ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система управління привілейованим доступом (Privileged Access Management)» на об’єктах критичної інфраструктури»

на здобуття освітнього ступеня магістра
зі спеціальності __125 _Кібербезпека та захист інформації»_____
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

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

Виконав: здобувач вищої освіти групи СЗДМ 62
Анна ХОМЕНКО

Керівник: ПЕПА Юрій
к.т.н., доцент *(ПРІЗВИЩЕ, Ім’я)*

Рецензент: _____
(ПРІЗВИЩЕ, Ім’я)

Київ 2025

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

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУРОБОТУ

Хоменко Анні Олеговні
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Система управління привілейованим доступом (Privileged Access Management)» на об'єктах критичної інфраструктури»
керівник кваліфікаційної роботи __ПЕПА Юрій к.т.н., доцент_____
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій
від « 15 » жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи 20.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи: об'єкт критичної інфраструктури, технічні канал витоку інформації, вимоги до захисту інформації з обмеженим доступом, сучасні засоби системи контролю та управління доступом, технічні засоби захисту та технічної системи охорони
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1 Аналіз основних теоретичних аспектів застосування автоматизованих систем біометричного розпізнавання
4.2 Дослідження методів та засобів створення системи біометричного розпізнавання особи для захисту об'єктів критичної інфраструктури
4.3 Розробка та впровадження системи біометричного розпізнавання особи для захисту об'єктів критичної інфраструктури

5. Перелік графічного матеріалу: ___Презентаційний матеріал на слайдах.

6. Дата видачі завдання 20.10.2024

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Анна ХОМЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Юрій ПЕПА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Дипломна робота складається зі вступу, основної частини із трьох розділів, висновків, переліку джерел посилання.

Зміст роботи викладено на 83 сторінках. Перелік джерел посилання складається із 30 найменувань.

Мета роботи – розробка та впровадження автоматизованої системи управління привілейованим доступом (Privileged Access Management)» на об’єктах критичної інфраструктури.

Об’єкт дослідження – системи фізичного захисту інформації від несанкціонованого доступу на об’єкті інформаційної діяльності.

Предмет дослідження – автоматизованої системи управління привілейованим доступом на об’єкті інформаційної діяльності.

Наукова новизна одержаних результатів: удосконалено модуль біометричного розпізнавання особи для захисту об’єктів критичної інфраструктури базі апаратно-програмного комплексу Arduino, RFID-карток та додатку Inter Systems Cache.

Практичне значення одержаних результатів. Практичну цінність мають рекомендації щодо впровадження інноваційних методик розробки сучасних клієнт-сервісних систем розпізнавання особи для захисту об’єктів інформаційної діяльності на базі апаратно-програмного комплексу Arduino за допомогою RFID- карток та додатку Inter Systems Cache. Крім того, висновки, що зроблені в результаті даного дослідження, можуть бути використані в процесі подальшого удосконалення сучасних систем дистанційного контролю управління доступом для захисту об’єктів критичної інфраструктури на базі впровадження методу біометричного розпізнавання особи СКУД.

Апробація:

А.О. Хоменко Ефективність застосування привілейованого доступу. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.11 - 13.

https://duikt.edu.ua/uploads/p_2661_93669247.pdf

Ключові слова: БІОМЕТРИЧНЕ РОЗПІЗНАВАННЯ ОСОБИ, АВТОМАТИЗОВАНА СИСТЕМА, ОБ’ЄКТИ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, УПРАВЛІННЯ ДОСТУПОМ, КІБЕРЗАХИСТ, ІНТЕЛЕКТУАЛЬНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, СИСТЕМА АУТЕНТИФІКАЦІЇ.

ABSTRACT

The diploma thesis on the topic "Protection of critical infrastructure objects using biometric identification methods" consists of an introduction, the main part of three sections, conclusions, and a list of reference sources.

The content of the work is laid out on 83 pages. The list of reference sources consists of 30 items.

The purpose of the work is to develop and implement an automated system of biometric personal recognition.

The object of the study is the process of designing a web application for remote control of access management using biometric personal recognition tools.

The subject of the study is the theoretical and methodological aspects and empirical principles of the use of the personal recognition system for the protection of objects of information activity.

The scientific novelty of the obtained results: the biometric face recognition module for the protection of critical infrastructure objects based on the Arduino hardware and software complex, RFID cards and the Inter Systems Cache application has been improved.

Practical significance of the obtained results. Recommendations for the implementation of innovative methods for the development of modern client-service systems of personal recognition for the protection of objects of information activity based on the Arduino hardware and software complex with the help of RFID cards and the Inter Systems Cache application have practical value. In addition, the conclusions drawn as a result of this study can be used in the process of further improvement of modern remote control access control systems for the protection of critical infrastructure facilities based on the implementation of the biometric identification method of the ACS.

Approbation:

A.O. Khomenko Efficiency of the use of privileged access. All-Ukrainian scientific and practical conference: Current problems of security of information and telecommunication systems. Kyiv, November 03, 2024, Kyiv: RVC DUIKT. – 024. P.11 - 13.

https://duikt.edu.ua/uploads/p_2661_93669247.pdf

Keywords: BIOMETRIC PERSONAL RECOGNITION, AUTOMATED SYSTEM, INFORMATION ACTIVITY OBJECTS, ACCESS MANAGEMENT, CYBER PROTECTION, INTELLIGENT INFORMATION TECHNOLOGIES, AUTHENTICATION SYSTEM.

ЗМІСТ

РЕФЕРАТ……4
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ……7
ВСТУП……...……..9
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ЗАСТОСУВАННЯ АВТОМАТИЗОВАНИХ СИСТЕМ ПРІВІЛІГІЄВАНОГО ДОСТУПУ НА ОСНОВІ БІОМЕТРИЧНОГО РОЗПІЗНАВАННЯ..……..……12
1.1.Загальна характеристика об’єкта дослідження 12
1.2. Дослідження ідентифікаційних факторів аутентифікації ……..25
1.3. Постановка задачі дослідження ……37
1.4 Висновки до розділу .....……37

РОЗДІЛ 2. МЕТОДИ ТА ЗАСОБИ СТВОРЕННЯ СИСТЕМИ БІОМЕТРИЧНОГО РОЗПІЗНАВАННЯ ОСОБИ ДЛЯ ЗАХИСТУ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ……39
2.1. Огляд існуючих систем розпізнавання особи ……..……39
2.2. Підходи до проектування СБР та алгоритм її функціонування……...44
2.3. Обґрунтування вибору програмно-апаратних засобів для СБР……54
2.4 Висновки до розділу ..……64

РОЗДІЛ 3. ВПРОВАДЖЕННЯ СИСТЕМИ БІОМЕТРИЧНОГО РОЗПІЗНАВАННЯ ОСОБИ ДЛЯ ЗАХИСТУ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ…….....66
3.1. Розробка структурної схеми та архітектури системи розпізнавання особи для захисту об’єктів інформаційної діяльності……66
3.2. Моделювання системи біометричного розпізнавання особи……66
3.3. Впровадження СБР, її тестування та валідація ……72
3.4 Висновки до розділу ..……75

ВИСНОВКИ ……76
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ ……79
ДОДАТКИ……..83

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АПК – апаратно-програмний комплекс;

АСУ - автоматизована система управління;

БД – база даних;

ЕЦП –електронно-цифровий підпис;

ІІТ – інтелектуальні інформаційні технології;

ІС – інформаційна система;

ЕОД – електронний обмін даними;

НСД –несанціонований доступ;

ПК – персональний комп’ютер;

СБР – система біометричного розпізнавання;

СКУД – система контролю управління доступом;

СУБД – система управління базою даних;

ШІ – штучний інтелект.

ВСТУП

Актуальність дослідження. Наразі розвиток соціуму вимагає впровадження ІТ, які стають невід'ємною частиною підвищення актуальності різноманітних галузей наукової діяльності, в тому числі і тих, що мають безпосереднє відношення до проектування реальних об'єктів та клієнт-орієнтованих систем засобами штучного інтелекту.

Не секрет, що за сучасних умов функціонування процесів постійно створюються нові компанії. Такі фірми постійно мають користуватися сучасними ІІТ, що являють собою базу діяльності ІТС підприємства. Крім того, для оптимізаційних цілей власної діяльності компанії прагнуть підвищити ефективність інформаційної системи захисту, в тому числі через застосування АС для дистанційного контролю управління доступом.

СКУД являє собою певний набір технічних приладів та ПЗ, що надає можливість обмежити можливість проникнення до певної території і контролювати їх. Такі системи полегшують роботу великих компаній, забезпечують координацію та моніторинг пересування робітників, провадять облік робочого часу і визначають елементи порушення безпеки.

Основним завданням СКУД є управління доступом на приватну територію, включаючи також обмеження доступу на певну територію, ідентифікація особи, яка має доступ на таку територію, а також контроль робочого часу; облік зарплати (за умов інтеграцій із системами бухгобліку); створення загального обліку контрагентів; визначає принципи інтеграції із загальними системами безпеки.

Принцип роботи всіх СКУД однаковий. Він полягає у контролі пропуску тих, кому дозволено вхід.

Отже, вирішення питання інформаційної безпеки призводить до забезпечення інформаційного захисту на рівні людини, фірми або країни. Кібербезпека – це усталена система захисту передачі, опрацювання і зберігання інформації, за якої зберігається її конфіденційність і цілісність. Водночас

кібербезпека включає в себе набір алгоритмів, що направлені на забезпечення процесу інформаційного захисту від проникнення сторонніх осіб, від їх застосування, поширення чи внесення несанкціонованих трансформацій.

В цьому сенсі процеси аутентифікації являють собою важливий аспект забезпечення безпеки, адже вони автоматично здатні підтверджувати ідентичність людини і зберігають конфеденційні дані під час їхньої передачі.

Виходячи з вищеокресленого, наше проектування емпіричної реалізації СБР з ціллю забезпечити процес управління контролем доступу на підприємстві є актуальним.

Мета дослідження – розробка та впровадження автоматизованої системи біометричного розпізнавання особи.

Завдання дослідження:

1. дослідити ідентифікаційні фактори процесу аутентифікації;

2. розглянути існуючі системи біометричного розпізнавання особи та обґрунтувати вибір програмно-апаратних засобів для неї;

3. розробити систему автоматизованого контролю біометричного розпізнавання особи для захисту об’єктів критичної інфраструктури;

4. розробити практичні пропозиції щодо застосування інструментів системного аналізу відносно впровадження клієнт-сервісних програм в процесі розробки СБР.

Об’єкт дослідження – процес проектування веб-застосунку для дистанційного контролю управління доступом за допомогою засобів біометричного розпізнавання особи.

Предмет дослідження – теоретико-методичні аспекти та емпіричні засади застосування біометричного системи розпізнавання особи для захисту об’єктів інформаційної діяльності.

Методи дослідження: системний аналіз; аналіз наукових джерел; спостереження; абстрагування; узагальнюючий метод.

Інформаційні джерела: С. Ардатський, С. Вислоух, О. Висоцька, В. Ворожко, А. Грушко, О. Корченко, О. Лотов, Ю. Самохвалов, В. Соколов, та інших.

Наукова новизна одержаних результатів. удосконалено модуль біометричного розпізнавання особи для захисту об’єктів критичної інфраструктури базі апаратно-програмного комплексу Arduino, RFID-карток та додатку Inter Systems Cache.

Практичне значення одержаних результатів. Практичну цінність мають рекомендації щодо впровадження інноваційних методик розробки сучасних клієнт-сервісних систем розпізнавання особи для захисту об’єктів інформаційної діяльності на базі апаратно-програмного комплексу Arduino за допомогою RFID- карток та додатку Inter Systems Cache. Крім того, висновки, що зроблені в результаті даного дослідження, можуть бути використані в процесі подальшого удосконалення сучасних систем дистанційного контролю управління доступом для захисту об’єктів критичної інфраструктури на базі впровадження методу біометричного розпізнавання особи СКУД.

Структура роботи. Диплом складається зі вступу, 3 розділів, висновків, переліку джерел посилання, додатків. Загальний обсяг - 82 сторінки. Перелік джерел посилання складається із 50 найменувань.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ АСПЕКТИ ЗАСТОСУВАННЯ АВТОМАТИЗОВАНИХ СИСТЕМ БІОМЕТРИЧНОГО РОЗПІЗНАВАННЯ

1.1 Загальна характеристика об’єкта дослідження

У широкому розумінні інформаційні системи - це наукова галузь досліджень, яка охоплює низку стратегічних, управлінських та операційних дій, пов’язаних із збиранням, обробкою, зберіганням, поширенням та використанням інформації та пов’язаних з нею технологій у суспільстві та організаціях. Термін «інформаційні системи» також використовується для опису організаційної функції, яка застосовує знання ІС у галузі, державних установах та некомерційних організаціях .

Інформаційні системи часто відносяться до взаємодії між алгоритмічними процесами та технологіями. Ця взаємодія може відбуватися всередині або за межами організації. Інформаційна система - це технологія, яку використовує організація, а також спосіб, яким організації взаємодіють з технологією, та спосіб, яким технологія працює з бізнес-процесами організації. Інформаційні системи відрізняються від ІТ тим, що інформаційна система має компонент інформаційної технології, який взаємодіє з компонентами процесів [44].

Існують різні типи інформаційних систем, наприклад: системи обробки транзакцій, системи підтримки прийняття рішень, системи управління знаннями, системи управління навчанням, системи управління базами даних та офісні інформаційні системи. Критично важливими для більшості інформаційних систем є інформаційні технології, які зазвичай призначені для того, щоб люди могли виконувати завдання, для яких мозок погано підходить, наприклад: обробка великих обсягів інформації, виконання складних обчислень і управління багатьма одночасними процесами.

Інформаційні технології є дуже важливим та податливим ресурсом, доступним керівникам. Багато компаній створили посаду директора з

інформаційних технологій, яка входить до складу виконавчої ради разом з головним виконавчим директором (CEO), головним фінансовим директором (CFO), головним операційним директором (COO) та головним технічним директором (технічний директор). Технічний директор також може виконувати функції IT-директора та навпаки. Головний спеціаліст з інформаційної безпеки (CISO) займається управлінням інформаційною безпекою [41]

Структуру ІС представимо на рис. 1.1.

Рис. 1- Структура ІС компанії

Основними компонентами комп’ютерних інформаційних систем є [20]:

• Апаратне забезпечення. У сучасній інформаційній системі до цієї категорії належить сам комп’ютер та все його допоміжне обладнання. Допоміжне обладнання включає пристрої введення і виведення, пристрої зберігання і пристрої зв’язку. У докомп’ютерних інформаційних системах апаратне забезпечення могло включати бухгалтерські книги та чорнило.

• Програмне забезпечення: термін програмне забезпечення відноситься до комп’ютерних програм та посібників, які їх підтримують. Комп’ютерні програми є інструкціями для машин, які управляють схемою апаратних частин

системи таким чином, щоб вона виробляла корисну інформацію з даних. Програми зазвичай зберігаються на деякому носії вводу/виводу, часто на диску чи стрічці. «Програмне забезпечення» для докомп'ютерних інформаційних систем включало підготовку обладнання до використання (наприклад, заголовки стовпців у бухгалтерській книзі) та інструкції щодо їх використання (посібник з карткового каталогу).

• Дані: дані - це факти, які використовуються системами для отримання корисної інформації. У сучасних інформаційних системах дані зазвичай зберігаються в машиночитаній формі на диску або стрічці до тих пір, поки вони не потрібні комп'ютеру. У докомп'ютерних інформаційних системах дані зазвичай зберігаються в легкочитаній формі.

• Процедури. Процедури – це політики, які регулюють роботу інформаційної системи. "Процедури для людей те саме, що програмне забезпечення для обладнання" - це звичайна аналогія, яка використовується для ілюстрації ролі процедур у системі.

• Люди: Кожній системі потрібні люди, якщо вона хоче бути корисною. Найчастіше найбільш упускаемым з уваги елементом системи є люди, мабуть, компонент, який найбільше впливає успіх чи невдачу інформаційних систем. Сюди входять «не лише користувачі, а й ті, хто експлуатує та обслуговує комп'ютери, ті, хто підтримує дані, та ті, хто підтримує мережу комп'ютерів».

• Інтернет: Інтернет є комбінацією даних і людей. (Хоча цей компонент не є обов'язковим для роботи).

Ієрархію ІС представимо на рис. 1.2.

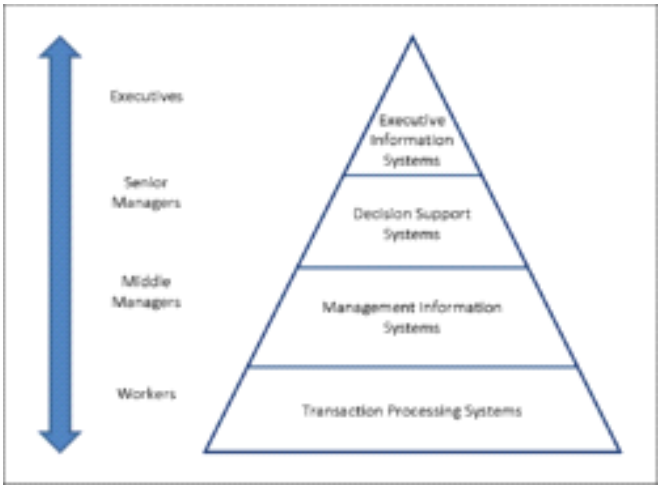


Рис. 1.2 - Чотирирівнева ієрархія ІС

Хоча ІС управління можуть використовуватися на будь-якому рівні управління, рішення про те, які системи впроваджувати, зазвичай приймається директорами з інформаційних технологій (CIO) та директорами з технологій. Ці співробітники зазвичай відповідають за загальну технологічну стратегію організації, включаючи оцінку того, як нові технології можуть допомогти їх організації. Вони виступають як особи, які приймають рішення у процесі впровадження нової ІС.

Нижче наведено типи інформаційних систем, що використовуються для створення звітів, отримання даних та допомоги в процесах прийняття рішень менеджерами середньої та оперативної ланки [27].

• Системи підтримки рішень (DSS) - це комп’ютерні програмні програми, які використовуються керівниками середньої та вищої ланки для збору інформації з широкого кола джерел для підтримки вирішення проблем та прийняття рішень. DSS використовується в основному для напівструктурованих та неструктурованих завдань прийняття рішень.

• Інформаційна система для керівників (EIS) – це інструмент звітності, який забезпечує швидкий доступ до зведених звітів, що надходять з усіх рівнів та відділів компанії, таких як бухгалтерія, відділ кадрів та операції.

• Маркетингові інформаційні системи - це управлінські інформаційні системи, розроблені спеціально управління маркетинговими аспектами бізнесу.

- Бухгалтерські інформаційні системи зосереджені облікових функціях.
- Системи управління людськими ресурсами застосовуються для кадрових аспектів.
- Системи автоматизації діловодства (OAS) підтримують зв’язок та продуктивність на підприємстві, автоматизуючи робочий процес та усуваючи вузькі місця. OAS може бути реалізований на будь-якому та всіх рівнях управління.
- Системи управління шкільною інформацією (SIMS) охоплюють адміністрацію школи, часто включаючи навчальні та навчальні матеріали.
- Програмне забезпечення для планування ресурсів підприємства (ERP) полегшує потік інформації між усіма бізнес-функціями всередині організації та управляє зв’язками із зовнішніми зацікавленими сторонами.
- Локальні бази даних можуть бути невеликими спрощеними інструментами для менеджерів і є первинною або базовою версією ІС.

Варто зазначити, що інформаційна безпека, що іноді скорочується до InfoSec - це практика захисту інформації шляхом зниження інформаційних ризиків. Це частина управління інформаційними ризиками. Зазвичай це включає запобігання або зниження ймовірності несанкціонованого/неналежного доступу до даних або незаконного використання, розкриття, порушення, видалення, спотворення, зміни, перевірки, запису або знецінення інформації. Це також включає дії, спрямовані на зниження несприятливих наслідків таких інцидентів.

Захищена інформація може приймати будь-яку форму, наприклад, електронну або фізичну, матеріальну (наприклад, документи) або нематеріальні (наприклад, знання). Основна увага в галузі інформаційної безпеки приділяється збалансованому захисту конфіденційності, цілісності та доступності даних (також відомої як тріада CIA), при цьому основна увага приділяється ефективної реалізації політик, і все це без шкоди для продуктивності організації [34].

Це значною мірою досягається за рахунок структурованого процесу управління ризиками, який включає [6]:

• виявлення інформації та пов’язаних активів, а також потенційних загроз, уразливостей та впливів;

• оцінка ризиків

• ухвалення рішення про те, як реагувати на ризики або обробляти їх, тобто уникати, пом’якшувати, розділяти або приймати їх

• там, де потрібне зниження ризику, вибір чи розробка відповідних заходів безпеки та їх реалізація

• моніторинг діяльності, внесення коригувань у міру необхідності для вирішення будь-яких проблем, змін та можливостей покращення.

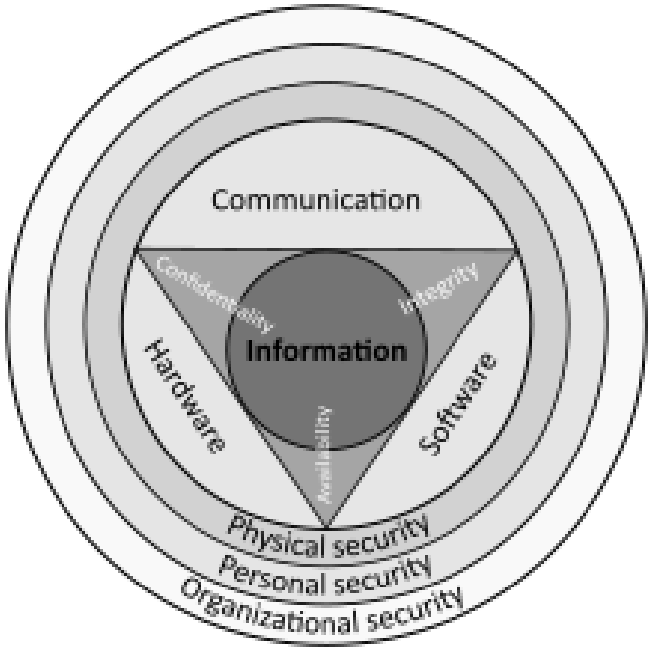


Рис. 1.3 - Атрибути інформаційної безпеки

Інформаційні системи складаються з трьох основних частин:

апаратного забезпечення, програмного забезпечення та засобів зв’язку, з метою допомогти визначити та застосувати галузеві стандарти інформаційної безпеки як механізми захисту та запобігання на трьох рівнях або рівнях: фізичному, особистому та організаційному.

По суті, процедури або політики реалізуються, щоб повідомити адміністраторів, користувачів та операторів, як використовувати продукти для забезпечення інформаційної безпеки в організаціях.

В основі інформаційної безпеки лежить гарантія інформації, дія підтримки конфіденційності, цілісності та доступності інформації, що гарантує, що інформація не буде скомпрометована будь-яким чином при виникненні критичних проблем. Ці проблеми включають, крім іншого, стихійні лиха, збої у роботі комп'ютерів/серверів та фізичну крадіжку. У той час як паперові бізнес-операції, як і раніше, переважають, вимагаючи власного набору методів інформаційної безпеки, все більше уваги приділяється корпоративним цифровим ініціативам.

Загрози інформаційної безпеки бувають різних форм. Одними з найпоширеніших сьогодні загроз є програмні атаки, крадіжка інтелектуальної власності, крадіжка особистих даних, крадіжка обладнання чи інформації, саботаж та вимагання інформації. Віруси, черв'яки, фішингові атаки і троянські коні - ось кілька поширених прикладів програмних атак. Крадіжка інтелектуальної власності також була серйозною проблемою для багатьох підприємств у галузі інформаційних технологій [16].

Крадіжка особистих даних це спроба діяти як хтось інший, зазвичай для отримання особистої інформації цієї людини або використання її доступу до життєво важливої інформації за допомогою соціальної інженерії. Крадіжка обладнання чи інформації сьогодні стає дедалі більш поширеною через те, що більшість сучасних пристроїв є мобільними, схильними до крадіжки, і навіть стають дедалі більше затребуваними зі збільшенням ємності даних. Саботаж зазвичай полягає у знищенні веб-сайту організації з метою викликати втрату довіри з боку її клієнтів.

Вимагання інформації складається з крадіжки майна або інформації компанії у спробі отримати платіж в обмін на повернення інформації або майна їхньому власнику, як у випадку з програмами-вимагачами. Є багато способів захистити себе від деяких з цих атак, але один з найбільш дієвих запобіжних

заходів - періодичне інформування користувачів. Загроза номер один для будь-якої організації - це користувачі або внутрішні співробітники, їх також називають внутрішніми загрозами.

Можливі відповіді на загрозу безпеці або ризику [9]:

- зменшити / пом’якшити - реалізувати заходи безпеки та контрзаходи для усунення вразливостей чи блокування загроз
- призначити/передати – покласти вартість загрози на іншу особу чи організацію, наприклад, на купівлю страховки чи аутсорсинг.
- прийняти - оцінити, чи перевищує вартість контрзаходу можливу вартість втрат через загрозу

Технології та інструменти безпеки та контролю.

Різні інструменти та технології, що використовуються для захисту від вторгнень або моніторингу, включають інструменти автентифікації, брандмауери, системи виявлення вторгнень, антивірусне програмне забезпечення та програмне забезпечення для шифрування.

Контроль доступу (політики та процедури, які компанія використовує для запобігання неправомірному доступу до систем з боку неавторизованих внутрішніх та сторонніх осіб) складається з усіх політик та процедур, які компанія використовує для запобігання неправомірному доступу до систем з боку неавторизованих внутрішніх та зовнішніх користувачів. Аутентифікація відноситься до здатності знати, що людина є тим, за кого себе видає. Програмне забезпечення контролю доступу призначене для того, щоб тільки авторизовані особи могли використовувати системи або отримувати доступ до даних, використовуючи будь-який метод аутентифікації. До нових технологій аутентифікації відносяться:

- Токен: фізичний пристрій, схожий на посвідчення особи, призначений для підтвердження особи окремого користувача.
- Смарт-карта: пристрій розміром із кредитну картку, що містить чіп, відформатований з дозволом доступу та іншими даними.

• Біометрична аутентифікація: порівнює унікальні характеристики людини, такі як відбитки пальців, зображення обличчя або сітківки ока зі збереженим заданим профілем.

Брандмауер являє собою комбінацію апаратного та програмного забезпечення, яке контролює потік вхідного та вихідного мережевого трафіку та запобігає несанкціонованому вхіду та виходу з мережі. Брандмауер ідентифікує імена, IP-адреси, програми та інші характеристики вхідного трафіку. Він звіряє цю інформацію за правилами доступу, запрограмованими в системі адміністратором мережі. Існує низка технологій екранування брандмауера:

Пакетна фільтрація досліджує поля у заголовках пакетів даних, що проходять між мережею та Інтернетом, досліджуючи окремі пакети ізольовано.

Перевірка стану визначає, чи є пакети частиною діалогу між відправником і одержувачем.

Перетворення мережевих адрес (NAT) приховує IP-адреси внутрішніх хост-комп’ютерів організації для захисту від програм-сніферів за межами брандмауера.

Фільтрування проксі програм перевіряє вміст пакетів програм.

Проксі-сервер зупиняє пакети даних, що виходять ззовні організації, перевіряє їх та передає проксі на інший бік брандмауера [14].

Якщо користувач за межами компанії хоче зв’язатися з користувачем всередині організації, зовнішній користувач спочатку розмовляє з проксі-додатком, а проксі-додаток зв’язується з внутрішнім комп’ютером фірми.

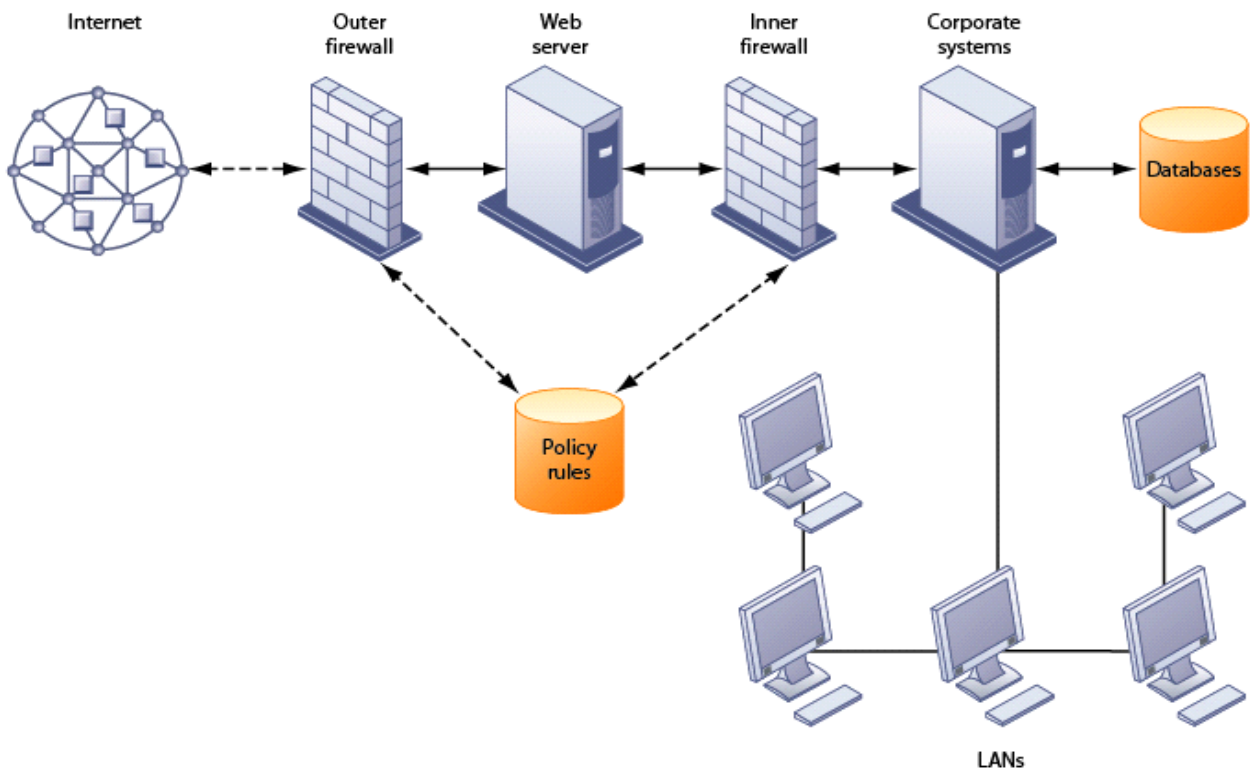


Рис. 1.4 - Корпоративний брандмауер

Брандмауер розміщується між приватною мережею фірми та загальнодоступним Інтернетом або іншою ненадійною мережею для захисту від несанкціонованого трафіку.

Системи виявлення вторгнень оснащені інструментами постійного моніторингу, розміщеними в найуразливіших точках корпоративних мереж для постійного виявлення та стримування зловмисників.

Програмне забезпечення для сканування шукає шаблони, що вказують на відомі методи комп'ютерних атак, такі як неправильні паролі, перевіряє, чи не було видалено або змінено важливі файли, і надсилає попередження про вандалізм або помилки системного адміністрування [4].

Антивірусне програмне забезпечення призначене для перевірки комп'ютерних систем та дисків на наявність комп'ютерних вірусів. Однак, щоб залишатися ефективним, антивірусне програмне забезпечення має постійно оновлюватись.

Постачальники обладнання Wi-Fi розробили суворіші стандарти безпеки. Специфікація 802.11i галузевої торгової групи Wi-Fi Alliance посилює безпеку продуктів для бездротових локальних мереж.

Багато організацій використовують шифрування для захисту конфіденційної інформації, що передається мережами.

Шифрування - це кодування та скремблювання повідомлень для запобігання доступу до них сторонніх осіб.

Два методи шифрування мережного трафіку в Інтернеті:

SecureSocketsLayer (SSL) :SSL та його наступник TransportLayerSecurity (TLS) дозволяють клієнтським та серверним комп'ютерам встановлювати сеанс безпечного з'єднання та керувати операціями шифрування та дешифрування.

Протокол захищеної передачі гіпертексту (S-HTTP) - це ще один протокол, який використовується для шифрування даних, що передаються через Інтернет, але обмежений окремими повідомленнями.

Дані шифруються шляхом застосування секретного числового коду, що називається ключем шифрування, так що дані передаються у вигляді зашифрованого набору символів. Щоб бути прочитаним, повідомлення має бути розшифроване (розшифроване) за допомогою відповідного ключа. Існує два альтернативні методи шифрування:

Шифрування із симетричним ключем: відправник та одержувач створюють спільний ключ шифрування (рис. 1.5).

Шифрування з відкритим ключем: безпечніший метод шифрування, в якому використовуються два різні ключі: закритий і відкритий.

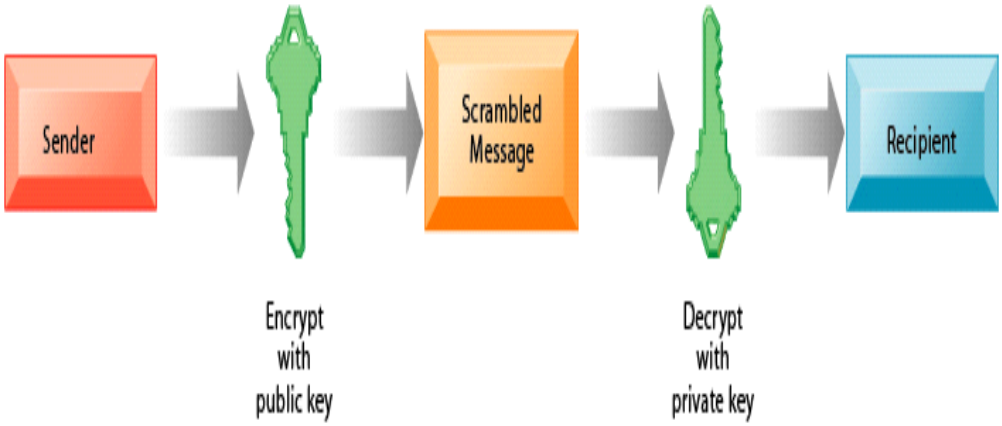


Рис. 1.5 –Схема шифрування з відкритим ключем

Систему шифрування з відкритим ключем можна розглядати як серію відкритих і закритих ключів, які блокують дані при їх передачі та розблокують дані при їх отриманні.

Відправник знаходить відкритий ключ одержувача в каталозі та використовує його для шифрування повідомлення.

Повідомлення надсилається у зашифрованому вигляді через Інтернет або приватну мережу. Коли надходить зашифроване повідомлення, одержувач використовує свій закритий ключ для розшифрування даних та читання повідомлення.

Цифрові підписи та цифрові сертифікати допомагають з автентифікацією. Цифровий підпис - це цифровий код, прикріплений до електронного повідомлення, який використовується для перевірки походження та змісту повідомлення [15].

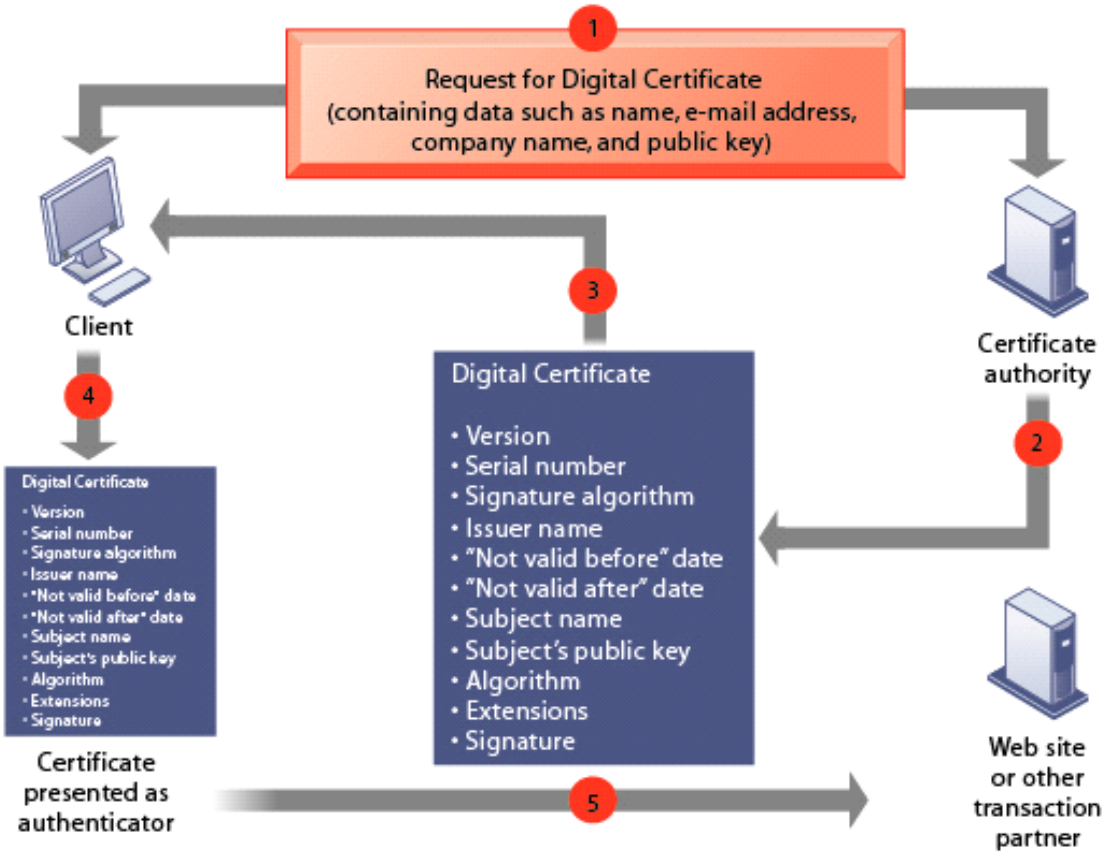


Рис. 1.6 – Цифрові сертифікати

Цифрові сертифікати – це файли даних, які використовуються для встановлення особи користувачів та електронних активів для захисту онлайн-транзакцій.

Система цифрових сертифікатів використовує довірену третю сторону, відому як центр сертифікації (ЦС), для перевірки особи користувача.

Система цифрових сертифікатів дозволить, наприклад, користувачу кредитної картки та продавцю підтвердити, що їх цифрові сертифікати були видані уповноваженою та довіреною третьою стороною, перш ніж вони обмінюватимуться даними [16].

Інфраструктура відкритих ключів (PKI), використання криптографії з відкритим ключем, що працює з центром сертифікації, є основною технологією забезпечення безпечної автентифікації особистості в Інтернеті (рис.1.6).

Цифрові сертифікати допомагають встановити особу людей або електронних активів. Вони захищають онлайн-транзакції, забезпечуючи безпечне, зашифроване онлайн-спілкування.

1.2 Дослідження ідентифікаційних факторів аутентифікації

Аутентифікація - це акт доказу твердження, такого як особистість користувача комп'ютерної системи. На відміну від ідентифікації, дії за вказівкою особи чи речі, автентифікація є процесом перевірки цієї особи.

Це може включати перевірку документів, що засвідчують особу, аутентифікацію веб-сайту за допомогою цифрового сертифіката , визначення віку артефакту за допомогою радіовуглецеве датування або перевірка того, що продукт або документ не є підробленими .

Аутентифікацію можна розділити на три типи:

Перший тип аутентифікації - це прийняття посвідчення особи, наданої заслуговує на довіру особою, яка має докази справжності особистості з перших рук. Коли потрібна автентифікація творів мистецтва чи фізичних об'єктів, цим доказом може бути друг, член сім'ї чи колега, що підтверджує походження предмета, можливо засвідчив предмет, що у володінні його творця [34].

У випадку зі спортивними пам'ятними речами з автографами це може включати підтвердження того, що хтось був свідком підписання об'єкта. Продавець, що продає фірмові товари, має на увазі справжність, хоча у нього може не бути доказів того, що кожен крок у ланцюжку поставок пройшов перевірку справжності.

Централізовані довірчі відносини, що ґрунтуються на авторитетах, підтримують найбільш безпечний інтернет-зв'язок через відомі загальнодоступні центри сертифікації; децентралізована рівноправна довіра, також відома як мережа довіри використовується для особистих послуг, таких як електронна пошта або файли (Pretty Good Privacy, GNU Privacy Guard), і довіра

встановлюється відомими людьми, які підписують криптографічний ключ один одного, наприклад, на сторонах, що підписують ключі.

Другий тип аутентифікації - це порівняння атрибутів самого об’єкта з тим, що відомо про об’єкти цього походження.

Наприклад, мистецтвознавець може знайти схожість у стилі живопису, перевірити розташування та форму підпису або порівняти об’єкт зі старою фотографією.

З іншого боку, археолог може використовувати вуглецевий аналіз .щоб перевірити вік артефакту, проведіть хімічний та спектроскопічний аналіз матеріалів, що використовуються, або порівняйте стиль конструкції або прикраси з іншими артефактами аналогічного походження.

Фізика звуку та світла, а також порівняння з відомим фізичним оточенням можна використовувати для перевірки автентифікації аудіозаписів, фотографій або відео.

Документи можуть бути перевірені як створені на чорнилі або папері, які були доступні під час створення елемента [21].

Порівняння атрибутів може бути вразливим для підробки. В цілому він спирається на той факт, що створення підробки, невідмінної від справжнього артефакту, вимагає експертних знань, що помилки легко допускаються і що кількість зусиль, необхідних для цього значно перевищує кількість прибутку, який можна отримати від підробки.

Як правило, користувач повинен вибрати ім’я користувача або ідентифікатор користувача та надати дійсний пароль для початку використання системи (рис. 1.7).

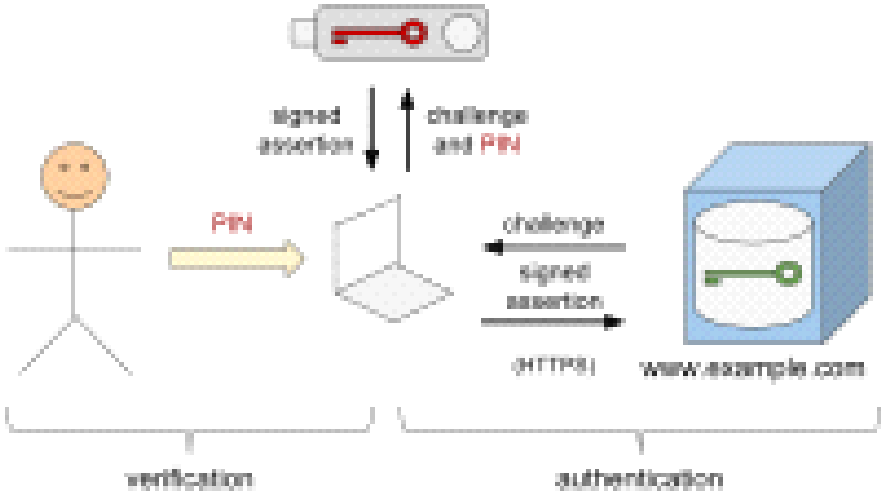


Рис. 1.7 – Схема типового потоку веб-аутентифікації (WebAuthn)

Третій тип аутентифікації ґрунтується на документації або інших зовнішніх підтвердженнях. У кримінальних судах правила доказування часто вимагають встановлення ланцюжка зберігання поданих доказів. Це можна зробити за допомогою журналу письмових доказів або показань свідків поліцейських детективів та судово-медичних експертів, які займалися цим. Деякі предмети антикваріату супроводжуються сертифікатами, що засвідчують їхню справжність. Підписані спортивні речі зазвичай супроводжуються сертифікатом автентичності. Ці зовнішні записи мають свої власні проблеми з підробкою та лжесвідченням, а також можуть бути відокремлені від артефакту та втрачені [26].

Способи аутентифікації будь-кого можна розділити на три категорії, засновані на так званих факторах аутентифікації: щось, що користувач знає, щось, що є у користувача, і щось, чим є користувач.

Кожен фактор аутентифікації охоплює ряд елементів, що використовуються для аутентифікації або перевірки особи перед наданням доступу, затвердженням запиту на транзакцію, підписанням документа або іншого робочого продукту, наданням повноважень іншим особам та встановленням ланцюжка повноважень.

Дослідження безпеки показало, що для позитивної аутентифікації повинні бути перевірені елементи як мінімум двох, а найкраще трьох факторів.

Три фактори (класу) та деякі елементи кожного фактора:

• фактори знань: щось, що знає користувач (наприклад, пароль, частковий пароль, фраза-пароль, персональний ідентифікаційний номер (ПІН-код), запит-відповідь (користувач повинен відповісти на запитання або шаблон), контрольне питання).

• фактори володіння: те, що є у користувача (наприклад, браслет, посвідчення особи, токен безпеки, імплантований пристрій, стільниковий телефон з вбудованим апаратним токеном, програмний токен або мобільний телефон з програмним токеном).

• фактори приналежності: щось, чим є або що робить користувач (наприклад, відбиток пальця, структура сітківки, послідовність ДНК (існують різні визначення того, що достатньо), підпис, особа, голос, унікальні біоелектричні сигнали або інші біометричні ідентифікатори).

Для компаній та інших структур аутентифікацію можна здійснити завдяки системі так званого єдиного входу (SSO), що надає доступ до декількох систем з єдиним набором облікових даних (рис. 1.8).

Рис. 1.8 – Приклад технології SSO

Способи аутентифікації включають в себе наступні етапи[23]:

- Двофакторна аутентифікація .
- Багатофакторна аутентифікація.
- Генерація одноразового паролю.
- Біометрична аутентифікація.
- Мобільна аутентифікація.
- Відкрита авторизація (OAuth).

Одним із відомих способів використання аутентифікації та авторизації є управління доступом. Комп'ютерна система, яка повинна використовуватися лише авторизованими особами, має намагатися виявляти та виключати неавторизованих. Тому доступ до нього зазвичай контролюється шляхом наполягання на процедурі аутентифікації для встановлення з певним ступенем впевненості особи користувача, надаючи привілеї, встановлені для цієї особи.

Біометрична аутентифікація (або реалістична аутентифікація) використовується в інформатиці як форма ідентифікації та контролю доступу. Він також використовується для виявлення осіб у групах, які перебувають під наглядом.

Біометричні ідентифікатори – це відмінні, вимірні характеристики, що використовуються для позначення та опису людей. palign="justify">.

Приклади включають, але не обмежуються відбитками пальців, венами долонь, розпізнаванням облич, ДНК, відбитком долоні, геометрією руки, розпізнаванням райдужної оболонки ока, сітківкою.

Поведінкові характеристики пов'язані з моделлю поведінки людини, включаючи, крім іншого, рух миші, ритм набору тексту, ходу, підпис, поведінкове профільування та облікові дані [40].

Деякі дослідники запровадили термін «біхевіометрія» для опису останнього класу біометрії.

До більш традиційних засобів контролю доступу належать системи ідентифікації на основі токенів, такі як права водія або паспорт, і системи

ідентифікації на основі знань, такі як пароль або особистий ідентифікаційний номер.

Оскільки біометричні ідентифікатори є унікальними для окремих осіб, вони більш надійні для перевірки особистості, ніж методи, що базуються на токенах і знаннях; однак збір біометричних ідентифікаторів викликає занепокоєння щодо конфіденційності кінцевого використання цієї інформації.

Для біометричної аутентифікації можна використовувати безліч різних аспектів людської фізіології, хімії чи поведінки. Вибір конкретної біометрії для використання в конкретній програмі включає зважування кількох факторів. Джейн та ін. (1999) визначили сім таких факторів, які слід використовувати при оцінці придатності будь-якої ознаки для використання в біометричній аутентифікації [34].

Універсальність означає, що кожна людина, яка використовує систему, повинна мати цю рису.

Унікальність означає, що ознака має бути досить різним для особин відповідної популяції, щоб їх можна було відрізнити один від одного.

Постійність відноситься до того, як ознака змінюється у часі. Зокрема, ознака з «хорошим» сталістю буде досить інваріантним з часом по відношенню до конкретного алгоритму зіставлення.

Вимірюваність відноситься до легкості придбання або вимірювання ознаки. Крім того, отримані дані повинні бути у формі, що дозволяє подальшу обробку та вилучення відповідних наборів ознак.

Продуктивність пов’язана з точністю, швидкістю та надійністю використовуваної технології (додаткову інформацію див. у розділі продуктивності).

Прийнятність пов’язана з тим, наскільки добре люди з відповідної групи населення приймають технологію, тому вони хочуть, щоб їхні біометричні характеристики були зафіксовані та оцінені.

Обхід відноситься до легкості, з якою риса може бути зімітована за допомогою артефакту або заміни.

Правильне використання біометричних даних дуже залежить від додатка. Деякі біометричні дані будуть кращими за інші залежно від необхідного рівня зручності та безпеки.

Жодна біометрична система неспроможна задовольнити всім вимогам кожного можливого докладання.

Блок-схема ілюструє два основних режими біометричної системи.

По-перше, в режимі верифікації (або аутентифікації) система виконує однозначне порівняння захоплених біометричних даних з певним шаблоном, що зберігається в біометричній базі даних, щоб переконатися, що людина є тим, за кого себе видає.

Три кроки беруть участь у перевірці людини. У першому етапі створюються еталонні моделі всім користувачів, які зберігаються у базі даних моделей.

На другому етапі деякі зразки зіставляються з еталонними моделями для отримання оцінок справжності та самозванця та розрахунку порога.

Третій крок – етап тестування. У цьому процесі можна використовувати смарт-картку, ім’я користувача або ідентифікаційний номер (наприклад, PIN-код), щоб вказати, який шаблон слід використовувати для порівняння.

"Позитивне розпізнавання" - це звичайне використання режиму перевірки, "де мета полягає в тому, щоб запобігти використанню однієї й тієї ж особистості кількома людьми".

По-друге, в режимі ідентифікації система виконує порівняння «один до багатьох» із біометричною базою даних, намагаючись встановити особу невідомої людини.

Системі вдасться ідентифікувати людину, якщо порівняння біометричного зразка з шаблоном у базі даних укладається раніше встановлений поріг.

Режим ідентифікації можна використовувати або для «позитивного розпізнавання» (щоб користувачу не потрібно було надавати будь-яку інформацію про шаблон, що використовується), або для «негативного

розпізнавання» людини, «де система встановлює, чи є людина тим, ким вона є». (явно чи неявно) заперечує бути».

Остання функція може бути досягнута тільки за допомогою біометрії, оскільки інші методи розпізнавання особистості, такі як паролі PIN-коди або ключі неефективні (рис. 1.9).

Перший раз, коли людина використовує біометричну систему, називається зарахуванням. Під час реєстрації біометрична інформація про людину збирається та зберігається [35].

Перший блок (сенсор) - це інтерфейс між реальним світом та системою; він має отримати всі необхідні дані. Найчастіше це система отримання зображень, але може змінюватися залежно від бажаних характеристик.

Другий блок виконує всю необхідну попередню обробку: він повинен видалити артефакти від датчика, для поліпшення введення (наприклад, видалення фонового шуму), для використання деякої нормалізації.

У третьому блоці витягуються необхідні функції. Цей крок є важливим кроком, оскільки правильні функції мають бути вилучені оптимальним чином. Для створення шаблону використовується вектор чисел або зображення з певними властивостями. Шаблон є синтезом відповідних характеристик, витягнутих з джерела. Елементи біометричного вимірювання, які не використовуються в алгоритмі порівняння, відкидаються у шаблоні, щоб зменшити розмір файлу та захистити особистість зарахованого (рис. 1.10).

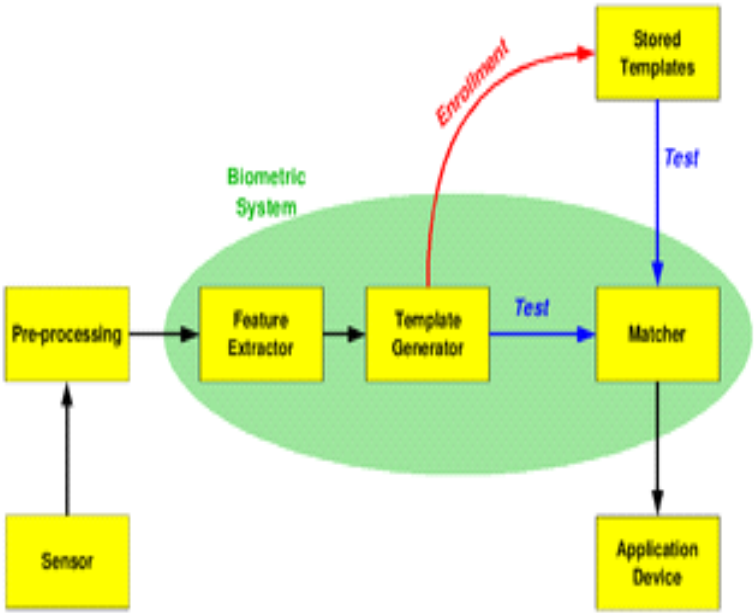


Рис. 1.9 – Алгоритм розпізнавання особи

Біометричний острів досліджує зображення обличчя у 2D та 3D, тембр голосу та перевіряє рукописний підпис.

На етапі реєстрації шаблон просто зберігається десь (на карті, у базі даних чи тому й іншому).

На етапі зіставлення отриманий шаблон передається у співставник, який порівнює його з іншими існуючими шаблонами, оцінюючи відстань між ними за допомогою будь-якого алгоритму (наприклад, відстань Хеммінга).

Програма зіставлення проаналізує шаблон із вхідними даними. Потім це буде виведено для певного використання або мети (наприклад, вхід до зони з обмеженим доступом), хоча є побоювання, що використання біометричних даних може мати справу з розповзанням місії.

Вибір біометрії для будь-якого практичного застосування залежно від характерних вимірів та вимог користувача [36].

Рис. 1.10 – Принцип роботи біометричного вимірювання

При виборі конкретного біометричного параметра слід враховувати такі фактори, як продуктивність, соціальна прийнятність, простота обходу та/або підробки, надійність, охоплення населення, розмір необхідного обладнання та захист від крадіжки особистих даних.

Вибір біометрії ґрунтується на вимогах користувача та враховує доступність датчиків та пристроїв, час обчислень та надійність, вартість, розмір датчика та енергоспоживання.

Мультимодальні біометричні системи використовують кілька датчиків чи біометричних даних для подолання обмежень одномодальних біометричних систем. Наприклад, системи розпізнавання райдужної оболонки можуть бути скомпрометовані через старіння райдужної оболонки, а розпізнавання електронних відбитків пальців може погіршитися через зношені або порізані відбитки пальців.

Хоча одномодальні біометричні системи обмежені цілісністю свого ідентифікатора, малоймовірно, що кілька одномодальних систем страждатимуть від однакових обмежень.

Мультимодальні біометричні системи можуть отримувати набори інформації від одного і того ж маркера (наприклад, кілька зображень райдужної оболонки ока або відскановані зображення одного й того ж пальця) або інформацію від різних біометричних даних (потрібне сканування відбитків пальців та, при використанні розпізнавання голосу, голосовий пароль).

Мультимодальні біометричні системи можуть об'єднувати ці одномодальні системи послідовно, одночасно їх комбінацією або послідовно, що відноситься до послідовного, паралельного, ієрархічного і послідовного режимів інтеграції відповідно.

Злиття біометричної інформації може відбуватися на різних етапах системи розпізнавання. У разі злиття на рівні функцій об'єднуються самі дані або функції, вилучені з кількох біометричних даних [39].

Злиття лише на рівні оцінки відповідності поєднує оцінки, отримані кількома класифікаторами, які стосуються різним модальностям.

Зрештою, у разі злиття на рівні прийняття рішень остаточні результати кількох класифікаторів об'єднуються за допомогою таких методів, як голосування з більшості.

Злиття на рівні ознак вважається більш ефективним, ніж злиття на інших рівнях, тому що набір ознак містить більш багату інформацію про вхідні біометричні дані, ніж оцінка відповідності або вихідне рішення класифікатора. Тому очікується, що злиття на рівні ознак забезпечить найкращі результати розпізнавання.

Підроблені атаки полягають у відправленні підроблених біометричних характеристик у біометричні системи і є серйозною загрозою, яка може знизити їхню безпеку.

Зазвичай вважається, що мультимодальні біометричні системи стійкіші до атак з підробкою, але недавні дослідження показали, що їх можна обійти, підмінивши навіть одну біометричну характеристику.

Адаптивні біометричні системи призначені для автоматичного оновлення шаблонів або моделей відповідно до внутрішньокласових змін робочих даних.

Подвійна перевага цих систем полягає у вирішенні проблеми обмежених навчальних даних та відстеження тимчасових змін вхідних даних за допомогою адаптації. Останнім часом адаптивна біометрія привернула значну увагу дослідницької спільноти.

Очікується, що цей напрямок досліджень набиратиме обертів через їх основні оприлюднені переваги.

По-перше, з адаптивною біометричною системою більше не потрібно збирати велику кількість біометричних зразків у процесі зарахування.

По-друге, більше не потрібно заново реєструватися або перенавчати систему з нуля, щоб впоратися із середовищем, що змінюється.

Ця зручність дозволяє значно знизити витрати на утримання біометричної системи. Незважаючи на ці переваги, існує кілька відкритих питань, пов’язаних із цими системами. При помилці класифікації (хибному прийомі) біометричної системи викликати адаптацію з використанням зразка-імпостера. Однак постійні дослідницькі зусилля спрямовані на вирішення відкритих питань, пов’язаних із областю адаптивної біометрії [29].

Останнім часом з’явилася біометрія, заснована на сигналах мозку (електренцефалограма) і серця (електрокардіограма).

Прикладом може бути розпізнавання вен на пальці з допомогою методів розпізнавання образів, заснованих на зображеннях судинних візерунків людини. Перевага такої «футуристичної» технології в тому, що вона більш стійка до шахрайства, порівняно із звичайними біометричними даними, такими як відбитки пальців.

Однак така технологія, як правило, більш громіздка і, як і раніше, має такі проблеми, як нижча точність і погана відтворюваність з часом.

Щодо портативності біометричних продуктів, то все більше і більше постачальників використовують значно мініатюризовані системи біометричної аутентифікації (BAS), тим самим домагаючись продуманої економії коштів, особливо при великомасштабному розгортанні.

1.3 Постановка задачі дослідження

Метою є проектування системи біометричного розпізнавання особи для захисту об’єктів критичної інфраструктури базі апаратно-програмного комплексу Arduino, RFID-карток та додатку Inter Systems Cache.

Ставимо перед собою наступні задачі:

1. дослідити ідентифікаційні фактори процесу аутентифікації;

2. розглянути існуючі системи біометричного розпізнавання особи та обґрунтувати вибір програмно-апаратних засобів для неї;

3.розробити систему автоматизованого контролю біометричного розпізнавання особи для захисту об’єктів критичної інфраструктури;

4.розробити практичні пропозиції щодо застосування інструментів системного аналізу відносно впровадження клієнт-сервісних програм в процесі розробки СБР.

1.4 Висновки до розділу

Підсумовуючи перший розділ, можемо зробити такі висновки:

• Визначено, що ІС являє собою організаційну систему, що призначається для процесів збору, оброблення, зберігання і поширення даних.

• Охарактеризовано, що аутентифікація – це процес перевірки особистості користувача. Технологія перевірки аутентичності спроможна здійснювати контроль за доступом для різних систем, здійснюючи інспекцію даних користувача. Вона перевіряє збіг даних із його обліковими даними в загальній БД користувачів на сервері аутентифікації. Таким чином аутентифікація - це структура функціонування будь-якого ПЗ та всі небезпеки, що пов’язані з нею, є критичними для більшості сучасних ІС.

• Оклеслено, що вибір біометрії для будь-якого практичного застосування залежить від характерних вимірів та вимог користувача. При виборі конкретного біометричного параметра слід враховувати такі фактори, як продуктивність,

соціальна прийнятність, простота обходу та/або підробки, надійність, охоплення населення, розмір необхідного обладнання та захист від крадіжки особистих даних. При цьому вибір біометрії ґрунтується на вимогах користувача та враховує доступність датчиків та пристроїв, час обчислень та надійність, вартість, розмір датчика та енергоспоживання.

• Мультимодальні біометричні системи використовують кілька датчиків чи біометричних даних для подолання обмежень одномодальних біометричних систем. Наприклад, системи розпізнавання райдужної оболонки можуть бути скомпрометовані через старіння райдужної оболонки, а розпізнавання електронних відбитків пальців може погіршитися через зношені або порізані відбитки пальців. Хоча одномодальні біометричні системи обмежені цілісністю свого ідентифікатора, малоймовірно, що кілька одномодальних систем страждатимуть від однакових обмежень. Мультимодальні біометричні системи можуть отримувати набори інформації від одного і того ж маркера (наприклад, кілька зображень райдужної оболонки ока або відскановані зображення одного й того ж пальця) або інформацію від різних біометричних даних (потрібне сканування відбитків пальців та, при використанні розпізнавання голосу, голосовий пароль). Мультимодальні біометричні системи можуть об’єднувати ці одномодальні системи послідовно, одночасно їх комбінацією або послідовно, що відноситься до послідовного, паралельного, ієрархічного і послідовного режимів інтеграції відповідно.

РОЗДІЛ 2.
МЕТОДИ ТА ЗАСОБИ СТВОРЕННЯ СИСТЕМИ БІОМЕТРИЧНОГО РОЗПІЗНАВАННЯ ОСОБИ ДЛЯ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Огляд існуючих систем розпізнавання особи

У сфері фізичної безпеки та інформаційної безпеки контроль доступу (АС) – це вибіркове обмеження доступу до місця або іншого ресурсу, а управління доступом описує процес. Акт доступу може означати споживання, вхід або використання. Дозвіл на доступ до ресурсу називається авторизацією.

Блокування та облікові дані для входу – це два аналогічні механізми контролю доступу [43].

Термін «контроль доступу» стосується практики обмеження доступу на територію, будинок або кімнату уповноваженим особам. Фізичний контроль доступу може здійснюватися людиною (охоронцем, вибивалою або секретарем) за допомогою механічних засобів, таких як замки та ключі, або за допомогою технологічних засобів, таких як системи контролю доступу, такі як пастки для людей. У цих середовищах управління фізичними ключами також може використовуватися як засіб подальшого управління та контролю доступу до областей з механічними ключами або доступу до певних невеликих активів.

Контроль фізичного доступу залежить від того, хто, де та коли. Система контролю доступу визначає, кому дозволено входити чи виходити, де їм дозволено виходити чи входити, і коли їм дозволено входити чи виходити. Історично це частково досягалося за допомогою ключів та замків. Коли двері замкнені, в неї може увійти тільки той, хто має ключ, залежно від конфігурації замка [42].

Механічні замки та ключі не дозволяють прив'язувати власника ключа до певного часу чи дати. Механічні замки та ключі не надають записів про ключ, використаний для будь-яких конкретних дверей, і ключі можна легко скопіювати або передати неуповноваженій особі. Коли механічний ключ загублений або

власник ключа більше не має права використовувати зону, що охороняється, замки повинні бути перекодовані.

Електронний контроль доступу (ЕАС) використовує комп'ютери для подолання обмежень механічних замків та ключів. Для заміни механічних ключів можна використовувати широкий спектр облікових даних. Електронна система контролю доступу надає доступ на основі облікових даних. Коли доступ надається, двері відчиняються на заданий час, і транзакція записується.

При відмові доступу двері залишаються замкненими, а спроба доступу фіксується. Система також контролюватиме двері і подаватиме сигнал тривоги, якщо двері відкриваються примусово або занадто довго залишаються відчиненими після розблокування.

Коли облікові дані надаються зчитувачу, зчитувач відправляє інформацію про облікові дані, зазвичай число, на панель управління, високонадійний процесор. Панель керування порівнює номер облікових даних зі списком контролю доступу, дозволяє або відхиляє поданий запит і надсилає журнал транзакцій до бази даних. Коли доступ заборонено на основі списку контролю доступу, двері залишаються замкненими.

Якщо є збіг між обліковими даними та списком контролю доступу, контрольна панель включає реле, яке, у свою чергу, відчиняє двері. Контрольна панель також ігнорує сигнал відкриття дверей, щоб запобігти спрацюванню сигналізації. Часто зчитувач забезпечує зворотний зв'язок, наприклад, миготіння червоного світлодіода при відмові в доступі та миготіння зеленого світлодіода при дозволі доступу [45].

Наведений вище опис ілюструє транзакцію з одним фактором. Облікові дані можуть передаватися по колу, порушуючи список контролю доступу. Наприклад, Аліса має права доступу в серверну , а Боб не має. Аліса або дає Бобу свої облікові дані, або Боб їх забирає; тепер він має доступ до серверну. Щоб запобігти цьому, можна використовувати двофакторну автентифікацію. У двофакторній транзакції представлені облікові дані та другий фактор необхідні

для надання доступу; іншим фактором може бути ПІН-код, друге посвідчення, втручання оператора або введення біометричних даних.

Розрізняють три види (фактори) автентифікуючої інформації [18]:

- щось відоме користувачеві, наприклад, пароль, кодова фраза або PIN-код
- те, що є у користувача, наприклад смарт-карта або брелок
- те, чим є користувач, наприклад, відбиток пальця користувача, підтверджений біометричним виміром.

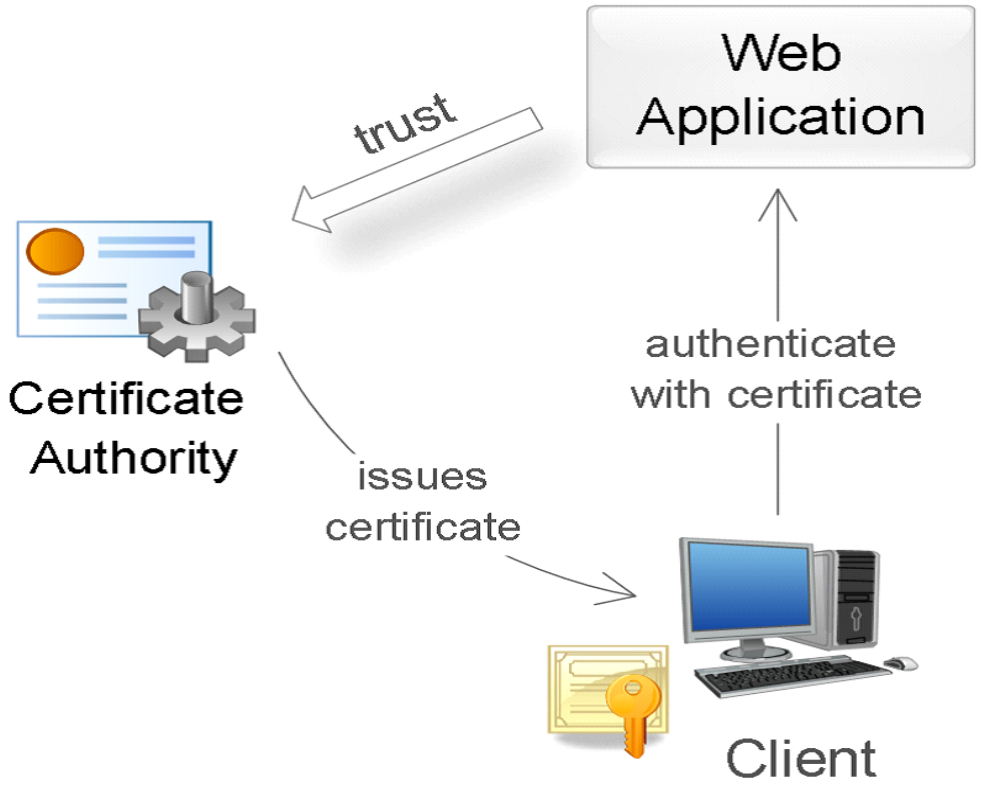


Рисунок 2.1 –Схема використання сертифікату для аутентифікації

Використання сертифікатів для аутентифікації - куди більш надійний спосіб, ніж аутентифікація за допомогою паролів. Це досягається створенням в процесі аутентифікації цифрового підпису, наявність якої доводить факт застосування закритого ключа в конкретній ситуації (non-repudiation).

До апаратних засобів захисту від пошкодження даних слід віднести використання джерел неперервного живлення, а також резервування та архівування даних, засобів апаратного шифрування даних.

При видачі USB карти користувачу вона реєструється в RSA менеджері авторизації, карта зберігає в собі приватний ключ і має внутрішній годинник. Зазвичай такі коди є валідними якийсь певний фіксований проміжок часу.

Приклад системи двофакторної авторизації на OTP (одноразових паролів) (рис. 2.2).

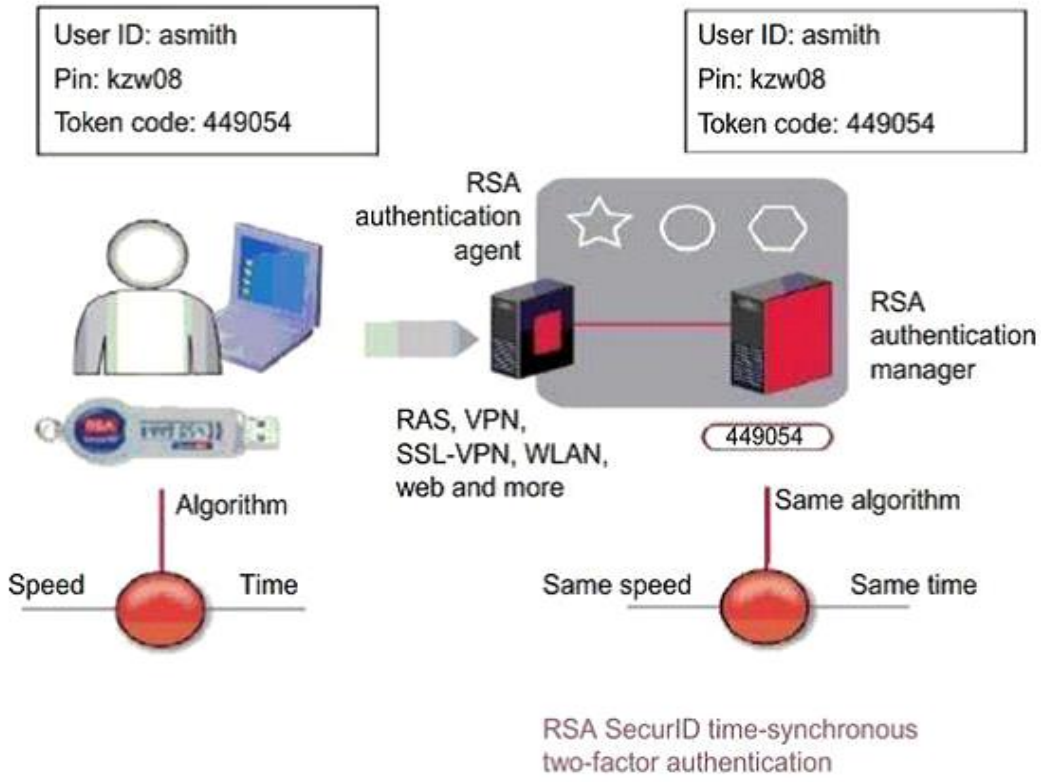


Рис. 2.2- Система RSA Secur ID система аутентифікації

Паролі є найпоширенішим засобом перевірки особи користувача перед наданням доступу до інформаційних систем. Крім того, тепер визнається четвертий фактор аутентифікації: хтось, кого ви знаєте, при цьому інша людина, яка знає вас, може надати людський елемент аутентифікації у ситуаціях, коли

системи налаштовані на такі сценарії. Наприклад, користувач може мати пароль, але він забув свою смарт-картку.

У такому сценарії, якщо користувач відомий призначеним групам, групи можуть надати свою смарт-карту та пароль у поєднанні з існуючим фактором розглянутого користувача і, таким чином, надати два фактори для користувача з відсутніми обліковими даними, що дає три фактори в цілому, щоб дозволити доступ.

Наведемо класифікацію СКУД у вигляді табл. 2.1

Таблиця 2.1.

Класифікація сучасних систем автоматизованого контролю доступу

Класифікація СКУД	
За технічними характеристиками і функціональними можливостями	• рівень ідентифікації; • кількість контрольованих місць; • пропускна здатність; • кількість користувачів; • умови експлуатації
За рівнем ідентифікації доступу	• одноріневі (ідентифікація здійснюється за однією ознакою, наприклад, з зчитування коду картки); • багаторівневі (ідентифікація здійснюється за кількома ознаками, наприклад, з зчитування коду картки і біометричних даних)
За кількістю контрольованих місць	• малої місткості (до 16 місць); • середньої місткості (від 16 до 64 місць); • великої місткості (понад 64 місць)
За умовами експлуатації	• у закритих приміщеннях; • у закритих неопалюваних приміщеннях; • під навісом на вулиці в умовах помірно-холодного клімату; • на вулиці в умовах помірно-холодного клімату;

	• в особливих умовах (підвищена вологість, запиленість, вібрації)
За основними функціональними можливостями	• можливість оперативного перепрограмування; • схемно-технічний та програмний захист від вандалізму і саботажу; • високий рівень секретності; • автоматична ідентифікація; • розмежування повноважень співробітників і відвідувачів з доступу в приміщення і на об’єкт у цілому; • надійне механічне замикання контрольованих місць з можливістю аварійного ручного відкриття; • автоматичний збір і аналіз даних; • вибіркова роздруківка даних

Однак, незважаючи на високу привабливість, бурхливий розвиток і, очевидно, хороші перспективи біометричної ідентифікації, сукупні показники швидкості і надійності розпізнавання в таких пристроях поки істотно поступаються пристроїв з зовнішніми ключами, переважна кількість яких має в своїй основі RFID (Radio Frequency Identification) технології.

2.2. Підходи до проектування СБР та алгоритм її функціонування

Компоненти системи контролю доступу включають [46]:

- Панель керування доступом (також відома як контролер)
- Вхід з контрольованим доступом, такий як двері, турнікет, паркувальні ворота, ліфт або інша фізична перешкода.
- Зчитувач встановлено біля входу. (У випадках, коли вихід також контролюється, використовується другий зчитувач на протилежному боці від входу).

• апорне обладнання, таке як електричні засувки дверей і електромагнітні замки.

• Магнітний дверний вимикач для контролю положення дверей

Пристрої запиту вихід (RTE) для дозволу виходу. Коли натиснута кнопка RTE або датчик руху виявляє рух біля дверей, тривога дверей тимчасово ігнорується, поки двері відчинені. Вихід із дверей без необхідності електричного відмикання дверей називається механічним вільним виходом. Це важлива безпекова функція. У тих випадках, коли замок повинен бути електрично розблокований під час виходу, пристрій запиту на вихід також відчиняє двері.

Зчитувачі контролю доступу можна класифікувати за функціями, які можуть виконувати [10]:

• Базові (неінтелектуальні) зчитувачі: просто зчитуйте номер картки або PIN-код та пересилайте його на панель керування. У разі біометричної ідентифікації, такі зчитувачі видають ідентифікаційний номер користувача. Зазвичай передачі даних на контрольну панель використовується протокол Wiegand , але нерідко й інші варіанти, такі як RS-232, RS-485 і Clock/Data. Це найпопулярніший тип зчитувачів контролю доступу. Прикладами таких зчитувачів є RF Tiny від RFLOGICS, ProxPoint від HID та P300 від Farpointe Data.

• Напівінтелектуальні зчитувачі: мають всі входи та виходи, необхідні для керування дверною фурнітурою (замок, дверний контакт, кнопка виходу), але не приймають жодних рішень про доступ. Коли користувач підносить картку або вводить PIN-код, зчитувач надсилає інформацію на головний контролер і чекає на його відповідь. При обриві зв'язку з основним контролером такі зчитувачі перестають працювати чи працюють у деградованому режимі. Зазвичай напівінтелектуальні зчитувачі підключаються до ПКП по шині RS-485. Прикладами таких зчитувачів є InfoProx Lite IPL200 від CEM Systems та AP-510 від Apollo.

Інтелектуальні зчитувачі: мають всі входи та виходи, необхідні для керування дверною фурнітурою; вони також мають пам'ять і обчислювальна потужність, необхідні незалежного прийняття рішень про доступ. Як і

напівінтелектуальні зчитувачі вони підключаються до панелі управління по шині RS-485. Панель керування відправляє оновлення конфігурації та отримує події від зчитувачів. Прикладами таких зчитувачів можуть бути InfoProx IPO200 від CEM Systems та AP-500 від Apollo.

Існує також нове покоління інтелектуальних зчитувачів, які називають «IP-зчитувачами». Системи з IP-зчитувачами зазвичай немає традиційних панелей управління, а зчитувачі підключаються безпосередньо до ПК, що у ролі хоста.

Деякі зчитувачі можуть мати додаткові функції, такі як РК-дисплей та функціональні кнопки для збору даних (тобто час приходу/догляду для звітів про відвідуваність), камера/динамік/мікрофон для внутрішнього зв'язку та підтримка читання/запису смарт-карток.

Правила встановлення автономного контролеру.

Автономні контролери СКУД - найдешевший спосіб організувати систему контролю доступу.

Отже, схематично модель контролерної СКУД можна представити у вигляді рис. 2.3.

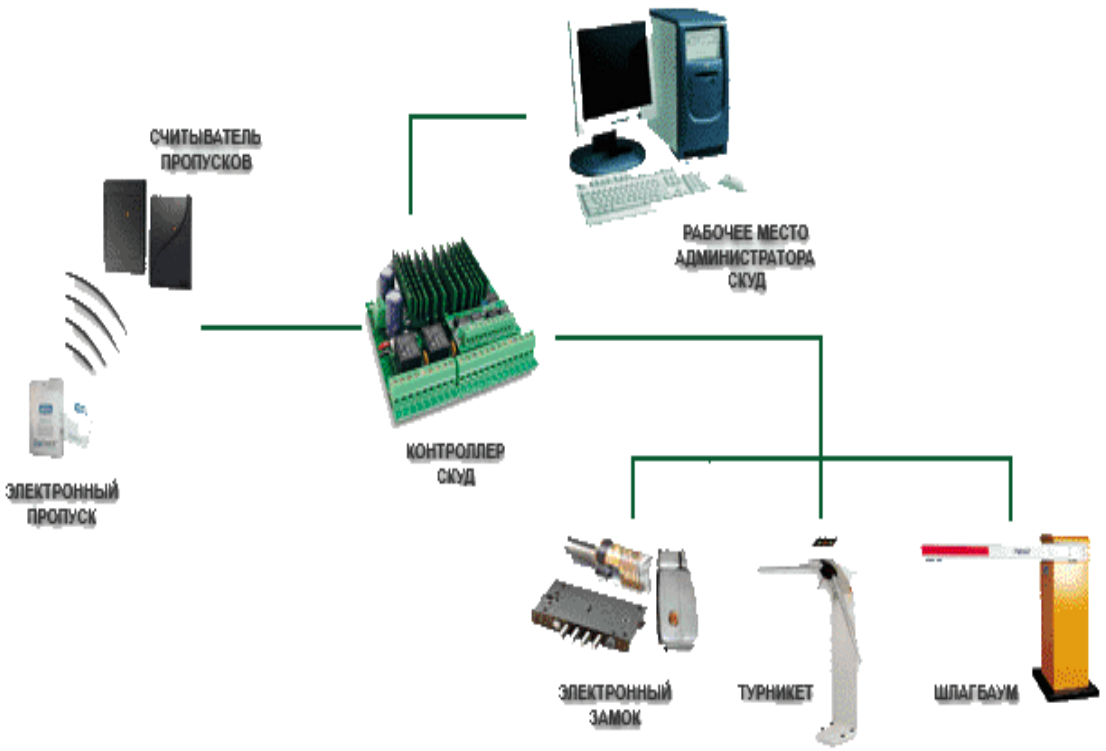


Рис. 2.3 – Схема моделі контролерної СКУД

Як бачимо зі схеми, центральним елементом даного класу СКУД є саме контролер - пристрій, призначений для обробки інформації, що надходить від зчитувачів, ідентифікаторів, для прийняття рішення і управління виконавчими пристроями. Тому його часто називають «серцем СКУД».

Отже, розглянемо як організувати систему контролю доступу за допомогою автономного контролера [22].

Автономним контролером прийнято вважати контролер, до якого не можна підключити інші контролери, об'єднавши їх в єдину мережу.

Другий важливий момент, який потрібно розуміти при використанні автономного контролера, це те, що не кожним автономним контролером можна керувати за допомогою програмного забезпечення, що встановлене на комп'ютер.

На практиці це означає, що не вийде отримати дані про те, хто, коли і скільки разів відкривав двері.

У деяких випадках ці дані дуже цінні, оскільки на їх підставі можна побудувати звіти про облік робочого часу.

Також не вийде розмежувати доступ за часом, наприклад, заборонити доступ певним співробітникам у вихідні.

Слід зауважити, що у більшості випадків такий широкий функціонал не потрібен, а значить автономний контролер – це відмінне рішення у випадках, коли перед вами стоїть завдання: виключно обмежити доступ небажаних відвідувачів на певну територію [44].

Використовуючи автономний контролер, який не підключається до програмного забезпечення, слід пам'ятати, що вже записану в пам'ять контролера карту неможливо видалити, якщо її фактично немає на місці.

На практиці така ситуація може виникати досить часто. Наприклад, звільнився співробітник, забув здати карту перед звільненням і пішов разом з нею. Також карту можна загубити, наприклад [13].

Якщо принциповим є видалення таких карт з пам’яті контролера, то доведеться повністю очистити його пам’ять, оскільки вибіркове видалення карти неможливе.

Щоб уникнути такої проблеми, потрібно вибирати такі автономні контролери, до яких можливо підключити програмне забезпечення. Якщо потрібно замовити автономну систему контролю доступу під ключ, слід врахувати, щоб у вартість увійшла також установка, налаштування програмного забезпечення і навчання.

Що стосується електроживлення систем керування та управління доступом, то воно відбувається наступним чином: всі професійні контролери, як правило, мають власний акумулятор, який підтримує працездатність контролера від декількох годин до декількох діб.

При використанні ж простого автономного контролера без власного блоку живлення, необхідно купувати джерело безперебійного живлення, спеціально для цього призначений.

Таким чином, у разі відключення електрики контролера потрібне додаткове живлення або ж контролер повинен мати акумулятор, що збільшує його вартість, або потрібно окреме джерело безперебійного живлення для контролера, що збільшує вартість всієї системи.

У той час як наявність джерела безперебійного живлення для комп’ютера – це само собою зрозумілий факт.

При цьому слід враховувати, що використання контролера не виключає необхідності установки комп’ютера на робочому місці [48].

1. Послідовні контролери. Контролери підключаються до хост-комп'ютера через послідовну лінію зв’язку RS-485 (або через струмову петлю 20 мА у деяких старих системах). Необхідно встановити зовнішні перетворювачі RS-232/485 або внутрішні карти RS-485, оскільки стандартні ПК не мають комунікаційних портів RS-485.

2. Серійний основний та допоміжний контролери. Вся дверна фурнітура підключена до субконтролерів (також званим контролерами дверей або

дверними інтерфейсами). Субконтролери зазвичай не приймають рішення про доступ, а натомість перенаправляють усі запити на головні контролери. Основні контролери зазвичай підтримують від 16 до 32 субконтролерів.

3. Серійні основні контролери та інтелектуальні зчитувачі. Вся дверна фурнітура підключається безпосередньо до інтелектуальних чи напівінтелектуальних зчитувачів. Читачі зазвичай не ухвалюють рішення про доступ і перенаправляють всі запити на головний контролер. Напівінтелектуальні зчитувачі, які не мають бази даних і не можуть функціонувати без основного контролера, повинні використовуватися тільки в областях, що не потребують високої безпеки. Головні контролери зазвичай підтримують від 16 до 64 зчитувачів (Рис. 2.4)

.

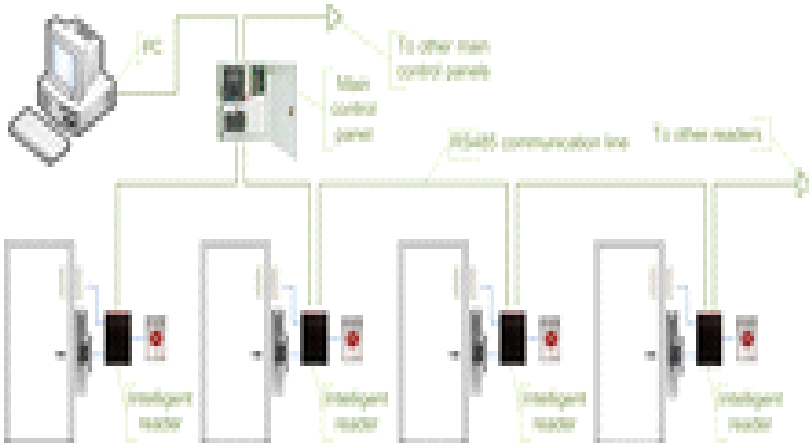


Рис. 2.4 - Система контролю доступу з використанням послідовного основного контролера та інтелектуальних зчитувачів

4. Послідовні контролери із термінальними серверами. Незважаючи на швидкий розвиток та дедалі ширше використання комп'ютерних мереж, виробники засобів контролю доступу залишалися консервативними і не поспішали впроваджувати мережеві продукти.

Коли вимагалося рішення з мережним підключенням, багато хто вибрав варіант, що вимагає менших зусиль: додавання термінального сервера,

пристрою, який перетворює послідовні дані для передачі через локальну або глобальну мережу [50].

Системи контролю доступу з використанням послідовних контролерів та термінальних серверів (рис. 2.5).

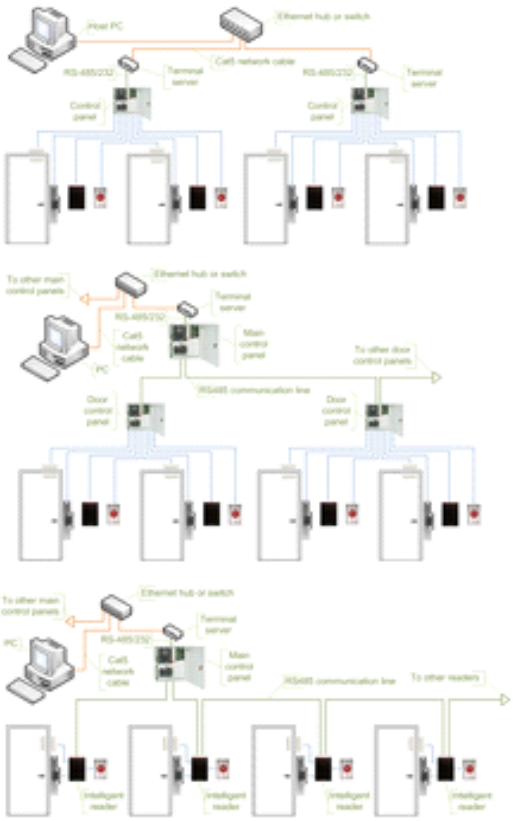


Рис. 2.5 - Системи контролю доступу з використанням послідовних контролерів та термінальних серверів

5. Головні контролери із підтримкою мережі. Топологія майже така сама, як описано у другому та третьому абзацах. Застосовуються самі переваги і недоліки, але вбудований мережевий інтерфейс пропонує кілька цінних поліпшень. Передача конфігурації та даних користувача на головні контролери відбувається швидше і може виконуватися параллельно (рис. 2.6).

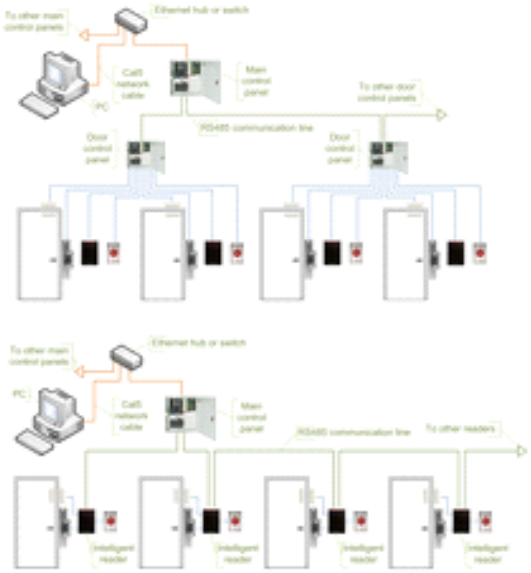


Рис. 2.6 - Система контролю доступу з використанням IP-контролерів

• IP-контролери. Контролери підключаються до головного комп'ютера через Ethernet LAN або WAN.

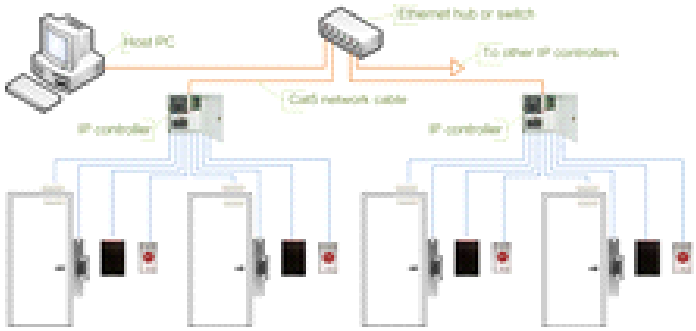


Рис. 2.7 - Система контролю доступу з використанням IP-контролерів

6. IP-зчитувачі. Зчитувачі підключаються до головного комп'ютера через Ethernet LAN або WAN.

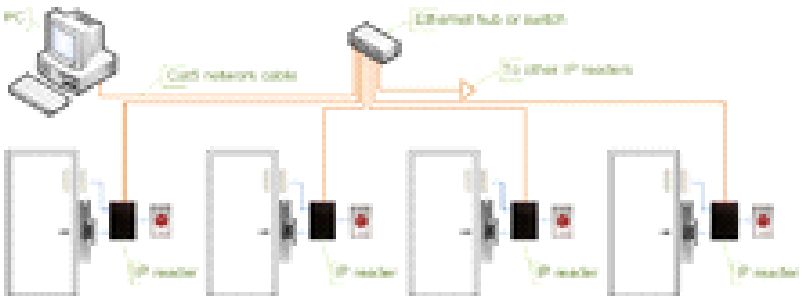


Рис. 2.8 - Система контролю доступу з використанням IP-зчитувачів

Схему алгоритму контролю доступу до веб-додатку, що проектується, представимо на рис. 2.9.

Для постійної експлуатації даної системи нам необхідна технологія, яка б надійно функціонувала в приміщенні, так і щоб переданий сигнал впевнено проходив через стіни.

З огляду на це, рішення використання інфрачервоного каналу для передачі даних стає ненадійним, незважаючи на позитивні сторони даної технології.

Технологія Ethernet поступається іншим видам в зручності прокладки інфраструктури для передачі даних і в протяжності дії технології.

Технологія Wi-Fi має потенційно вищу швидкість передачі даних, ніж Bluetooth.

Але дана характеристика не грає великої ролі в системі, що розробляється, тому що обсяг даних з яким даній системі доведеться працювати транслюватиметься обома технологіями за однаковий інтервал часу [29].

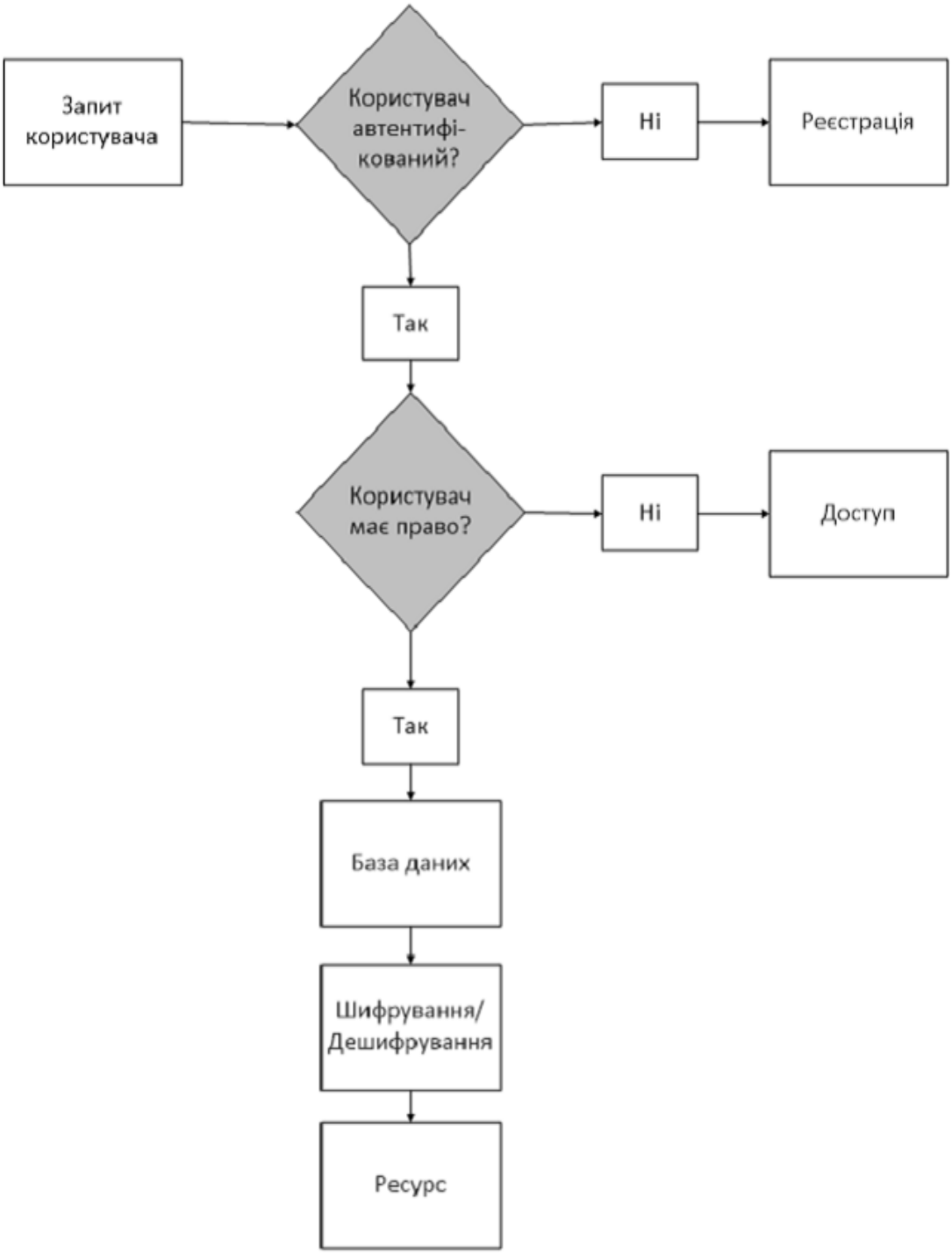


Рис. 2.9 – Схема алгоритму контролю доступу до веб-додатку

З метою зробити роботу цієї системи зручною для більшої кількості людей, доцільніше буде зробити вибір на користь технології Wi- Fi.

Цей вид передачі даних набагато більш поширений в порівнянні з Bluetooth. До того ж Wi-Fi продовжує набирати свою популярність, тому що на

сьогоднішній день Wi-Fi модуль вбудований практично в усіх мобільних телефонах, ноутбуках і навіть деяких електронних книгах. Така поширеність дозволить реалізувати по-справжньому дистанційну систему стеження.

2.3. Обґрунтування вибору програмно-апаратних засобів для СБР

В даному проекті планується реалізувати систему, що складається з 4 основних компонентів, що взаємодіють через об’єкт управління, роль якого виконуватиме мікроконтролер.

- RFID (англ. RadioFrequencyIDentification, радіочастотна ідентифікація) - спосіб автоматичної ідентифікації об’єктів, у якому за допомогою радіосигналів зчитуються або записуються дані, що зберігаються в так званих транспондерах, або RFID-мітках. Будь-яка RFID-система складається з зчитувального пристрою (зчитувач, рідер або Інтеррогатор) і транспондера (він же RFID-мітка, іноді також застосовується термін RFID-тег).За дальністю зчитування RFID-системи можна поділити на системи [22]:
  - ближню ідентифікацію (зчитування проводиться на відстані до 20 см);
  - ідентифікації середньої дальності (від 20 см до 5 м);
  - дальньої ідентифікації (від 5 м до 300 м).

Більшість RFID-міток складається з двох частин.

Перша - інтегральна схема (IC) для зберігання та обробки інформації, модулювання та демодулювання радіочастотного (RF) сигналу та деяких інших функцій.

Друга - антена для прийому та передачі сигналу.

З введенням RFID-міток у повсякденне життя пов’язана низка проблем.

Рис. 2.10 – Приклад RFID-міткиSIMATICRF620T, що відповідає стандартам ISO 18000-6CEPCCLASS 1 GEN.
По центру нанесений штрих-код, праворуч - DMC

Як вже було доведено, радіочастотна ідентифікація затребувана в безлічі виробничих сфер. Щоб дані системи ефективно функціонували в будь-якій області, було розроблено велику кількість різних за виконання радіоміток. Умовно всі ці мітки класифікуються наступним чином:

1) За наявності живлення [44]:

– Активні - для передачі інформації використовують енергію вбудованого джерела живлення, радіус реєстрації таких міток досягає ста метрів;

– Пасивні - радіопозначки, що використовують для різних дій з даними енергію, що випромінюється пристроєм ідентифікації. Радіус дії міток цього типу досягає 9 метрів.

2) За видами пам’яті:

– Тільки для читання (RO) - інформація на мітку записується лише один раз, при виробництві. Даний тип міток використовується тільки для ідентифікації. Записати будь-яку інформацію в мітки для читання не можна. Також їх практично неможливо підробити;

– Запис одного разу, читання багаторазово (WORM) - крім унікального ідентифікатора дані тип радіоміток містить блок одноразово записуваної інформації. Надалі інформацію з цього блоку можна зчитувати багаторазово;

– Для читання і запису (RW) - такі RFID - мітки зберігають унікальний ідентифікатор і кілька блоків пам’яті, призначених для читання і перезапису інформації.

3) За видом виконання [28]:

– Самоклеючі паперові або лавсанові мітки;

– Стандартні пластикові карти;

– Дискові;

– Різні види брелків;

– Спеціальне виконання для тяжких та жорстких умов експлуатації.

В наш час існує велика кількість різноманіття міток, тому відповідне виконання можна підібрати для індивідуального завдання, в залежності від потреб коистувача.

У даній роботі для ідентифікації різних радіочастотних безконтактних міток використовується сканер RFIDRC522 (рис. 2.11).

Даний сканер дозволяє виявити і вважати ідентифікатори безконтактних карт, міток, пропусків стандарту 13,56 МГц на відстані до 10 см. При зв’язуванні з мікроконтролером дозволяє створити ряд цікавих проектів: пропускні системи, електронні замки, складський облік і багато іншого.

Технічні параметри [40]:

– базується на мікросхемі MFRC522;

– напруга живлення: 3,3В;

– струм: 13-26 мА;

– Робоча частота: 13,56 МГц;

– Відстань зчитування: 0 ~ 60 мм

– Інтерфейс: SPI, максимальна швидкість передачі 10Мбіт/с

– Розмір: 40мм х 60мм

– Читання і програмуваня запису RFID-міток.

Рис. 2.11 – Радіочастотний зчитувач RC522

- Контролер Arduino.

Arduino - це електронна платформа з відкритим вихідним кодом, заснована на простому у використанні апаратному та програмному забезпеченні (рис. 2.12).

Рис. 2.12- Arduino IDE із прикладом простої програми

Класичні Arduino та Arduino-сумісні плати спроектовані для монтажу в стопки через штирьові роз'єми. Таким чином, базову мікропроцесорну плату доповнюють необхідною периферією і зовнішніми підключеннями [18].

Існують плати Uno, Pro, Leonardo, Mega 2560, Due та плати, наприклад,Zero, з розширеним набором штирьових роз'ємів для них. Плати розширення стандартної довжини можуть встановлюватися і розширені процесорні плати (рис. 2.13).

Рис. 2.13 - Класичний конструктив Arduino з платами розширення

Arduino приймає навколишнє середовище, отримуючи дані від безлічі датчиків, і впливає на навколишнє середовище, керуючи освітленням, двигунами та іншими виконавчими механізмами.

Основне призначення плати Arduino - взаємодія з сенсорами і пристроями, тому Arduino відмінно підходить для апаратних проектів, де потрібно просто реагувати на різні сигнали сенсорів і ручне введення.

Може здатися, що в цьому немає нічого особливого, проте на ділі Arduino - складна вивірена система, значно полегшує управління пристроями [20].

Вона відмінно підходить саме для організації взаємодії інших пристроїв і виконавчих механізмів, де повновага операційна система просто не потрібно, так як мова йде просто про отримання сигналів з сенсорів і реагуванні на них (рис.2.9).

Рис. 2.9 – Arduino UNOR 3 - версія SMD з інтерфейсом USB та мікроконтролером ATmega 328

Апаратне забезпечення типової плати Arduino засноване на мікроконтролері MicrochipAVR із серії megaAVR, такому як ATmega328. Відхилення від цього можна знайти, наприклад, у платах ArduinoDue (32-бітний процесор AtmelSAM3X8EArmCortex-M3), Yun, Tre, Gemma та Zero, де використовуються інші мікроконтролери Atmel. Плати Arduino Yún і Tre, які мають потужніший мікропроцесор на додаток до мікроконтролера, також є особливими [22].

Також є варіанти з напругою живлення 3,3 Ві варіанти з іншою тактовою частотою.

Ряд інших мікроконтролерів, таких як ESP8266, ESP32, STM32 або MSP430 також можна запрограмувати через ArduinoIDE через розширення.

Arduino поставляється з власним інтегрованим середовищем розробки (IDE), заснованим на Wiring IDE.

Ця програма Java доступна безкоштовно для поширених операційних систем Windows, Linux і macOS . Він заснований на Processing IDE, середовищі розробки, що спеціалізується на графіку, моделюванні та анімації. Arduino IDE поставляється з редактором коду і інтегрує gcc як компілятор. Крім того, бібліотека avr-gcc та інші бібліотеки Arduino («бібліотеки»), які значно спрощують програмування на C та C++.

У даній модифікації платформи ArduinoUno, на платформі розташовані 11 контактів. Але, на відміну від оригіналу, не всі з них можуть бути використані для цифрового введення і виведення.

Всі вони працюють з напругою 3,3 В і розраховані на струм до 40 мА. Також кожен контакт має вбудований, але відключений за замовчуванням резистор на 20 - 50 кОм.

ESP8266 - мікроконтролер китайського виробника Espressif з інтерфейсом Wi-Fi. Крім Wi-Fi мікроконтролер відрізняється важливою для даного проекту можливістю виконувати програми з зовнішньої flash-пам’яті з інтерфейсом SPI. Цей чіп вбудований в плату Wemos D1 і використовується для взаємодії з Wi-Fi з Web сервером.

Софтверна частина розробки САК включає в себе [14]:

• Flutter - це програмний каркас із відкритим кодом для створення додатків для платформ Android та iOS, а також на вебі, розроблений компанією Google. Він є основним способом створення додатків для Google HYPERLINK "https://uk.wikipedia.org/wiki/Google_Fuchsia"Fuchsia.

• Весь графічний інтерфейс Google Fuchsia створено за допомогою Flutter. Архітектура Flutter відрізняється від інших програмних каркасів (React, Apache HYPERLINK "https://uk.wikipedia.org/wiki/Apache_Cordova"Cordova) тим, що він не використовує для побудови інтерфейсу мови HTML, CSS та Javascript,

відповідно і вбудований рушій WebView. Використовується власний рушій для рендерингу. Flutter використовує тільки одну мову програмування Dart.

• Flask - мікрофреймворк для вебдодатків, створений з використанням Python. Його основу складає інструментарій Werkzeug та рушій шаблонів Jinja2. Поширюється відповідно до умов ліцензії BSD. Flask називається мікрофреймворком, оскільки він не вимагає спеціальних засобів чи бібліотек. У ньому відсутній рівень абстракції для роботи з базою даних, перевірки форм або інші компоненти, які надають широковживані функції за допомогою сторонніх бібліотек.

Властивості мікрофреймворку Flask [36]:

- Містить сервер для розробки та відлагоджувач.
- Вбудована підтримка юніт-тестів.
- Управління запитами RESTful.
- Використовує шаблони Jinja2.
- Має підтримку безпечних куків (сесії на стороні клієнта).
- 100% відповідність WSGI 1.0.
- Підтримка Unicode.
- Докладна документація.
- Сумісністьз Google App Engine.
- Наявність розширень для забезпечення бажаної поведінки
- Бібліотека Servo.h.

Ця бібліотека функцій для контролера Arduino надає набір функцій для управління сервоприводами.

Стандартні сервоприводи дозволяють повертати привод на певний кут від 0 до 180 градусів. Деякі сервоприводи дозволяють здійснювати повні оберти заданої швидкості.

У загальному випадку сервопривід підключається трьома проводами: живлення, земля та сигнальний. Зазвичай живлення – червоний провід і може бути підключений до виведення +5V на платі Arduino. Чорний дріт земля

підключається до GND виводу Arduino, сигнальний, зазвичай жовтий, провід підключається до цифрового виводу котроллера Arduino.

Слід зазначити, що потужні сервоприводи можуть створювати велике навантаження, у цьому випадку він повинен бути окремо (не через вихід +5V Arduino).

Теж правильне для випадку підключення відразу декількох сервоприводів. Переконайтеся, що привід та контролер підключено до спільної землі.

- СУБД – NoSQL.

Inter Systems Caché (/ k æ ʃ eɪ / kashay) - Комерційна система управління операційними базами даних від InterSystems , що використовується для розробки програмних додатків для управління охороною здоров’я, банківськими та фінансовими послугами, урядом та іншими секторами.

Програмне забезпечення замовника може використовувати базу даних з об’єктним та SQL-кодом.

Caché також дозволяє розробникам безпосередньо маніпулювати базовими структурами даних: ієрархічними масивами, відомими як M-технологія.

Всередині Caché зберігає дані у багатовимірних масивах, здатних зберігати ієрархічно структуровані дані.

Це ті самі «глобальні» структури даних, які використовуються мовою програмування MUMPS, які вплинули на дизайн Caché, і аналогічні тим, що використовуються в системах MultiValue (також відомих як PICK).

Технологія Caché ServerPages (CSP) дозволяє створювати веб-застосунки на основі тегів, які генерують динамічні веб-сторінки, зазвичай використовуючи дані з бази даних Caché [24].

Caché також включає Inter Systems Zen, реалізацію AJAX, яка дозволяє розробляти багатофункціональні веб-програми на основі компонентів.

Inter Systems Caché надає найважливішим додаткам наших клієнтів можливість зберігати, використовувати та аналізувати транзакційні та історичні дані одночасно у будь-яких необхідних формах. Високошвидкісний SQL працює послідовно та безперешкодно у всіх моделях даних.

У міру збільшення вимог до пропускної спроможності та обсягу даних Caché підтримує незмінно високу продуктивність.

У Caché дані можна моделювати та зберігати у вигляді таблиць, об’єктів або багатовимірних масивів (ієрархій). Різні моделі можуть безперешкодно отримувати доступ до даних без необхідності зіставлення між моделями, що знижує продуктивність.

Вбудована підтримка об’єктів динамічних даних (таких як XML та JSON) забезпечує простоту взаємодії та швидку розробку веб-додатків [18].

SQL – це мова спілкування для запитів до даних Caché у всіх моделях даних. Завдяки своїй ефективній архітектурі Caché забезпечує більш високу продуктивність SQL ніж інші технології баз даних.

Він підтримує традиційні індекси, а також індекси з бітовою карткою та бітовими зрізами, які можна використовувати з транзакційними даними у реальному часі. Дзеркала бази даних Caché не вимагають великих інвестицій у обладнання, підтримку, ліцензії на операційну систему чи сховище. Крім того, дзеркала баз даних Caché легко налаштовуються та обслуговуються, тому витрати на адміністрування зведені до мінімуму.

Рішення NoSQL відрізняються як проектуванням з урахуванням масштабування. Іншими характерними рисами NoSQL-рішень є [4]:

- Впровадження різноманітних типів сховищ.
- Можливість проектування БД без схем.
- Принцип лінійної масштабованості (кількість процесорів підвищує продуктивність).
- Принцип інновації: не тільки SQL відкриває можливості для зберігання та оброблення інформації.

2.4 Висновки до розділу

- Підсумовуючи другий розділ, можемо зробити такі висновки:

• З’ясовано, що наразі система контролю доступу є структурою в комплексі дотримання безпеки і успішно взаємодіє із іншими АС приміщення чи території та може бути загальною АСУ компанії. Насамперед це стосується загальної АСУ, підприємства. Такий рівень синхронізації СКУД з іншими системами відбувається завдяки наявності прямого контакту з користувачами. Постійно присутній обмін інформацією між СКУД та іншими ІС.

• Проаналізовано, що у захищеній ІС передачу можна здійснювати виключно у парі із засобами захисту мережевого трафіку. Методи розпізнавання особи СКУД ділять на кілька груп. Першу з них представляють методи, що засновуються на впровадженні зовнішніх по відношенню до користувача ідентифікаторів - електронних ключів, які у складі містять унікальний код, що розпізнається СКУД і якому в її БД присутні персональні дані особи, яка проходить процес розпізнавання. Другу групу утворюють ідентифікаційні методи, що створені на використанні біометричних характеристик користувачів.

• Виявлено, що біометричне розпізнавання є досить популярним, адже ідентифікаційна ознака є невід’ємною рисою конкретного користувача, її неможливо втратити, забути, передати, дуже складно або неможливо підробити, його не потрібно видавати, поновлювати. Саме тому біометрична ідентифікація швидко розвивається на ринку систем безпеки. Навіть історично перші біометричні технології ідентифікації - по контурах долоні і відбитками пальців - постійно удосконалюються. Так, за допомогою телевізійних пристроїв створені з використанням безконтактної технології зчитувачі цих ознак. На відміну від традиційних, вони більш гігієнічні, так як вони передбачають контакту пальця з будь-якої поверхнею, а тому значно простіше в обслуговуванні.

• Досліджено, що Inter Systems Caché - це комерційна система управління операційними базами даних від InterSystems , що використовується для розробки

програмних додатків для управління охороною здоров’я, банківськими та фінансовими послугами, урядом та іншими секторами. Програмне забезпечення замовника може використовувати базу даних з об’єктним та SQL-кодом. Caché також дозволяє розробникам безпосередньо маніпулювати базовими структурами даних: ієрархічними масивами, відомими як M-технологія. Всередині Caché зберігає дані у багатовимірних масивах, здатних зберігати ієрархічно структуровані дані.

РОЗДІЛ 3.
ВПРОВАДЖЕННЯ СИСТЕМИ БІОМЕТРИЧНОГО РОЗПІЗНАВАННЯ ОСОБИ ДЛЯ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1 Розробка структурної схеми та архітектури системи розпізнавання особи для захистуоб'єктів інформаційної діяльності

У додатку Arduino присутніі такі контакти до системи живлення:

– Він має такий самий вольтаж, який застосовується для живлення програми. При підключенні через USB це 5 В.

– 5 V надає 5 В в незалежності від вхідної напруги. На цій напрузі функціонує процесор. Максимально допустимий струм контакту складає 800мА.

– 3.3 V надає 3,3 В. Максимально допустимий струм контакту складає - 50 мА.

– GND - заземлення.

Крім цього, плата має вхідний контакт Reset. Налаштування контакту до логічного нуля призводить до скидання функцій процесора. Це аналог кнопки Reset звичайного ПК.

Щоб контролер та ідентифікатор комунікували між собою завдяки даному середовищу програмування, слід завантажити і налаштувати програму Arduino «RFID Library for MFRC522» . Ця бібліотека потрібна для того, щоб в Arduino IDE з'явилися команди для синхронізації з RC522.

Отже, представимо алгоритм роботи СБР на рис. 3.1.

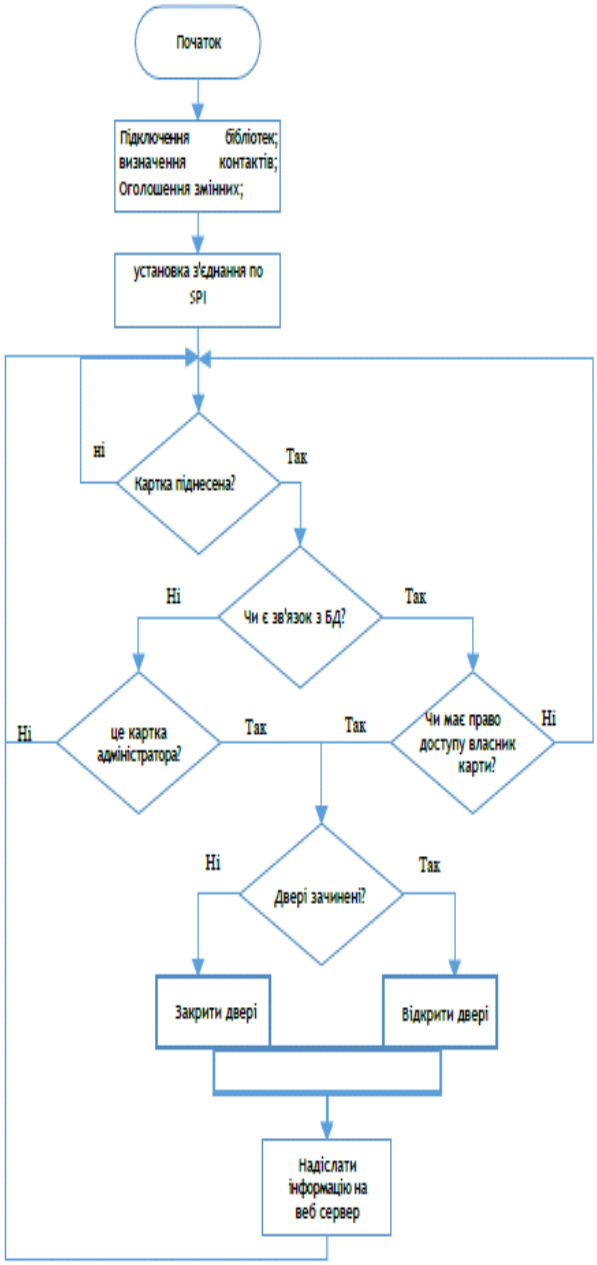


Рис. 3.1 - Алгоритм роботи СБР

3.2 Моделювання системи біометричного розпізнавання особи

Система СБР складатиметься з 5 головних взаємодіючих елементів.

Функціональна схема даної системи зображена на рис. 3.2:

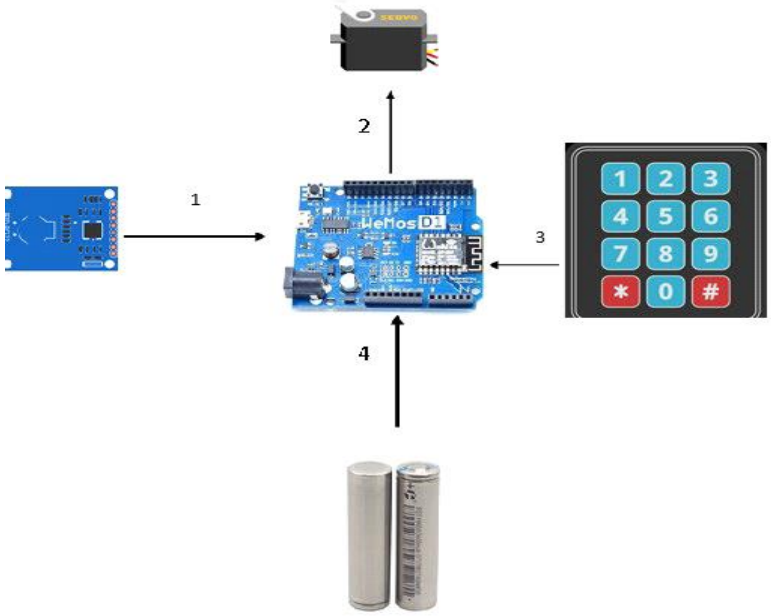


Рис. 3.2 - Структурна схема та архітектура СБР

1) Сигнали наявності мітки приходить з RFID-картки на мікроконтролер;

2) МК посилає запит на сервер з БД. Зясовується, чи є права доступу у користувача;

3) Веб-сервер надає відповідь. Далі з’являються альтернативи розвитку сценарію: користувачу дозволено увійти чи відмовлено у доступі.

В разі відмови у доступі СБР не чинить ніяких дій в очікуванні наступного сеансу розпізнавання;

4) В разі, якщо особа отримує доступ, то МК посилає сигнал на сервопривід із задачею дозволити доступ, за умови, якщо доступу не було надано;

5) Далі на веб-сервер, створений платою Wemos D1 R2, посилаються дані стосовно періоду відвідування та унікальний номер картки.

Організація взаємодії WiFiWemosD1 R2 і RC522 (рис.3.3).

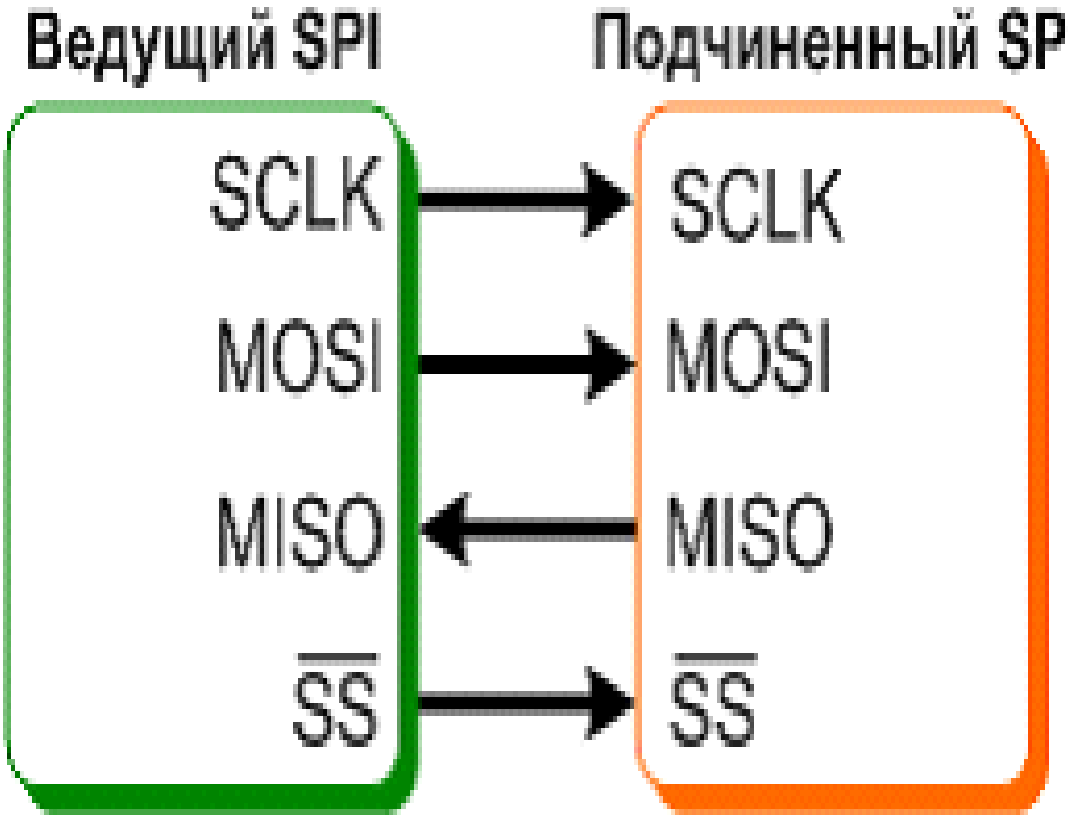


Рис. 3.3 - Приклад пристроїв, пов’язаних SPI, для взаємодії WiFiWemosD1 R2 і RC522

Платформа WemosD1 R2 і радіочастотний ідентифікатор RC522 пов’язуються через послідовний периферійний інтерфейс SPI.

SPI є популярним інтерфейсом для реалізації послідовного обміну даними між мікросхемами.

Нарівні з I2C він є найбільш розповсюджених інтерфейсів для з’єднання мікросхем.

Цей тип інтерфейсу змодельовано для організації оперативного обміну даних між компонентами всієї системи: МК та периферійним обладнанням.

На шині завжди присутній головний пристрій і кілька додаткових, master і slave відповідно.

Інтерфейс застосовує наступний алгоритм для обміну даних:

– SCK - Serial Clock: тактовий сигнал;

– MOSI - Master Output, Slave Input: дані від головного до додаткового;

–MISO – Master Input,Slave Out put;

–SS (SDA) – SlaveSelect: вибір веденого.

На початку роботи головний пристрій налаштовує за замовчуванням низький рівень сигналу на тій ділянці SDA, де є потрібне йому обладнання.

В даному проекті наявним є виключно один пристрій-RC522, відповідно, перед початком кожного сеансу роботи на контакті SD. У цього пристрою низький рівень сигналу.

Після цього, головний пристрій задає режим роботи завдяки синхронізації виходу SCK.

З кожним сеансом каналами зв'язку MOSI і MISO відбувається передача потрібного рівеня сигналу від головного до другорядного пристрою.

Для того, що завершити сесію передачі даних, головний пристрій має відправити високий рівень сигналу каналами SDA..

Традиційна швидкість роботи шини становить 1-50 МГц.

За допомогою цій простоті алгоритму передачі даних SPI має широке розпосюдження серед різних електронних пристроїв - наприклад, у датчиках, чіпах пам'яті, радіо-модулях (рис. 3.4-3.5).

Схема з'єднання сервоприводу і Arduino наведено на рис. 3.6.

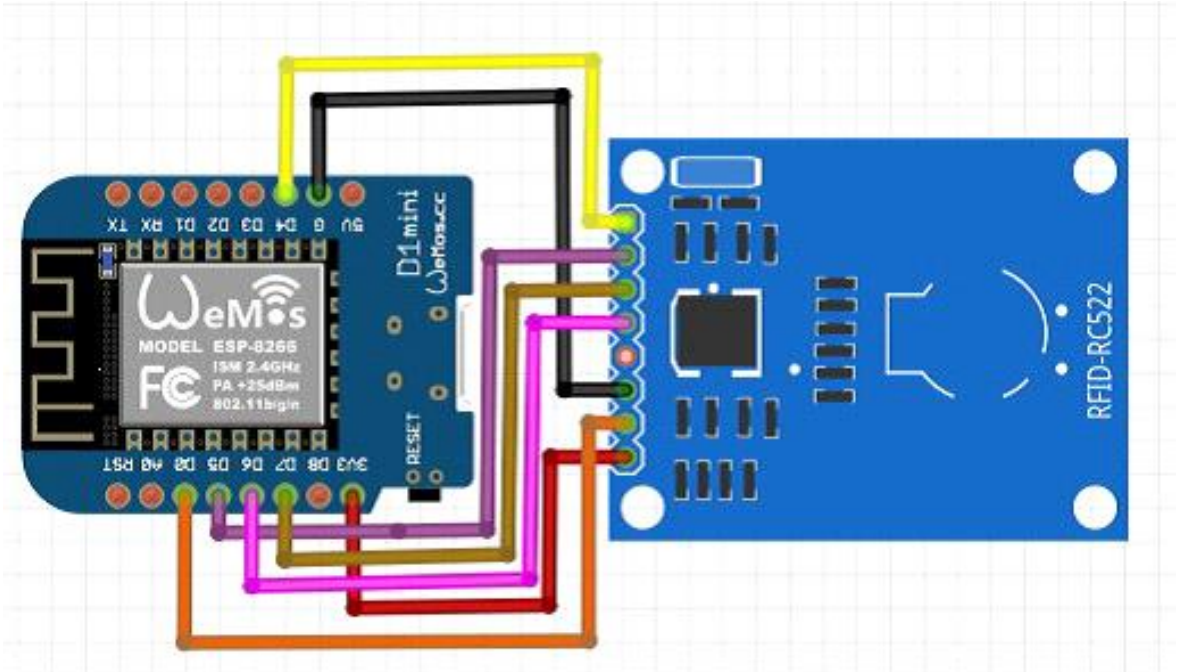


Рис 3.4 - Схема з’єднання RC522 і WemosD1 Mini

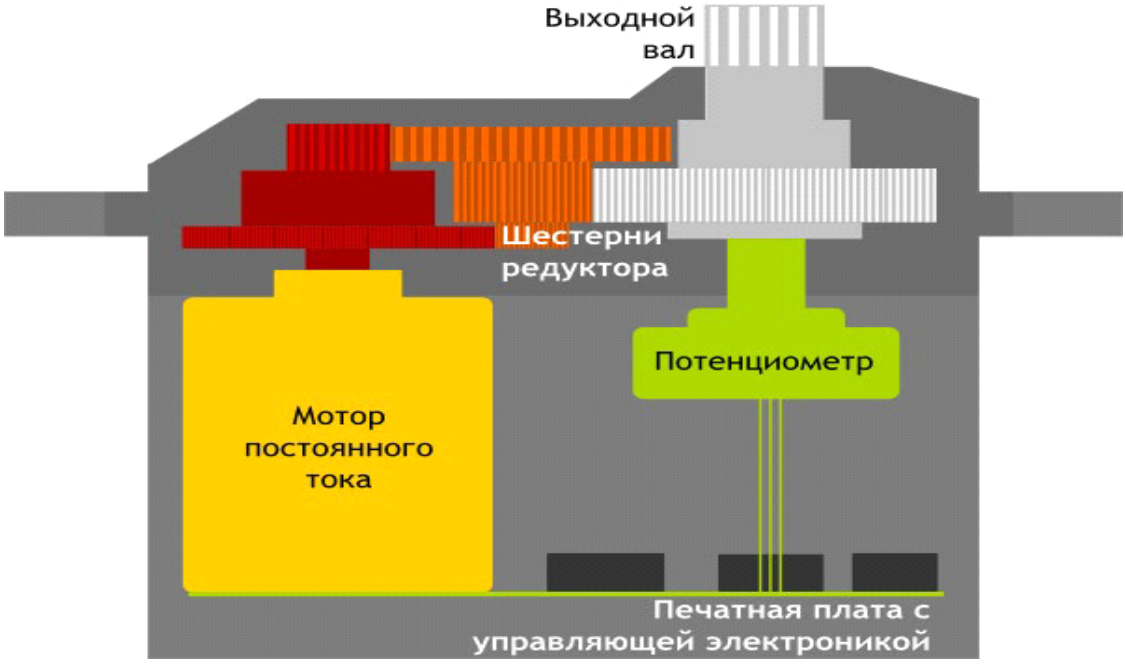


Рис. 3.5 - Механізм сервоприводу СБР

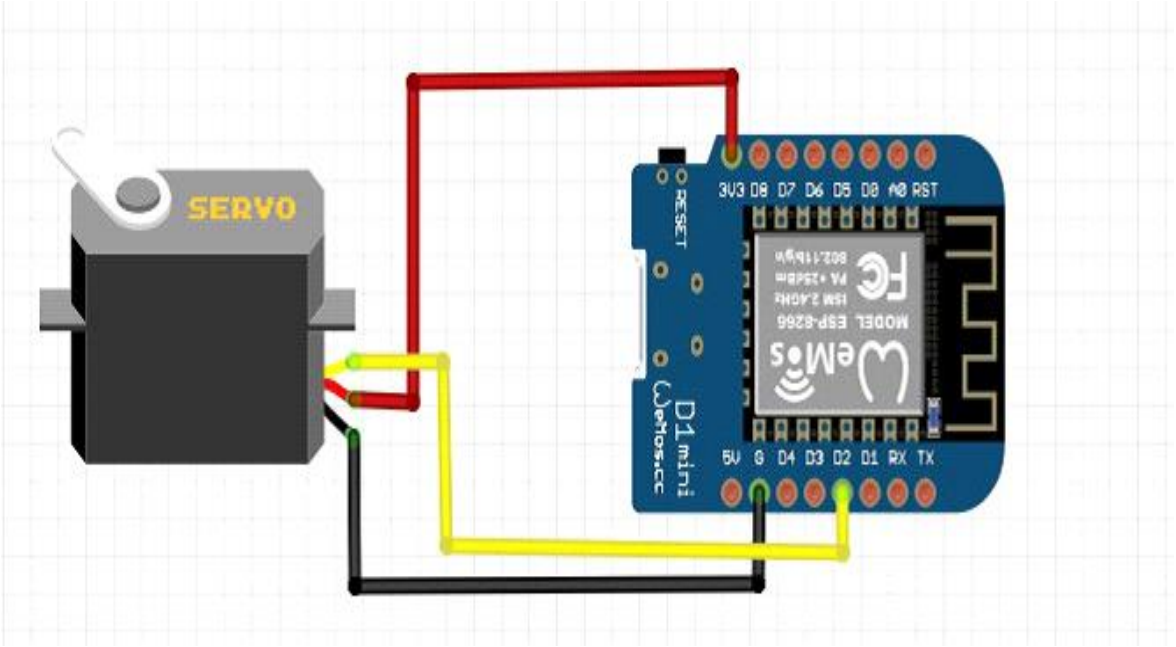


Рис. 3.6 - Схема з’єднання сервоприводу і Wemos D1 Mini

3.3 Впровадження СБР, її тестування та валідація

Для проектування та експлуатації веб-сервера на ПК варто встановити додаткове ПЗ.

Платформа Apache виконуватиме функції http-сервера. Завдяки ній буде відбуватися робота даного веб-серверу. Цей додаток спроможний виконувати всі потрібні функції, а також завдяки йому функціонує більшість ресурсів мережі.

Сервер, що розробляється, не є винятком через гнучкість та універсальність. Apache для розробки веб-сервера застосовуватиметься дана утиліта.

Конфігураційна система Apache існує у вигляді текстових конфігураційних файлів. Вона має 3 умовні рівні конфігурації:

– Конфігурацію сервера (файлове наповнення httpd.conf).

– Конфігурацію віртуального хосту (файлове наповнення httpd.conf с версії 2.2, extra / httpd-vhosts.conf).

– Конфігурацію рівня директорії (файлове наповнення - Htaccess).

– Частина модулів застосовує у власній роботі конфігураційні файли ОС на кшталь / etc / passwd і / etc / hosts.

Після встановлення Apache, під час вдалого запуску веб-сервера, - на панелі швидкого доступу з’явиться ярлик ApacheMonitor (рис. 3.7).

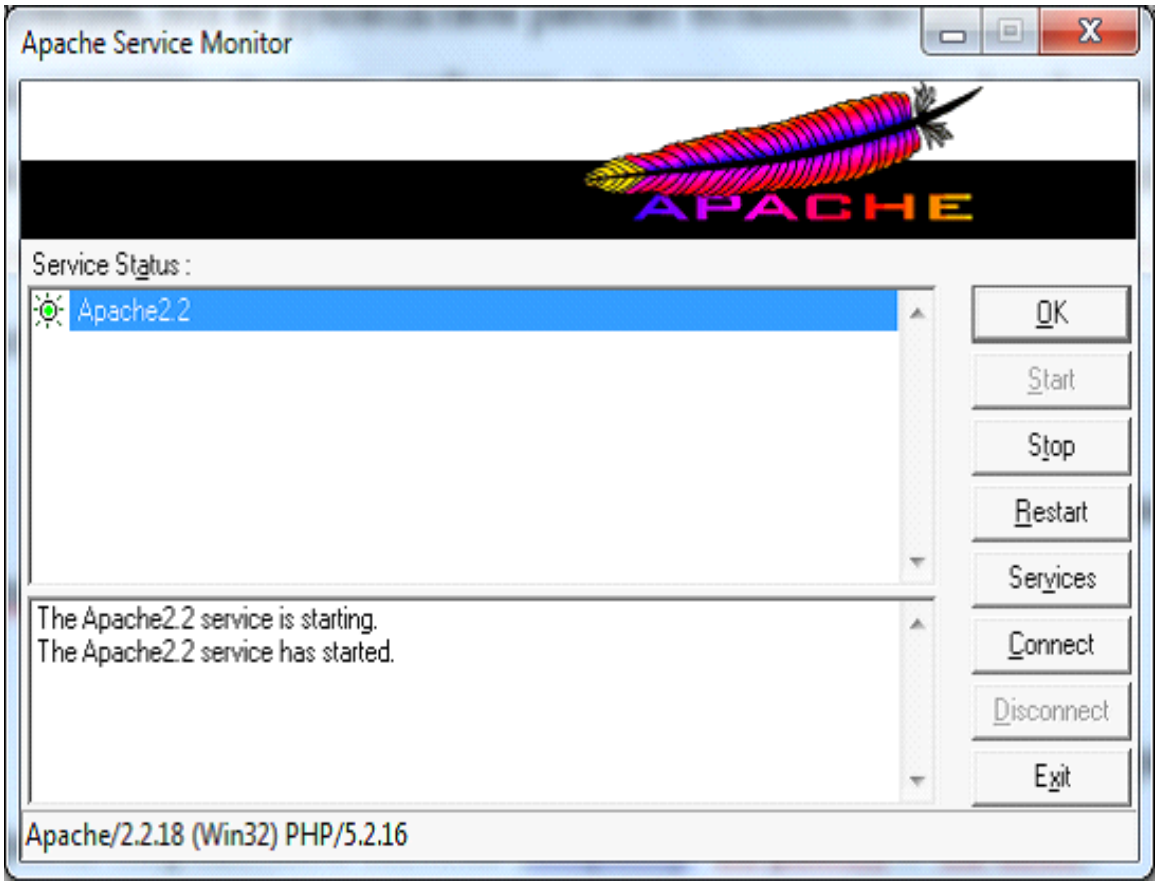


Рисунок 3.7 – Apache Monitor

Представимо лістинг коду програми біометричного розпізнавання особи.

#include <SPI.h> #include <MFRC522.h> #define RST_PIN2 // #define SS_PIN4 //

unsigned long uidDec, uidDecTemp;

MFRC522 mfr522 (SS_PIN, RST_PIN); // Створенняоб'єкта mrfc522 класу

MFRC522

void setup () {Serial.begin (115200); SPI.begin ();

mfrc522.PCD_Init (); // Init MFRC522

}

}

void loop () {if (mfrc522.PICC_IsNewCardPresent ()) {first_card_come = true;

unsigned long uid = getID (); if (uid! = -1) {

reader = String (uid); reader.toCharArray (from_card, 12); Serial.println

(from_card);

```
for (i = 11; i <305; i = i + 1) {int x = i;
for (int a = 11; a> = 0; a = a-1) {arr_id [a] = all [i];
i = i-1;
}
i = x;
int a = 0; for (i = 0; i <strlen (from_card); i = i + 1) {if (arr_id [i] ==
from_card [i]) a = a + 1; } If (a == strlen (from_card) and all [x + 8] == ‘1’) {
Serial.println ( "Welcome!");
}
else if (a == strlen (from_card) and all [x + 9] == ‘0’) {Serial.println ( "You’re not
welcome here :(");
}
i = x;
}
}
}
}
voidShowReaderDetails () {
// Get the MFRC522 software version
byte v = mfrc522.PCD_ReadRegister (mfrc522.VersionReg); Serial.print (F (
"MFRC522 SoftwareVersion: 0x")); Serial. print (v, HEX);
if (v == 0x91) Serial.print (F ( "= v1.0")); else if (v == 0x92) Serial.print (F ( "=
v2.0")); else
Serial.print (F ( "(unknown)")); Serial.println ( "");
// When 0x00 or 0xFF is returned, communication probably failed if ((v == 0x00) ||
(v == 0xFF)) {
Serial.println (F ( "WARNING: Communication failure, is the MFRC522 properly
connected?"));
}
}
```

unsigned long getID () {

if (! mfrc522.PICC_ReadCardSerial ()) {// Since a PICC placed get Serial and continue

return -1;

}

unsigned long hex_num;

hex_num = mfrc522.uid.uidByte [0] << 24; hex_num + = mfrc522.uid.uidByte [1] << 16; hex_num + = mfrc522.uid.uidByte [2] << 8; hex_num + = mfrc522.uid.uidByte [3]; mfrc522.PICC_HaltA (); // Stop reading return hex_num;

7.3 Висновки до розділу

Підсумовуючи третій розділ, можемо зробити такі висновки:

• Для вдалої комунікації між контролером та ідентифікатором СБР завдяки даному середовищу програмування, слід завантажити і налаштувати програму Arduino «RFID Library for MFRC522». Ця бібліотека потрібна для того, щоб в Arduino IDE з’явилися команди для синхронізації з RC522.

• Алгоритм роботи розробленої СБР має такі етапи:

• Сигнали наявності мітки приходить з RFID-картки на МК;

• МК посилає запит на сервер з БД. Зясовується, чи є права доступу у користувача;

• Веб-сервер надає відповідь. Далі з’являються альтернативи розвитку сценарію: користувачу дозволено увійти чи відмовлено у доступі. В разі відмови у доступі СБР не чинить ніяких дій в очікуванні наступного сеансу розпізнавання;

• В разі, якщо особа отримує доступ, то МК посилає сигнал на сервопривід із задачею дозволити доступ, за умови, якщо доступу не було надано;

• Далі на веб-сервер, створений платою Wemos D1 R2, посилаються дані стосовно періоду відвідування та унікальний номер картки.

ВИСНОВКИ

Підсумовуючи загальний зміст роботи, можемо констатувати наступне:

• Аутентифікація – це процес перевірки особистості користувача. Технологія перевірки аутентичності спроможна здійснювати контроль за доступом для різних систем, здійснюючи інспекцію даних користувача. Вона перевіряє збіг даних із його обліковими даними в загальній БД користувачів на сервері аутентифікації. Таким чином аутентифікація - це структура функціонування будь-якого ПЗ та всі небезпеки, що пов’язані з нею, є критичними для більшості сучасних ІС.

• Вибір біометрії для будь-якого практичного застосування залежить від характерних вимірів та вимог користувача. При виборі конкретного біометричного параметра слід враховувати такі фактори, як продуктивність, соціальна прийнятність, простота обходу та/або підробки, надійність, охоплення населення, розмір необхідного обладнання та захист від крадіжки особистих даних. При цьому вибір біометрії ґрунтується на вимогах користувача та враховує доступність датчиків та пристроїв, час обчислень та надійність, вартість, розмір датчика та енергоспоживання.

• Мультимодальні біометричні системи використовують кілька датчиків чи біометричних даних для подолання обмежень одномодальних біометричних систем. Наприклад, системи розпізнавання райдужної оболонки можуть бути скомпрометовані через старіння райдужної оболонки, а розпізнавання електронних відбитків пальців може погіршитися через зношені або порізані відбитки пальців. Хоча одномодальні біометричні системи обмежені цілісністю свого ідентифікатора, малоймовірно, що кілька одномодальних систем страждатимуть від однакових обмежень. Мультимодальні біометричні системи можуть отримувати набори інформації від одного і того ж маркера (наприклад, кілька зображень райдужної оболонки ока або відскановані зображення одного й того ж пальця) або інформацію від різних біометричних даних (потрібне сканування відбитків пальців та, при використанні розпізнавання голосу, голосовий пароль). Мультимодальні біометричні системи можуть об’єднувати ці

одномодальні системи послідовно, одночасно їх комбінацією або послідовно, що відноситься до послідовного, паралельного, ієрархічного і послідовного режимів інтеграції відповідно.

• Наразі система контролю доступу є структурою в комплексі дотримання безпеки і успішно взаємодіє із іншими АС приміщення чи території та може бути загальною АСУ компанії. Насамперед це стосується загальної АСУ, підприємства. Такий рівень синхронізації СКУД з іншими системами відбувається завдяки наявності прямого контакту з користувачами. Постійно присутній обмін інформацією між СКУД та іншими ІС.

• У захищеній ІС передачу можна здійснювати виключно у парі із засобами захисту мережевого трафіку. Методи розпізнавання особи СКУД ділять на кілька груп. Першу з них представляють методи, що засновуються на впровадженні зовнішніх по відношенню до користувача ідентифікаторів - електронних ключів, які у складі містять унікальний код, що розпізнається СКУД і якому в її БД присутні персональні дані особи, яка проходить процес розпізнавання. Другу групу утворюють ідентифікаційні методи, що створені на використанні біометричних характеристик користувачів.

• Біометричне розпізнавання є досить популярним, адже ідентифікаційна ознака є невід'ємною рисою конкретного користувача, її неможливо втратити, забути, передати, дуже складно або неможливо підробити, його не потрібно видавати, поновлювати. Саме тому біометрична ідентифікація швидко розвивається на ринку систем безпеки. Навіть історично перші біометричні технології ідентифікації - по контурах долоні і відбитками пальців - постійно удосконалюються. Так, за допомогою телевізійних пристроїв створені з використанням безконтактної технології зчитувачі цих ознак. На відміну від традиційних, вони більш гігієнічні, так як вони передбачають контакту пальця з будь-якої поверхнею, а тому значно простіше в обслуговуванні.

• Inter Systems Caché - це комерційна система управління операційними базами даних від InterSystems , що використовується для розробки програмних додатків для управління охороною здоров'я, банківськими та фінансовими

послугами, урядом та іншими секторами. Програмне забезпечення замовника може використовувати базу даних з об’єктним та SQL-кодом. Caché також дозволяє розробникам безпосередньо маніпулювати базовими структурами даних: ієрархічними масивами, відомими як M-технологія. Всередині Caché зберігає дані у багатовимірних масивах, здатних зберігати ієрархічно структуровані дані.

• Для вдалої комунікації між контролером та ідентифікатором СБР завдяки даному середовищу програмування, слід завантажити і налаштувати програму Arduino «RFID Library for MFRC522». Ця бібліотека потрібна для того, щоб в Arduino IDE з’явилися команди для синхронізації з RC522.

• Алгоритм роботи розробленої СБР має такі етапи:

• Сигнали наявності мітки приходить з RFID-картки на МК;

• МК посилає запит на сервер з БД. Зясовується, чи є права доступу у користувача;

• Веб-сервер надає відповідь. Далі з’являються альтернативи розвитку сценарію: користувачу дозволено увійти чи відмовлено у доступі. В разі відмови у доступі СБР не чинить ніяких дій в очікуванні наступного сеансу розпізнавання;

• В разі, якщо особа отримує доступ, то МК посилає сигнал на сервопривід із задачею дозволити доступ, за умови, якщо доступу не було надано;

• Далі на веб-сервер, створений платою Wemos D1 R2, посилаються дані стосовно періоду відвідування та унікальний номер картки.

Отже, в результаті виконання дипломного проекту вдосконалено модуль біометричного розпізнавання особи для захисту об’єктів критичної інфраструктури базі апаратно-програмного комплексу Arduino, RFID-карток та додатку Inter Systems Cache. Враховуючи отримані в ході напрацювань результати, можна стверджувати, що визначена мета досягнена, а окреслені завдання проекту повністю виконані.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Юдін О. К. Інформаційна безпека держави / О. К. Юдін. — К. : Консум. — 2005. — 576 с.

2. Гинце А. А. Особенности СКУД систем доступа крупных распределенных объектов / А. А. Гинце. ААМ Систем, 2005.

3. Юдін О. Критеріальний аналіз сучасних операційних систем у задачах захисту інформаційних ресурсів / О. Юдін, О. Весельська // Наукоємні технології. — 2012. — Т. 14. — №. 2. — С. 74-79.

4. Волхонский В.В. Системы контроля и управления доступом - СПб: Университет ИТМО, 2015.

5. Класифікація загроз державним інформаційним ресурсам інженерно-технічного спрямування. Методологія побудови класифікатора / О. К. Юдін, С. С. Бучик // Наукоємні технології. - 2015. - № 2. - С. 188-195

6. Аналіз та класифікація систем контролю та управління доступом на підприємстві О. К. Юдін, д-р техн. наук, проф. Національний авіаційний університет orcid.org/0000-0001-5098-7796; О. М. Весельська Національний авіаційний університет orcid.org/0000-0002-4914-2187.

7. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу – Київ, 1999. – 20 с.

8. Принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних системах / Ю.В. Землянко, О.А. Замула, О.О. Ткач, Н.І. Литвинова, Я.А. Пересічанська.]., 2010.

9. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.]–Вінниця : ВНТУ, 2017.– 120 с.

10. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення – Київ, 2007. – 6 с.

11. НД ТЗІ 3.1-001-07. Захист інформації на об’єктах інформаційної діяль-ності. Створення комплексу технічного захисту інформації. Передпроектні роботи – Київ, 2007. – 5 с.

12. Принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних систем [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: http://openarchive.nure.ua/bitstream/document/861/1/460-469.pdf.

13. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі – Київ, 2005. – 20 с.

14. Засоби створення шкідливого програмного забезпечення [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://studfile.net/preview/5206321/page:17/.

15. Безпека інформаційно-комунікаційнихсистем. Шкідливе програмне забезпечення [Електронний ресурс] – Режим доступу до ресурсу: http://virt.ldubgd.edu.ua/pluginfile.php/39805/mod_resource/content/3/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%201.4.pdf.

16. ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО УРЯДУВАННЯ Навчальний посібник у 15 частинах Загальна редакціяАндрій Іванович Семенченко, Валерій Михайлович Дрешпак Формат 60×90/16.Папір офс. 80 г/м2. Гарн. Таймс. Друк офс.Ум. друк. арк. 4,5. Авт. арк. 3,0. Наклад 500 прим. Видавець та друк: ФОП Москаленко О. М.

17. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації [Електронний ресурс] : навчальний посібник / С. О. Іванченко, О. В. Гавриленко, О. А. Липський [та ін.] ; НТУУ «КПІ». – Електронні текстові дані (1 файл: 615 Кбайт). – Київ : НТУУ «КПІ», 2016. – 104 с. – Назва з екрана.

18. Безпека систем підтримки прийняття рішень [Текст] : навч. посіб. / Ковтунець В. В., Нестеренко О. В., Савенков О. І. ; Нац. акад. упр. - Київ : Нац. акад. упр., 2016. - 189 с. : рис., табл. - Бібліогр.: с. 183-184. - 300 прим. - ISBN 978-617-7386-00-0

19. ЗАКОН УКРАЇНИ Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

20. до ресурсу: https://www.rfc-editor.org/rfc/rfc2104.

21. Лужецький В. А. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця: ВНТУ, 2009. – 268 с.

22. Аліпов Ілля Миколайович. Методи захисту інформації при її передаванні : Автореф. дис... канд. техн. наук: 05.13.08 / Харківський держ. технічний ун-т радіоелектроніки. - Х., 1997. - 22с

23. Богуш Володимир Михайлович, Мухачов Владислав Андрійович. Криптографічні застосування елементарної теорії чисел : Навч. посібник / Державний ун-т інформаційно-комунікаційних технологій. - К. : ДУІКТ, 2006. – 126 с.

24. Ємець Володимир, Мельник Анатолій, Попович Роман. Сучасна криптографія: Основні поняття . - Л. : БаК, 2003. - 144с. : рис., табл. - (Захист інформації в комп'ютерних та телекомунікаційних мережах). - Бібліогр.: с. 128.

25. Hung-JenLiao. Intrusion detection system: A comprehensive review / Hung-JenLiao, Kuang-YuanTunga. // Journal of Network and Computer Applications. – 2013. – №36. – С. 16–24.

26. Snort IDS and IPS Toolkit [Електронний ресурс]. – 2007. – Режим

27. доступу до ресурсу: https://www.amazon.com/Snort-Toolkit-Beales-SourceSecurity/dp/1597490997.

28. Polymorphic Blending Attacks [Електронний ресурс]. – 2006. – Режим доступу до ресурсу:

29. https://www.usenix.org/legacy/event/sec06/tech/full_papers/fogla/fogla.pdf.

30. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с.

ДОДАТКИ

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

Кваліфікаційна робота здобувача освітнього ступеня «Магістр»

СИСТЕМА УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ (PRIVILEGED ACCESS MANAGEMENT) НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Спеціальність: 125 – Кібербезпека та захист інформації

Виконала: Анна ХОМЕНКО

Керівник: к.т.н., доцент Юрій ПЕПА

Київ – 2025

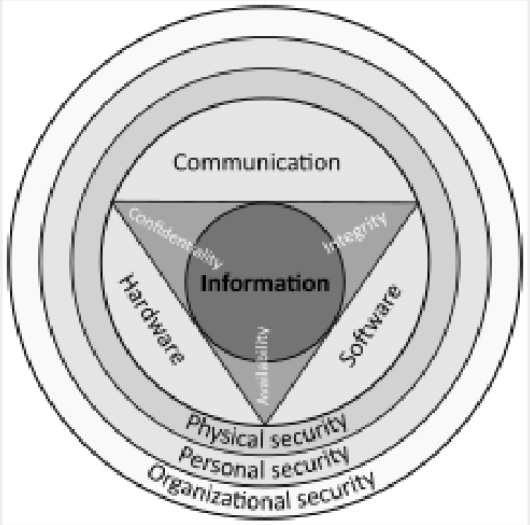
АКТУАЛЬНІСТЬ, МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

- Актуальність роботи зумовлена потребою захисту об’єктів критичної інфраструктури від несанкціонованого доступу та компрометації привілейованих облікових записів.
- Мета роботи - розробка та впровадження автоматизованої системи управління привілейованим доступом на основі біометричного розпізнавання особи.
- Об’єкт дослідження - системи фізичного захисту інформації від несанкціонованого доступу на об’єкті інформаційної діяльності.
- Предмет дослідження - автоматизована система управління привілейованим доступом на об’єкті інформаційної діяльності.
- Завдання: дослідити фактори аутентифікації, проаналізувати засоби біометричного розпізнавання, обґрунтувати програмно-апаратну платформу та виконати моделювання СБР.

ІНФОРМАЦІЙНА СИСТЕМА ТА ЇЇ СКЛАДОВІ

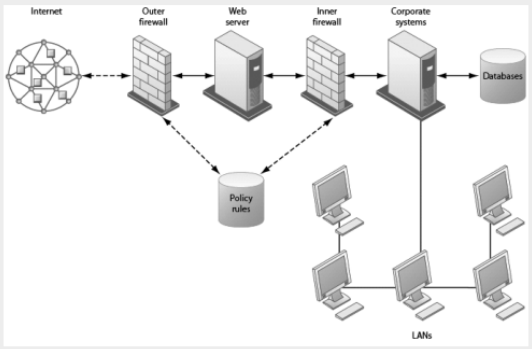
- Інформаційна система розглядається як сукупність технічного, програмного, математичного, інформаційного, організаційного та правового забезпечення.
- Захист такої системи повинен охоплювати апаратні, програмні, мережеві та організаційні компоненти.
- Для об’єктів критичної інфраструктури особливе значення має контроль доступу до сервісів, баз даних і адміністративних функцій.

АТРИБУТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ



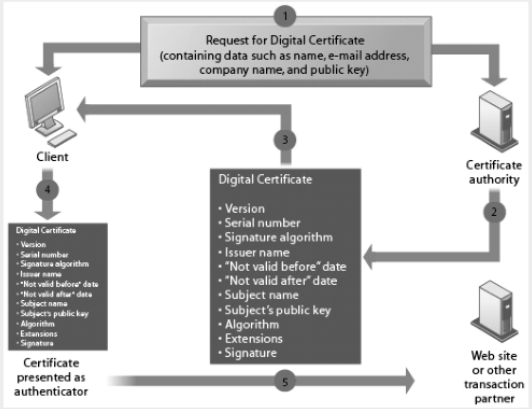
- Основними властивостями інформаційної безпеки є конфіденційність, цілісність і доступність.
- Управління ризиками передбачає ідентифікацію активів, загроз, уразливостей, оцінювання ризиків і вибір заходів безпеки.
- Система PAM має зменшувати ризики, пов’язані з підвищеними правами користувачів і адміністраторів.

МЕРЕЖЕВІ ЗАСОБИ ЗАХИСТУ ТА КОНТРОЛЬ ДОСТУПУ



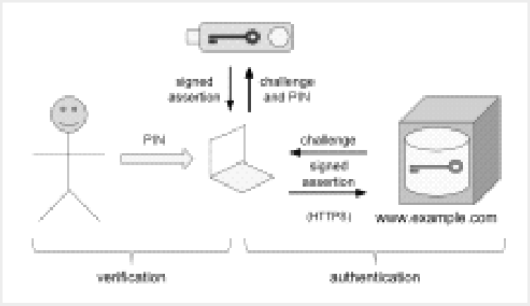
- У роботі розглянуто брандмауери, системи виявлення вторгнень, антивірусний захист, шифрування та інструменти аутентифікації.
- Брандмауер контролює мережевий трафік між приватною мережею та зовнішнім середовищем.
- Контроль доступу визначає правила допуску користувачів до систем, даних і критичних функцій.

КРИПТОГРАФІЧНИЙ ЗАХИСТ І ЦИФРОВІ СЕРТИФІКАТИ



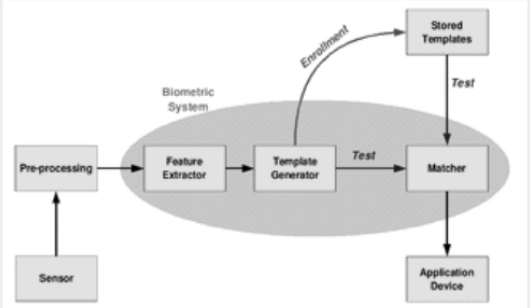
- Цифрові сертифікати застосовуються для підтвердження особи користувачів і захисту онлайн-транзакцій.
- PKI забезпечує автентифікацію та захищений обмін даними через використання відкритих і закритих ключів.
- Криптографічний рівень доповнює біометричну ідентифікацію та зменшує ризик підміни суб’єкта доступу.

WEB-АУТЕНТИФІКАЦІЯ ТА ФАКТОРИ ІДЕНТИФІКАЦІЇ



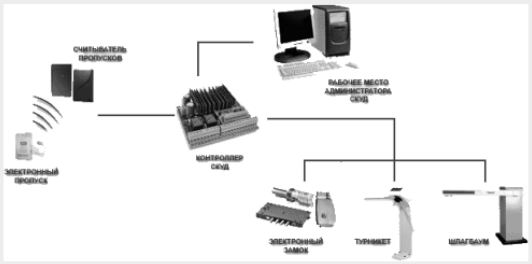
- Аутентифікація підтверджує, що користувач є саме тим суб’єктом, за якого себе видає.
- У системах безпеки використовуються фактори знання, володіння та біометричні характеристики.
- WebAuthn і схожі механізми дозволяють реалізувати сучасну стійку аутентифікацію для веб-додатків.

БІОМЕТРИЧНЕ РОЗПІЗНАВАННЯ ОСОБИ



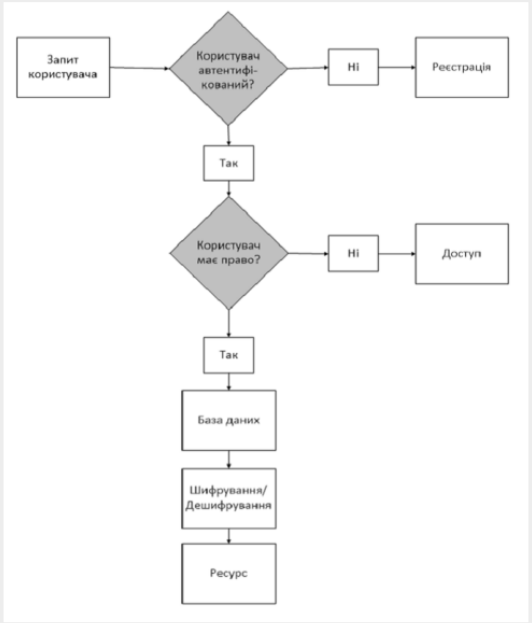
- Біометричне розпізнавання ґрунтується на аналізі унікальних фізіологічних характеристик людини.
- Алгоритм розпізнавання передбачає отримання зображення, виділення ознак, порівняння з шаблонами та ухвалення рішення про допуск.
- Перевагою біометрії є складність передачі або втрати фактора аутентифікації порівняно з паролем чи карткою.

СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ



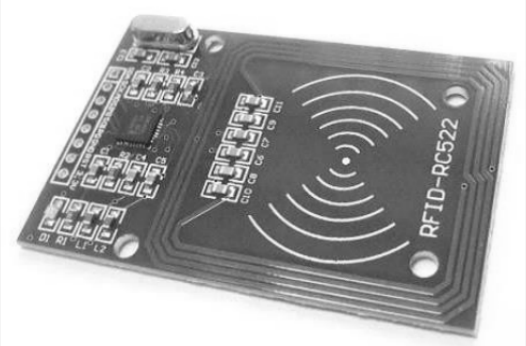
- СКУД забезпечує обмеження доступу до приміщень, зон і ресурсів об’єкта інформаційної діяльності.
- У складі СКУД застосовуються контролери, зчитувачі, виконавчі механізми, бази даних користувачів та журналювання подій.
- Інтеграція СКУД із PAM підвищує контроль над привілейованими діями користувачів.

АЛГОРИТМ КОНТРОЛЮ ДОСТУПУ ДО ВЕБ-ДОДАТКУ



- Алгоритм контролю доступу передбачає перевірку користувача, його прав і відповідності політикам безпеки.
- У разі успішної ідентифікації система відкриває доступ до дозволених функцій; у разі відмови - блокує запит і фіксує подію.
- Журналювання дозволяє виконувати аудит привілейованих дій та реагувати на інциденти.

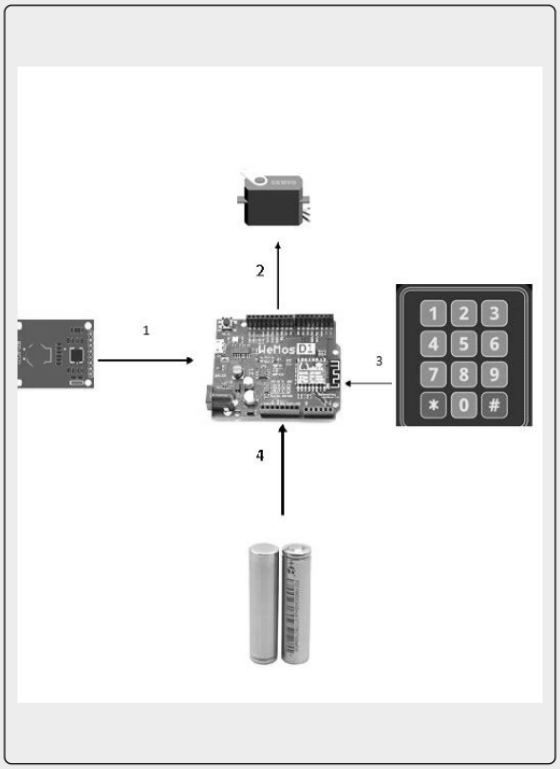
ОБҐРУНТУВАННЯ ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ



- Для реалізації системи обґрунтовано використання апаратно-програмного комплексу Arduino, RFID-карток і клієнт-серверного додатку.
- RFID-зчитувач виконує ідентифікацію носія, а біометричний модуль уточнює належність доступу конкретній особі.
- Комбінація факторів підвищує стійкість системи до компрометації одного з механізмів контролю.

АЛГОРИТМ РОБОТИ СИСТЕМИ БІОМЕТРИЧНОГО РОЗПІЗНАВАННЯ

- Розроблений алгоритм описує послідовність зчитування ідентифікатора, перевірки біометричних даних і ухвалення рішення про допуск.
- У процесі роботи система порівнює поточні дані з еталонними записами бази та формує результат аутентифікації.
- Алгоритм забезпечує взаємодію з апаратними модулями та програмною частиною системи.



- Структурна схема відображає взаємодію RFID-модуля, контролера, сервоприводу, користувацького інтерфейсу та бази даних.
- Моделювання дозволило перевірити логіку обміну даними між апаратною і програмною частинами.
- Реалізована архітектура може бути використана для підвищення захищеності об’єктів критичної інфраструктури.

ДЯКУЮ ЗА УВАГУ!

Доповідь підготувала здобувачка вищої освіти Анна ХОМЕНКО

Тема: «Система управління привілейованим доступом (PAM)»

Київ – 2025