо він знає пароль або має фізичний пристрій.

Фактори власності

Фактори власності в контексті багатофакторної автентифікації орієнтовані на використання власності або характеристик, що належать користувачу, для підтвердження його ідентичності. Ці фактори базуються на тому, що кожна особа має унікальні атрибути, які можуть бути використані для автентифікації.

Основні приклади факторів власності включають:

1. IP-адреса: IP-адреса є унікальним ідентифікатором пристрою в мережі Інтернет. Використання IP-адреси для автентифікації може полягати в тому, щоб система перевіряла, чи використовується звичайна IP-адреса користувача, або включати інші функції, такі як геолокація для визначення місцезнаходження користувача.
2. MAC-адреса: MAC-адреса (Media Access Control) відноситься до унікального ідентифікатора мережевої карти пристрою. Використання MAC-адреси може допомогти перевірити, чи використовується певний пристрій для автентифікації.
3. Телефонний номер: Використання телефонного номера може включати надсилання SMS-повідомлень з кодами підтвердження або здійснення голосового дзвінка на підтвердження особи.
4. Електронна пошта: Використання електронної пошти може передбачати надсилання кодів підтвердження або посилань для підтвердження особи.
5. Фізичні об'єкти: Це можуть бути фізичні предмети, такі як спеціальні токени, картки або ключі, які користувач повинен мати фізично при собі для автентифікації.

Використання факторів власності разом з іншими факторами, такими як фактор знання та фактор володіння, створює більш надійну систему автентифікації, оскільки зловмиснику буде складніше отримати доступ до всіх необхідних факторів для успішної автентифікації.[6].

Фактор місцезнаходження

Фактори місцезнаходження в багатофакторній автентифікації використовуються для визначення географічного положення користувача під час процесу автентифікації. Цей фактор базується на інформації про місце знаходження пристрою, з якого користувач намагається отримати доступ до системи.

Деякі приклади факторів місцезнаходження включають:

1. Геолокація за IP-адресою: При спробі автентифікації система може використовувати IP-адресу користувача для визначення його приблизного географічного положення. Наприклад, якщо звичайний IP-адреса користувача пов'язана з певним регіоном, а поточна IP-адреса відрізняється від звичної, це може бути підозрілою ситуацією.
2. Геолокація за GPS: Якщо пристрій користувача має GPS-модуль, система може запитувати його поточні координати для визначення точного місцезнаходження користувача.
3. Wi-Fi місцезнаходження: Деякі системи можуть використовувати інформацію про доступні Wi-Fi мережі навколо пристрою користувача для визначення місцезнаходження. Це може бути особливо корисно на великих територіях, наприклад, у великих офісних приміщеннях або кампусах.
4. Bluetooth-місцезнаходження: З використанням Bluetooth-сигналів можливо визначити наближене місцезнаходження користувача, якщо навколо є пристрої, з якими він парувався раніше.

Використання факторів місцезнаходження може забезпечити додатковий рівень безпеки та допомогти виявити ситуації, коли автентифікація здійснюється з незвичного місця або пристрою. Однак варто зазначити, що цей фактор може бути обмежений в разі використання VPN, анонімайзерів або інших методів, що маскують справжнє місцезнаходження користувача.

Багатофакторна автентифікація використовується для забезпечення більшого рівня безпеки, вимагаючи введення додаткових факторів

підтвердження ідентифікації користувача. Окрім традиційного логіна та пароля, вона включає додаткові елементи, які користувач повинен мати або знати для успішної автентифікації.

Один з таких факторів - фактор володіння - вимагає наявності у користувача фізичного об'єкта або інформації, яку тільки він має. Найпоширенішим прикладом є використання одноразових паролів, які змінюються кожен раз при автентифікації. Ці одноразові паролі можуть бути згенеровані мобільним додатком або апаратним пристроєм, які користувач має при собі. Це забезпечує додатковий рівень захисту, оскільки навіть якщо пароль стає відомим комусь іншому, він не зможе використати його без фізичного об'єкта (токену, мобільного пристрою) користувача.

Іншими прикладами факторів володіння є фізичні пристрої, такі як USB-ключі або смарт-карти, які містять інформацію, необхідну для автентифікації. Ці пристрої можуть бути з'єднані з комп'ютером або мобільним пристроєм, і їх використання вимагає фізичного наявності користувача, що забезпечує додатковий рівень безпеки.

Технології, такі як RFID (ідентифікація радіочастот), також можуть використовуватись як фактор володіння. Наприклад, смарт-карти з RFID-мітками можуть бути використані для автентифікації, вимагаючи прикладання картки до спеціального считувача.

Комбінація різних факторів, таких як знання (логін-пароль), володіння (токен, смарт-карта) і можливо навіть біометричні дані (відбиток пальця, розпізнавання обличчя), забезпечує більш надійний механізм автентифікації, оскільки зловмиснику потрібно буде мати доступ до кількох факторів одночасно для успішного вторгнення в систему.

Застосування багатофакторної автентифікації має численні переваги, включаючи підвищену безпеку, запобігання несанкціонованому доступу та захист важливих даних та ресурсів.

Застосування багатофакторної автентифікації має декілька додаткових переваг:

1. Захист від втрати або компрометації пароля: Оскільки автентифікація вимагає додаткового фактора, навіть якщо пароль стає відомим комусь іншому, зловмиснику все одно буде потрібний другий фактор для отримання доступу. Це знижує ризик використання викраденого або скомпрометованого пароля.
2. Запобігання фішингу та соціальному інжинірингу: Фішери та зловмисники, що використовують соціальний інжиніринг, можуть намагатися викрасти паролі шляхом обману користувачів. Однак, з впровадженням багатофакторної автентифікації, навіть якщо зловмисник отримує доступ до пароля, він не зможе отримати доступ без додаткового фактора.
3. Можливість використання різних факторів: Багатофакторна автентифікація не обмежується одним конкретним фактором. Користувачі можуть використовувати різні комбінації факторів в залежності від рівня безпеки, зручності та вимог системи. Це може включати паролі, фізичні пристрої, біометричні дані або навіть місцезнаходження користувача.
4. Застосування в різних сферах: Багатофакторна автентифікація широко використовується в багатьох сферах, включаючи банківські послуги, електронну комерцію, соціальні мережі та корпоративні системи. Вона дозволяє забезпечити захист конфіденційних даних, фінансових транзакцій та особистої інформації користувачів.
5. Сумісність з різними пристроями та платформами: Багатофакторна автентифікація може бути використана на різних пристроях і платформах, включаючи комп'ютери, смартфони, планшети та інші пристрої. Це дає користувачам гнучкість та зручність у використанні автентифікаційних методів, які найкраще відповідають їх потребам.

Узагальнюючи, багатофакторна автентифікація є потужним інструментом для забезпечення безпеки та захисту від несанкціонованого доступу. Шляхом використання декількох незалежних факторів, вона підвищує безпеку

автентифікаційного процесу і знижує ризик компрометації облікових записів та важливих даних.

2.1 Математичні моделі

Багатофакторну ідентифікацію / автентифікацію не можна виділити в окремій формі. Тим не менш, у таких системах для визначення ідентифікації користувача в ICS використовується відразу кілька параметрів. Причому ці параметри можна комбінувати в будь-якому порядку. Однак сьогодні, у переважній більшості випадків, використовується лише одна пара: захист паролем та маркер. У цьому випадку користувач може не боятися хакера, 30 який вгадує свій пароль (він не буде працювати без електронного ключа), а також крадіжки токена (він не буде працювати без пароля). У деяких системах використовуються найнадійніші процедури ідентифікації, які одночасно використовують паролі, токени та біометричні характеристики людини. Впровадження комбінованих систем збільшує кількість ідентифікаційних ознак і, отже, підвищує безпеку. На сьогодні існують комбіновані системи наступних типів:

– системи на базі безконтактних смарт-карт і USB-ключів;

– системи на базі гібридних смарт-карт;

– біоелектронні системи.

Безконтактні смарт-карти і USB-ключі. Антена та мікросхема вбудовані в корпус брелока USB для створення безконтактного інтерфейсу. Це дозволить організувати контроль доступу до приміщень та до комп'ютера за допомогою одного ідентифікатора. Ця схема використання ідентифікатора може виключити ситуацію, коли працівник, залишаючи робоче місце, залишає USB-ключ у роз'ємі комп’ютера, що дозволить працювати під його ідентифікатором. У випадку, коли неможливо вийти з кімнати без використання безконтактного ідентифікатора, цієї ситуації можна уникнути.

Математичні моделі багатофакторної автентифікації використовуються для аналізу та оцінки ефективності та безпеки систем автентифікації.Є декілька прикладів таких моделей:

Математичні моделі багатофакторної автентифікації використовуються для забезпечення безпеки ідентифікаційних процесів, в яких використовуються кілька факторів перевірки. Основна ідея полягає в тому, що кожен фактор має свою вагу і внесок у загальний результат автентифікації.

Одним з популярних підходів до багатофакторної автентифікації є модель оцінки ризику. Ця модель використовує різні фактори, такі як пароль, біометричні дані (відбиток пальця, сканер обличчя) і геолокація користувача, для обчислення ризику шахрайства або несанкціонованого доступу. Кожен фактор має свою вагу, яка відображає його важливість у процесі автентифікації. Наприклад, біометричні дані можуть мати більшу вагу, оскільки вони вважаються більш надійними, ніж простий пароль.

Модель оцінки ризиків є одним з підходів до багатофакторної автентифікації. Вона використовується для оцінки рівня ризику шахрайства або несанкціонованого доступу на основі різних факторів перевірки, що використовуються в процесі автентифікації.

Основною ідеєю моделі оцінки ризиків є призначення ваги кожному фактору, який використовується в автентифікації, відповідно до його важливості і надійності. Наприклад, біометричні дані, такі як відбиток пальця або сканер обличчя, можуть мати вищу вагу, оскільки вони вважаються більш надійними, ніж пароль або PIN-код.

Для використання моделі оцінки ризиків зазвичай встановлюються певні правила і параметри. Наприклад, кожному фактору може бути присвоєно числове значення, яке відображає його вагу. Потім здійснюється обчислення або вагова сума всіх факторів, яка представляє загальний ризик. Якщо отриманий ризик перевищує певний поріг, то можуть застосовуватися додаткові заходи безпеки або вимоги автентифікації.

Важливим етапом розробки моделі оцінки ризиків є збір та аналіз історичних даних, а також встановлення кореляцій між різними факторами та випадками шахрайства або несанкціонованого доступу. Це дозволяє моделі виявляти незвичайну або підозрілу активність та зменшувати ризик помилкових позитивних або негативних результатів.

Модель оцінки ризиків може бути інтегрована в існуючі системи автентифікації, забезпечуючи додатковий рівень безпеки. Вона може бути застосована в різних сферах, таких як банківські послуги, електронна комерція, системи управління ідентифікацією, соціальні мережі тощо.

Важливо пам'ятати, що модель оцінки ризиків є лише одним інструментом в системі безпеки та автентифікації. Вона повинна поєднуватися з іншими методами, такими як шифрування даних, захист від вторгнень, моніторинг активності користувачів та іншими технологіями, для створення надійної та ефективної системи захисту.

Інша модель, яка використовується для багатофакторної автентифікації, - це модель рішень на основі правил. Вона використовує набір правил і умов для прийняття рішення щодо автентифікації користувача. Кожен фактор перевірки порівнюється зі встановленими правилами, і в результаті приймається рішення щодо доступу.

Модель рішень на основі правил (англ. rule-based decision model) є одним з підходів до багатофакторної автентифікації. Ця модель використовує набір правил і умов для прийняття рішення щодо автентифікації користувача.

Основна ідея моделі рішень на основі правил полягає в тому, що кожен фактор перевірки порівнюється зі встановленими правилами. Якщо фактори задовольняють певні умови, то автентифікація вважається успішною, і користувачу надається доступ. Якщо умови не виконуються, можуть застосовуватися додаткові заходи безпеки або вимоги автентифікації.

Правила можуть бути визначені вручну або на основі аналізу експертних знань та історичних даних. Вони можуть включати порівняння значень факторів зі заздалегідь встановленими межами, виконання логічних

операцій, перевірку послідовності кроків та інші умови. При виконанні правил автентифікація здійснюється безпроблемно, а в іншому випадку потрібні додаткові перевірки або процедури.

Модель рішень на основі правил має кілька переваг. Вона дозволяє гнучко налаштувати автентифікаційні правила відповідно до потреб конкретної системи або організації. Вона також може бути відносно простою у реалізації і зрозумілою для адміністраторів і користувачів.

Однак, модель рішень на основі правил може мати свої обмеження. Вона може стати недостатньо гнучкою для складних сценаріїв автентифікації, де необхідні більш розширені логічні або статистичні методи. Крім того, ця модель може страждати від проблеми "жорсткості правил", коли вона може бути надто строгою і виключати легітимних користувачів на основі незначних відхилень.

У практиці модель рішень на основі правил часто використовується разом з іншими підходами, такими як статистичні моделі або моделі оцінки ризиків, для створення комплексних систем багатофакторної автентифікації.

Існують також статистичні моделі, які використовують методи статистичного аналізу для оцінки ризику. Вони аналізують історичні дані та шаблони поведінки користувачів для виявлення відхилень та потенційно несанкціонованої активності.

Моделі, які не використовують динамічну або змінну інформацію для автентифікації, але базуються на статичних факторах, як-от паролі, PIN-коди або власність (наприклад, фізичний об'єкт), можна розглянути наступні методи:

1. Пароль-базова автентифікація: Це найпоширеніший і статичний спосіб автентифікації. Користувач вводить пароль або PIN-код, який порівнюється зі збереженим значенням для перевірки автентичності.
2. Власність-базова автентифікація: Цей метод використовує статичні фізичні або матеріальні об'єкти для ідентифікації, наприклад, фізичний ключ, картка доступу або ідентифікаційний пристрій.

Важливо відзначити, що традиційні статичні методи автентифікації можуть бути менш надійними в порівнянні з багатофакторними або біометричними методами. Вони часто піддаються атакам шляхом підбору паролю, крадіжки фізичних об'єктів або шахрайства через підробку.

З огляду на це, у багатофакторній автентифікації акцент здебільшого зроблений на використанні комбінації різних динамічних факторів, таких як біометрика (відбиток пальця, розпізнавання обличчя) або одноразові паролі, які забезпечують вищий рівень безпеки.

Тому, якщо ви шукаєте інформацію про статичні моделі багатофакторної автентифікації, то це поняття не використовується в загальному контексті сучасних методів автентифікації.

Байєсовські мережі: Байєсовські мережі - це графічні моделі, що використовують ймовірнісні залежності між різними факторами автентифікації. Вони використовуються для моделювання та оцінки ймовірностей подій, пов'язаних з автентифікацією.

Байєсовська мережа - це графічна модель, яка використовується для моделювання залежностей між подіями за допомогою ймовірностей. У контексті багатофакторної автентифікації байєсовські мережі можуть бути використані для аналізу та прийняття рішень щодо автентифікації користувачів на основі різних факторів.

Основна ідея байєсовських мереж полягає в тому, що вони використовують ймовірності для моделювання взаємозв'язків між різними факторами автентифікації та їх впливу на факт автентичності користувача. Мережа складається з вузлів, які представляють події, та сполучень, які відображають залежності між цими подіями.

В байєсовській мережі кожен вузол відповідає певному фактору автентифікації, наприклад, паролю, біометричним даним або контексту користувача. Вузли пов'язуються зі сполученнями, які вказують на залежності між цими факторами. Ймовірності, що визначаються в кожному вузлі, відображають вплив цього фактора на факт автентичності користувача.

Після побудови байєсовської мережі можна використовувати алгоритми для вирішення різних задач, таких як:

1. Прогнозування ймовірності автентичності: За допомогою байєсовської мережі можна обчислити ймовірність того, що користувач є автентичним на основі доступних факторів автентифікації.
2. Діагностика причини невдачі автентифікації: Якщо автентифікація не пройшла успішно, байєсовська мережа може допомогти визначити, які фактори сприяли невдачі та їх ймовірні впливи.
3. Оптимізація вибору факторів автентифікації: Байєсовські мережі можуть допомогти вибрати найефективніші фактори для використання в процесі автентифікації на основі їх впливу та значущості.

Використання байєсовських мереж у багатофакторній автентифікації дозволяє створити комплексні моделі, які враховують взаємодію різних факторів та їх вплив на автентичність користувача. Це допомагає покращити точність і надійність процесу автентифікації та забезпечити більш безпечний доступ до системи.[7]

Модель машинного навчання в багатофакторній автентифікації використовується для розробки систем, які можуть автоматично визначати автентичність користувача на основі різних факторів. Вона використовує алгоритми та статистичні методи для навчання з даних та прийняття рішень.

Основні етапи роботи з моделлю машинного навчання в багатофакторній автентифікації включають:

1. Збір та підготовка даних: Збираються дані про користувачів, включаючи різні фактори автентифікації, такі як паролі, біометричні дані, контекст тощо. Дані піддаються попередній обробці, включаючи очищення, нормалізацію та видалення аномалій.
2. Вибір моделі: Вибирається підходяща модель машинного навчання для завдання багатофакторної автентифікації. Популярними моделями можуть бути нейронні мережі, дерева рішень, метод опорних векторів або ансамблі моделей.

3. Навчання моделі: Модель навчається на тренувальних даних, щоб встановити зв'язки між факторами автентифікації та автентичністю користувачів. В цьому процесі модель пристосовується до даних та встановлює оптимальні параметри.
4. Оцінка та валідація моделі: Оцінюється ефективність моделі за допомогою тестових даних. Використовуються метрики, такі як точність, відновлення, F-мера, щоб оцінити якість моделі.
5. Використання моделі для прийняття рішень: Після навчання модель може бути використана для автоматичного визначення автентичності нових користувачів на основі їх факторів автентифікації. За результатами моделі можуть бути прийняті рішення про надання або відмову у доступі.

Модель машинного навчання в багатофакторній автентифікації може бути дуже потужним інструментом для виявлення шахрайства та покращення безпеки. Вона дозволяє системі автоматично аналізувати великі обсяги даних та знаходити складні залежності між факторами автентифікації, що допомагає впроваджувати більш надійні системи автентифікації.[8]

Усі ці моделі можуть використовуватися окремо або в поєднанні, залежно від конкретних потреб і вимог системи автентифікації. Важливо враховувати, що жодна модель не є бездоганною, і вона може мати свої обмеження та вразливості. Тому важливо розробляти комплексні системи багатофакторної автентифікації, які поєднують кілька моделей та застосовують різноманітні фактори перевірки для забезпечення найвищого рівня безпеки.

Існує багато додатків для мобільних пристроїв які реалізує алгоритм TOTP. Вони дозволяють створювати тимчасові паролі, які можуть бути використані для авторизації користувачів на сервері автентифікації, який використовує таємний ключ користувачів. Наприклад Google Authenticator використовується переважно для доступу до служб Google, використовуючи

двофакторну автентифікацію, однак його можна використати і в розробці рішень автентифікації для web додатків.

Алгоритм Time-based One-Time Password Algorithm(TOTP) використовується для визначення того, чи справді користувач вказує достовірний пароль, визначений на основі на спільного секретного часу та часової мітки.

Створення облікових даних - це процес, в якому сервер спыльний секретний ключ і ділиться ним з клієнтом. Спільний таємний ключ створюється за допомогою сильного криптографічного генератора псевдовипадкових чисел. Далі ключ повідомляється клієнту, щоб він міг налаштовувати свій токен.

Найпоширеніший спосіб передачі цієї інформації - це відправка його клієнту у вигляді закодованого QR-коду. Користувач має лише сканувати QR-код за допомогою програми Google Authenticator або іншої, а потім видалити цей код. З метою забезпечення безпеки генератори токенів TOTP зазвичай не дозволяють користувачам отримувати спільні таємні ключі після налаштування облікового запису. Таким чином, лише власники мобільних пристроїв, на яких відбувалися налаштування, які володіють токеном, можуть використовувати цей ключ для створення паролів TOTP.

Автентифікація облікових даних - це процес, в якому сервер застосовує алгоритм генерації TOTP до спільного ключа та паролю, введеного користувачем, для підтвердження його автентичності. Створення спільного ключа є важливим процесом, тому що здатність перехопити чи вгадати чужий ключ може призвести до викрадення облікового запису. Таким чином, варто використовувати сильні генератори псевдовипадкових чисел.

Програма Google Authenticator може бути швидко налаштована за допомогою QR-коду: програма запитує користувача сфотографувати код, а програма використовує дані, закодовані в ньому, для налаштування нового облікового запису. Цей підхід має кілька переваг: людські помилки зведені до мінімуму або взагалі усуваються, процес встановлення простий та

швидкий, але найголовніше, загальний секретний ключ ніколи не відображається в звичайному тексті. Якщо злочинцеві не вдасться викрасти використане зображення QR-коду, щоб налаштувати інший обліковий запис автентифікатора, то спільний таємний ключ не буде доступним для прочитання навіть для самого законного власника.

Тому QR-код значно зменшує ризик перехоплення під час фази початкової взаємодії.

Щоб перевірити пароль, алгоритм TOTP вимагає:

- Пароль для перевірки.
- Загальний секрет.
- Часова фактор руху.

Клієнт та сервер повинні узгодити спосіб обчислення фактору зсуву на основі часу. RFS 6238 рекомендує використовувати розмір за замовчуванням 30 секунд.

Таким чином, принцип роботи автентифікації на основі одноразового згенерованого паролю буде наступний:

1. Генерується секретний ключ на основі якого створюється QR код що показується користувачу
2. Користувач сканує даний QR код власним додатком Google Authenticator
3. Йому відображається згенерований TOTP який необхідно ввести протягом певного часу в додаток для підтвердження особистості
4. Введений пароль перевіряється за допомогою секретного ключа

По суті, TOTP є варіантом HOTP алгоритму, в якому в якості значення лічильника підставляється величина, що залежить від часу. Позначимо:

T — дискретне значення часу, що використовується в якості параметра.

X — інтервал часу, протягом якого дійсний пароль.

T_o — початковий час, необхідний для синхронізації сторін.

K— спільний секрет.

Current time— поточний час.

Тоді

$$T = (Current\ time — To)/X$$

$$HOTP(K,T) = Truncate(HMAC\text{-}SHA\text{-}1\ (K, T))$$

$$TOTP = HOTP(K,T)$$

де

- *HMAC-SHA-1(K,T)* - генерація 20-ти байт на основі таємного ключа і часу за допомогою хеш-функції SHA-1.
- *Truncate* — функція вибору певним способом 4 байт:

позначимо String — результат *HMAC-8HA-1(K,T); OffsetBits* — молодші 4 біта рядка *String*; *OffsetBits = StringToNumber(OffsetBits)* і результатом *Truncate* буде рядок з чотирьох символів — *String[Offset]…String[Offset + 3]*

Також варто відзначити, що на відміну від HOTP, який заснований тільки на *SHA-1*, *TOTP* може також використовувати *HMAC-SHA-256, HMAC-SHA-512* та інші HMAC-хеш-функції:

$$TOTP\ (K,T) = Truncate\ (HMAC\text{-}SHA\text{-}256(K, T)$$

Отже, автентифікація користувача на основі TOTP може слугувати надійним способом автентифікації, оскільки дозволяє переконатися у тому, що саме співрозмовник має безпосередній доступ до необхідного мобільного пристрою. Також, на початку спілкування за відсутності великої кількості даних, достатніх для розпізнавання поведінкового патерну користувача за новими повідомленнями, даний метод являється основним методом запобігання витоку конфіденційної інформації.

За словами прихильників, багатофакторна автентифікація може значно знизити випадки онлайн крадіжок ідентичності інших онлайн злочинів,оскільки лише паролю жертви вже не буде достатнім, щоб дати злодієві постійний доступ до важливої інформації. Тим не менш, методи багатофакторної автентифікації все ще залишаються вразливими для фішингу, атак людини в браузері і людина посередині.

Таким чином, навіть при наявності такого надійного механізму, як багатофакторна автентифікація, загрози витоку інформації все ж можуть залишатися актуальними, тому необхідно забезпечити додаткові методи для їх запобігання, а саме, застосування додаткового рівня автентифікації користувача за надісланими повідомленнями.

2.2 Структурні моделі

Структурні моделі багатофакторної автентифікації використовуються для візуалізації та аналізу структури системи автентифікації, включаючи фактори автентифікації, зв'язки між ними та потоки даних.

Блок-діаграма (або діаграма потоку) - це візуальне зображення процесу або алгоритму за допомогою блоків, які представляють кожен етап процесу та зв'язки між ними.

Отже, для представлення багатофакторної автентифікації у вигляді блок-діаграми можна використовувати блоки, які представляють різні фактори автентифікації та зв'язки між ними для відображення послідовності або умов переходу від одного фактора до іншого.

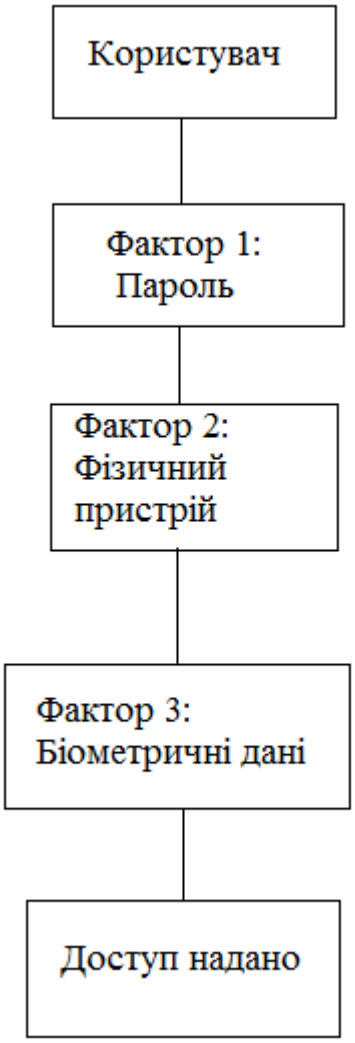


Рисунок 2.1 – блок-діаграма

У цій блок-діаграмі першим фактором автентифікації є пароль, який вводить користувач. Якщо пароль вірний, процес переходить до другого фактора - фізичного пристрою. Після успішної перевірки фізичного пристрою, процес продовжується до третього фактора - біометричних даних. Якщо всі фактори успішно пройдено, дозволяється доступ.

Основними елементами блок-діаграми є:

1. Блоки: Блоки представляють окремі етапи або дії в процесі. Кожен блок містить певну інформацію про виконувану дію. Наприклад, блок може містити назву дії, виконувану операцію або умову, що повинна бути виконана.

2. Зв'язки: Зв'язки вказують на послідовність або умови переходу між блоками. Вони показують, як дані або керування переміщуються від одного блоку до іншого. Зв'язки можуть мати різні типи, такі як лінії зі стрілками, лінії з умовами або лінії з маркерами.
3. Поток керування: Блок-діаграма демонструє послідовність дій або потік керування в процесі. Вона показує, як дані або керування переміщуються від початку до кінця процесу, проходячи через різні блоки та зв'язки.
4. Початок та кінець: Блок-діаграма має блоки початку та кінця, які позначають початок та кінець процесу. Блок початку вказує, звідки починається виконання процесу, а блок кінця вказує, де процес завершується.

Завдяки блок-діаграмам можна легко візуалізувати складні процеси та алгоритми, зрозуміти послідовність дій та знайти можливі недоліки або покращення в проекті системи.

Наприклад, для багатофакторної автентифікації можна побудувати блок-діаграму, де блоки відображатимуть окремі фактори автентифікації, а зв'язки вказуватимуть послідовність переходу між факторами в залежності від результатів перевірки.

Діаграма компонентів в багатофакторній автентифікації відображає структуру системи та взаємодію компонентів, необхідних для реалізації багатофакторної автентифікації. Основна мета діаграми компонентів - показати, які компоненти існують у системі та як вони взаємодіють один з одним.

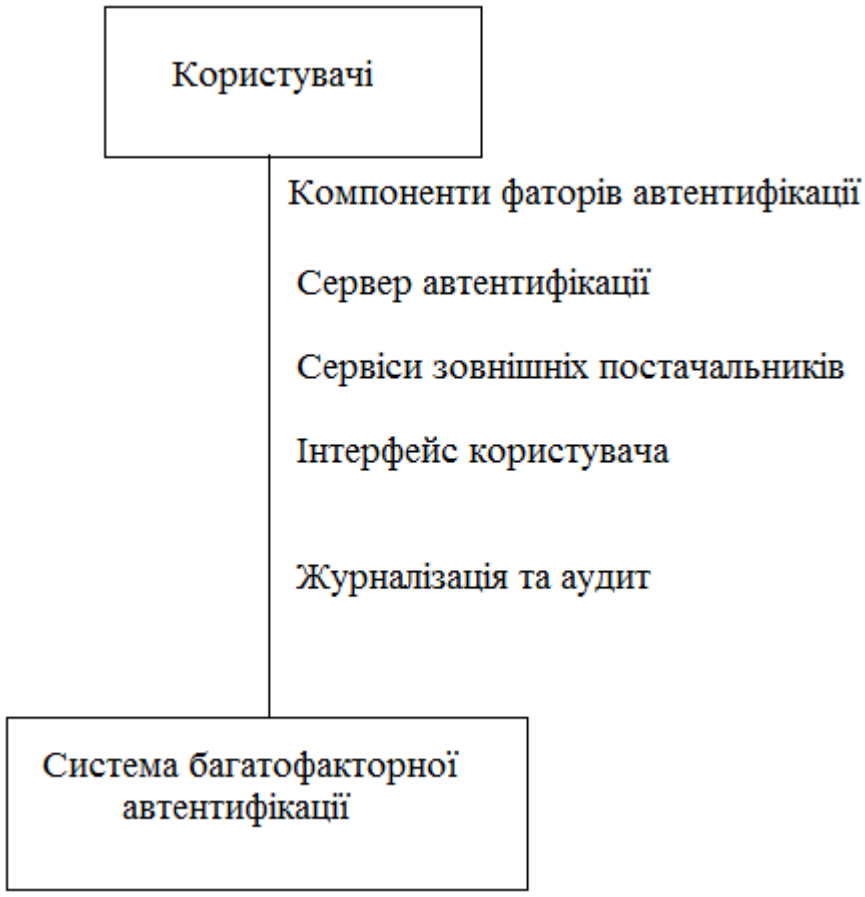


Рисунок 2.2 – Діаграма компонент

Основні компоненти, які можуть бути включені в діаграму компонентів для багатофакторної автентифікації, включають:

1. Користувач: Це представляє собою кінцевого користувача, який намагається отримати доступ до системи чи ресурсів, що потребує автентифікації.
2. Фактори автентифікації: Це компоненти, що відповідають за перевірку різних факторів для підтвердження ідентичності користувача. Наприклад, це можуть бути компоненти для перевірки паролів, фізичних пристроїв (таких як токени або смарт-карти) або біометричних даних (таких як сканер відбитків пальців або системи розпізнавання обличчя).
3. Сервер аутентифікації: Цей компонент відповідає за збереження і управління інформацією про користувачів, таку як хеші паролів або

біометричні шаблони. Він також виконує перевірку факторів автентифікації та приймає рішення про надання чи відмову в доступі.

4. Сервіси зовнішніх постачальників: У багатофакторній автентифікації можуть бути використані сервіси зовнішніх постачальників, які надають додаткові фактори автентифікації або виконують перевірку на основі даних, що не зберігаються в системі. Наприклад, це може бути сервіс підтвердження SMS-повідомленнями або система одноразових паролів.
5. Інтерфейс користувача: Цей компонент забезпечує взаємодію між користувачем і системою багатофакторної автентифікації. Він може бути представлений у вигляді веб-сторінок, мобільних додатків або інших інтерфейсів, де користувач може ввести свої дані або отримати вказівки щодо процесу автентифікації.
6. Журналізація та аудит: Цей компонент відповідає за запис і збереження інформації про автентифікаційні події, такі як спроби входу, успішні та невдачні автентифікації. Він може включати лог-файли або базу даних, що містить історію автентифікації для подальшого аналізу та моніторингу.

Діаграма компонентів може бути побудована з урахуванням конкретної системи багатофакторної автентифікації та враховувати специфічні компоненти, які використовуються у вашому випадку.

Діаграма послідовності (Sequence Diagram) в багатофакторній автентифікації може допомогти проілюструвати взаємодію між різними компонентами системи під час процесу автентифікації. Вона показує послідовність повідомлень, що передаються між об'єктами (компонентами) у певному часовому порядку.

Основні компоненти, які можуть бути включені в діаграму послідовності для багатофакторної автентифікації, включають:

1. Користувач: Це представляє собою кінцевого користувача, який намагається автентифікуватися в системі.

2. Компоненти факторів автентифікації: Ці компоненти виконують перевірку різних факторів автентифікації, таких як пароль, фізичний пристрій або біометричні дані. Вони можуть взаємодіяти з сервером аутентифікації та іншими компонентами для обміну необхідною інформацією.
3. Сервер аутентифікації: Цей компонент відповідає за обробку запитів на автентифікацію, перевірку факторів автентифікації та прийняття рішення щодо надання доступу.
4. Сервіси зовнішніх постачальників: Ці компоненти можуть включати сервіси, які надають додаткові фактори автентифікації або здійснюють перевірку на основі зовнішніх джерел даних.
5. Інтерфейс користувача: Цей компонент забезпечує взаємодію з користувачем шляхом відображення інтерфейсу, запитування необхідних даних та передачі їх до інших компонентів.

Діаграма послідовності дозволяє показати, які повідомлення передаються між компонентами під час процесу автентифікації, включаючи запити на перевірку факторів автентифікації, відповіді з результатами перевірки та рішення щодо надання доступу.

Контекстна діаграма в багатофакторній автентифікації допомагає відобразити систему автентифікації в контексті зовнішніх сутностей, з якими вона взаємодіє. Це високорівнева діаграма, яка ілюструє головні компоненти системи та їх зовнішніх сутностей, але не вдається в деталі внутрішньої взаємодії між цими компонентами.

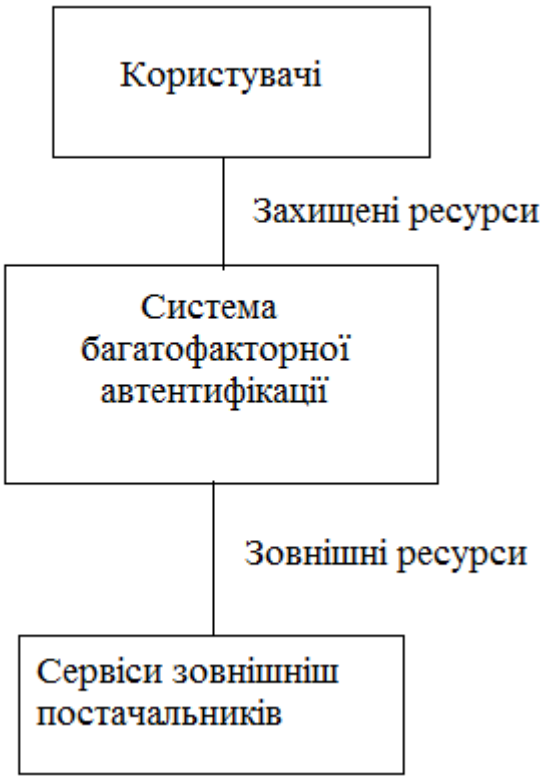


Рисунок 2.3 – Контекстна діаграма

Основні елементи, які можуть бути включені в контекстну діаграму для багатофакторної автентифікації, включають:

1. Система багатофакторної автентифікації: Це центральна система, яка виконує процес автентифікації користувачів та приймає рішення про надання чи відмову в доступі. Вона може включати компоненти для перевірки факторів автентифікації, управління сесіями та журналізації подій.
2. Користувачі: Ці зовнішні сутності представляють самих користувачів системи, які намагаються отримати доступ до захищених ресурсів.
3. Захищені ресурси: Це зовнішні сутності, до яких користувачі намагаються отримати доступ. Це можуть бути веб-сайти, додатки, бази даних або інші системи.
4. Зовнішні сервіси: Ці зовнішні сутності можуть включати сервіси зовнішніх постачальників, які надають додаткові фактори автентифікації або інші послуги, необхідні для процесу автентифікації.

Контекстна діаграма демонструє взаємодію між цими основними сутностями та надає загальне уявлення про систему багатофакторної автентифікації. Вона може бути використана як вихідний пункт для подальшого деталізованого моделювання внутрішніх компонентів та взаємодії в межах системи.

Структурні моделі багатофакторної автентифікації використовуються для забезпечення вищого рівня безпеки ідентифікації користувачів. Ці моделі враховують різні фактори, такі як щось, що користувач знає (наприклад, пароль або PIN-код), щось, що користувач має (такі як фізичний об'єкт або смарт-карта), або щось, що користувач є (таке як біометричні дані).

Основним принципом багатофакторної автентифікації є використання комбінації різних факторів, щоб забезпечити впевненість в тому, що користувач є тим, за ким він себе видає. Нижче наведено декілька структурних моделей багатофакторної автентифікації:

Модель з трьома факторами: Ця модель використовує комбінацію чогось, що користувач знає, чогось, що користувач має, і чогось, що користувач є. Наприклад, при вході в систему користувач може ввести свій пароль (щось, що він знає), вставити фізичний об'єкт, такий як смарт-карту (щось, що він має), і пройти сканування відбитка пальця (щось, що він є).

Модель з трьома факторами в багатофакторній автентифікації використовує комбінацію трьох різних типів факторів для підтвердження ідентичності користувача. Ці фактори включають щось, що користувач знає, щось, що користувач має, і щось, що користувач є.

1. Щось, що користувач знає: Цей фактор вимагає від користувача знання певної інформації, яка пов'язана з його ідентичністю. Це може бути пароль, PIN-код, відповіді на контрольні питання або будь-яка інша таємна інформація, яку тільки користувач повинен знати.
2. Щось, що користувач має: Цей фактор вимагає наявності фізичного об'єкта або пристрою, який належить користувачеві. Це може бути смарт-карта, токен, USB-ключ, спеціальний пристрій або мобільний

телефон, на якому встановлена аутентифікаційна програма або мобільний додаток.

3. Щось, що користувач є: Цей фактор використовує біометричні дані користувача для підтвердження його ідентичності. Це може бути сканування відбитка пальця, розпізнавання обличчя, розпізнавання ірису або голосове визначення. Ці біометричні дані порівнюються з заздалегідь збереженими унікальними шаблонами, що належать конкретному користувачеві.

Поєднання цих трьох факторів утворює багатофакторний підхід до автентифікації, який забезпечує вищий рівень безпеки, оскільки зламувачеві потрібно мати доступ до трьох різних типів інформації або об'єктів для успішної атаки. Комбінація цих факторів забезпечує більш надійний механізм перевірки ідентичності користувача.

Модель з двома факторами: Ця модель використовує комбінацію будь-яких двох факторів для автентифікації. Наприклад, користувач може ввести пароль і використовувати біометричний сканер, щоб підтвердити свою особу.

Модель з двома факторами в багатофакторній автентифікації використовує комбінацію двох різних типів факторів для підтвердження ідентичності користувача. Основні комбінації факторів, що часто використовуються, включають:

1. Щось, що користувач знає: Це може бути пароль, PIN-код, відповіді на контрольні питання або будь-яка інша таємна інформація, яку тільки користувач повинен знати. Наприклад, користувач вводить свій пароль, який є щось, що він знає.
2. Щось, що користувач має: Це може бути фізичний об'єкт або пристрій, який належить користувачеві. Наприклад, це може бути смарт-карта, токен або мобільний телефон, на якому встановлена аутентифікаційна програма або мобільний додаток. Користувач повинен мати доступ до цього об'єкта або пристрою, щоб підтвердити свою ідентичність.

Комбінація цих двох факторів створює більш надійний механізм автентифікації, ніж використання лише одного фактора. Зламувачеві потрібно мати доступ до обох факторів для успішної атаки. Це підвищує безпеку системи автентифікації та ускладнює завдання для потенційних зловмисників.

Модель з багатьма факторами: У цій моделі використовуються три або більше факторів для автентифікації. Це може включати комбінацію паролів, біометричних даних (таких як відбитки пальців або розпізнавання обличчя), фізичних об'єктів або одноразових кодів, які надсилаються на мобільний пристрій користувача.

Модель з багатьма факторами в багатофакторній автентифікації використовує комбінацію трьох або більше різних типів факторів для підтвердження ідентичності користувача. Ця модель може включати широкий спектр факторів, які можуть бути класифіковані в такі групи:

1. Щось, що користувач знає: Це може бути пароль, PIN-код, відповіді на контрольні питання або будь-яка інша таємна інформація, яку тільки користувач повинен знати.
2. Щось, що користувач має: Це може бути фізичний об'єкт або пристрій, який належить користувачеві, наприклад, смарт-карта, токен або мобільний телефон.
3. Щось, що користувач є: Цей фактор використовує біометричні дані користувача, такі як відбиток пальця, розпізнавання обличчя, голосове визначення або розпізнавання ірису.
4. Щось, що користувач робить: Цей фактор включає дії користувача, такі як введення коду з одноразового підтвердження, натискання певних клавіш або виконання певної послідовності дій.
5. Щось, що користувач має в мережі: Цей фактор використовується для підтвердження наявності користувача в певній локації або мережі, наприклад, через IP-адресу, MAC-адресу або використання VPN.

6. Щось, що користувач отримує: Цей фактор включає отримання коду або повідомлення, яке надсилається користувачеві на зареєстрований мобільний телефон або інші пристрої.

Комбінація цих багатьох факторів створює додатковий рівень безпеки, оскільки зламувачам буде набагато складніше отримати доступ до всіх використовуваних факторів. При виборі моделі з багатьма факторами важливо збалансувати безпеку та зручність для користувачів, оскільки більш складна автентифікація може призвести до збільшення зусиль для користувачів під час входу до системи.

Вибір конкретної структурної моделі багатофакторної автентифікації залежить від потреб і ризиків конкретної системи або організації, яка використовує автентифікацію. Чим більше факторів використовується, тим вищий рівень безпеки можна досягти, проте це може мати вплив на зручність використання системи користувачами.

2.3 Висновки до розділу

У цьому розділі ми розглянули різні математичні та структурні моделі, які використовуються в багатофакторній автентифікації. Вони допомагають покращити безпеку та надійність процесу автентифікації, забезпечуючи ідентифікацію користувачів на основі багатьох факторів.

Модель оцінки ризиків дозволяє оцінити рівень ризику для кожного користувача на основі його поведінки, контексту та інших параметрів. Це допомагає виявляти потенційно шкідливі дії та надавати адаптивний рівень доступу.

Модель рішень на основі правил використовує набір правил і умов для визначення, коли надавати доступ або відмовляти у доступі. Ця модель може бути простою в імплементації і зрозумілою для користувачів, але може бути обмежена в гнучкості.

Статичні моделі багатофакторної автентифікації використовують фіксований набір факторів та їх комбінацію для визначення автентичності користувача. Ці моделі можуть бути ефективними, але не здатні адаптуватися до змінних умов або нових загроз.

Байєсовська мережа в багатофакторній автентифікації використовує ймовірності та статистичні методи для визначення ймовірності автентичності користувача на основі його факторів. Ця модель може враховувати взаємодію між факторами та забезпечувати більш точну оцінку автентичності.

Модель машинного навчання в багатофакторній автентифікації використовує алгоритми та статистичні методи для навчання з даних та прийняття рішень. Вона дозволяє системі автоматично аналізувати великі обсяги даних та знаходити складні залежності між факторами автентифікації.

Кожна з цих моделей має свої переваги та обмеження, і їх вибір залежить від конкретних потреб та вимог системи багатофакторної автентифікації. Комбінація різних моделей та підходів може забезпечити більш ефективну та безпечну систему автентифікації.

3 РОЗРОБКА ЗАСОБУ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

3.1 Опис засобу багатофакторної автентифікації

Автентифікація за двохстроковим паролем та біометричною автентифікацією.

Багатофакторна автентифікація - це метод автентифікації, який використовує кілька факторів для підтвердження ідентифікації користувача. Він додає додатковий рівень безпеки, оскільки потребує не тільки знання логіна та пароля, але й додаткові фактори, такі як біометричні дані (наприклад, відбиток пальця, розпізнавання обличчя) або фізичні токени.

У даному засобі багатофакторної автентифікації використовуються наступні компоненти алгоритму:

Логін та довгостроковий пароль:

- Кожен суб'єкт в системі має свій унікальний логін (персональне ім'я входу) та довгостроковий пароль, що складається з послідовності символів.
- При введенні логіна та довгострокового пароля на клієнтській частині вони відправляються на серверну частину.

Біометрична автентифікація:

- Використовується біометрична автентифікація, яка базується на біометричних даних користувача (наприклад, відбиток пальця, розпізнавання обличчя).
- Після введення логіна та довгострокового пароля на клієнтській частині, суб'єкт підтверджує свою ідентичність шляхом сканування відбитка пальця або розпізнавання обличчя на пристрої з біометричними можливостями.

Автентифікація та розмежування доступу:

- Серверна частина обробляє запит та перевіряє правильність введеного логіна та довгострокового пароля.

- Якщо введені дані вірні, і біометрична автентифікація пройшла успішно, то користувачу надається доступ до системи.
- В іншому випадку, на клієнтську частину повертається відповідь з помилкою.

Застосування біометричної автентифікації дозволяє покращити безпеку та зручність входу до системи, оскільки вона базується на унікальних фізичних характеристиках користувача.

Багатофакторна автентифікація використовує різні типи факторів для перевірки ідентичності користувача. Основні типи факторів включають:

Щось, що ви знаєте (наприклад, пароль або PIN-код): Цей фактор вимагає від користувача знання секретної інформації, яку тільки вони повинні знати.

Щось, що ви маєте (наприклад, фізичний пристрій або токен): Цей фактор включає використання фізичних об'єктів, таких як смартфон, USB-ключ або спеціальний токен, який генерує одноразові паролі.

Щось, що ви є (наприклад, біометричні дані): Цей фактор використовує унікальні біологічні характеристики користувача, такі як відбиток пальця, розпізнавання обличчя або структура голосу.

Комбінація цих факторів створює більш безпечне середовище для автентифікації. Наприклад, після введення правильного пароля (щось, що ви знаєте), користувач може отримати запит на підтвердження на своєму смартфоні (щось, що ви маєте) або сканування відбитка пальця (щось, що ви є). Таким чином, навіть якщо зловмисник дізнається пароль, він не зможе отримати доступ без наявності додаткового фактора.

Засоби багатофакторної автентифікації можуть бути реалізовані як програмне забезпечення або вбудовані в системи аутентифікації. Вони можуть використовувати різні методи перевірки факторів, такі як одноразові паролі, SMS-повідомлення, мобільні додатки для генерації кодів або біометричні сканери.

Багатофакторна автентифікація стала популярним і необхідним рішенням для захисту облікових записів, особистої інформації та конфіденційних даних у багатьох сферах, включаючи фінанси, медицину, електронну комерцію та багато інших. Вона забезпечує додатковий рівень безпеки і запобігає несанкціонованому доступу до чутливої інформації.

3.2 Алгоритм роботи програми

Основний алгоритм роботи даного коду можна описати наступним чином:

1. Відображається сторінка з формою для логіну.
2. Користувач вводить своє ім'я користувача та пароль.
3. При натисканні кнопки "Увійти" виконується обробка події "submit" форми.
4. Виконується функція isValidUser, яка перевіряє, чи є введені дані коректними.
   - Якщо дані коректні (ім'я користувача: "admin", пароль: "password"), виконується функція showBiometricAuth.
   - Якщо дані некоректні, виводиться повідомлення про помилку.
5. У функції showBiometricAuth перевіряється наявність біометричної автентифікації за допомогою функції isBiometricAuthAvailable.
   - Якщо біометрична автентифікація підтримується, показується контейнер для біометричної автентифікації.
   - Якщо біометрична автентифікація не підтримується, виводиться повідомлення про успішну автентифікацію.
6. При натисканні кнопки "Автентифікація за допомогою біометрії" виконується функція simulateBiometricAuth, яка симулює процес біометричної автентифікації з деякою затримкою.

- Якщо автентифікація успішна, виводиться повідомлення про успішну автентифікацію.
- Якщо автентифікація не вдалася, виводиться повідомлення про помилку.

7. Функції showSuccessMessage та showErrorMessage використовуються для виведення повідомлень про успішну автентифікацію або помилку.
8. У разі успішної біометричної автентифікації користувач отримує доступ до відповідних ресурсів або функціоналу.
9. В разі невдалої біометричної автентифікації або некоректних даних логіну/паролю користувач повинен повторити процес автентифікації.

Таким чином, алгоритм полягає у введенні користувачем імені користувача та пароля, перевірці їх на коректність, показі контейнера для біометричної автентифікації або повідомлення про помилку, симуляції біометричної автентифікації та виведенні відповідних повідомлень, а також управлінні доступом до ресурсів або функціоналу на основі результату автентифікації.

3.3 Програмна реалізація

Мова і засоби розробки

Це є веб-сторінкою, яка демонструє автентифікацію з використанням біометрії. Сторінка містить форму логіна, де користувач повинен ввести ім'я користувача та пароль. Після натискання кнопки "Увійти" перевіряється правильність введених даних.

Якщо дані автентифікації вірні і на пристрої доступні біометричні функції, то з'являється кнопка "Автентифікація за допомогою біометрії". При натисканні цієї кнопки запускається функція authenticateWithBiometrics(), яка викликає API для біометричної автентифікації.

Код написаний на мові JavaScript і використовує такі технології як HTML, CSS і Web API. Залежно від можливостей пристрою, сторінка використовує `window.PasswordCredential` або `window.PublicKeyCredential` для біометричної автентифікації.

Цей код може бути використаний як основа для розробки функціоналу автентифікації з використанням біометрії на веб-сайтах або веб-додатках.

Як середовище розробки був обраний інструмент Sublinr Text 3, який є найбільш актуальною версією програми на момент написання роботи. Основною перевагою даного середовища є підтримка безлічі плагінів для зручної роботи, а також вільний доступ.

3.4 Ресурси

У коді HTML немає окремого розділу для підключення зовнішніх ресурсів, таких як CSS-файли або JavaScript-бібліотеки. Додавання ресурсів може допомогти покращити вигляд та функціональність вашої сторінки.

Наприклад, якщо ви бажаєте змінити зовнішній вигляд елементів на сторінці, ви можете додати власний CSS-файл та описати в ньому правила стилів для певних елементів.

Ось приклад коду, який додає зовнішній CSS-файл до вашої сторінки:

```
<link rel="stylesheet" href="styles.css">
```

У цьому прикладі використали <link> елемент, який вказує на розташування CSS-файлу. Можна замінити "styles.css" на шлях до свого власного CSS-файлу.

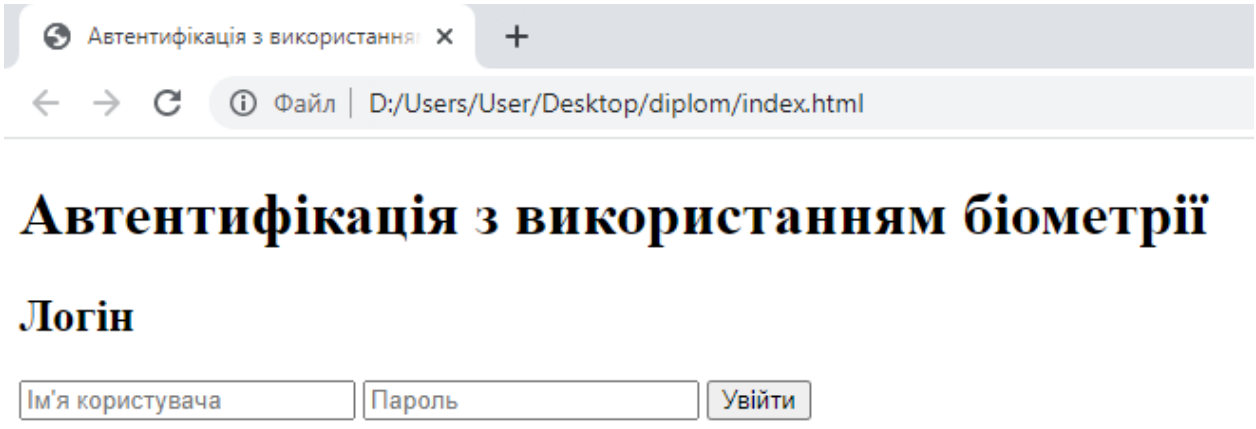
Також, якщо є додаткові JavaScript-бібліотеки або ви бажаєте використовувати власні скрипти, ви можете додати <script> елементи до вашої сторінки. Наприклад:

```
<script src="script.js"></script>
```

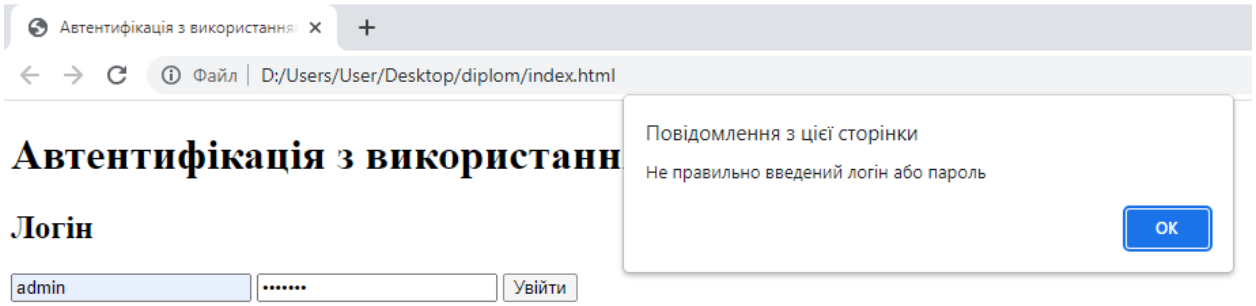
Можна додати <script> елементи, які посилаються на різні JavaScript-файли, в яких описуєте свою власну функціональність.

3.5 Тестування програмного додатку

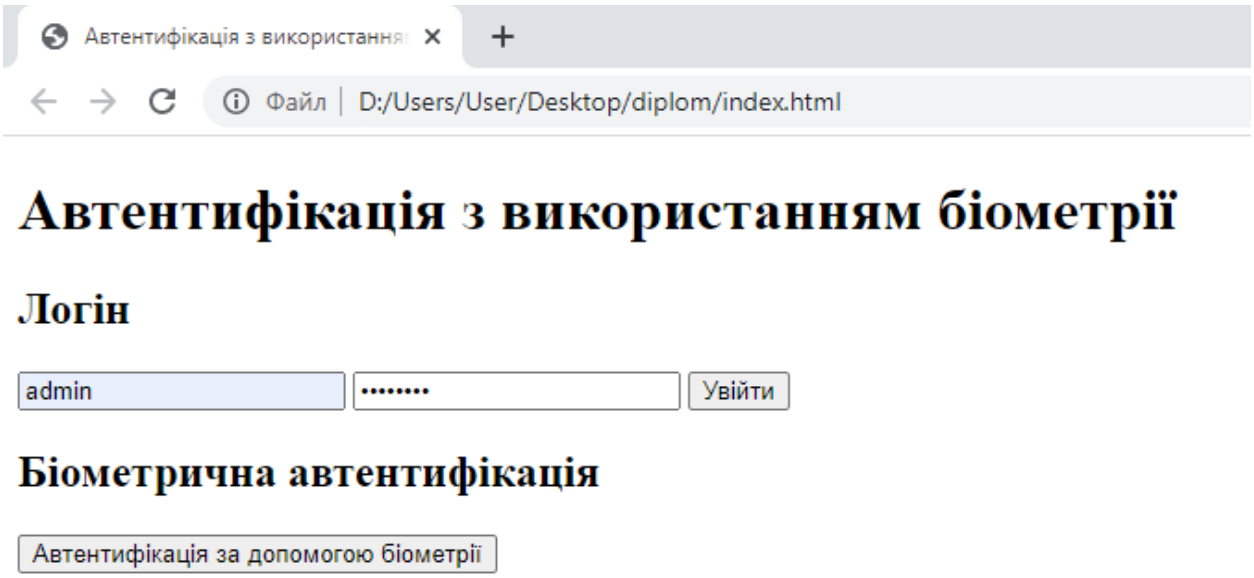
Заходимо на сайт та провіряємо працездасть даного сайту:



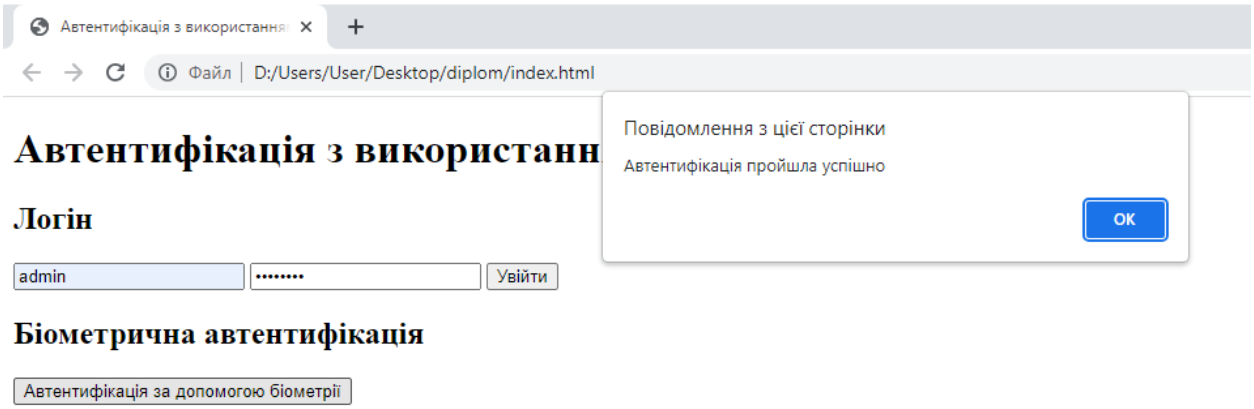
Спробуємо одразу перевірити працездатність системи, набравши довільні дані у віконцях логіну та паролю. Отримуємо результат:



Переходимо до авторизації та вносимо свої дані. Після введення правильного логіну та паролю система переходить до налаштування другого фактору автентифікації, а саме біометричної автентифікації.



Коли натиснута кнопка "Автентифікація за допомогою біометрії", викликається функція `authenticateWithBiometrics()`, яка перевіряє доступність біометричних функцій і проводить біометричну автентифікацію. Якщо автентифікація успішна, виводиться повідомлення про успішну автентифікацію. У разі невдачі виводиться повідомлення про помилку.



Автентифікація пройшла успішно.

ВИСНОВКИ

Після аналізу існуючих систем багатофакторної автентифікації та розмежування доступу до інформаційних систем можна зробити висновок, що парольні методи все ще переважно використовуються, але з розвитком інформаційних систем постало питання підвищення рівня безпеки. У цьому контексті двохфакторна автентифікація з використанням двохфакторного паролю та біометричних способів набуває все більшої популярності та перспективності.

В результаті виконаної роботи проведено аналіз та порівняння сучасних факторів автентифікації до інформаційних систем, а також розроблено програмний модуль для двохфакторної автентифікації з використанням двохфакторного паролю та біометричних методів.

Під час виконання роботи було здійснено наступні кроки:

Проведено аналіз сучасних методів автентифікації та розмежування доступу до інформаційних систем, що послужило основою для розробки програмного веб-додатку з системою двохфакторної автентифікації за допомогою двохфакторного паролю та біометричних методів.

Розроблено веб-додаток з системою двохфакторної автентифікації, який використовує двохфакторний пароль та біометричну автентифікацію. Для цього була використана платформа мови програмування HTML JavaScript CSS, що дозволило забезпечити авторизований доступ користувачів до ресурсів інформаційних систем.

Проведено тестування розробленої системи двохфакторної автентифікації з використанням двохфакторного паролю та біометричних методів для перевірки її здатності вирішувати поставлені завдання.

Отже, на основі проведеного аналізу можна стверджувати, що двохфакторний пароль та біометрична автентифікація представляють собою перспективні методи підвищення рівня безпеки інформаційних систем та забезпечення надійного розмежування доступу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ідентифікація та автентифікація URL : https://sites.google.com/site/identifikaciataautentifikacia/ponatta-pro-autentifikaciu/metodi-autentifikaciie (дата звернення: 21.06.2021)
2. Yubikey-Україна URL : https://yubikey.com.ua/shcho-take-bahatofaktorna-avtentyfikatsiia-ta-koly-dotsilno-ii-vykorystovuvaty (дата звернення: 21.06.2021)
3. Що таке багатофакторна аутентифікація? URL: https://hideez.com/uk/blogs/news/what-is-multifactor-authentication-advantages-and-limitations-hideez (дата звернення: 21.06.2021)
4. Парольна аутентифікація URL : https://sites.google.com/site/identifikaciataautentifikacia/ponatta-pro-autentifikaciu/parolna-autentifikacia (дата звернення: 21.06.2021)
5. Чи можуть хакери викрасти ваш відбиток пальця – недоліки біометричної автентифікації. Malware Protection & Internet Security | ESET. URL: https://www.eset.com/ua/about/newsroom/blog/data-protection/mogut-li-khakery-pokhitit-vash-otpechatok-paltsa-nedostatki-biometricheskoy-autentifikatsii/ (дата звернення: 21.06.2021)
6. Дослідження методів багатофакторної автентифікації та їх практичного застосування URL : https://openarchive.nure.ua/server/api/core/bitstreams/087ebf7e-8e83-42d0-b50d-5f69b199a764/content (дата звернення: 21.06.2021)
7. Учасники проектів Вікімедіа. Баєсова мережа – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Баєсова_мережа (дата звернення: 21.06.2021)
8. Учасники проектів Вікімедіа. Машинне навчання – Вікіпедія.URL: https://uk.wikipedia.org/wiki/Машинне_навчання (дата звернення: 21.06.2021)

ДОДАТКИ

58

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ
БАКАЛАВРСЬКОЇ ДИПЛОМНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Засіб багатофакторної автентифікації користувачів
Автор роботи: Качай Роман Володимирович
Тип роботи: бакалаврська дипломна робота .
Підрозділ кафедра захисту інформації ФІТКІ .

Показники звіту подібності Unicheck

Оригінальність – 83.4%. Схожість – 16.4%.
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 _____ Каплун В. А.
(підпис) (прізвище, ініціали)

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

Автор роботи _____ Качай Р. В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Дудатьєв А. В.
(підпис) (прізвище, ініціали)

Додаток В

Код програми

Index.html

```
<!DOCTYPE html>
<html>
<head>
  <title>Автентифікація з використанням біометрії</title>
  <style>
    .hidden {
      display: none;
    }
  </style>
</head>
<body>
  <h1>Автентифікація з використанням біометрії</h1>

  <div id="login-container">
    <h2>Логін</h2>
    <form id="login-form">
      <input type="text" id="username-input"
placeholder="Ім'я користувача" required>
      <input type="password" id="password-input"
placeholder="Пароль" required>
      <button type="submit">Увійти</button>
    </form>
  </div>

  <div id="biometric-container" class="hidden">
    <h2>Біометрична автентифікація</h2>
    <button id="biometric-button">Автентифікація за
допомогою біометрії</button>
  </div>

  <script>
```

```
    const loginForm = document.getElementById('login-
form');
    const usernameInput =
document.getElementById('username-input');
    const passwordInput =
document.getElementById('password-input');
    const biometricContainer =
document.getElementById('biometric-container');
    const biometricButton =
document.getElementById('biometric-button');
    loginForm.addEventListener('submit', e => {
      e.preventDefault();

      const username = usernameInput.value;
      const password = passwordInput.value;
      if (isValidUser(username, password)) {
        showBiometricAuth();
      } else {
        showErrorMessage('Invalid credentials');
      }
    });
    function isValidUser(username, password) {
      if (username === 'admin' && password === 'password')
{
        return true;
      } else {
        alert("Не правильно введений логін або пароль")
        return false;
      }
    }

    function showBiometricAuth() {
      if (isBiometricAuthAvailable()) {
        biometricContainer.classList.remove('hidden');
      } else {
```

```
        showSuccessMessage('Authentication successful');
      }
    }

    function isBiometricAuthAvailable() {
      if (window.PasswordCredential &&
window.PublicKeyCredential) {
        return true;
      } else {
        return false;
      }
    }

    biometricButton.addEventListener('click', () => {
      simulateBiometricAuth()
        .then(() => {
          showSuccessMessage('Authentication successful');
        })
        .catch(error => {
          showErrorMessage('Biometric authentication
failed: ' + error);
        });
    });

    function simulateBiometricAuth() {
      return new Promise((resolve, reject) => {
        setTimeout(() => {
        alert("Автентифікація пройшла успішно")
          resolve();
        }, 2000);
      });
    }

    function showSuccessMessage(message) {
      alert(message);
```

```
    }

    function showErrorMessage(message) {
      console.error(message);
      alert('Помилка: ' + message);
    }
  </script>
</body>
</html>
```

63

ІЛЮСТРАТИВНА ЧАСТИНА

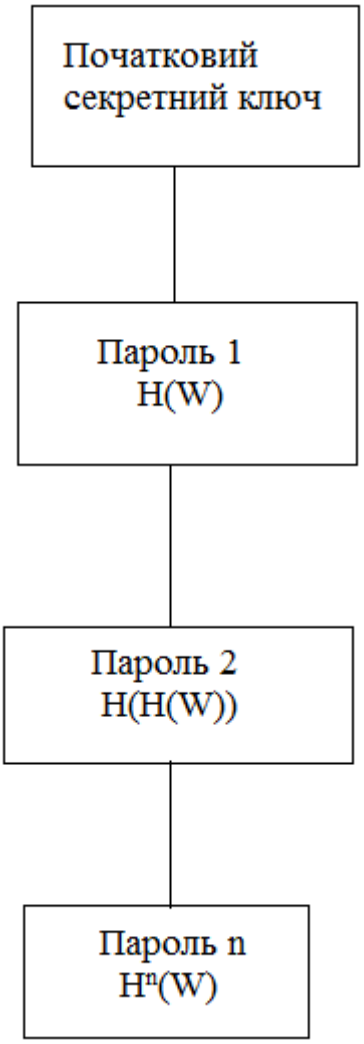
Засіб попередження фішингових атак на основі гейміфікації

(Назва бакалаврської кваліфікаційної роботи)

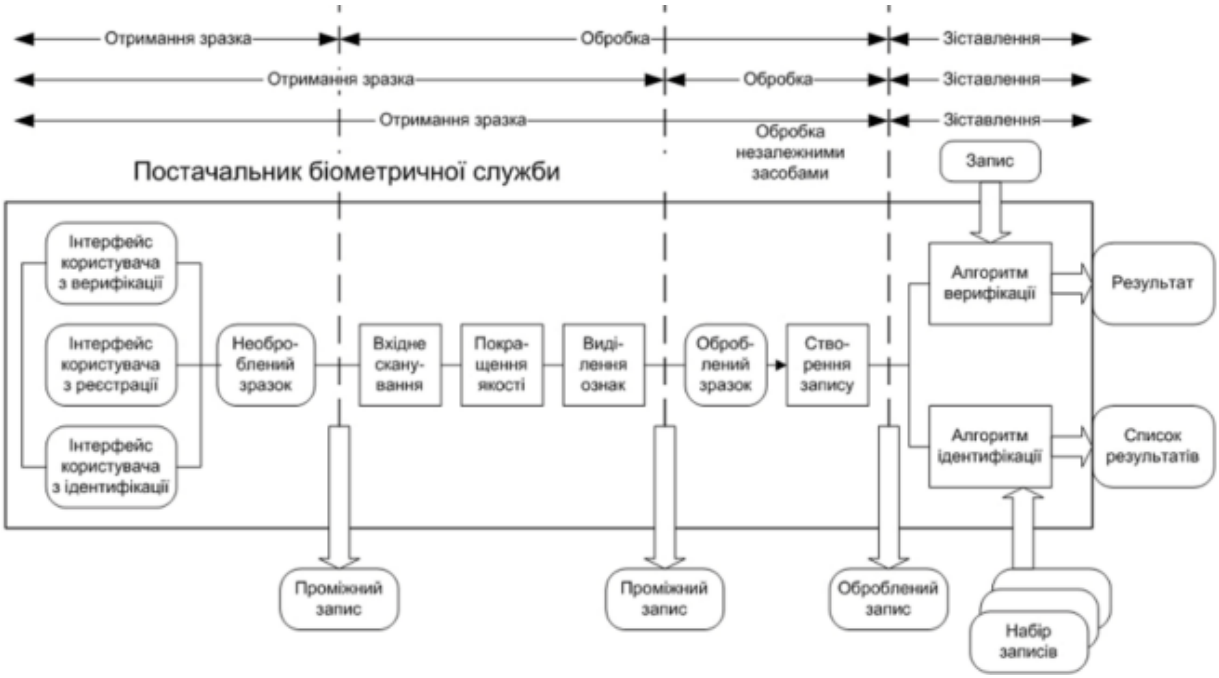
Виконав: студент 4 курсу групи 1БС-19б
спеціальності 125 Кібербезпека
_____ Роман КАЧАЙ
19 червня 2023 р.

Керівник: к. т. н., доцент каф. ЗІ
_____ Андрій ДУДАТЬЄВ
19 червня 2023 р.

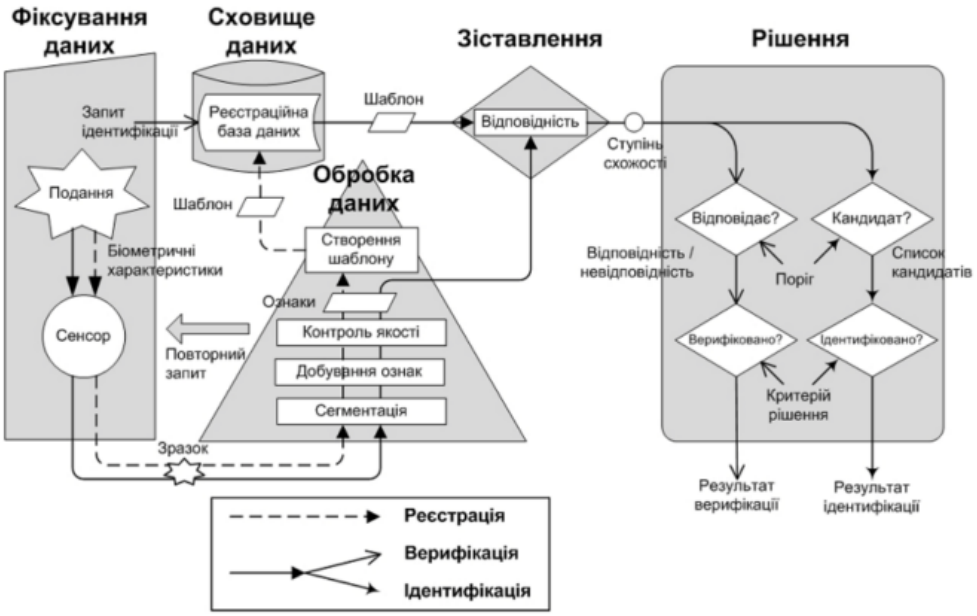
Стуруктура парольної автентифікації



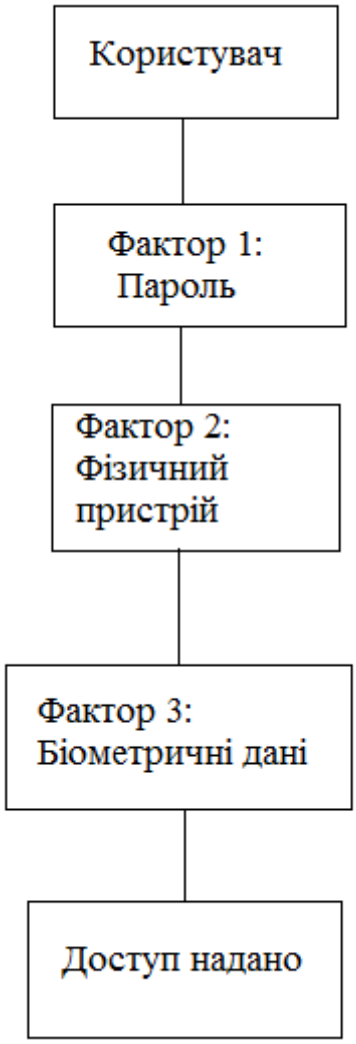
Архітектурна реалізація базової моделі біометричної системи



Концептульна схема базової моделі узагальної біометричної систему

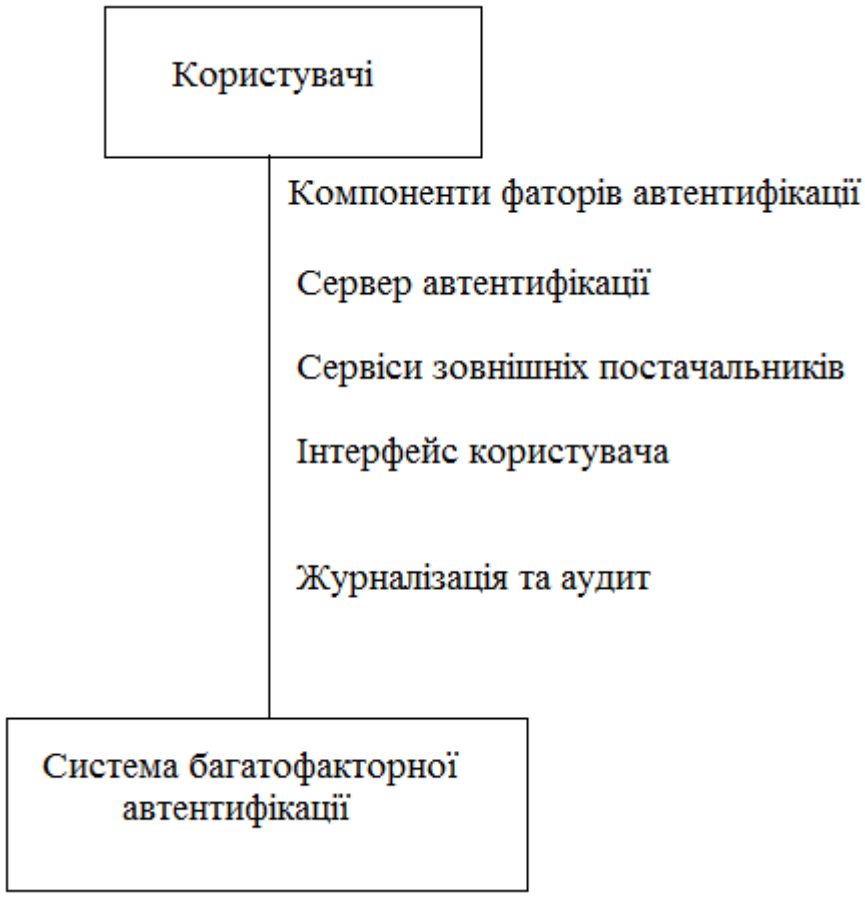


Блок-діаграма

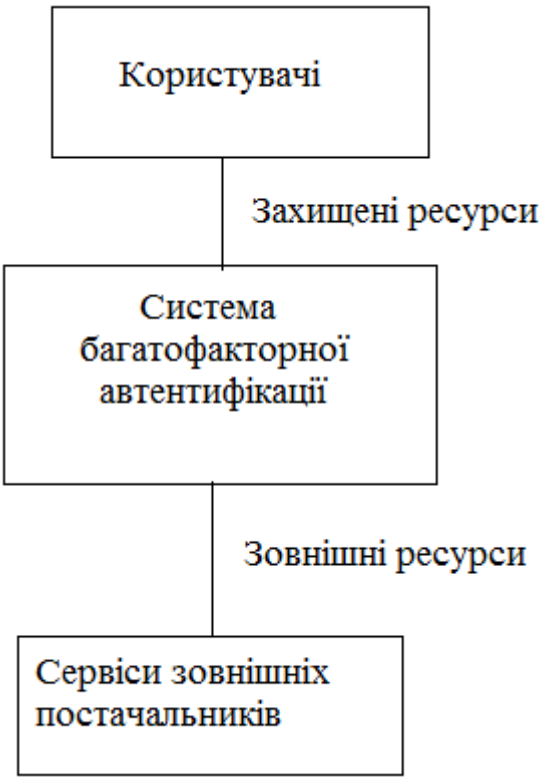


-

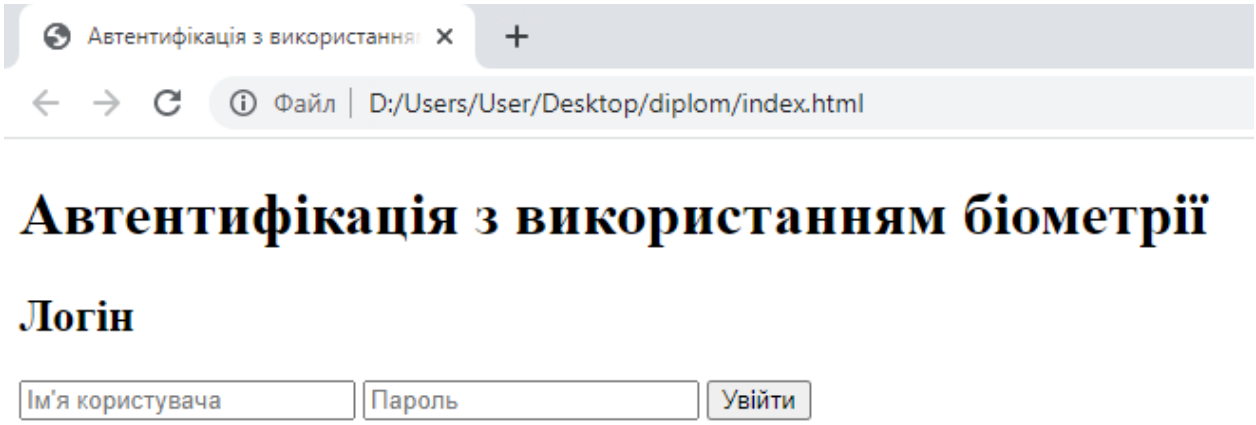
Діаграма-компонент

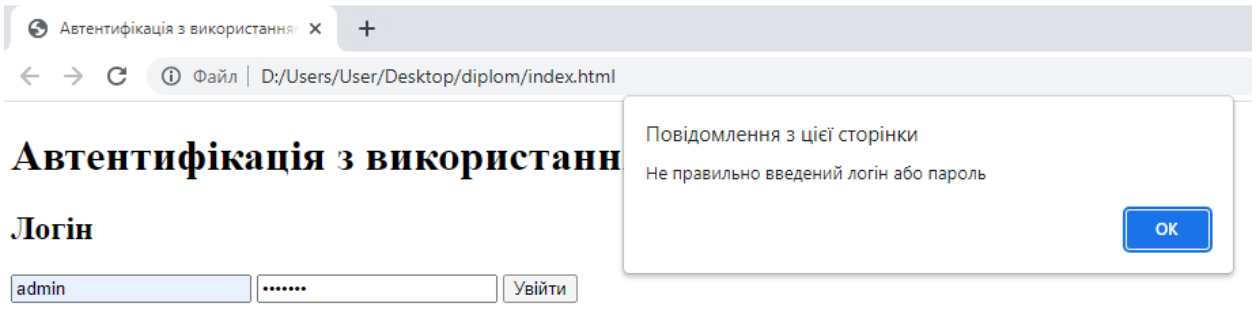


Контестна діаграма



Робота програми





Робота програми