МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Західноукраїнський національний університет

Факультет комп’ютерних інформаційних технологій

Кафедра кібербезпеки

БОДНАРУК Володимир Богданович

Система контролю доступу на основі двофакторної автентифікації / Access control system based on two-factor authentication

спеціальність 125 Кібербезпека

освітньо-професійна програма - Кібербезпека

кваліфікаційна робота

Виконав студент групи КБм-21

В.Б. Боднарук

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Науковий керівник:

д.т.н., професор В.В. Яцків

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кваліфікаційну роботу

допущено до захисту

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ р.

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_В.В. Яцків

підпис

Тернопіль – 2021

АНОТАЦІЯ

Кваліфікаційна робота на тему «Система контролю доступу на основі двофакторної автентифікації» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека» освітньо-професійної програми «Кібербезпека» написана обсягом \_\_\_ сторінки і містить 14 ілюстрації, 3 таблиця, 2 додатки та 21 джерело за переліком посилань.

Метою кваліфікаційної роботи є підвищення ефективності системи контролю доступу на основі використання двофакторної автентифікації.

Методи досліджень. Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: методи автентифікації користувачів, методи контролю доступу, методи проектування.

Результати дослідження: удосконалено алгоритми автентифікації користувачів в системах контролю доступу за рахунок використання двох факторів автентифікації.

Розроблено структуру системи контролю доступу з реалізацією на одноплатному комп’ютері Raspberry Pi та використанням двох факторів автентифікації.

Результати роботи можуть успішно застосовуватися при реалізації систем контролю доступу на основі біометричної автентифікації.

Ключові слова: СИСТЕМА КОНТРОЛЮ ДОСТУПУ, ФАКТОРИ АВТЕНТИФІКАЦІЇ, БІОМЕТРИЧНА АВТЕНТИФІКАЦІЯ, ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ.

ABSTRACT

Qualification work on "Access control system based on two-factor authentication" for the degree of "Master" in the specialty 125 "Cybersecurity" educational and professional program "Cybersecurity" is written in \_\_\_ pages and contains 14 illustrations, 3 tables, 2 appendices and 21 source according to the list of links.

The purpose of the qualification work is to increase the efficiency of the access control system based on the use of two-factor authentication.

Research methods. To solve the tasks in this qualification work used: methods of user authentication, access control methods, design methods.

Research results: algorithms for user authentication in access control systems have been improved through the use of two authentication factors.

The structure of the access control system with the implementation on a single-board computer Raspberry Pi and the use of two authentication factors has been developed.

The results of the work can be successfully applied in the implementation of access control systems based on biometric authentication.

Keywords: ACCESS CONTROL SYSTEM, AUTHENTICATION FACTORS, BIOMETRIC AUTHENTICATION, TWO-FACTOR AUTHENTICATION

ЗМІСТ

Вступ 7

1 Аналіз підходів до автентифікації в системах контролю доступу 9

1.1 Фактори автентифікації 9

1.2 Двофакторна автентифікація 10

1.3 Двофакторна біометрична автентифікація 15

1.4 Вибір методу автентифікації 19

1.5 Переваги двофакторної автентифікації 22

2 Концепції доступу до системи 24

2.1 Методи доступу до системи 24

2.2 Модель електронної автентифікації користувача30

2.3 Алгоритм роботи системи біометричної автентифікації 33

2.4 Загрози безпеки біометричній автентифікації 35

2.5 Параметри систем контролю доступу 38

3 Структура та опис функціонування системи контролю доступу 41

3.1 Загальна структура системи контролю доступу на основі

двофакторної автентифікації 41

3.2 Алгоритм розпізнавання відбитку пальців 44

3.3 Підключення та налаштування сканера відбитків пальців 46

3.4 Підключення модуля NFC PN532 до Raspberry Pi 50

Висновки 56

Список використаних джерел 57

Додатки 58

ВСТУП

На сьогоднішній день цифровізація досягає значних успіхів у всіх сторонах сучасного суспільства. Автентифікація є одним із засобів забезпечення безпеки цього процесу. Він стосується багатьох різних областей підключеного світу, включаючи платежі, комунікації та керування правами доступу.

Постійне зростання кількості розумних пристроїв і пов’язаних з ними навантаження на підключення вплинуло на мобільні послуги, які безперешкодно пропонуються в усьому світі. У такому зв’язаному світі засобом, що забезпечує безпеку переданих даних, є, в першу чергу, автентифікація. Відповідно до роботи в [1], автентифікація – це процес, коли «користувач ідентифікує себе, надсилаючи x до системи; система автентифікує його особу, обчислюючи F(x) і перевіряючи, чи воно дорівнює збереженому значенню y”. Це визначення істотно не змінилося з часом, незважаючи на той факт, що простий пароль більше не є єдиним фактором для перевірки користувача з точки зору інформаційних технологій. Автентифікація залишається основним захистом від незаконного доступу до пристрою або будь-якої іншої конфіденційної програми, незалежно від мережі чи онлайн. Колись трансакції підтверджувалися насамперед фізичною присутністю, тобто, наприклад, накладенням сургучної печатки [2]. На даний час та з розвитком цифрових послуг стало зрозуміло, що перевірка лише на основі ідентифікації відправника не завжди є адекватною у глобальному масштабі. Спочатку для автентифікації суб’єкта використовувався лише один фактор. До того часу однофакторна автентифікація була в основному прийнята спільнотою через її простоту та зручність для користувачів. Як приклад можна розглянути використання пароля (або PIN-коду) для підтвердження права власності на ідентифікатор користувача. При цьому, це найслабший рівень автентифікації. Подаючи пароль, можна негайно зламати обліковий запис. Крім того, неавторизований користувач також може спробувати отримати доступ, використовуючи атаку на словник, райдужну таблицю або методи соціальної інженерії [3]. Зазвичай, при використанні цього типу автентифікації необхідно враховувати мінімальну вимогу щодо складності пароля. Крім того, було зрозуміло, що автентифікація лише з одним фактором не є надійною для забезпечення належного захисту через низку загроз безпеці. Як інтуїтивно зрозумілий крок вперед, була запропонована двофакторна автентифікація (2FA), яка поєднує (комбінація імені користувача/паролю) з фактором особистої власності, таким як смарт-карта або телефон.

Згодом багатофакторна автентифікація (MFA) була запропонована для забезпечення більш високого рівня безпеки та полегшення безперервного захисту комп’ютерних пристроїв, а також інших критично важливих служб від несанкціонованого доступу за допомогою використання більш ніж двох категорій облікових даних. Здебільшого MFA базується на біометрії, яка є автоматизованим розпізнаванням індивідів на основі їх поведінкових та біологічних характеристик. Цей крок запропонував покращений рівень безпеки, оскільки від користувачів вимагалося надати докази своєї особистості, що залежить від двох або більше різних факторів.

Агентство з кібербезпеки та безпеки інфраструктури (CISA) вже давно рекомендує використовувати багатофакторну автентифікацію (MFA) замість паролів для захисту вашої присутності в Інтернеті. Використання MFA рекомендується не тільки банками, які використовують PIN-коди для захисту входу, а й у нашому повсякденному житті.

**Мета і завдання дослідження.** Метою роботи є підвищення ефективності системи контролю доступу на основі використання двофакторної автентифікації.

Досягнення визначеної мети передбачає вирішення таких завдань:

– провести аналіз відомих факторів автентифікації;

– виділити переваги двофакторна автентифікації та біометричної автентифікації;

– дослідити методи доступу до системи;

– модель електронної автентифікації користувача;

– розробити алгоритм роботи системи біометричної автентифікації;

– провести аналіз загроз безпеки біометричній автентифікації;

– розробити загальну структура системи контролю доступу на основі двофакторної автентифікації;

– розробити алгоритм розпізнавання відбитку пальців;

– розробити систему контролю доступу на основі двофакторної автентифікації.

**Об’єкт дослідження** –процеси автентифікації користувачів в системах контролю доступу;

**Предмет дослідження –** алгоритми автентифікації користувачів в системах контролю доступу.

**Методи досліджень.** Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: методи автентифікації користувачів, методи контролю доступу, методи проектування.

**Наукова новизна одержаних результатів.** Удосконалено алгоритми автентифікації користувачів в системах контролю доступу за рахунок використання двох факторів автентифікації.

**Практичне значення отриманих результатів.** Розроблено структуру системи контролю доступу з реалізацією на одноплатному комп’ютері Raspberry Pi та використанням двох факторів автентифікації.

**Публікації та апробація КР**.

1. Цаволик Т.Г., Боднарук В.Б.Системи контролю доступу на основі двофакторної автентифікації. Матеріали наукової конференції «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ - 2021), Тернопіль, 2021. - С.

2. Цаволик Т.Г., Боднарук В.Б.Загрози безпеки для біометричної системи автентифікації. Матеріали наукової конференції «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ - 2021), Тернопіль, 2021, С.

1 АНАЛІЗ ПІДХОДІВ ДО АВТЕНТИФІКАЦІЇ В СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ

1.1 Фактори автентифікації

Фактор автентифікації належить до категорії облікових даних, що використовуються для підтвердження особистості та авторизації користувача, перш ніж цей користувач зможе отримати доступ до свого облікового запису, надіслати повідомлення або запитати інформацію із захищеної мережі, системи чи програми. Широко використовуються три загальні фактори автентифікації: 1) те, що ви є, 2) те, що ви знаєте, 3) те, що ви маєте [4].

1. Те, що ви є. Цей тип включає біометричні методи, такі як відбитки пальців, сканування сітківки або обличчя, аналіз почерку або розпізнавання мови. Більшість сучасних смартфонів використовують розпізнавання обличчя, ноутбуки часто використовують зчитувачі відбитків пальців, і вас навіть можуть попросити ввести відбиток руки, коли купуєте абонемент у парк розваг. Хоча цей тип автентифікації забезпечує найнадійнішу автентифікацію серед будь-яких двофакторних методів автентифікації, він не є ідеальним. Кожен, хто коли-небудь володів пристроєм, який може сканувати обличчя або відбитки пальців, відчував розчарування через те, що iPhone не розпізнає їх обличчя або відбитки пальців і не приймає їх.

2. Те, що ви знаєте. Це, можливо, найпоширеніший фактор, який використовується при двофакторній автентифікації. Зазвичай це пароль або персональний ідентифікаційний номер (PIN). На жаль, ці фактори автентифікації також є найбільш вразливими до атак безпеки. Багато людей використовують однакові паролі для різних облікових записів, і якщо навіть один обліковий запис зламано, це означає, що всі інші облікові запису також зламано.

3) Те, що у вас є. Цей фактор зазвичай контролюється пристроєм, який, як відомо, є у законного користувача (наприклад смартфон). Спочатку користувач реєструє обліковий запис з адресою електронної пошти та паролем, а потім записує свій номер телефону. Потім користувач входить у свій обліковий запис за допомогою цієї адреси електронної пошти та пароля, після чого одноразовий пароль надсилається на номер мобільного телефону користувача. Як тільки користувач вводить це на своєму пристрої, він отримує доступ до свого облікового запису та системи.

1.2 Двофакторна автентифікація

Двофакторна автентифікація (2FA)  - даний метод безпеки вимагає від користувачів вказати два різні фактори автентифікації, щоб підтвердити свою особу та отримати доступ до свого облікового запису. Цей процес забезпечує кращий захист особистої інформації користувача, облікових даних та інших ресурсів, одночасно покращуючи безпеку ресурсів, до яких користувач може отримати доступ. Звичайно, двофакторна автентифікація пропонує вищий рівень безпеки, ніж методи автентифікації, які покладаються лише на один фактор автентифікації (однофакторна автентифікація), у якому користувач вказує лише один фактор (зазвичай пароль або PIN-код) [5].

Метод 2FA вимагає від користувача ввести не просто пароль або PIN-код, а й другий фактор, починаючи від біометричного фактора (обличчя, сітківки ока або сканування відбитків пальців) до фактора володіння (унікальний код, надісланий на смартфон). Цей додатковий рівень безпеки означає, що навіть якщо зловмисник знає пароль користувача, він не зможе отримати доступ до свого облікового запису в Інтернеті або мобільного пристрою. Насправді, двофакторна автентифікація вже давно використовується для контролю, хто може отримати доступ до конфіденційних даних і систем, і фахівці з безпеки наполягають на тому, щоб увімкнути двофакторну автентифікацію на всіх онлайн-облікових записах, комп’ютерах і мобільних пристроях.

Двофакторна автентифікація (2FA) відноситься до методу безпеки, який використовується для захисту облікових записів і систем від несанкціонованого доступу шляхом запиту потенційних користувачів підтвердити свою особу. Двофакторну автентифікацію можна використовувати для забезпечення безпеки телефону, облікового запису в Інтернеті або навіть дверей. Вона працює, запитуючи у користувача два типи інформації: першим фактором зазвичай є пароль або персональний ідентифікаційний номер (PIN), а другий фактор може бути відбитком пальця або одноразовим кодом, надісланим на ваш телефон. Хоча двофакторна автентифікація покращує безпеку, вона не є повністю надійною .

Двоетапна перевірка проти двофакторної автентифікації. Хоча ми часто використовуємо двофакторну автентифікацію і двоетапну перевірку як взаємозамінні і, здається, які значно перетинаються, вони не зовсім однакові. Apple розрізняє двоетапну перевірку та 2FA, вказуючи на двоетапну перевірку як на старіший і нижчий метод безпеки, який вимагає від користувача ввести як пароль, так і одноразовий код, надісланий на їхній iPhone або інший надійний пристрій. Хоча це одна з його форм, двофакторна автентифікація також охоплює методи автентифікації, які є на сучасних iPhone, оснащених технологією сканування обличчя, і Macbook, доступ до яких можна отримати після сканування відбитків пальців.

Двофакторний код автентифікації. Двофакторний код автентифікації - це унікальний код, який створюється для підтвердження особи користувача під час спроби отримати доступ до облікового запису або системи в Інтернеті. Код буде надіслано за допомогою SMS або за допомогою автоматичного дзвінка на номер телефону, призначений користувачеві. Після введення двофакторного коду автентифікації користувач отримує доступ до свого облікового запису в мережі. Ці коди часто закінчуються через короткий період часу, якщо вони не використовуються.

Типи двофакторної автентифікації. Існує кілька основних типів 2FA, які зазвичай використовуються, і варто знати відмінності та відповідні переваги та недоліки різних методів. Двофакторна автентифікація працює, додаючи ще один рівень безпеки до онлайн-облікових записів і систем. 2FA вимагає, щоб кожен користувач, який намагається ввійти, мав свій перший фактор автентифікації - пароль або особистий ідентифікаційний номер - пов'язаний з другим фактором, який зазвичай є тим, що ви знаєте, маєте або є. З 2FA користувачі повинні вказати обидва фактори, щоб отримати доступ до своїх облікових записів або системи. Якщо 2FA реалізовано правильно, хакери не зможуть отримати доступ до вашого облікового запису лише за допомогою вкрадених паролів та облікових даних. Хоча це не зовсім непроникно, оскільки хакери придумали деякі обхідні шляхи, 2FA, безумовно, пропонує набагато більше безпеки, ніж просто вимога імені користувача або адреси електронної пошти та пароля.

Оскільки двофакторна автентифікація набуває все більшого визнання як абсолютна безпека, як для окремих осіб, так і для компаній, необхідно розглянути найпоширеніші типи 2FA. SMS-повідомлення та голосова 2FA. Завдяки текстовим SMS-повідомленням і голосовій двофакторній автентифікації користувачі вказують номери телефонів під час реєстрації, а коли їм потрібно увійти в обліковий запис, генерується одноразовий код, який надсилається на номер телефону, на який вони зареєстровані (через SMS або автоматичний дзвінок). Кожен, хто заходить в Інтернет, знає, що це дуже популярний варіант, оскільки він простий у використанні і не вимагає спеціального обладнання. Хоча будь-яка форма 2FA краще, ніж нічого, експерти з безпеки все частіше застерігають від цієї форми 2FA. Рівень безпеки не такий високий, як у інших форм 2FA, оскільки існує безліч обхідних шляхів, які хакери можуть використовувати, щоб поставити під загрозу безпеку вашого облікового запису. Наприклад, зловмисники можуть обманом змусити користувачів встановити шкідливий додаток на їхній телефон, який потім зможе читати та пересилати текстові повідомлення. Інший варіант, експлойт - зламати стільниковий сервіс для перенаправлення SMS-повідомлень за допомогою різних технічних методів або соціальної інженерії. Інші недоліки. Деякі люди мають занепокоєння щодо надання свого номера телефону веб-сайту, програмі чи платформі. І їх занепокоєння легко зрозуміти, оскільки багато компаній неправильно використовували цю інформацію з такими речами, як цільова реклама та відстеження конверсій. А скидання паролів на основі номера телефону, наданого для 2FA, може бути серйозною проблемою безпеки паролів, оскільки зловмисники, які захоплюють номери телефонів, можуть отримати доступ до вашого облікового запису, навіть якщо вони не знають вашого пароля. SMS 2FA також не працюватиме, якщо ваш телефон не працює або не може підключитися до стільникової мережі. Це може бути великою проблемою для тих, хто подорожує за кордон.

Push-повідомлення для 2FA. Кожен, хто глибоко занурюється в екосистему Apple, знає цей тип двофакторної автентифікації завдяки методу Apple Trusted Devices. Цей метод надсилає запит на різні пристрої користувача, коли робиться спроба ввійти під ім’ям цього користувача. Підказка містить приблизне місце входу на основі IP-адреси. У таких системах, як цей метод Trusted Devices, користувач може вирішити, схвалити чи відхилити спробу входу. Однак для того, щоб надійні пристрої та інші системи push-повідомлень працювали (ще одним прикладом є Duo Push), вашому пристрою потрібне підключення до Інтернету або даних. Цей метод трохи зручніше, ніж мати справу з QR-кодами. Оскільки ці сповіщення зазвичай вказують на приблизне місце спроби входу – і оскільки дуже мало фішингових атак відбувається з тієї ж IP-адреси, що й жертва, – цей метод може допомогти вам виявити триваючу фішингову атаку.

### Програмний маркер для 2FA / TOTP 2FA.Ця форма 2FA вимагає від користувача спершу завантажити та встановити програму двофакторної автентифікації на своєму телефоні або робочому комп’ютері. На будь-якому сайті, сумісному з програмою для автентифікації, користувачі можуть спочатку ввести ім’я користувача та пароль, перш ніж перейти до програми автентифікації, щоб отримати згенерований програмним забезпеченням одноразовий пароль (також називається TOTP або програмний маркер), який ви необхідно завершити спробу входу. Популярними прикладами є Google Authenticator, Microsoft Authenticator, Duo Mobile від Duo Security і FreeOTP. Основна технологія цього типу 2FA називається одноразовим паролем на основі часу (TOTP). Коли сайт пропонує цей тип 2FA, буде відображатися QR-код, який містить секретний ключ. Ви можете відсканувати цей QR-код у своїй програмі. Код можна сканувати кілька разів і зберігати в безпечному місці або роздрукувати. Після сканування QR-коду ваша програма генеруватиме новий шестизначний код кожні 30 секунд, і вам знадобиться один із цих кодів разом із вашим іменем користувача та паролем для входу. Перевага цієї двофакторної автентифікації полягає в тому, що вам не потрібно підключатися до стільникової мережі. Якщо хакер перенаправляє ваш номер телефону на свій телефон, він все одно не має ваших QR-кодів. Недоліком, однак, є те, що при частому вході на різних пристроях може бути незручно розблокувати телефон, відкривати програму та щоразу вводити код.

Апаратний маркер для 2FA. Апаратні токени, можливо, найстаріша форма 2FA, генерують новий числовий код через регулярні проміжки часу. Коли користувач хоче отримати доступ до облікового запису, все, що йому потрібно зробити, це перевірити пристрій – зазвичай це брелок невеликого розміру – і ввести код 2FA, який відображається на веб-сайті або в додатку. Інші версії цієї технології 2FA можуть автоматично передавати двофакторний код автентифікації, коли ви підключаєте ключ безпеки до порту USB. Як правило, апаратна двофакторна автентифікація частіше використовується компаніями, але її також можна реалізувати на персональних комп’ютерах. Великі технологічні та фінансові компанії створюють стандарт під назвою U2F, і тепер можна використовувати фізичний апаратний токен U2F для захисту облікових записів Dropbox, Google і GitHub. Це просто невеликий USB-ключ, який закріплюється на брелку. Якщо ви хочете увійти в обліковий запис з нового комп’ютера, вставте USB-накопичувач і натисніть на ньому кнопку. В майбутньому ці пристрої повинні працювати з NFC і Bluetooth для зв’язку з мобільними пристроями без USB-портів. Переваги цього методу в тому, що він безпечний і не вимагає підключення до Інтернету. Недолік? Налаштувати й обслуговувати його дорого, а обладнання можна втратити.

1.3 Двофакторна біометрична автентифікація

За останні два десятиліття двофакторна біометрична автентифікація перетворилася з того, що все ще здавалося фантастичною мрією, до надзвичайно поширеної. При біометричній верифікації користувач стає токеном. Обличчя, відбиток пальця, сітківка або голос користувача можуть стати маркером 2FA, необхідним для підтвердження його особистості та доступу до облікового запису. Скрізь є приклади. Останній iPhone оснащений технологією сканування обличчя, і більшість інших сучасних телефонів використовують цю функцію або сканування відбитків пальців для зручного та швидкого доступу для користувачів. Багатьом сучасним ноутбукам потрібно лише бачити відбиток пальця користувача, є багато інших пристроїв, які можуть підтвердити особу користувача, скануючи фізичні характеристики або голос. Це вважається найбезпечнішим методом 2FA і теоретично найпростішим у використанні, тому що він потрібен лише користувачу. Однак ці технології все ще вдосконалюються, і системи все ще іноді намагаються підтвердити, що має бути разом. Іншими недоліками є те, що при зберіганні біометричної інформації користувача можуть виникнути проблеми з конфіденційністю. А для цього способу потрібні спеціальні пристрої, такі як сканери та камери.

Інші форми 2FA. Іншим поширеним методом є 2FA через електронну пошту. Він працює шляхом надсилання автоматичного повідомлення на зареєстровану електронну адресу користувача під час спроби входу. Подібно до текстового повідомлення або телефонного дзвінка, цей електронний лист буде містити код або просто посилання, яке, натиснувши, підтверджує, що це законна спроба входу. Так само, як 2FA по телефону або SMS, це легко та інтуїтивно зрозуміло для користувачів, і воно працює як на комп’ютерах, так і на телефонах. Однак, на відміну від 2FA SMS і опцій телефону, користувач повинен бути підключений до Інтернету, щоб отримати свій код або активувати своє унікальне посилання. На жаль, це найнебезпечніша форма 2FA, тому її популярність зростає. Захист паролів є занадто поширеною проблемою, щоб бути ефективною. Незважаючи на багаторічні попередження, багато людей використовують ідентичні паролі для багатьох облікових записів і пристроїв, і, можливо, або навіть ймовірно, що їхні облікові дані для облікового запису, до якого вони намагаються отримати доступ, та їхня адреса електронної пошти збігаються. Є й інші проблеми. Є велика ймовірність того, що електронна пошта опиниться в папці зі спамом або непотрібною поштою, і якщо хакери мають правильний пароль для чиєсь онлайн-рахунку, велика ймовірність, що вони також отримають пароль своєї електронної пошти.

Використання 2FA. Безпека облікового запису має життєво важливе значення, тому більшість веб-сайтів, програм і пристроїв тепер пропонують певну форму двофакторної автентифікації, хоча отримання 2FA залежить від платформи, пристрою чи веб-сайту. Apple може провести вас через процес увімкнення двофакторної автентифікації для всіх своїх пристроїв, хоча цю функцію можна знайти в розділі «Пароль і безпека» у «Налаштуваннях» на iPhone або в «Системних налаштуваннях» на Mac. У Google, Facebook, Amazon, Twitter, Reddit та багатьох інших популярних веб-сайтах є посібники щодо того, як налаштувати двофакторну автентифікацію для вашого облікового запису.

Майбутнє двофакторної автентифікації. Хоча 2FA абсолютно підвищує безпеку загалом, майбутнє двофакторної автентифікації має ґрунтуватися на створенні ще більш безпечних систем, які позбавлені слабких місць, які все ще існують сьогодні.

Компрометація 2FA. У серпні 2019 року зламали обліковий запис генерального директора Twitter Джека Дорсі, і повідомлення, опубліковані на його акаунті, не були доброю рекламою їхньої системи безпеки 2FA. Через місяць з’явилися повідомлення, що, незважаючи на 2FA, 23 мільйони користувачів YouTube були зламані, оскільки хакери використовували інструментарій зворотного проксі для перехоплення двофакторних кодів автентифікації, надісланих через SMS. Криптовалютна біржа Binance скомпрометувала свою систему 2FA і втратила десятки мільйонів. Один з найпростіших і найпоширеніших способів зламати систему 2FA - це зробити заміну симулятора. У цьому сценарії хакер може використовувати ряд методів, щоб змінити номери телефонів жертв, щоб будь-які наступні повідомлення або дзвінки, наприклад, з кодом 2FA, перенаправлялися на новий телефон. Це одна з причин, чому експерти все частіше закликають відмовитися від систем 2FA на основі SMS і телефонних дзвінків. Відомо, що деякі системи двофакторної автентифікації скомпрометовані шкідливими програмами. Навіть програма автентифікації, яка так широко використовується, як Google Authenticator, не є ідеальною - у лютому 2020 року було виявлено зловмисне програмне забезпечення на базі Android, яке краде коди 2FA.

Зловмисне програмне забезпечення TrickBot – це ще один обхідний шлях для двофакторної автентифікації, який перехоплює одноразові коди, які використовуються банківськими додатками та надсилаються за допомогою SMS і push-повідомлень.

У сценаріях соціальної інженерії, наприклад, хакер може зв’язатися з об’єктом, який видає себе за банк, перш ніж спробувати підтвердити особу жертви, надавши щойно надісланий код безпеки.

З цих та інших причин багато експертів з безпеки вважають, що майбутнє 2FA полягає в розширенні біометричної безпеки. За дуже короткий час біометрична безпека перетворилася з футуристичної фантазії на всюдисущу частину нашого життя. У майбутньому біометрична 2FA має стати ще кращою, чутливішою та бездоганною. Двофакторні біометричні системи автентифікації виявилися менш безпомилковими. Як лише один приклад, були випадки, коли технологію розпізнавання облич обдурили 3D-рендерінг фотографій Facebook. Але оскільки біометрична 2FA поширена повсюдно, це також правда, що кожен, хто користувався нею, в якийсь момент стикався з помилково негативними і, можливо, навіть помилковими позитивними результатами. Помилкові спрацьовування трапляються, коли знайдено збіг, якого не існує, що найчастіше зустрічається при розпізнаванні обличчя. Помилково негативні результати виникають, коли збіг не знайдено, навіть якщо це правда. Це особливо дратує зі сканерами відбитків пальців, де найменша волога на пальці може мати руйнівні наслідки. Поступово розумні пристрої стають все більш досконалими, а біометрична автентифікація стає більш гладкою та швидшою. Камери мають все більш високу роздільну здатність, а також інфрачервоні технології в межах видимості. Також, необхідно більше уваги приділяти скануванню райдужної оболонки ока, яке вважається однією з найбільш безпечних форм автентифікації особи.

Багатофакторна автентифікація та бази даних. В майбутньому, ймовірно, буде зосереджено більше уваги на багатофакторній автентифікації. Комбінація трьох (або більше) рівнів автентифікації з певною формою біометричних даних забезпечить надійний рівень безпеки, якого не може забезпечити проста 2FA. Організації, де системи містять конфіденційну інформацію, швидше за все, вже використовують багатофакторну автентифікацію, а інші впровадять її незабаром. Те, як ці компанії зберігають цю інформацію, є ще однією областю, яка, ймовірно, буде розвиватися з часом. Багато експертів з безпеки вважають, що будь-який метод автентифікації на основі пристрою в кінцевому підсумку є недостатнім. Натомість вони рекомендують компаніям розглянути можливість безпечного зберігання та автентифікації ідентифікаційних даних у централізованій базі даних. Для багатьох компаній це може бути ще неможливим, але зростання біометричної автентифікації показало, як швидко ці технології можуть розвиватися і стати значною частиною нашого повсякденного життя.

1.4 Вибір методу автентифікації

SP 800-63B визначає дев'ять різних типів автентифікації, які можна використовувати окремо або в комбінації для створення методу автентифікації. [16]:

1) збережений секрет: пароль або PIN-код;

2) секрет пошуку: фізичний або електронний запис, у якому зберігається набір секретів, якими ділиться заявник і CSP. Заявник використовує автентифікатор для пошуку відповідного(их) секрету(ів), необхідних для відповіді на запит від верифікатора. Це схоже за концепцією на одноразову прокладку;

3) Позадіапазонний пристрій: фізичний пристрій, який однозначно адресований і може безпечно спілкуватися з верифікатором через окремий канал зв'язку, який називається вторинним каналом. Пристрій володіє і контролює заявник і підтримує приватний зв’язок через цей вторинний канал, окремий від основного каналу для електронної автентифікації;

4) однофакторний пристрій OTP: одноразовий пароль, який використовується як єдиний фактор для автентифікації. Описано в розділі 10.4;

5) багатофакторний OTP-пристрій: пристрій, подібний до однофакторного однофакторного пристрою, за винятком того, що для отримання одноразового пароля для отримання одноразового пароля потрібно ввести запам'ятований секрет або використовувати біометричні дані;

6) однофакторне криптографічне програмне забезпечення: криптографічний ключ, що зберігається на диску або іншому програмному носії. Автентифікація здійснюється шляхом підтвердження володіння та контролю ключа. Вихід автентифікатора сильно залежить від конкретного криптографічного протоколу, але, як правило, це певний тип підписаного повідомлення з використанням криптографії з відкритим ключем;

7) однофакторний криптографічний пристрій: апаратний пристрій, який виконує криптографічні операції з використанням захищених криптографічних ключів і забезпечує вихід автентифікатора через пряме підключення до кінцевої точки користувача. Пристрій використовує вбудовані симетричні або асиметричні криптографічні ключі і не вимагає активації за допомогою другого фактора автентифікації. Автентифікація здійснюється шляхом підтвердження володіння пристроєм за допомогою протоколу автентифікації;

8) багатофакторне криптографічне програмне забезпечення: програмне забезпечення, подібне до однофакторного криптографічного програмного забезпечення, але для активації якого потрібен другий фактор автентифікації;

9) багатофакторний криптографічний пристрій: пристрій, схожий на однофакторний криптографічний пристрій, але для активації якого потрібен другий фактор автентифікації.

Рівні гарантії автентифікатора. NIST SP 800-63 надає корисний спосіб характеристики ризику системи аутентифікації, використовуючи концепцію рівня автентифікації (КРА). Вищий КРА означає, що зловмисник повинен мати кращі можливості та витрачати більше ресурсів, щоб успішно порушити процес автентифікації. NIST SP 800-63B визначає типи засобів контролю безпеки з точки зору факторів автентифікації, які відповідають трьом визначеним КРА. Таким чином, можна оцінити рівень ризику для різних рівнів ресурсів, призначених для контролю безпеки, і вирішити, які засоби контролю необхідні, щоб задовольнити вимоги організації щодо ризику для автентифікації в різних контекстах. Три КРА, від найнижчого до найвищого, є:

– КРА1: надає певну гарантію того, що заявник контролює автентифікатор, прив’язаний до облікового запису передплатника. КРА1 вимагає однофакторної або багатофакторної автентифікації з використанням широкого спектру доступних технологій автентифікації. Успішна автентифікація вимагає, щоб заявник підтвердив володіння автентифікатором і контроль над ним за допомогою безпечного протоколу автентифікації.

– КРА2: забезпечує високу впевненість у тому, що заявник контролює автентифікатор(и), прив’язаний до облікового запису передплатника. Доказ володіння та контролю над двома різними факторами автентифікації потрібні за допомогою безпечного протоколу(ів) автентифікації. Для КРА2 та КРА3 потрібні затверджені криптографічні методи.

– КРА3: КРА3 забезпечує дуже високу впевненість у тому, що заявник контролює автентифікатор, прив'язаний до облікового запису абонента. Автентифікація в КРА3 заснована на підтвердженні володіння ключем за допомогою криптографічного протоколу. Автентифікація КРА3 вимагає використання апаратного криптографічного автентифікатора та автентифікатора, який забезпечує стійкість верифікатора від імітації; один і той самий пристрій може задовольняти обидві ці вимоги. Щоб пройти автентифікацію в КРА3, заявники повинні довести володіння двома різними факторами автентифікації та контроль над ними за допомогою безпечного протоколу(ів) автентифікації. Потрібні схвалені криптографічні методи.

Після визначення рівня автентифікації вибір методу автентифікації складається з одного або комбінації перерахованих вище типів автентифікаторів. Для КРА1 будь-який з дев’яти типів може використовуватися сам по собі, що відображає той факт, що потрібно менше безпеки, ніж на вищих рівнях. Для КРА2 є два основних варіанти. Перший полягає у використанні апаратного або програмного забезпечення, яке поєднує два фактори автентифікації. По-друге, об’єднати пароль із однофакторним типом автентифікатора. Для КРА 3, щоб досягти високої впевненості, він повинен включати підтвердження володіння ключем за допомогою криптографічного протоколу плюс автентифікатор, який захищає від видавання себе за сутність верифікатора.

1.5 Переваги двофакторної автентифікації

Переваги двофакторної автентифікації полягають у тому, що вона забезпечує необхідний додатковий рівень захисту від атак і може підвищити безпеку систем, підприємств і звичайних людей. 2FA пропонує користувачам додатковий захист, оскільки ім’я користувача та пароль вже просто недостатні.

З одного боку, крадіжка особистих даних зростає із загрозливою швидкістю. У 2018 році дослідження Javelin Strategy & Research про шахрайство з ідентифікацією зросла на вісім відсотків до 17,1 мільйонів споживачів у США лише в 2017 році. Загальна вартість шахрайства досягла 17,3 млн доларів. Впровадження незалежної від пароля двофакторної автентифікації значно підвищує безпеку та знижує ризик викрадення особистих даних. Крім того, численні порушення даних, які ми спостерігали протягом останніх кількох років, створили ситуацію, коли мільйони людей несвідомо мають свою особисту інформацію (включаючи своє ім’я користувача та пароль) доступною для всіх. Крім того, багато людей використовують один і той самий пароль на кількох веб-сайтах, тому хакер може спробувати використовувати однакові облікові дані на різних веб-сайтах, доки не отримає той, який працює. У звіті Verizon про розслідування злому даних за 2017 рік було виявлено, що 81 відсоток порушень облікового запису можна простежити за паролями, які витікають таким чином, або паролями, які занадто слабкі та такі, що легко вгадати. Проте недостатньо людей прийняли 2FA. Наприклад, нещодавно Google оголосив, що менше 10 відсотків користувачів Gmail використовують доступні заходи безпеки 2FA для захисту своїх облікових записів.

Переваги впровадження 2FA для бізнесу очевидні - сьогодні ніхто не може дозволити собі нехтувати кібербезпекою. Двофакторна автентифікація також може допомогти зменшити витрати на ІТ. Скидання паролів є однією з найпоширеніших причин, чому люди звертаються до служби підтримки. Дослідження галузевої асоціації HDI показало, що більше третини заявок до служби підтримки включають скидання пароля.

Надійність двофакторної автентифікації. Хоча двофакторну автентифікацію можна зламати, шанси дуже невеликі, і 2FA, безумовно, є найкращим методом, коли мова йде про захист облікових записів і систем. Одним із способів зламати двофакторну автентифікацію є метод SMS - або, іншими словами, метод відправки одноразового коду на номер телефону користувача за допомогою SMS або автоматичного телефонного дзвінка. Були історії про те, що хакери обманювали постачальників послуг бездротового зв’язку, щоб вони вказали чужий номер телефону на власному телефоні. Хакери звертаються до операторів стільникового зв’язку, які видають себе за їх жертви, і вимагають нову SIM-карту з номером жертви. Тоді ви матимете доступ до будь-якого коду автентифікації, надісланого на цей номер телефону. Це відомо, як заміна SIM-картки і, ймовірно, є найпоширенішим способом обходу 2FA.

2 КОНЦЕПЦІЇ ДОСТУПУ ДО СИСТЕМИ

2.1 Методи доступу до системи

Методи доступу до системи поділяються на дві області та 10 категорій:

1. Управління доступом. Метою цієї області є обмеження доступу до бізнес-додатків, мобільних пристроїв, систем і мереж уповноваженим особам для певних бізнес-цілей шляхом надання їм відповідних авторизацій доступу, аутентифікованих за допомогою доступу, механізмів контролю (наприклад, пароль, маркер або контроль). біометричні механізми) і підлягають суворому процесу входу, перш ніж надаватимуться затверджені рівні доступу [11].

1.1. Контроль доступу: перелічує елементи, які повинні бути включені в політику контролю доступу, включаючи міркування щодо методів контролю доступу, обмежень на основі ролі або особистості особи та типів контролю

1.2. Права користувача: вказує на те, що використовується офіційний процес і документується, щоб дозволити особам отримати доступ до ресурсів.

1.3. Механізми контролю доступу: обговорює необхідність проведення оцінки ризику, визначення вимог контролю доступу, оцінки та вибору механізмів контролю доступу.

1.4. Механізми контролю доступу – Пароль: описує вказівки щодо створення, використання та керування паролями.

1.5. Механізми контролю доступу – маркер: описує вказівки щодо використання маркерів.

1.6. Механізми контролю доступу – Біометричні: окреслює вказівки щодо використання біометрії.

1.7. Процес реєстрації: визначає вказівки щодо процесу реєстрації.

2. Доступ клієнта. Метою цієї області є захист бізнес-програм, які надають клієнтам доступ, виконуючи оцінку інформаційних ризиків для визначення вимог інформаційної безпеки та вжиття заходів безпеки, що підтримуються узгодженими, затвердженими контрактами.

2.1. Угоди про доступ клієнтів: ця тема зосереджена на доступі фізичних осіб до бізнес-програм (наприклад, покупця, який замовляє товари на веб-сайті, користувачів онлайн-банкінгу або представників організації, яким надано доступ від імені компанії).

2.2. Контракти з клієнтами: надає детальну інформацію про рекомендований вміст для контрактів з клієнтами, щоб гарантувати, що клієнти за законом і контрактом зобов'язані захищати інформацію компанії, бізнес-додатки та системи, а також забезпечити дотримання зобов'язань компанії щодо безпеки.

2.3. Взаємовідносини з клієнтами: обговорює політику та процедури для захисту конфіденційної чи важливої інформації, що стосується компанії чи клієнта.

Доступ до системи - це можливість, яка обмежує доступ до бізнес -додатків, мобільних пристроїв, систем та мереж авторизованими особами для конкретних комерційних цілей.

Доступ до системи включає три різні функції [12].

1.Аутентифікація. Перевірка ідентичності користувача, процесу чи пристрою, часто як необхідна умова для надання доступу до ресурсів в інформаційній системі. Цю функцію часто називають автентифікацією користувача, щоб відрізнити її від автентифікації повідомлень або автентифікації даних.

2. Авторизація. У контексті доступу до системи авторизація - це надання доступу або інших прав користувачеві, програмі чи процесу доступу до системних ресурсів. Авторизація визначає, що особа або програма може зробити після успішної автентифікації.

3. Контроль доступу. Процес надання або відхилення конкретних запитів щодо доступу та використання інформації та відповідних служб обробки інформації та входу до певних фізичних приміщень. Контроль доступу забезпечує авторизацію та обмеження доступу до активів на основі вимог бізнесу та безпеки. Три функції показані на рисунку 2.1.

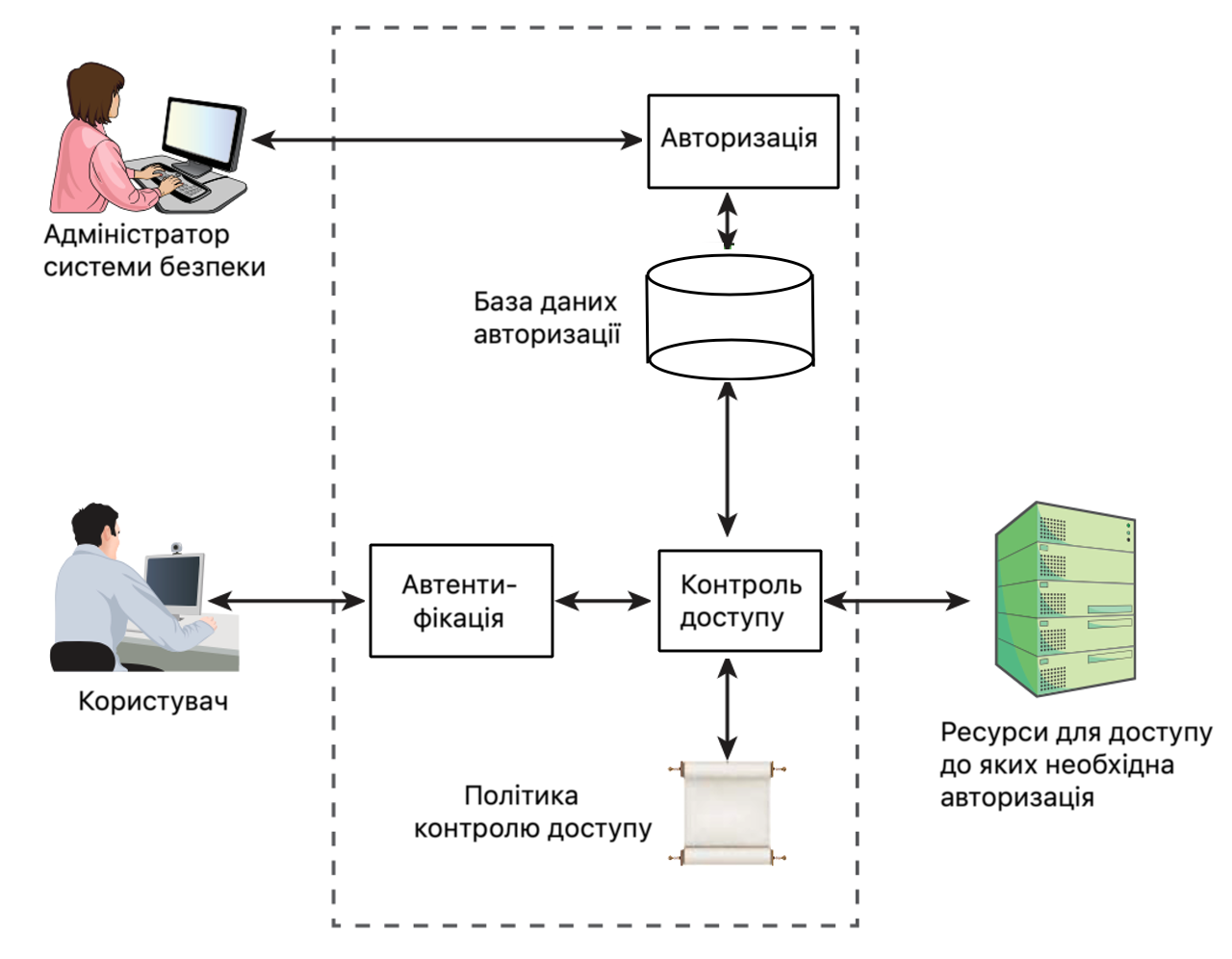


Рисунок 2.1 – Функції доступу до системи

Усі елементи, зображені в пунктирних лініях на рисунку 2.1, називаються контролем доступу. Щоб було зрозуміло, що всі перераховані функції пов’язані між собою, Стандарт ISF використовує термін системний доступ для посилання на послуги, що надаються шляхом авторизації, автентифікації та контролю доступу, які працюють разом [17].

Доступ до системи пов'язаний із забороною доступу неавторизованих користувачів та обмеженням діяльності законних користувачів лише тими діями, які вони мають право виконувати над системними ресурсами.

Функція контролю доступу опосередковує спроби доступу до об’єкта в системі користувача або програми, що виконує від імені цього користувача.

Функція автентифікації встановлює особу користувача.

Функція авторизації підтримує базу даних авторизації, яка визначає права доступу для кожного користувача.

Функція контролю доступу звертається до бази даних авторизації та використовує політику контролю доступу, яка визначає, як права користувача перетворювати на дозволені дії для певних елементів даних чи інших ресурсів.

Авторизація.Визначений адміністратор безпеки відповідає за створення та підтримку бази даних авторизації. Адміністратор встановлює ці повноваження на основі політики безпеки організації та ролей та відповідальності окремих працівників.

Процес авторизації користувачів повинен включати [18]:

1. Пов’язування привілеїв доступу з однозначно визначеними особами, наприклад, за допомогою унікальних ідентифікаторів, таких як ідентифікатори користувачів.

2. Ведення центрального запису прав доступу, наданих ідентифікатору користувача для доступу до інформаційних систем та послуг.

3. Отримання дозволу від власника інформаційної системи чи послуги на використання інформаційної системи чи послуги. Окреме затвердження прав доступу від керівництва також може бути доречним.

4. Застосування принципу найменших привілеїв, щоб надати кожній людині мінімальний доступ, необхідний для виконання її роботи.

5. Призначення індивідуальних прав доступу до ресурсів на основі рівнів інформаційної безпеки та класифікації інформації.

6. Визначення мереж та мережевих служб, до яких потрібно отримати доступ, таких як файли та бази даних.

7. Визначення вимог щодо закінчення терміну дії привілейованих прав доступу.

8. Забезпечення повторного використання ідентифікаторів. Це означає видалення авторизацій, пов’язаних з ідентифікатором користувача, коли особа, якій призначено цей ідентифікатор користувача, змінює ролі або залишає організацію.

На додаток до прийняття звичайних засобів захисту, що використовуються для захисту баз даних, регулярно переглядайте базу даних авторизації, щоб переконатися, що права доступу залишаються належними, а застарілі дозволи видалені.

Усі методи, які правильно реалізовані та використовуються, забезпечують безпечну автентифікацію користувачів. Однак кожен метод має певні проблеми (таблиця 2.1).

Зловмисник може вгадати або вкрасти пароль. Точно так само зловмисник може підробити або вкрасти карту. Користувач може забути пароль або втратити картку.

Користувач може поділитися паролем або карткою з колегою. Крім того, існують значні адміністративні витрати на управління інформацією про паролі та картки в системах та забезпечення такої інформації в системах. Що стосується біометричних автентифікаторів, існує безліч проблем, включаючи вирішення помилкових та хибнонегативних спрацьовувань, вартість, безпека самого датчика та зручність.

Таблиця 2.1 – Фактори автентифікації

|  |  |  |
| --- | --- | --- |
| Фактор | Приклад | Властивості |
| Знання | ID користувача  Пароль | Можна поділитися;  Багато паролів легко вгадати, їх можна забути |
| Володіння | Smart картка;  електронний бейдж;  електронний ключ | Можна поділитися;  Можна дублювати (клонувати);  Можна втратити або вкрасти |
| Невід'ємність | Відбитки пальців  Розпізнавання обличчя;  Голосовий ввід | Неможливо поділитися;  Можливі хибнопозитивні та  хибнонегативні спрацювання;  Створити важко |

Багатофакторна автентифікація. Багатофакторна автентифікація відноситься до використання більш ніж одного із засобів автентифікації (рисунок 2.2).

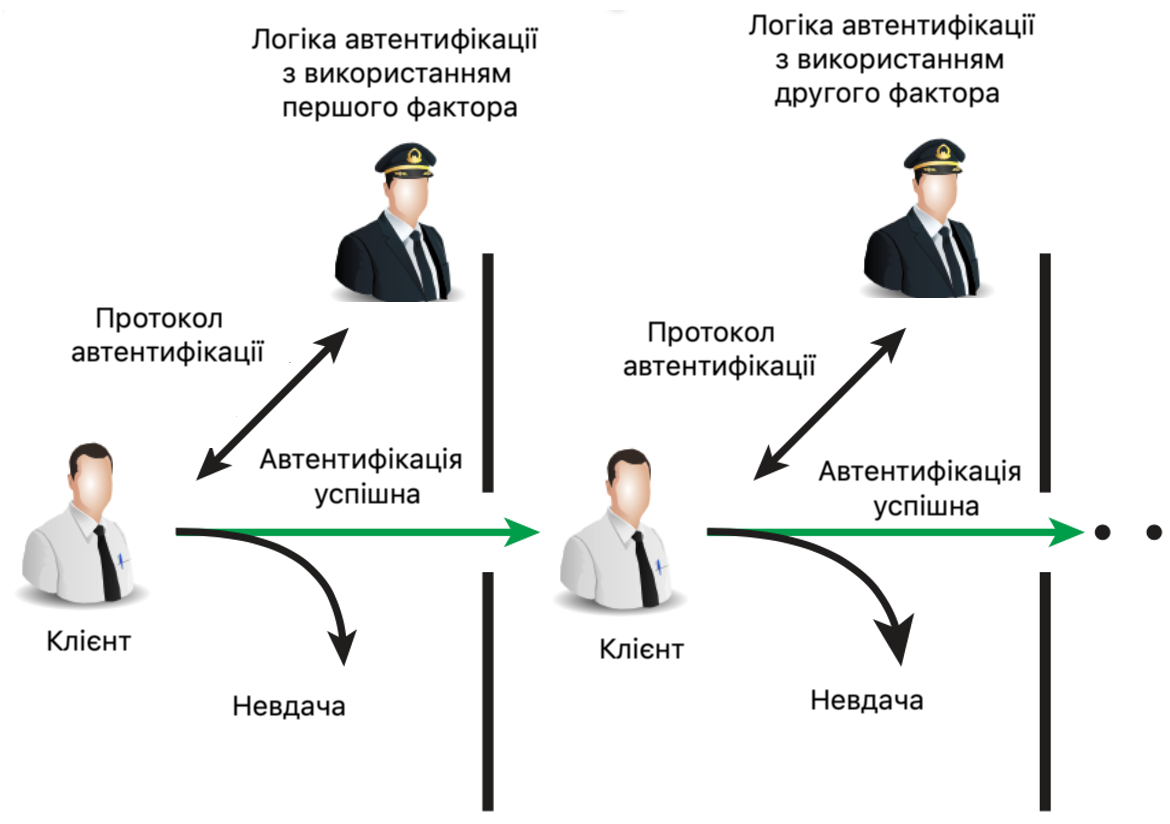
****

Рисунок 2.2 – Багатофакторна автентифікація

Міцність системи автентифікації багато в чому визначається кількістю факторів, включених у систему. Система, яка вимагає двох факторів, як правило, сильніша, ніж система, що використовує один фактор, припускаючи, що окремі фактори досить сильні.

Трифакторна система, як правило, сильніша за двофакторну, хоча в якийсь момент настає зменшення віддачі.

2.2 Модель електронної автентифікації користувача

Національний інститут стандартів і технологій (NIST) SP 800-63, «Керівні принципи цифрової ідентичності», визначає загальну модель автентифікації користувачів, яка включає низку організацій та процедур, як показано на рисунку 2.3 [16].

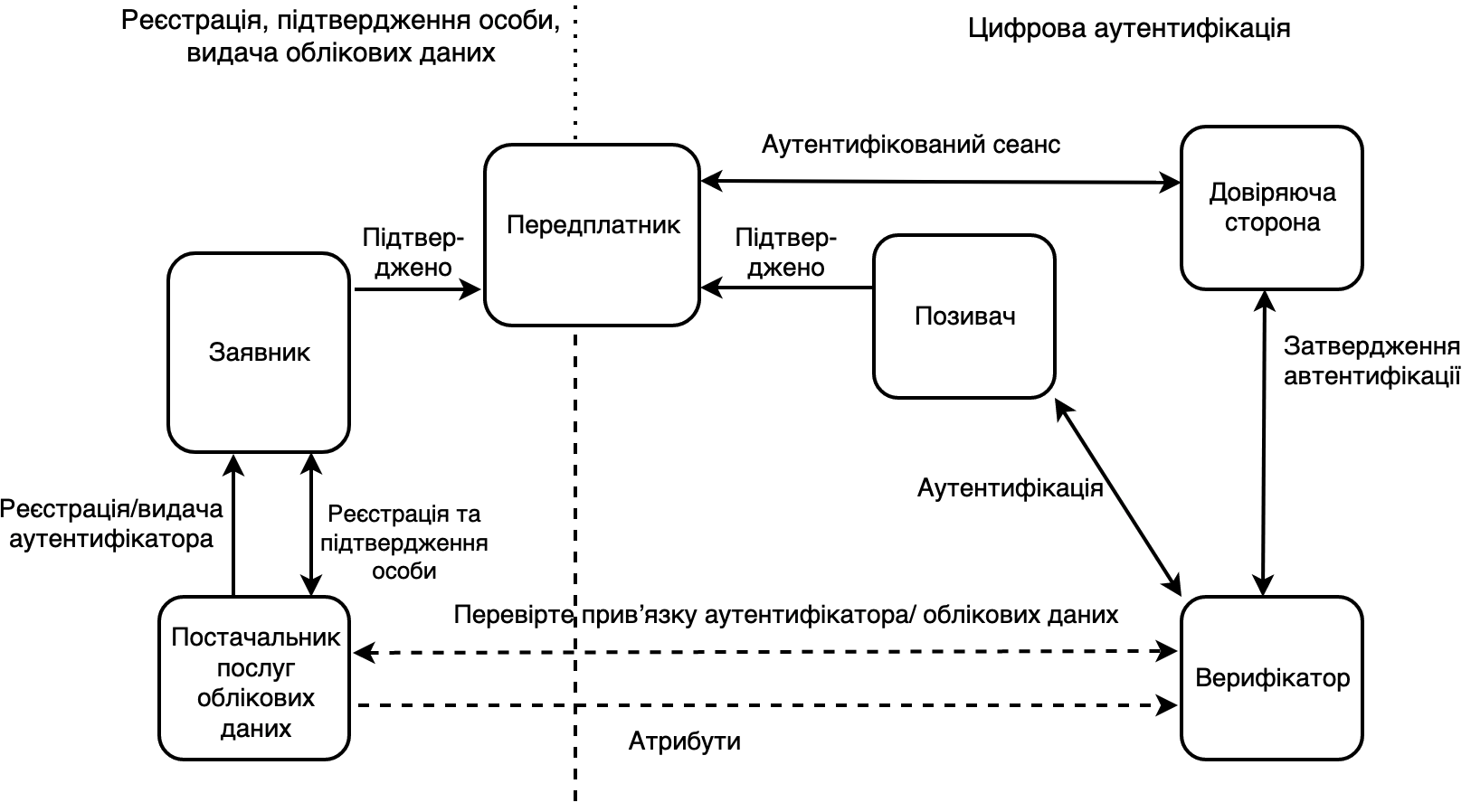


Рисунок 2.3 – Модель цифрової ідентифікації NIST 800-63 [16]:

Приведена на рисунку 2.3 модель базується на наступних поняттях [16]:

1. Цифрова ідентичність. Цифрова ідентичність – це унікальне зображення суб’єкта, який здійснює онлайн – транзакції. Представлення складається з атрибута або набір атрибутів, які однозначно описують предмет у певному контексті цифрової послуги, але не обов’язково однозначно ідентифікують предмет у всіх контекстах.

2. Перевірка особи. цей процес встановлює, що суб’єкт є тим, ким він чи вона претендує, на певний рівень впевненості. Цей процес передбачає збір, перевірку та перевірку інформації про людину.

3. Цифрова автентифікація. Цей процес передбачає визначення дійсності одного або декількох автентифікаторів, які використовуються для отримання цифрової ідентичності.

Автентифікація встановлює, що суб’єкт, який намагається отримати доступ до цифрової послуги, контролює технології, що використовуються для автентифікації.

Успішна автентифікація дає обґрунтовані гарантії на основі ризику, що суб’єкт, який сьогодні звертається до послуги, такий самий, як суб’єкт, який раніше звертався до послуги.

На рисунку 2.3 визначено шість сутностей:

1. Постачальник облікових даних (ПОД): Довірена організація, яка видає або реєструє автентифікатори абонентів. Для цього ПОД встановлює цифрові облікові дані для кожного абонента та видає абонентам електронні дані. CSP може бути незалежною третьою стороною або видавати облікові дані для власного використання.

2. Верифікатор. Сутність, яка перевіряє особу заявника, перевіряючи володіння заявника та контроль над одним або двома автентифікаторами, використовуючи протокол автентифікації. Для цього верифікатору також може знадобитися перевірити облікові дані, які пов'язують автентифікатор (и) з ідентифікатором абонента, і перевірити їх статус.

3. Довіряюча сторона (ДС): Суб’єкт, який покладається на автентифікатор (и) та облікові дані абонента або на підтвердження особи, що заявляє, перевіряючого, як правило, для обробки транзакції або надання доступу до інформації чи системи.

4. Заявник. Суб’єкт, який проходить процес зарахування та підтвердження особи.

5. Позивач. Суб’єкт, особа якого має бути перевірена за допомогою одного або кількох протоколів автентифікації.

6. Абонент. Сторона, яка отримала облікові дані або автентифікатор від СОД.

Ліва частина рисунку 2.3 ілюструє процес, за допомогою якого заявник зараховується до системи для доступу до певних послуг та ресурсів.

По - перше, заявник подає до ПОД докази володіння атрибутами, які мають бути пов’язані з цією цифровою ідентичністю. Після успішної перевірки ПОД заявник стає абонентом. Потім, залежно від деталей загальної системи автентифікації, ПОД видає абоненту якусь електронну облікову інформацію.

Облікові дані- це структура даних, яка авторитетно пов'язує ідентичність та додаткові атрибути з одним або кількома автентифікаторами, якими володіє абонент, і перевіряється, коли вона представлена верифікатору у транзакції автентифікації.

Автентифікатор це або ключ шифрування, або зашифрований пароль, який ідентифікує абонента. Автентифікатор видається ПОД, генерується безпосередньо абонентом або надається третьою стороною. Автентифікатор та облікові дані можна використовувати у наступних подіях автентифікації. Після того, як користувач зареєстрований як абонент, процес автентифікації відбувається між абонентом та однією або кількома системами, які виконують автентифікацію (див. рисунок 2.3).

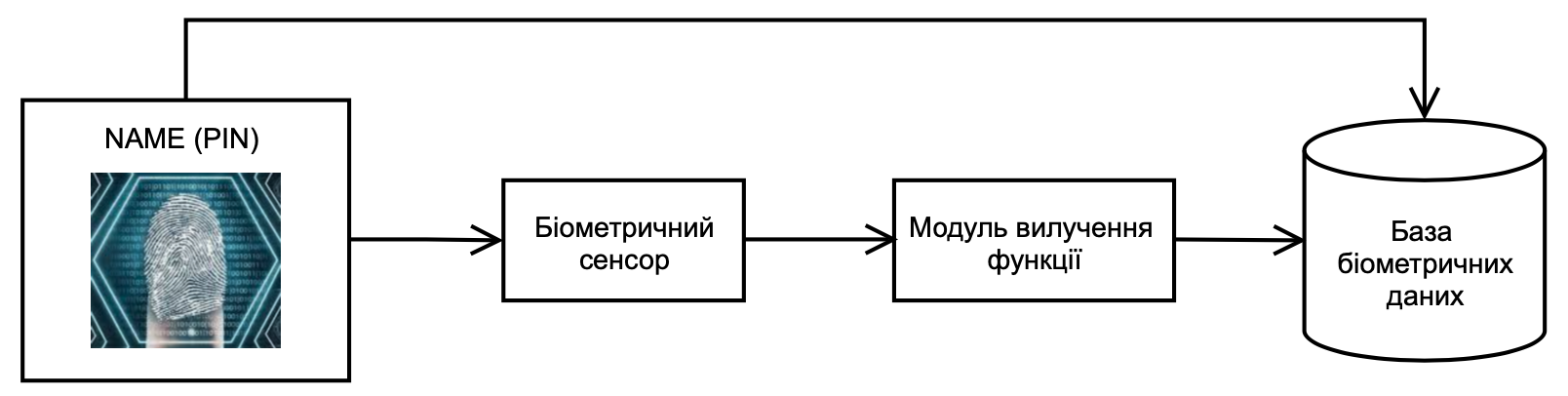
Сторона, яка підлягає автентифікації, називається заявником, а сторона, яка перевіряє цю особу - верифікатором. Коли позивач успішно демонструє верифікатору володіння та контроль над автентифікатором за допомогою протоколу автентифікації, верифікатор перевіряє, що заявник є абонентом, зазначеним у відповідних облікових даних. Верифікатор передає ДС заяву про особу абонента. Це твердження містить інформацію про особу абонента, таку як ім’я абонента, ідентифікатор, присвоєний під час реєстрації, або інший атрибут абонента, перевірений у процесі реєстрації. ДС використовує автентифіковану інформацію, надану верифікатором, для прийняття рішень щодо контролю доступу або авторизації.

У деяких випадках верифікатор взаємодіє з ПОД для доступу до облікових даних, які пов'язують особу абонента та автентифікатора, а також для отримання за бажанням атрибутів заявника. В інших випадках верифікатору не потрібно спілкуватися в режимі реального часу з ПОД для завершення діяльності з автентифікації (як у деяких випадках використання цифрових сертифікатів). Таким чином, пунктирна лінія між верифікатором та ПОД на рисунку 3.2 являє собою логічний зв'язок між двома сутностями.

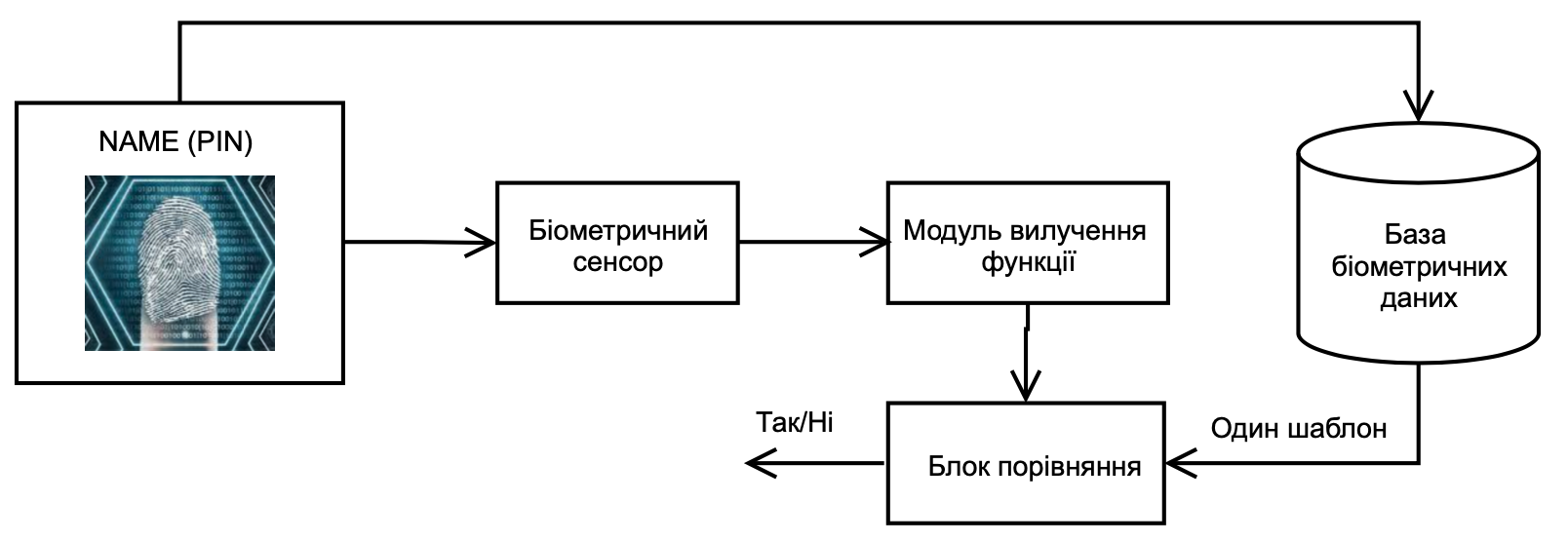
Реалізована система автентифікації відрізняється від цієї спрощеної моделі і, як правило, є більш складною, але ця модель ілюструє ключові ролі та функції, необхідні для безпечної системи автентифікації.

2.3 Алгоритм роботи системи біометричної автентифікації

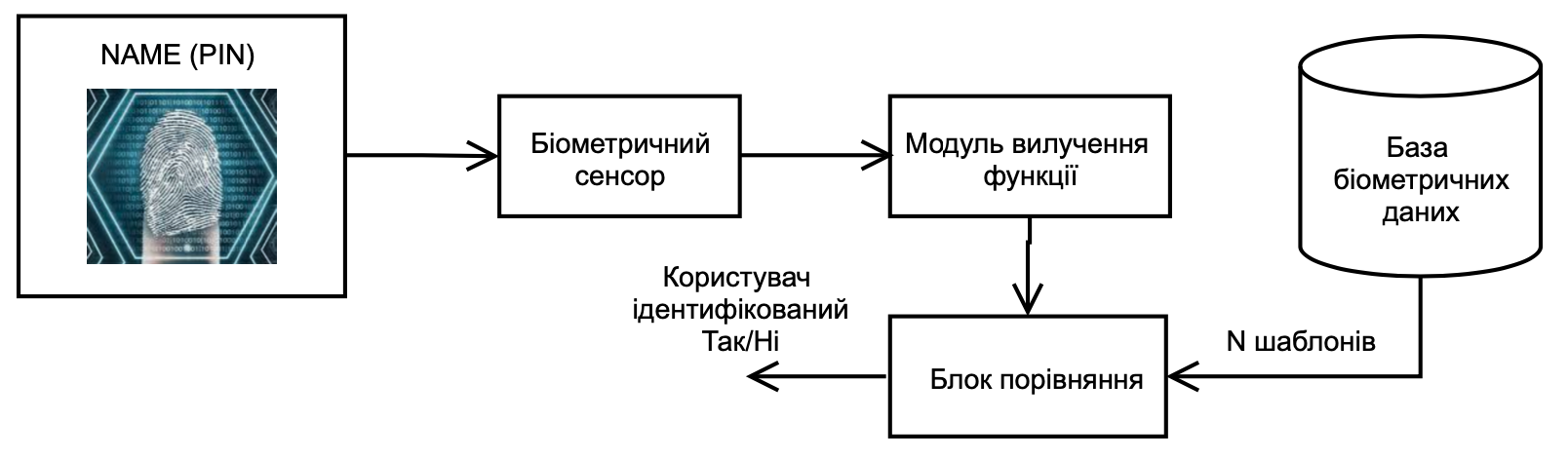
На рисунку 2.4 показано, як працює біометрична система. Кожна особа, яка має бути включена в базу даних авторизованих користувачів, має бути попередньо зареєстрована в системі. Це еквівалентно призначенню пароля користувачеві. У біометричній системі користувач представляє системі ім’я та, як правило, певний тип пароля або PIN-коду. У той же час система фіксує деякі біометричні характеристики цього користувача (наприклад, відбиток правого вказівного пальця). Система оцифровує вхідні дані, а потім завантажує набір ознак, збережених у вигляді набору чисел, які представляють цю унікальну біометричну функцію; цей набір чисел відомий як шаблон користувача. Тепер користувач зареєстрований в системі, яка керує ім’ям (ID), можливо, PIN-кодом або паролем, а також біометричним значенням для користувача.



а)



б)



в)

Рисунок 2.4 – Загальна схема біометричної системи автентифікації

Залежно від програми автентифікація користувача в біометричній системі включає перевірку або ідентифікацію. Перевірка відповідає входу користувача в систему за допомогою карти пам’яті або смарт-картки разом із паролем або PIN-кодом. Для біометричної перевірки користувач вводить PIN-код, а також використовує біометричний датчик. Система витягує відповідну характеристику і порівнює її з шаблоном, збереженим для цього користувача. Якщо вони збігаються, система автентифікує цього користувача. Для системи ідентифікації людина використовує біометричний датчик, але ніякої додаткової інформації не подає. Потім система порівнює представлений шаблон з набором збережених шаблонів. Якщо вони збігаються, цей користувач ідентифікується. Інакше користувач буде відхилений.

2.4 Загрози безпеки біометричній автентифікації

Для біометричної автентифікації, яка приведена на рисунку 2.4в, типова послідовність кроків така:

1. Отримання біометричного зразка.

2. Дані фіксуються сенсором.

3. Обробка отриманих даних, здійснюється як правило, для вилучення ознак.

4. Записані дані порівнюються з шаблонами біометричних характеристик користувача, які були отримані з пам'яті.

5. Прийняття рішення про автентифікацію.

Рисунок 2.5 побудований на основі NIST для вимірювання автентифікації, на якому показано 11 точок поверхні атаки в системі, в яких зловмисник може втрутитися в потік, щоб порушити рішення про автентифікацію [15].

Усі ці 11 елементів можуть бути автономними в одному пристрої (наприклад, мобільному пристрої) або розподілені між кількома фізичними системами.

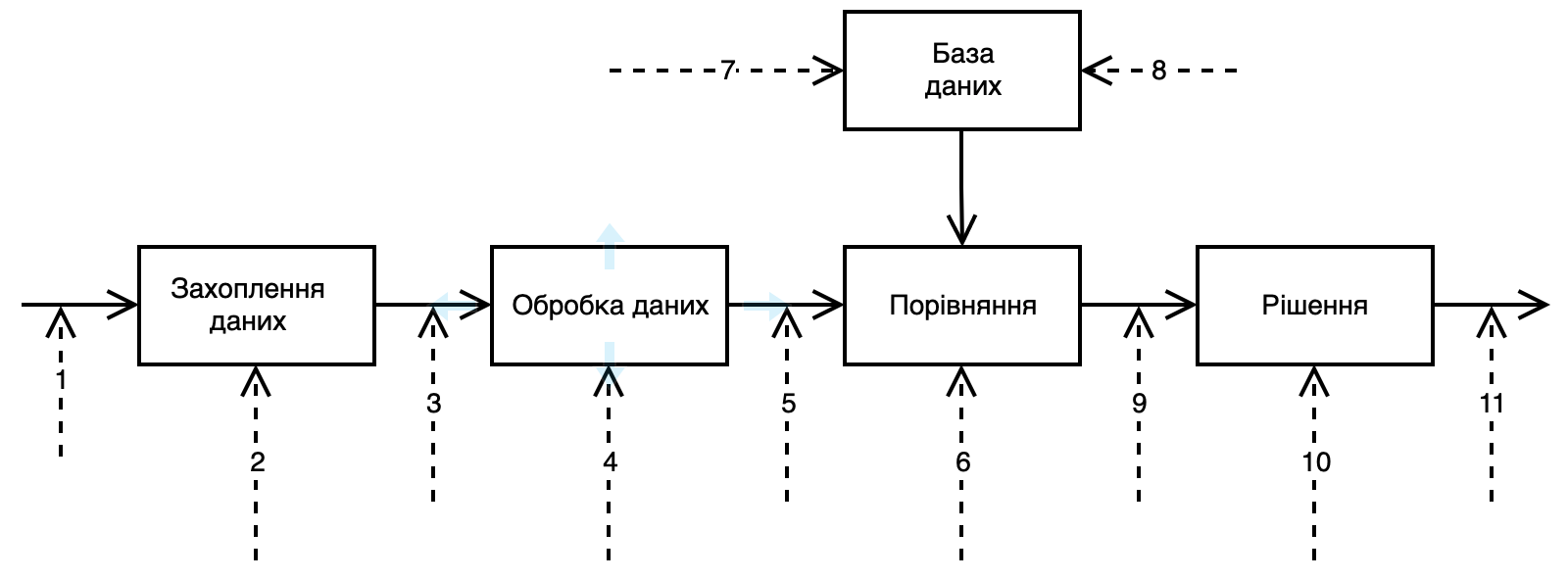


Рисунок 2.5 – Схема атаки біометричної системи

Розглянемо типи потенційної атаки в кожній точці біометричної системи (числа відповідають числам на рисунку 2.5).

1. Зловмисник може надати датчику фальсифіковані біометричні дані.

2. Зловмисник може змінити апаратне чи програмне забезпечення пристрою збору даних.

3. Тут можлива атака повтору, при якій зловмисник знову подає раніше збережений оцифрований біометричний сигнал.

4. Зловмисник може змінити апаратне чи програмне забезпечення в пристрої обробки сигналів.

Наприклад, засіб вилучення функцій може бути атакований троянським конем, щоб він генерував набори функцій, попередньо обрані зловмисником.

5. Якщо процесор сигналів і компаратор фізично розділені, зловмисник може втрутитися в шлях зв'язку і замінити вилучені функції іншим шахрайським набором функцій.

6. Алгоритм порівняння порівнює вхідні дані датчика із збереженим біометричним зразком для користувача. Ефективність компаратора залежить від двох основних факторів: від того, наскільки відмітним є біометричний шаблон (тобто, вроджені характеристики модальності та скільки різних індивідуальних шаблонів може існувати) та підходу алгоритму постачальника до аналізу модальності. Зловмисник може спробувати змінити алгоритм або іншим чином порушити його.

7. Зловмисник може спробувати витягти та змінити збережену інформацію.

8. Зловмисник може атакувати канал між збереженими шаблонами та порівнюваним зразком. У цьому випадку збережені шаблони надсилаються в блок порівняння через канал зв’язку. Дані, що передаються по цьому каналу, можуть бути перехоплені та змінені.

9. Результатом алгоритму порівняння є оцінка відповідності між двома біометричними зразками: представленим користувачем і тим, що є в базі даних шаблонів. Якщо алгоритм порівняння і механізм прийняття рішень фізично розділені, цей канал повинен запобігати модифікації будь-яких даних, оскільки результати відповідності надсилаються до механізму прийняття рішень.

10. Зловмисник може змінити апаратне чи програмне забезпечення в машині прийняття рішень.

11. Зловмисник може перехопити рішення, передане механізмом прийняття рішень, і змінити його.

Багато з наведених вразливостей належать до добре відомих категорій, які є поширеними в інших системах аутентифікації.

Однак з перелічених є дві вразливості, які не захищені основними засобами контролю кібербезпеки: презентаційна атака і перевизначення компаратора.

1. Презентаційна атака. Головне джерело вразливостей безпеки, які не охоплюються основними засобами контролю кібербезпеки, відома як презентаційна атака. Цей тип атаки намагається імітувати біометричну характеристику з достатньою точністю, щоб система визнала її дійсною - атака, відома як біометричний спуфінг. Існує додатковий ризик у неконтрольованих середовищах, де немає оператора, який контролює представлення біометричних даних.

2. Перевизначення компаратора. Зловмисник може не тільки запровадити зловмисне програмне забезпечення, щоб змінити поведінку компаратора, але й спробувати використати властивості конкретного алгоритму порівняння. Помилки, виявлені в алгоритмі, можуть сприяти біометричному спуфінгу.

2.5 Параметри систем контролю доступу

Незалежно від того, яку схему контролю доступу використовує підприємство, це має значну складність, і організація повинна оцінити ефективність системи контролю доступу.

Керівництво з оцінки метрик системи контролю доступу (NISTIR 7874), визначає ряд показників, які використовуються при оцінці контролю доступу, розділених на чотири категорії:

– Адміністрування: властивості, які загалом впливають на вартість, ефективність та продуктивність адміністрування системи контролю доступу.

– Примусове застосування: властивості механізмів або алгоритмів, які система контролю доступу використовує для застосування вбудованих моделей і правил контролю доступу. Ці властивості впливають на ефективність надання рішень щодо контролю доступу.

– Продуктивність: властивості, які впливають на продуктивність на додаток до виконання процесів системи контролю доступу.

– Підтримка: властивості, які не є суттєвими, але підвищують зручність використання та портативність системи контролю доступу.

У таблиці 2.1 наведено окремі показники для кожної категорії.

Для кожного показника NISTIR 7874 перелічує ряд питань, які потрібно використовувати при оцінці.

Наприклад, показник аудиту включає такі запитання:

– Чи система контролю доступу реєструє збій системи? Журнал джерела помилок записує, коли система контролю доступу не приймає рішення про надання.

– Чи відхиляє журнал системи контролю доступу запити на доступ? Журнал для спроб порушення політики фіксує відхилені запити користувачів щодо відповідних політик контролю доступу.

– Чи надано в журналі системи контролю доступу запити на доступ? Журнал для відстеження доступу фіксує надані можливості суб'єкта. Оскільки об’єкти можна перейменовувати, копіювати та віддавати, відстеження поширення та збереження доступу важко або неможливо досягти за допомогою лише виразів привілеїв.

– Чи забезпечує система контролю доступу додаткові функції журналу, необхідні організації? Можна налаштувати можливості надання інформації аудиту для керування даними журналів (наприклад, встановити максимальний розмір журналів аудиту).

Таблиця 2.1 – Метрики оцінки для систем контролю доступу

|  |  |
| --- | --- |
| Адміністративні властивості | Властивості примусового виконання |
| Аудит  Виявлення привілеїв/можливостей Простота призначення привілеїв Синтаксична та семантична підтримка визначення правил AC  Управління політикою  Делегування адміністративних повноважень  Гнучкість конфігурації в існуючих системах  Горизонтальний діапазон контролю (для платформ і програм)  Вертикальна область контролю (між програмою, СУБД та ОС). | Комбінація політик, склад і обмеження  Обхід  Підтримка принципу найменших привілеїв розділення обов'язків (SoD)  Безпека (утримання та обмеження) Розв’язання або запобігання конфлікту  Оперативна/ситуативна обізнаність Детальність контролю  Властивості виразу (політики/моделі).  Адаптований до впровадження та розвитку політики AC |
| Допоміжні властивості | Властивості продуктивності |
| Політика імпорту та експорту  Сумісність з ОС  Управління джерелами політики Інтерфейси користувача та API  Підтримка функції перевірки та відповідності | Час реакції  Репозиторій політики та пошук Поширення політики  Інтегрована з функцією аутентифікації |

Наприклад, показник аудиту включає такі запитання:

– Чи система контролю доступу реєструє збій системи? Журнал джерела помилок записує, коли система контролю доступу не приймає рішення про надання.

– Чи відхиляє журнал системи контролю доступу запити на доступ? Журнал для спроб порушення політики фіксує відхилені запити користувачів щодо відповідних політик контролю доступу.

– Чи надано в журналі системи контролю доступу запити на доступ? Журнал для відстеження доступу фіксує надані можливості суб'єкта. Оскільки об’єкти можна перейменовувати, копіювати та віддавати, відстеження поширення та збереження доступу важко або неможливо досягти за допомогою лише виразів привілеїв.

– Чи забезпечує система контролю доступу додаткові функції журналу, необхідні організації? Можна налаштувати можливості надання інформації аудиту для керування даними журналів (наприклад, встановити максимальний розмір журналів аудиту).

Компроміси та обмеження пов’язані з усіма механізмами контролю доступу розглядаються під час вибору властивостей, тому організація несе відповідальність за визначення найкращих показників контролю доступу, які працюють для конкретних функцій та вимог. Правильний вибір показників залежить не тільки від врахування адміністративних витрат, але й від гнучкості використовуваного механізму.

3 СТРУКТУРА ТА ОПИС ФУНКЦІОНУВАННЯ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

3.1 Загальна структура системи контролю доступу на основі двофакторної автентифікації

Пропонована система контролю доступу для автентифікації користувачів використовує два фактори: RFID мітки та біометрику. Оскільки мобільні пристрої з підтримкою мікросхеми NFC вже достатньо поширені на ринку, то в якості першого фактору пропонується використати мобільний телефон, який підтримує технологію NFC. Таким чином, користувачу не потрібно отримувати додаткові картки або брелки для автентифікації.

Загальна структура системи контролю доступу на основі двофакторної автентифікації приведена на рисунку 3.1. Основою системи контролю доступу є одноплатний комп’ютер Raspberry Pi до якого підключені сканер відбитку пальців, модуль NFC, дисплей, реле, блок живлення та блок безперебійного живлення.

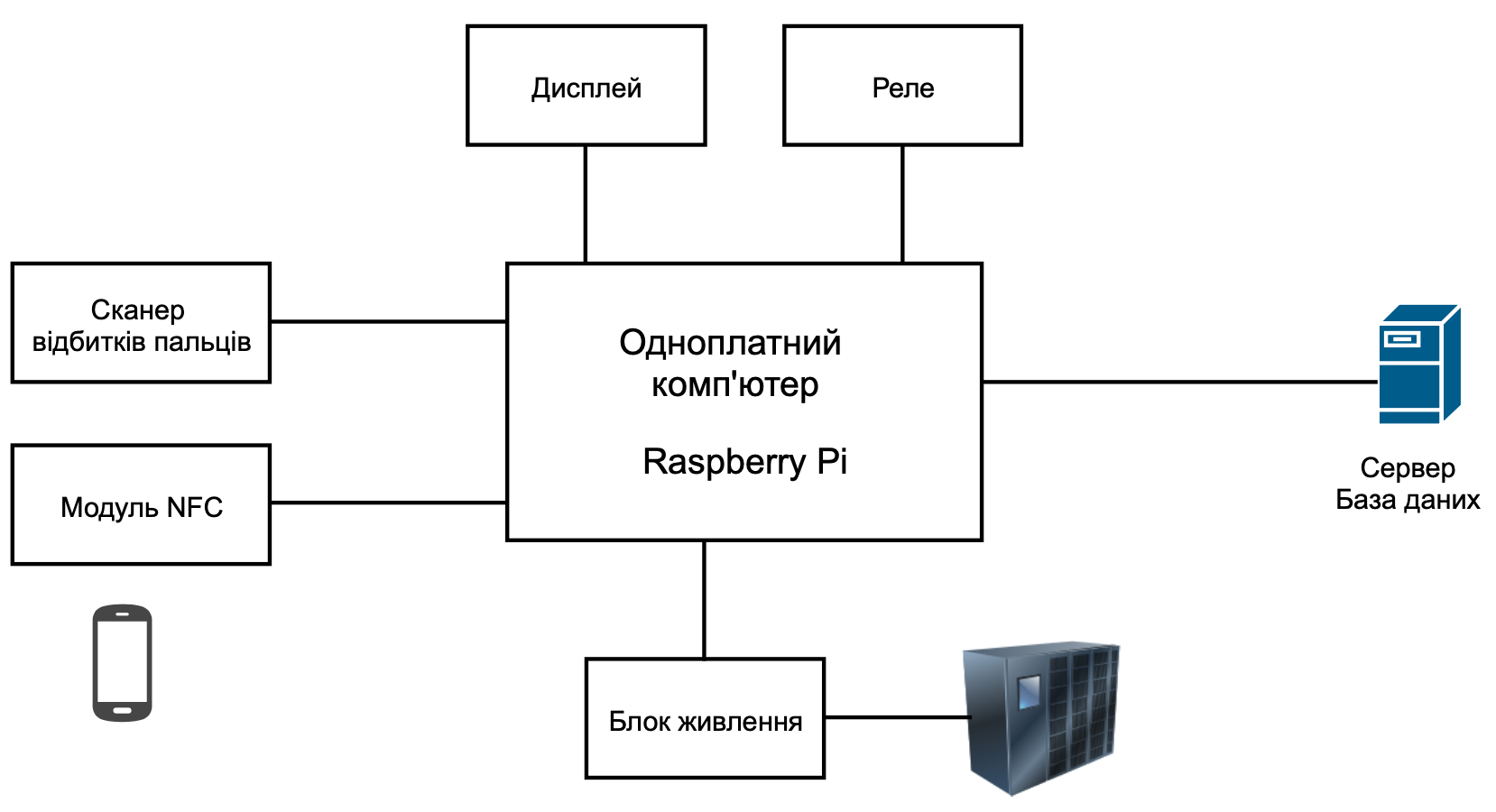


Рисунок 3.1 – Структура системи контролю доступу

Система працює наступним чином. Для автентифікації користувач підносить до зчитувача NFC модуль при розпізнаванні якого на дисплей виводиться повідомлення про успішний перший етап автентифікації (рисунок 3.2).

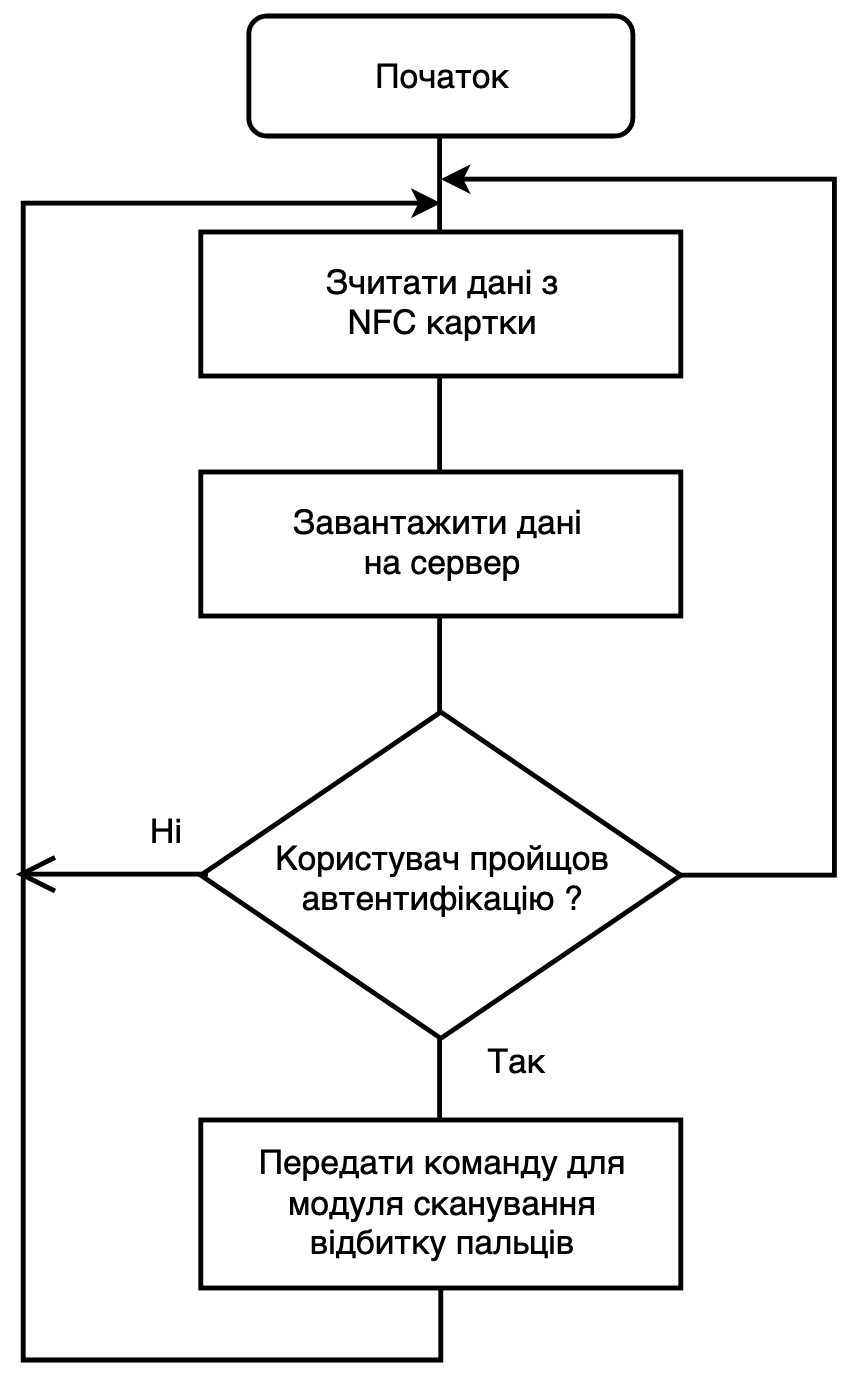


Рисунок 3.2 – Блок-схема алгоритму автентифікації на основі NFC картки

Наступним кроком користувачу необхідно прикласти палець до сканера відбитків пальців (рисунок 3.3).

Функціональна схема розпізнавання відбитків пальців приведена на рисунку 3.3.

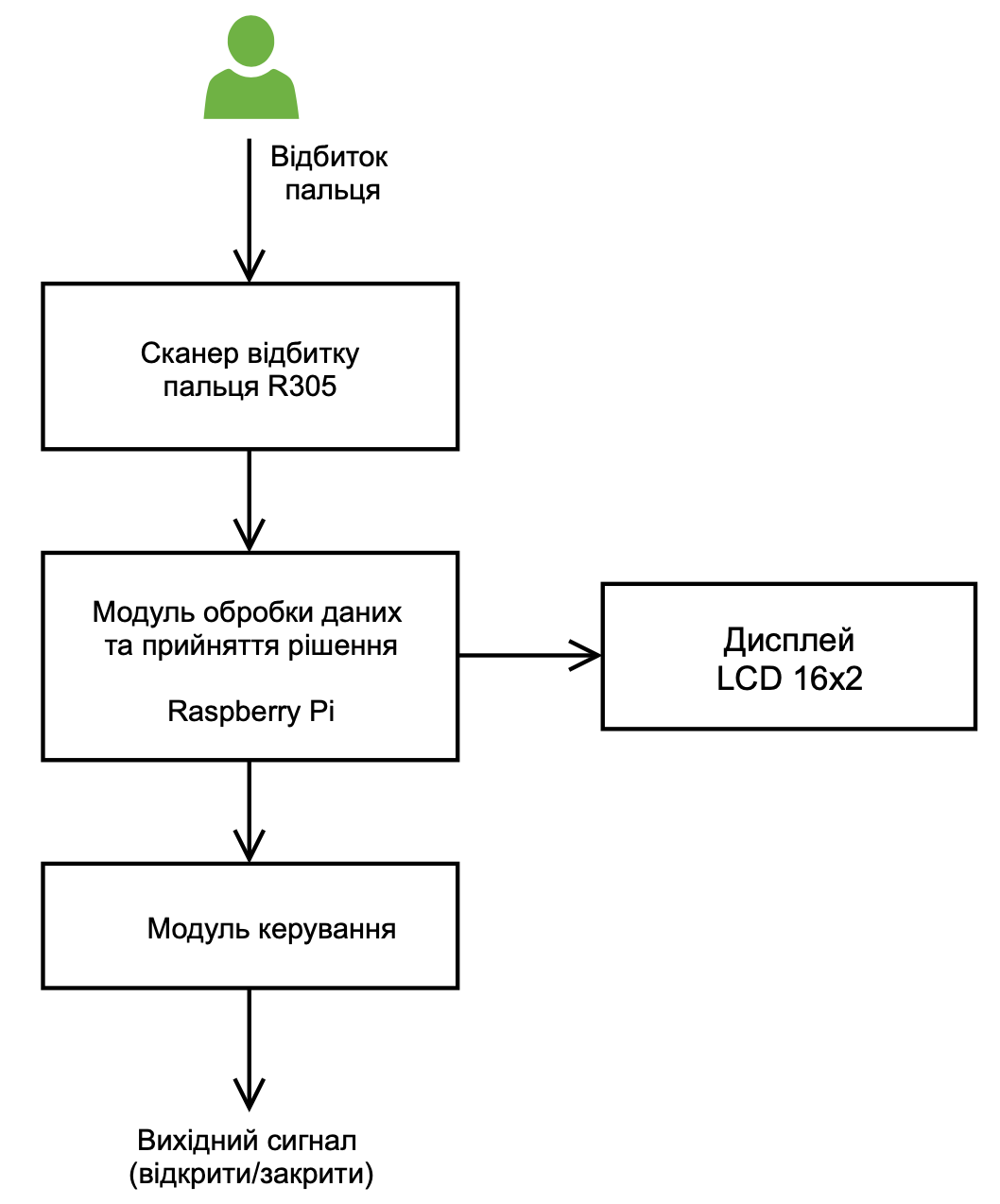


Рисунок 3.3 – Система розпізнавання відбитків пальців

При успішному скануванні дані передаються через одноплатний комп’ютер Raspberry Pi на сервер, де відбувається обробка та порівняння з базою даних зареєстрованих користувачів.

При співпадінні отриманого відбитку пальця з наявним у базі даних з сервера надходить відповідний код, який формує команду реле та виводить повідомлення на дисплей про успішну автентифікацію. При відхиленні одного з факторів, RFID мітка або відбиток пальця, система повідомляє про помилку автентифікації. При цьому всі спроби автентифікації фіксуються та зберігаються у файлах на сервері.

Відбиток пальця отримується за допомогою сканера відбитків пальців і обробляється на Raspberry Pi. Після ідентифікації надається доступ до системи, яка контролюється і на РК-дисплеї відображається відповідне повідомлення.

3.2 Алгоритм розпізнавання відбитку пальців

Алгоритм роботи модуля розпізнавання відбитку пальців складається з наступних кроків.

Крок 1. Початок

Крок 2.Сканування відбитку пальців

Крок 3. Перевірка наявності дійсного відбитка пальця. Якщо так: перехід до кроку 3, якщо ні перехід то до кроку 2.

Крок 4. Дані надсилаються на Raspberry Pi.

Крок 5: Перевірка, чи відповідає відбиток пальця чи ні, якщо так то перехід до кроку 6, якщо ні то перехід до кроку 2.

Крок 6. Відправка сигналу роботи на модуль керування і відображення повідомлення на дисплеї.

Крок 7. Перехід до кроку 2.

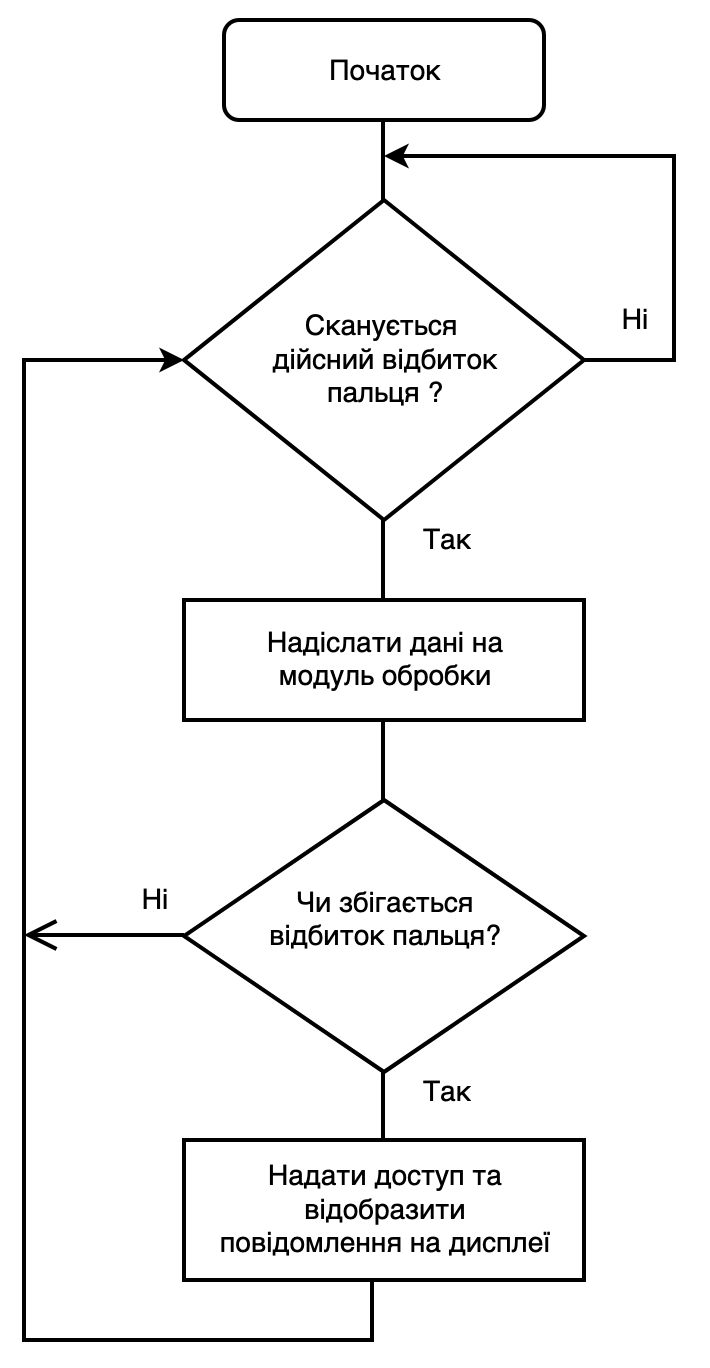


Рисунок 3.4 – Блок-схема роботи системи розпізнавання відбитків пальців

# 3.3 Підключення та налаштування сканера відбитків пальців

Сканери відбитків пальців все частіше зустрічаються в системах контролю доступу і використовуються для безпечної перевірки осіб. Розглянемо підключення сенсора відбитків пальців до Raspberry Pi для реалізації автентифікації особи.

Однією з переваг є те, що паролі та/або цифрові коди можна забути, хоча вони все ще використовуються досить часто, як спосіб автентифікації особи.

Ці датчики спочатку були розроблені для Arduino і можуть бути підключені через UART. Raspberry Pi має два контакти (контакт 8 / GPIO14 і контакт 10 / GPIO 15), але вони працюють з 3,3 В. Оскільки існують різні датчики відбитків пальців, однак не всі працюють із напругою 3,3 В, тому рекомендується використовувати конвертер USB UART. Деякі моделі можна використовувати як з напругою 3,3 В, так і з напругою 5 В.

Необхідне обладнання:

- датчик відбитків пальців (рисунок 3.5);

- Raspberry Pi;

- послідовний USB-конвертер з виходами 3,3 В і 5 В;

- перемикаючі дроти;

- блок живлення.

|  |  |
| --- | --- |
|  |  |

Рисунок 3.5- Сканер відбитків пальців

Підключення сканера відбитків пальців до Raspberry Pi. USB-адаптер позначений, але кабелі датчика відбитків пальців – ні. Однак кабелі мають чіткий колір, який ми можемо визначити і підключити до USB-конвертера. Для цього необхідно лише чотири кабелі:

Червоний: залежно від прийнятої напруги датчика (3,3 В або 5 В).

Білий: RXD Зелений: TXD

Чорний: GND

Якщо вашому датчику потрібна напруга вище 3,3 В (а максимальне значення дорівнює або перевищує 5 В), ви можете підключити червоний кабель до контакту 5 В.

Для перевірки, чи правильно підключені кабелі та чи виявлено сканер, необхідно відкрити консоль і виконати наступні команди до та після підключення:

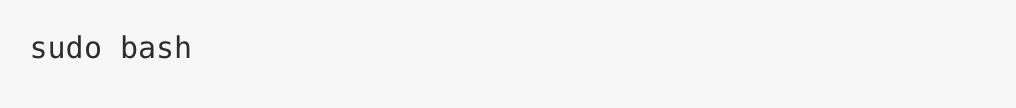


При цьому, якщо інші послідовні пристрої не підключені через USB, то відповідно спочатку нічого не повинно відображатися, а пізніше /dev/ttyUSB0.

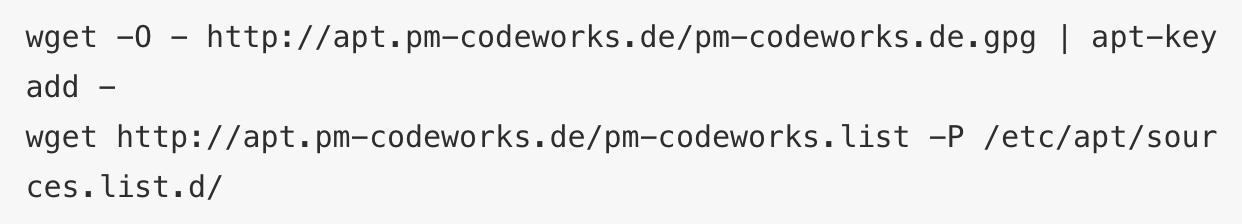
Якщо назва відрізняється (наприклад, підключені інші пристрої), її потрібно відповідно адаптувати, виконавши наступні кроки.

Другий варіант підключення через GPIO. Якщо у вас є датчик з необхідною вхідною напругою 3,3 В, ви також можете підключити його безпосередньо до GPIO без USB-перетворювача. Теоретично ви можете зробити це також за допомогою 5 В і TTL перетворювача. Однією з переваг варіанту підключення USB є те, що легше перевірити, чи був виявлений датчик.

Встановлення бібліотеки відбитків пальців на Raspberry Pi. Для деяких команд встановлення потрібні права root. Для цього запускаємо сеанс у терміналі і вводимо наступну команду, яка виконує всі наступні команди як root:



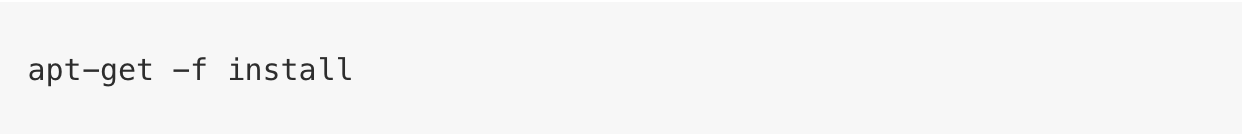
Тепер додаємо необхідні пакети:



Наступним кроком ми оновлюємо доступні пакунки та встановлюємо бібліотеку Python:



Якщо сталася помилка (або не всі залежні пакети були встановлені), необхідно виконати наступну команду:

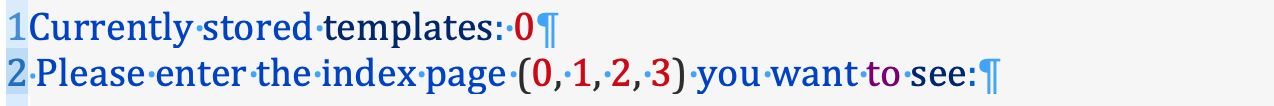


Щоб повернутися до звичайної оболонки (під користувачем Pi), треба ввести команду exit.

Тестовий код і приклад сценарію. Спочатку проводимо тест, щоб перевірити, чи датчик виявлений і чи готовий до доступу. Для цього запускаємо один із зразків файлів: в:



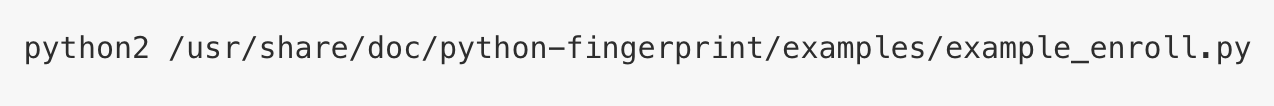
Система дозволяє зберігати до 1000 різних відбитків пальців. Наприклад, палець також можна використовувати кілька разів. Його можна зберігати в різних положеннях, щоб вони виявлялися швидше / чіткіше. Повинно з’явитися наступне, що дозволяє відобразити позиції, під якими зберігається відбиток, вибравши сторінку (0-3).



Якщо повідомлення про помилку «Повідомлення про виключення: порт датчика відбитків пальців» / dev / ttyUSB0 ″ не знайдено!» Отже, щось не так з кабелем або датчиком. Необхідно перевірити ще раз.

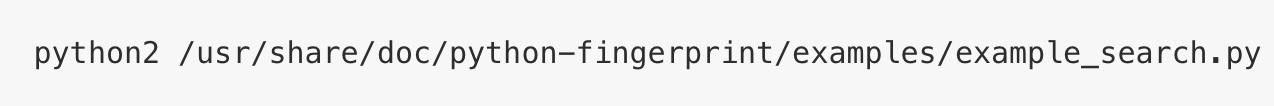
Збереження і читання Приклади файлів для зберігання нового відбитка пальця, зчитування та видалення збережених відбитків пальців.

1. Запису відбитку пальця. Вводимо наступну команду:

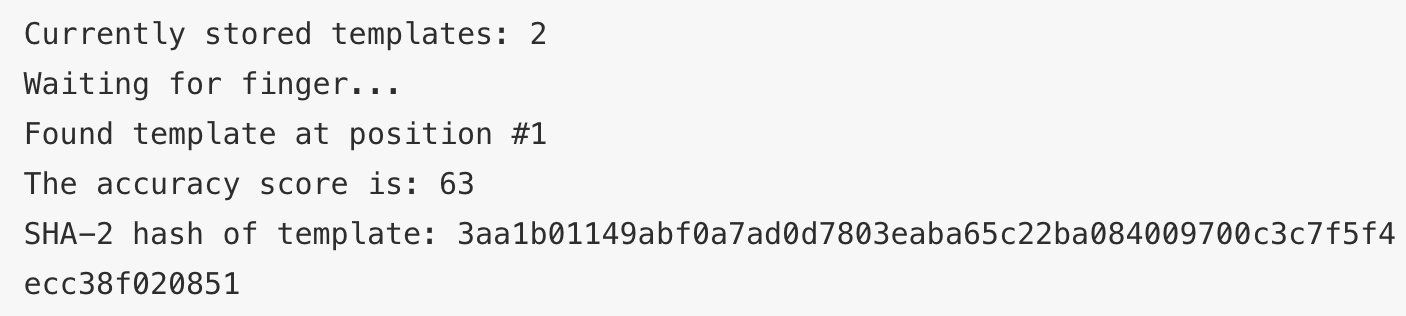


Для отримання відбитку покладіть палець на скляну поверхню, дочекайтеся інструкції в терміналі і зніміть палець. Після цього необхідно вдруге покласти палець для перевірки, і відбиток збережеться під наступним номером.

Давайте також подивимося, чи розпізнає система наш палець. Тому знімаємо палець зі сканера і запускаємо наступний скрипт:



Покладіть палець на сканер. Якщо відбиток пальця розпізнано на Raspberry Pi, появиться таке повідомлення:



У цьому випадку також задається значення точності (чим більше, тим краще). Цей каталог також містить інші скрипти, які можна використовувати для видалення збережених сканів або завантаження їх як зображення. Можна використати команду: ls / usr / share / docs / python-fingerprint / для перегляду всіх цих файлів.

3.4 Підключення модуля NFC PN532 до Raspberry Pi

Модуль NFC Raspberry Pi PN532 базується на мікроскемі PN532 і використовує зв’язок на частоті 13,56 МГц. Даний модуль оснащений вбудованою антеною, тому немає зовнішньої антенної котушки. Модуль сумісний з інтерфейсами SPI, IIC для підключення. Raspberry Pi може підключати продукти з функцією NFC, завдяки підтримці бібліотеки NFC і тому простий у налаштуванні (рисунок 3.6).

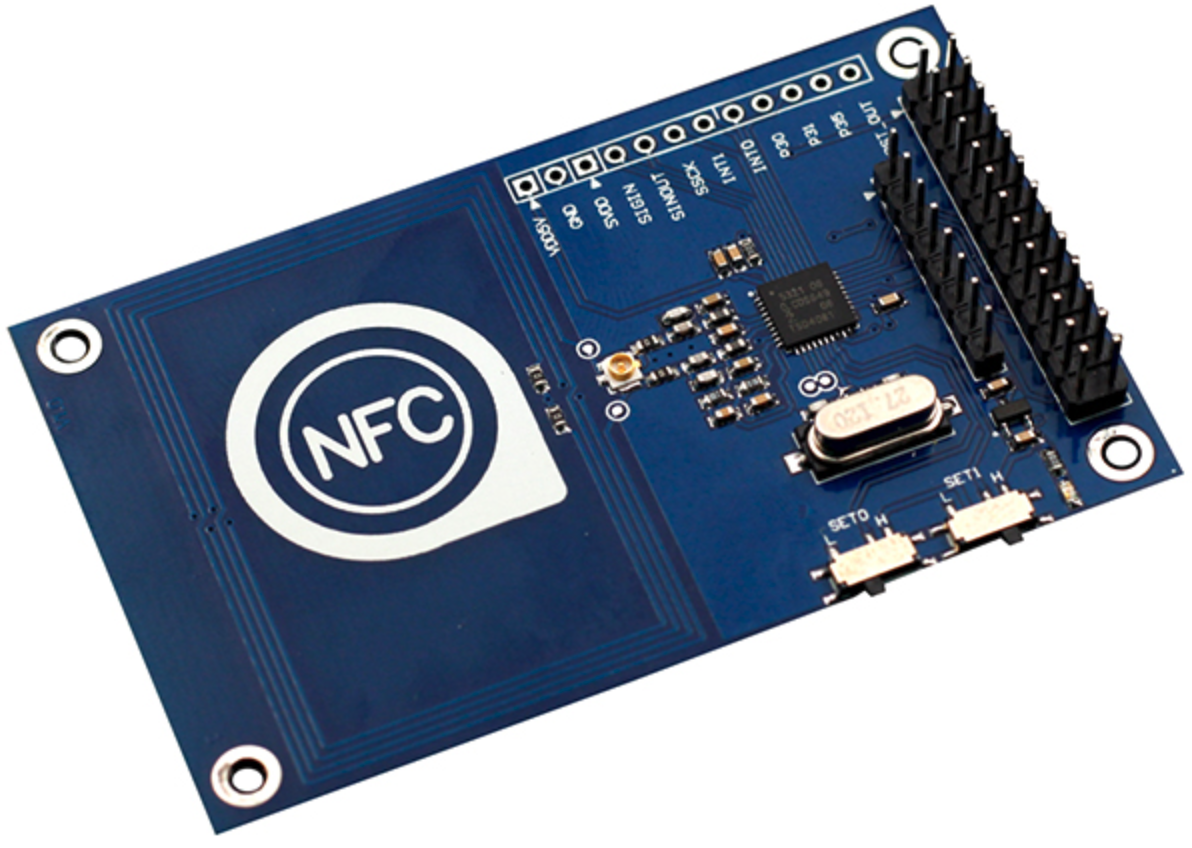


Рисунок 3.6 - Модуль NFC PN532

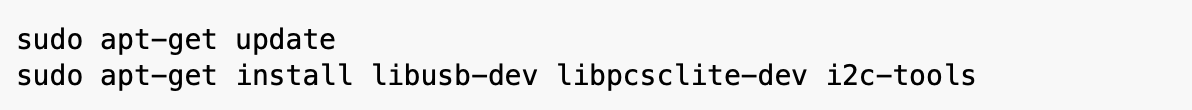
Інструкції по зв’язку I2C для Raspberry Pi.

1. Відкриваємо I2C Raspberry Pi:



Вибираємо 5 параметрів інтерфейсу -> I2C -> так.

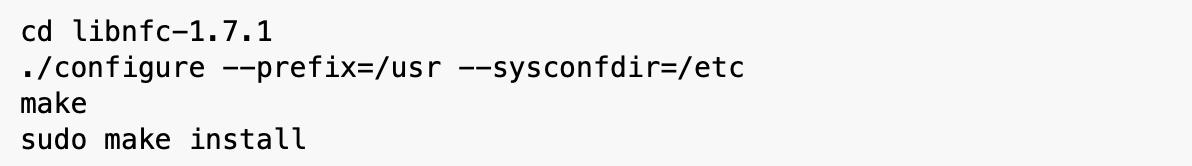
2. Встановлюємо деякі залежні пакети



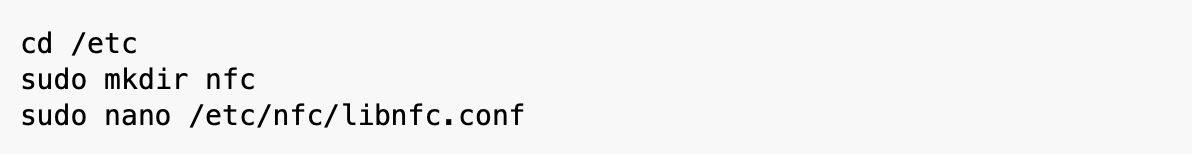
3. Завантажуємо та розпаковуємо пакет вихідного коду libnfc



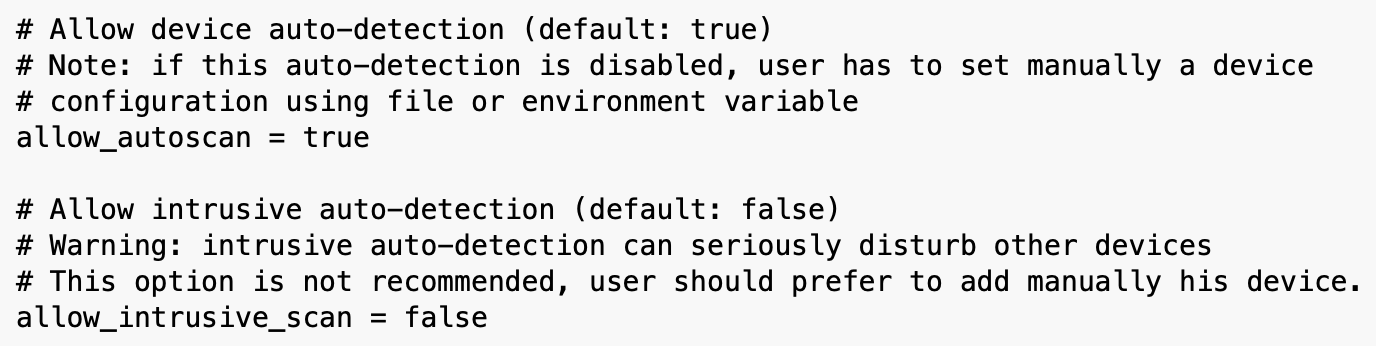
4. Компілюємо та встановлюємо

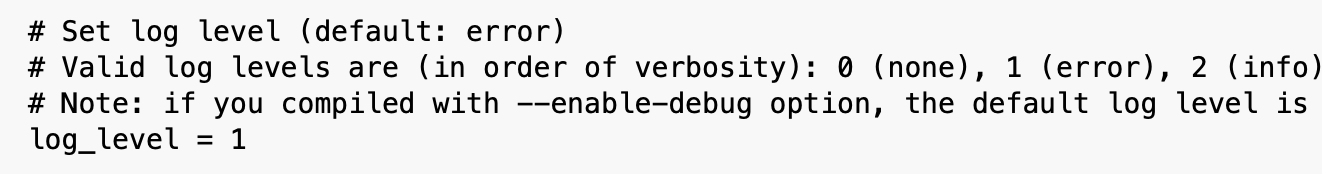


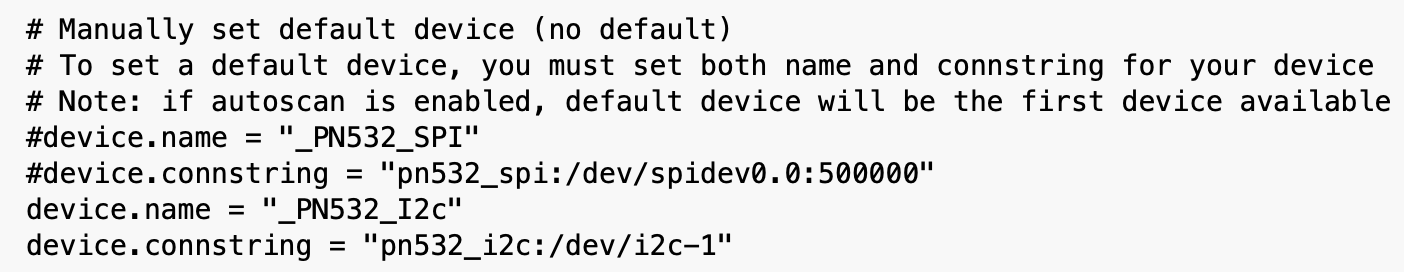
5. Файл конфігурації для зв'язку NFC



Перевіряємо файл конфігурації etc/nfc/libnfc.conf:

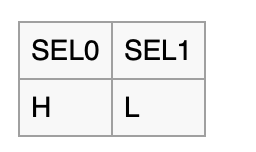






6. Підключення.

Переводимо перемикач у режим I2C (рисунок 3.7)



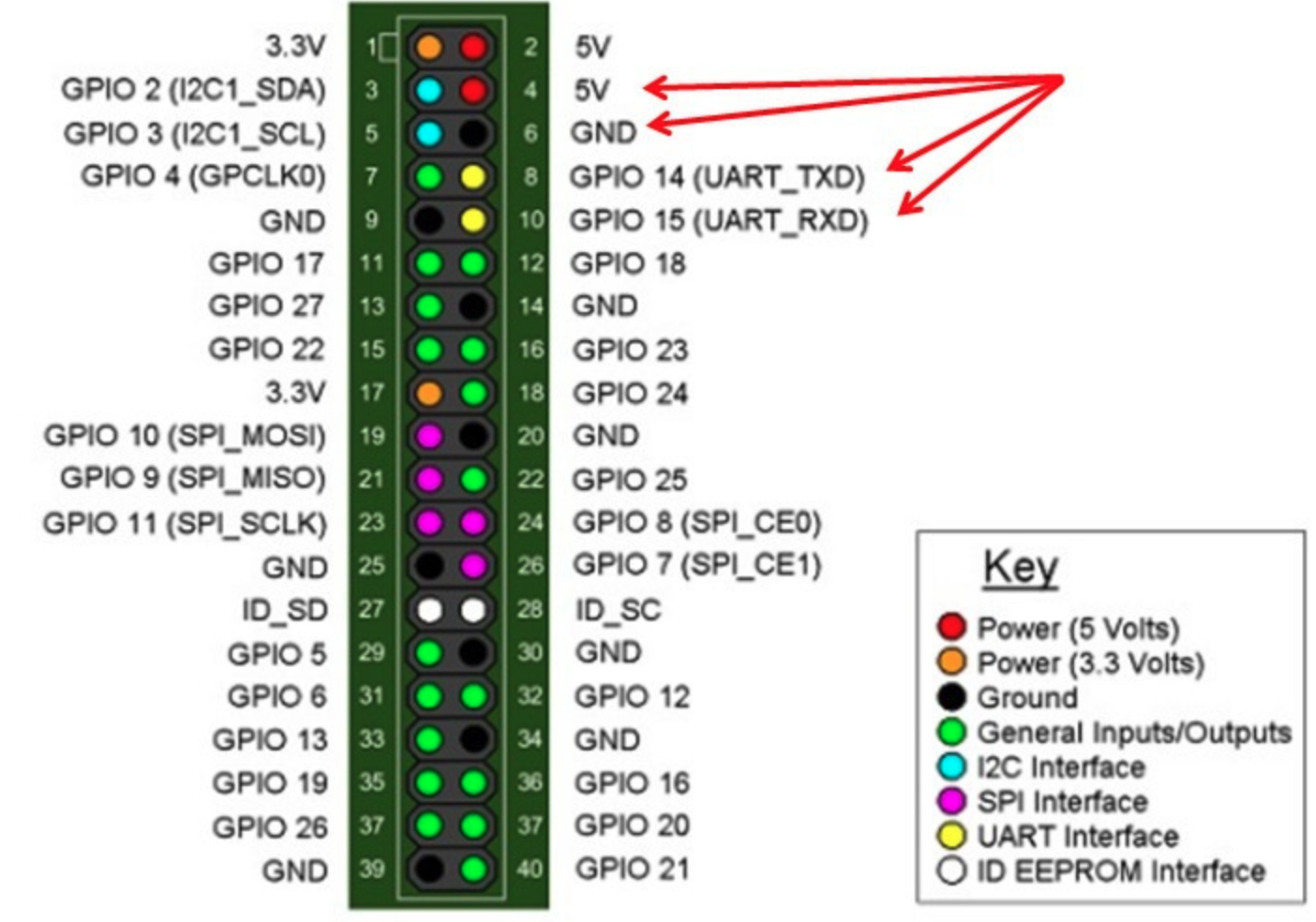
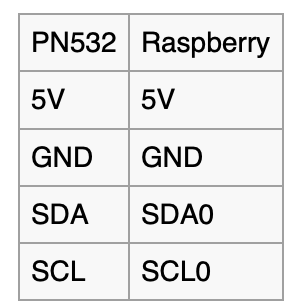


Рисунок 3.7 – Діаграма розміщення виводів Raspberry pi

Таблиця 3.1 – Підключення пристроїв



7. Для перевірки, чи розпізнається пристрій I2C запускаємо i2cdetect –y

1. Якщо так, це означає, що і модуль, і підключення працюють добре. Вводимо nfc-list, щоб перевірити модуль NFC:

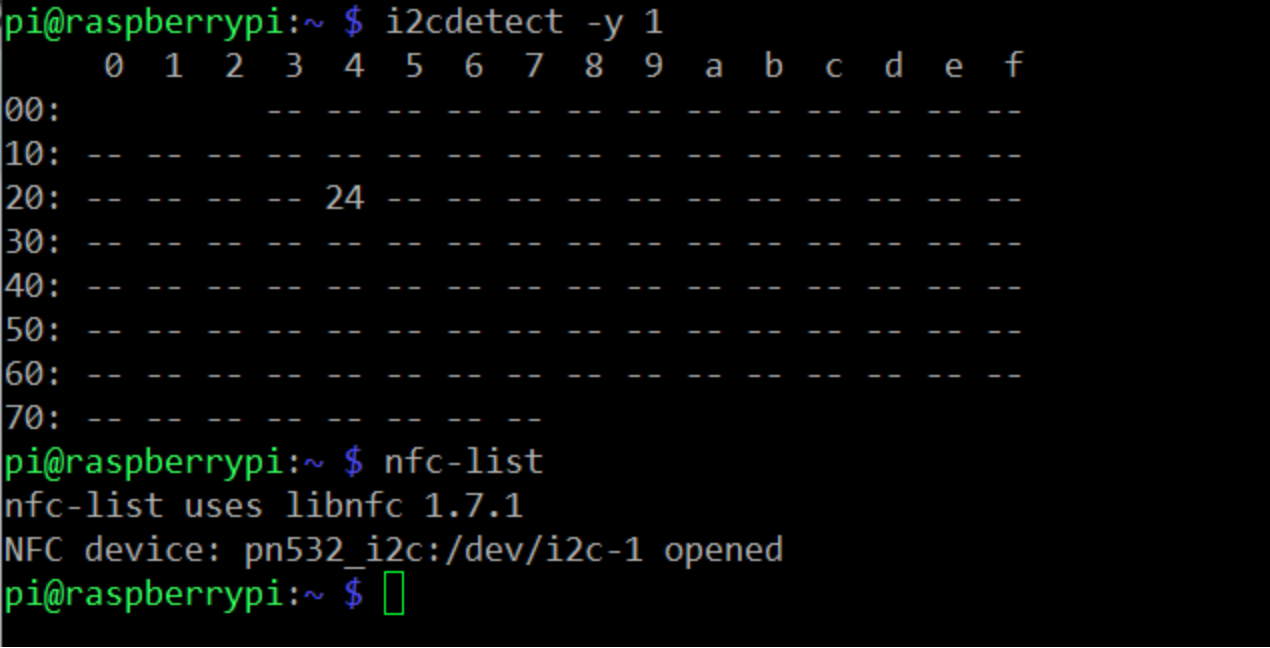


Рисунок 3.8 – Перевірка роботи модуля

Запускаємо nfc-poll, щоб відсканувати RFID-мітку, і можемо прочитати інформацію на картці (рисунок 3.9).

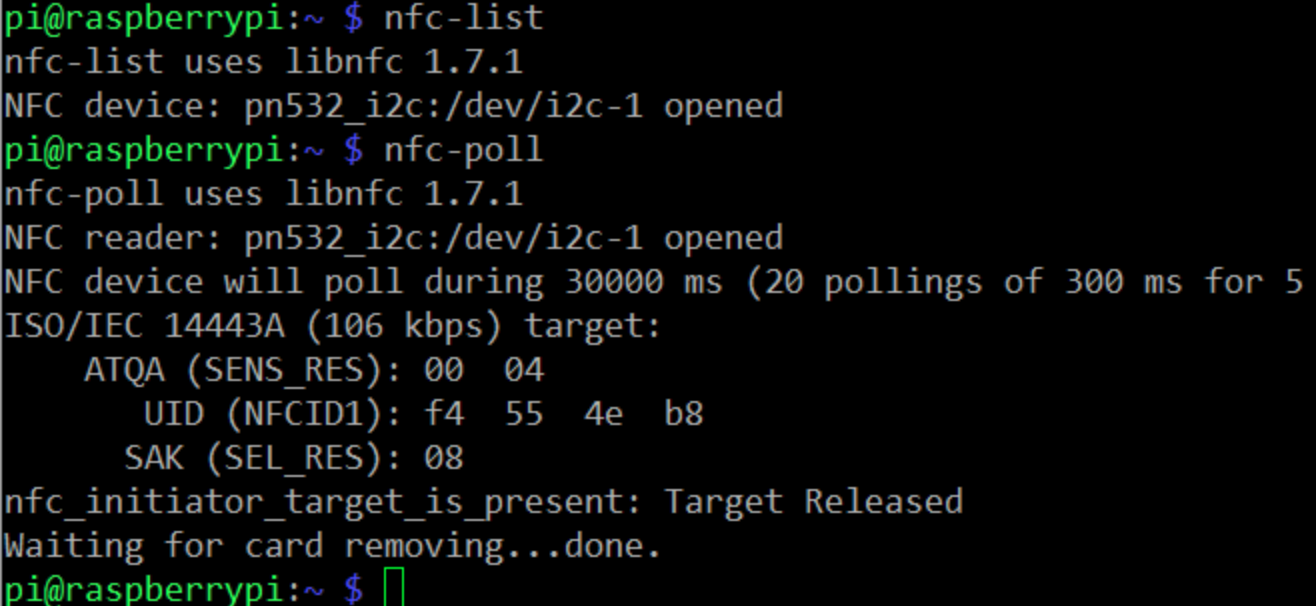


Рисунок 3.9 – Зчитування даних з картки

Використовуючи концепцію подвійної автентифікації, було реалізовано систему контролю доступу. Використання цієї концепції автентифікації на основі біометричної автентифікації та NFC, де також використовується сервер, забезпечує високу безпеку будь-якої захищеної зони, наприклад, центр обробки даних та інших приміщень. У багатьох випадках крадіжка ставить під загрозу безпеку викрадення картки та можливість обходу відбитку пальця при їх окремому використанню. Результати показують, що це рішення може забезпечити кращий захист з точки зору контролю доступу.

В загальному за допомогою розробленого рішення корпоративний офіс може забезпечити максимальний рівень безпеки автентифікації в системах контролю доступу.

ВИСНОВКИ

В кваліфікаційній роботі розв’язано актуальну задачу підвищення ефективності системи контролю доступу на основі використання двофакторної автентифікації. При цьому отримано наступні результати.

1. Проведено аналіз підходів до автентифікації в системах контролю доступу. Детально розглянуто фактори автентифікації. Обґрунтовано вибір методу автентифікації та переваги двофакторної автентифікації та двофакторної біометричної автентифікації.

2. Проаналізовано методи доступу до системи. Розроблено модель електронної автентифікації користувача та алгоритм роботи системи біометричної автентифікації. Проведено аналіз загроз безпеки біометричній автентифікації. Виділено параметри систем контролю доступу, які необхідно враховувати при розробці систем автентифікації.

3. Розроблено загальну структуру системи контролю доступу на основі двофакторної автентифікації. Розроблено алгоритм розпізнавання відбитку пальців для автентифікації користувачів в системі контролю доступу. Розроблена система контролю доступу на основі двофакторної автентифікації з використанням біометричного відбитку пальця та чіпу NFC.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lamport, L. Password authentication with insecure communication. Commun. ACM 1981, Volume 24, – pp. 770–772.

2. Ometov A., Bezzateev S., Mäkitalo N., Andreev, S., Mikkonen T., Koucheryavy Y. Multi-factor authentication: A survey. *Cryptography*, 2018, Volume *2*(1), 1.

3. Ibrokhimov, S., Hui, K. L., Al-Absi, A. A., & Sain, M. Multi-factor authentication in cyber physical system: A state of art survey. In *2019 21st International Conference on Advanced Communication Technology (ICACT)* 2019, February, – pp. 279-284. IEEE.

4. Ometov, A., & Bezzateev, S. Multi-factor authentication: A survey and challenges in V2X applications. In *2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT),* 2017, November. – pp. 129-136. IEEE.

5. Yang, T., Zhang, G., Liu, L., Yang, Y., Zhao, S., Sun, H., & Wang, W. New features of authentication scheme for the IoT: a survey. In *Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things*, 2019, November, – pp. 44-49.

6. Padma, P., & Srinivasan, S.. A survey on biometric based authentication in cloud computing. In *2016 International Conference on Inventive Computation Technologies (ICICT)*, Vol. 1, 2016, August, – pp. 1-5. IEEE.

7. Sharmila, K., Janaki, V., & Nagaraju, A. (). A Survey on User Authentication Techniques. *Oriental Journal of Computer Science & Technology*, *10*(2), 2017, – рр.513-519.

8. Shah, S. W., & Kanhere, S. S. (). Recent trends in user authentication–a survey. *IEEE access*, Volume *7*, 2019, – рр.112505-112519.

9. Paul Slovic and Ellen Peters. 2006. Risk Perception and Affect. Current Directions in Psychological Science 15, Volume 6, 2006, – рр. 322–325.

10. B. Chen, Y L. Huang, M G. Unes, “S-CBAC: A secure access control model for supporting group access for internet of things.” 2015 IEEE.

11. Hu V., Ferraiolo D., and Gavrila S, “Specification of Attribute Relations for Access Control Policies and Constraints Using Policy Machine”, Proceeding p32-35, the “Sixth International Conference on Information Assurance and Security” (IAS 2010), Atlanta, August 23-25, 2010

12. Hu V., Kuhn D., Xie T., and Hwang J., “Model Checking for Verification of Mandatory Access Control Models and Properties”, Int'l Journal of Software Engineering and Knowledge Engineering (IJSEKE) regular issue, Vol. 21, No. 1, 2011

13. NIST Special Publication 800-53A, Revision 4, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans, June 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

14. NIST Special Publication 800-53, Revision 5, Recommended Security Controls for Federal Information Systems and Organizations, Publ. 800-53, Rev. 5, 492 pages (September 2020) <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

15. Hu, V. C.; Scarfone, K. Guidelines for Access Control System Evaluation Metrics NIST-IR-7874. Gaithersburg, MD, 2012. – 49 р. Режим доступу: <https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7874.pdf>

16. Burr, W. E., Dodson, D. F., Newton, E. M., Perlner, R. A., Polk, W. T., Gupta, S., & Nabbus, E. A. Sp -1. Electronic authentication guideline, 2011.– 123. Режим доступу: https://nvlpubs.nist.gov/nistpubs/Legacy/ SP/nistspecialpublication800-63-1.pdf

17. Joshi, M., Mazumdar, B., & Dey, S. Security vulnerabilities against fingerprint biometric system. *arXiv preprint arXiv:1805.07116*, 2018.

18. E. Newton, S. Schuckers, “Recommendations for Presentation Attack Detection: Mitigation of threats due to spoof attacks,” International Biometric Performance Conference, 2016.

19. Roberts C. Biometric attack vectors and defences. Comput. Secur., vol. 26, no. 1, Feb. 2007. [Online]. pp. 14–25. Режим доступу: <http://dx.doi.org/10.1016/j.cose.2006.12.008>

20. Joshi M., Mazumdar B., Dey, S. Security vulnerabilities against fingerprint biometric system. *arXiv preprint arXiv:1805.07116*. 2018.

21. NIST, Strength of Function for Authenticators-Biometrics (SOFA-B): Discussion Draft Open for Comments. November 14, 2017. <https://pages.nist.gov/SOFA/SOFA.html>.