Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Розробка багатофункціональної системи контролю доступу підвищеної захищеності до критичних об'єктів від електромагнітних завад і функцією адаптивного екранування

Виконав: студент 4 курсу, гр.2КІТС-21б
спеціальності 125– Кібербезпека
Освітня програма – Кібербезпека
інформаційних технологій та систем
(шифр і назва напряму підготовки, спеціальності)

Римаренко М.В
(прізвище та ініціали)

Керівник: к.т.н., доц., зав. каф. МБІС
Карпінець В.В.
(прізвище та ініціали)
« 4 » червня 2025 р.

Рецензент: к.т.н., доцент каф. ОТ
Боголомов С.В.
(прізвище та ініціали)
« 4 » червня 2025 р.

Допущено до захисту
Голова секції УБ кафедри МБІС
д.т.н., проф. Яремчук Ю.Є.
" 4 " червня 2025р.

Вінниця ВНТУ – 2025

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

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

ЗАТВЕРДЖУЮ
Голова секції УБ, кафедра МБІС
д.т.н., проф. Яремчук Ю.Є.
" 20 " березня 2025 р.

З А В Д А Н Н Я
на бакалаврську кваліфікаційну роботу студенту
Римаренку Миколі Вікторовичу
(прізвище, ім`я, по-батькові)

1. Тема роботи Розробка багатофункціональної системи контролю доступу підвищеної захищеності до критичних об'єктів від електромагнітних завад і функцією адаптивного екранування.
Керівник роботи Карпінець Василь Васильович, к.т.н., доц., зав. каф. МБІС
(прізвище, ім`я, по-батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "20" березня 2025року № 97
2. Термін подання студентом роботи 3 червня 2025р
3. Вихідні дані до роботи Електронні джерела, підручники та наукові статті по темі. Існуюче програмне забезпечення, яке стосується теми бакалаврської дипломної роботи.
4. Зміст текстової частини:
Для досягнення мети було поставлено такі задачі: проаналізувати сучасні системи контролю доступу та їх вразливість до електромагнітних завад; розробити алгоритм роботи багатофункціональної системи з використанням мікропроцесора ESP32; реалізувати функції біометричної авторизації та адаптивного екранування; створити прототип пристрою та перевірити його працездатність в умовах, наближених до реальних.
5. Перелік ілюстративного матеріалу: презентація у форматі PowerPoint з ілюстраціями структурної схеми приладу та скріншотами моделювання схеми приладу

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ I	Карпінець В.В. к.т.н., доц., зав. каф. МБІС		
Розділ II	Карпінець В.В. к.т.н., доц., зав. каф. МБІС		
Розділ III	Карпінець В.В. к.т.н., доц., зав. каф. МБІС		

7.Дата видачі завдання 20 березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва та зміст етапу	Термін виконання		Примітка
		початок	закінчення	
1	Аналіз потреб у сфері систем контролю доступу	01.04.2025	07.04.2025	Виконано
2	Дослідження існуючих рішень та методів реалізації СКУД	08.04.2025	14.04.2025	Виконано
3	Формулювання задачі та визначення технічних характеристик пристрою	15.04.2025	17.04.2025	Виконано
4	Вибір апаратної архітектури системи доступу та захисту від ЕМВ	18.04.2025	21.04.2025	Виконано
5	Розробка структурної та принципової електричної схеми пристрою	22.04.2025	26.04.2025	Виконано
6	Проєктування алгоритму роботи пристрою контролю доступу	27.04.2025	01.05.2025	Виконано
7	Розробка програмного забезпечення для ESP32 з підтримкою Telegram-повідомлень	02.05.2025	10.05.2025	Виконано
8	Монтаж та збирання апаратної частини прототипу системи	11.05.2025	14.05.2025	Виконано
9	Проведення практичного тестування СКУД із екрануванням	15.05.2025	20.05.2025	Виконано

Студент (підпис) Римаренко М.В. (прізвище та ініціали)

Керівник роботи (підпис) Карпінець В.В. (прізвище та ініціали)

АНОТАЦІЯ

Дана бакалаврська кваліфікаційна робота присвячена розробці багатофункціональної системи контролю доступу з підвищеним рівнем захищеності, орієнтованої на використання в умовах критичних об’єктів. У роботі проаналізовано сучасні загрози безпеці інформації та фізичного доступу, зокрема ті, що виникають під впливом зовнішніх електромагнітних завад.

Розглянуто основні технічні та програмні компоненти систем контролю доступу, проведено аналіз факторів, що можуть впливати на їхню стабільну роботу. Особливу увагу приділено функціональним можливостям системи – багаторівневій автентифікації, веденню журналу подій, реагуванню на несанкціоновані спроби доступу тощо. Система також враховує вплив несприятливих зовнішніх умов та передбачає базові заходи захисту електроніки від типових електромагнітних впливів.

Результатом роботи стала технічно обґрунтована модель багатофункціонального пристрою контролю доступу, адаптована до реальних загроз і вимог об’єктів з підвищеним рівнем безпеки.

Ключові слова: контроль доступу, технічний захист інформації, критичні об’єкти, електромагнітні завади, інформаційна безпека, система безпеки.

ABSTRACT

This bachelor's thesis is devoted to the development of a multifunctional access control system with an increased level of security, focused on use in critical facilities. The work analyses modern threats to information security and physical access, in particular those arising from external electromagnetic interference.

The main technical and software components of access control systems are considered, and the factors that may affect their stable operation are analysed. Particular attention is paid to the functionality of the system – multi-level authentication, event logging, response to unauthorised access attempts, etc. The system also takes into account the impact of adverse external conditions and provides basic measures to protect electronics from typical electromagnetic influences.

The result of the work is a technically sound model of a multifunctional access control device adapted to the real threats and requirements of high-security facilities.

Keywords: access control, technical protection of information, critical facilities, electromagnetic interference, information security, security system.

ЗМІСТ

ВСТУП

Актуальність. Сучасний рівень розвитку технологій у сфері систем безпеки та контролю доступу постійно вдосконалюється, зумовлюючи потребу у впровадженні нових технічних рішень або модернізації наявних пристроїв. З огляду на підвищення рівня загроз, пов’язаних із несанкціонованим доступом до критично важливих об'єктів, виникає необхідність у розробці багатофункціональних, захищених та адаптивних систем, здатних ефективно протидіяти як фізичним, так і технічним методам вторгнення. Особливої актуальності набуває створення системи, яка не лише забезпечує надійну автентифікацію користувача, а й здатна протистояти зовнішнім електромагнітним завадам, має зручний мобільний інтерфейс керування, підтримує двофакторну авторизацію, та інтегрується в сучасні інформаційні інфраструктури.

Мета роботи. Метою роботи є розробка інноваційної багатофункціональної системи контролю доступу з підвищеним рівнем захисту від електромагнітних завад та логуванням подій у месенджері.

Об’єкт дослідження. Об’єктом дослідження є технічні засоби та інформаційні технології, що застосовуються у системах контролю доступу для захисту критичних об'єктів.

Предмет дослідження. Предметом дослідження є процес розробки та функціонування багатофункціональної системи контролю доступу, що поєднує в собі мобільне керування, біометричну автентифікацію, лазерну детекцію, екранування від електромагнітних завад та логування подій.

Новизна роботи. Новизна роботи полягає у розробці комплексної системи контролю доступу, яка поєднує:

– використання мікроконтролера ESP32 для централізованого управління доступом;
– логування спроб доступу та реагування датчика руху;
– лазерну сітку для детекції вторгнень у режимі реального часу;
– застосування екрануючих матеріалів для захисту від електромагнітних завад;

– використання біометричної ідентифікації для підвищення рівня безпеки.

Практична цінність. Практична цінність роботи полягає у можливості впровадження розробленої системи контролю доступу в реальних умовах для підвищення безпеки державних, комерційних та наукових об’єктів. Система може ефективно використовуватись для захисту інформаційних та фізичних ресурсів, забезпечуючи швидке реагування на несанкціоновані дії, зручність керування через месенджер, та стійкість до зовнішніх впливів, зокрема електромагнітного випромінювання.

1 АНАЛІЗ СУЧАСНИХ СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

Системи контролю та управління доступом є ключовим елементом сучасної безпеки, що забезпечують захист об'єктів різної критичності. Попри впровадження новітніх рішень, таких як біометрична ідентифікація та бездротові технології, наявні системи залишаються вразливими до електромагнітних завад, мають обмежену функціональність і ризик несанкціонованого доступу. У цьому розділі буде проаналізовано сучасні технології контролю доступу, їх переваги та недоліки, що дозволить визначити напрями для вдосконалення та стане основою для створення нової захищеної багатофункціональної системи.

1.1 Аналіз відомих підходів до реалізації СКУД

Системи контролю та управління доступом (СКУД) є невіддільною частиною сучасних рішень у сфері безпеки, які використовуються для забезпечення фізичного або інформаційного захисту об'єктів. Вони виконують завдання ідентифікації, верифікації та контролю доступу, що робить їх необхідними для запобігання несанкціонованому проникненню чи використанню критично важливих ресурсів. Аналіз сучасних підходів до реалізації СКУД дозволяє виявити тенденції їх розвитку та підкреслити ключові аспекти застосування різних технологій у цій галузі.

Різноманіття систем контролю та управління доступом обумовлене їхньою адаптацією до специфічних потреб і масштабів об'єктів. Класифікація СКУД відбувається не лише за технічними параметрами, але й за моделями доступу, які визначають рівень і спосіб обмеження прав користувачів. Одним із найпоширеніших підходів є **Role-Based Access Control (RBAC)**, що базується на ролях користувачів у системі [1]. У цій моделі доступ визначається виключно через призначення ролей, де кожна роль має специфічний набір дозволів. Такий підхід виявився надзвичайно ефективним у великих організаціях, де контроль над доступом пов'язаний із функціональними обов'язками співробітників. Перевагою

RBAC є його гнучкість у визначенні прав доступу для конкретних категорій користувачів, але головним недоліком можна вважати складність управління ролями у випадках швидкої зміни функціональної структури

Основні компоненти RBAC:

- Користувачі (U) – суб’єкти, які взаємодіють із системою.
- Ролі (R) – набір функціональних обов’язків у системі.
- Об’єкти (O) – ресурси, до яких надається доступ.
- Права доступу (P) – дії (наприклад, читання, запис).

Призначення ролей (UA) – зв’язок між користувачами та ролями:

$$UA \subseteq U \times R$$

Призначення прав (PA) – зв’язок між ролями та правами:

$$PA \subseteq R \times PPA \subseteq R \times P$$

Ієрархія ролей (RH) – відношення часткового порядку між ролями:

$$RH \subseteq R \times RRH \subseteq R \times R$$

Можливий доступ (Can-Access):

Користувач *u* може отримати доступ до об’єкта *o* з правом *p*, якщо його роль (або успадкована роль) має відповідне право:

$$\langle u,o,p \rangle can \iff \exists r \in R \cdot ((u,r) \in UA \wedge (r,p,o) \in PA) \langle u,o,p \rangle$$

Поточний доступ (Current-Access):

Сесія *s* (активний екземпляр користувача) отримує доступ до об’єкта *o* з правом *p*, якщо:

1. Користувач сесії *s* має відповідну роль.
2. Ця роль активна в сесії *s*.
3. Роль має необхідне право.

$(s,o,p) current \Leftrightarrow \exists u \in U, \exists r \in R \cdot ((u,r) \in UA \wedge (s,r) \in active\_roles(s) \wedge (r,p,o) \in PA)$

де active_roles(s)active_roles(s) – множина ролей, активних у сесії s.

Іншим важливим підходом є **Mandatory Access Control (MAC)**, що передбачає суворе управління доступом на основі політики безпеки, яка є незмінною для користувачів. У MAC права визначаються на основі рівня довіри користувача або об'єкта, а всі рішення щодо доступу приймаються автоматично (рис 1.1).

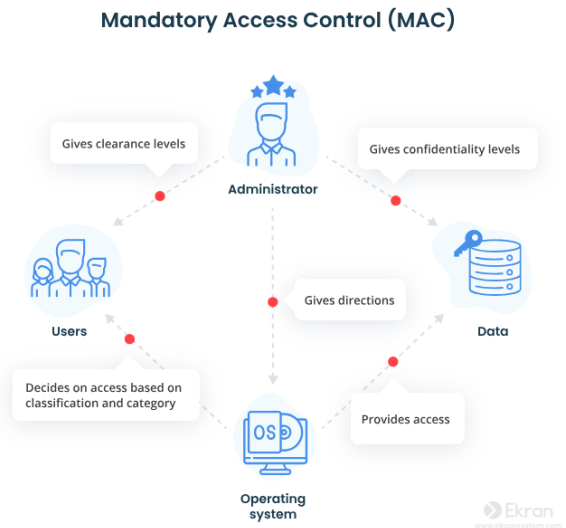


Рисунок 1.1 – Принцип роботи MAC

Така модель ідеально підходить для військових та урядових установ, де критичність інформації та контроль за нею мають ключове значення. Водночас жорсткість правил MAC робить його менш адаптивним до динамічних середовищ [2].

Використання **Discretionary Access Control (DAC)** часто зустрічається в системах, орієнтованих на більш ліберальне управління доступом. DAC дозволяє власникам об'єктів встановлювати правила доступу до них (рис 1.2).

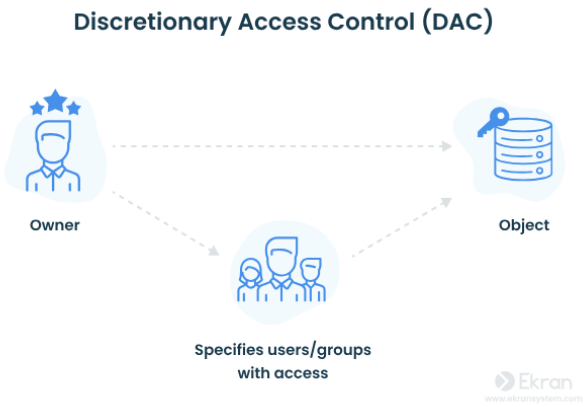


Рисунок 1.2 – Принцип роботи DAC

Це забезпечує високий рівень гнучкості, але створює ризики, пов'язані із людським фактором, оскільки користувачі можуть помилково надати права доступу неавторизованим особам [3].

Отже, можемо зробити висновок, що:

MAC – це централізована модель, де адміністратори або ОС визначають доступ на основі суворих правил безпеки та принципу "необхідності знання". Вона забезпечує високий рівень безпеки завдяки класифікації даних та обмеженням доступу, що ідеально підходить для державних, військових та фінансових установ. Проте MAC вимагає значних адміністративних ресурсів і обмежує гнучкість.

DAC, навпаки, є децентралізованою моделлю, де власники даних самостійно керують доступом до своїх ресурсів. Вона надає користувачам більше свободи та легко адаптується до потреб, що робить її популярною для малого та середнього бізнесу завдяки простоті використання та низьким витратам на адміністрування. Однак, гнучкість DAC призводить до нижчого рівня безпеки через потенційні зловживання.

З точки зору масштабованості, MAC вимагає значних зусиль для розширення через індивідуальне налаштування правил, тоді як DAC легко адаптується. Вартість впровадження MAC значно вища через складність налаштування та підтримки.

На практиці, багато організацій використовують гібридні рішення, поєднуючи MAC для критичних даних та DAC для внутрішньої співпраці. Це дозволяє досягти оптимального балансу між безпекою та продуктивністю.

Окремо варто виділити **Non-Discretionary Access Control**, який є розвитком MAC і RBAC. У цьому підході доступ керується через автоматизовані політики безпеки, але з додаванням логіки, яка враховує контекст доступу, наприклад, час доби, місце знаходження користувача чи інші динамічні чинники. Такий підхід має великий потенціал завдяки його адаптивності до сучасних вимог кібербезпеки [4].

Розвиток технологій суттєво вплинув на еволюцію СКУД. Зокрема, інтеграція **біометричних технологій** дозволила підвищити точність ідентифікації користувачів. Системи, що базуються на скануванні відбитків пальців, розпізнаванні обличчя або голосу, дедалі більше використовуються в критичних галузях, таких як фінанси та охорона здоров'я. Біометричний підхід мінімізує ризик втрати чи крадіжки фізичних носіїв доступу, як-от карток або ключів, однак вимагає додаткових заходів захисту для зберігання біометричних даних.

Ще однією важливою інновацією є впровадження **хмарних рішень** у СКУД, які дозволяють централізовано управляти доступом через віддалені сервіси. Хмарні системи забезпечують гнучкість, інтеграцію з іншими інфраструктурними рішеннями та зменшують витрати на підтримку локального обладнання. Однак ці переваги супроводжуються новими викликами у сфері кібербезпеки, такими як загрози несанкціонованого доступу до хмарної інфраструктури [5].

Сучасні системи також активно інтегрують **інтернет речей (IoT)** та алгоритми **штучного інтелекту (ШІ)**, які дозволяють автоматизувати процеси прийняття рішень щодо доступу. Наприклад, IoT дозволяє створювати мережі взаємодії пристроїв, де кожен елемент СКУД може передавати дані в режимі реального часу, а ШІ може аналізувати ці дані для виявлення потенційних загроз [6].

Разом з тим, впровадження сучасних підходів до СКУД не обходиться без проблем. Одним із ключових викликів залишається захист даних, зокрема у випадку біометричних та хмарних рішень. Іншим аспектом є висока вартість систем із розширеним функціоналом, що може обмежувати їх використання серед малих підприємств.

1.2 Різновиди та відмінності методів реалізації СКУД

Системи контролю та управління доступом (СКУД) є одним із ключових інструментів для забезпечення безпеки на об'єктах різного призначення – від офісів і промислових підприємств до багатоквартирних будинків. Їх головною метою є обмеження та моніторинг доступу до певних зон шляхом використання різних технологій. Методи реалізації СКУД відрізняються залежно від способів ідентифікації осіб, типів обладнання, рівня інтеграції системи, а також технологій підключення.

Сучасні СКУД можна поділити на кілька основних категорій. Перший важливий аспект – це спосіб ідентифікації. Наприклад, біометричні системи використовують унікальні фізіологічні або поведінкові характеристики людини, такі як відбитки пальців, сітківку ока або навіть розпізнавання обличчя. Вони забезпечують високий рівень безпеки, оскільки ці параметри важко підробити або передати іншій особі. Однак, такі системи потребують складного та дорогого обладнання, а також викликають питання щодо конфіденційності даних.

Альтернативою біометрії є використання карткових систем. У цьому випадку кожному користувачу видається картка доступу з магнітною стрічкою, штрих-кодом або безконтактним чипом. Вартість такого рішення зазвичай нижча, а встановлення простіше. Однак ці системи мають свої недоліки, адже картки можуть бути втрачені, скопійовані чи передані іншій людині, що знижує рівень безпеки [7].

Ще одним популярним методом є кодові системи, які передбачають введення спеціального цифрового коду для доступу до приміщення. Вони досить прості у використанні та не потребують фізичних носіїв, таких як картки. Проте цей підхід має ризик: якщо код стане відомим стороннім особам, безпеку об’єкта буде зламано.

Мобільні СКУД – сучасний тренд у сфері безпеки. Вони використовують смартфони або носимі пристрої для автентифікації користувачів. Це може відбуватися за допомогою Bluetooth, NFC чи QR-кодів. Основними перевагами такого підходу є зручність і можливість інтеграції з іншими мобільними додатками,

але його недоліками залишаються залежність від роботи смартфона та ризик втрати доступу через технічні несправності [8].

Іншим важливим аспектом класифікації СКУД є рівень централізації системи. Автономні системи працюють незалежно одна від одної. Це означає, що кожен пристрій керується локально, без потреби в об’єднанні з іншими елементами системи. Такі рішення підходять для невеликих об’єктів із обмеженою кількістю точок доступу. Натомість мережеві СКУД інтегрують усі точки доступу в єдину мережу, дозволяючи централізовано керувати доступом, отримувати звіти та контролювати систему в реальному часі. Вони є більш гнучкими та масштабованими, але потребують складнішого налаштування та вищих витрат.

Технології підключення також мають значення. Провідні СКУД відрізняються високою надійністю передачі даних завдяки використанню кабельного з'єднання. Вони особливо ефективні на об'єктах, де можлива прокладка кабелів, проте їх встановлення може бути трудомістким. У свою чергу, бездротові СКУД працюють через Wi-Fi, Bluetooth або інші протоколи зв’язку, що значно спрощує процес встановлення, але може знизити стабільність роботи в умовах завад.

На додаток до основних функцій багато сучасних СКУД є інтелектуальними. Вони інтегруються з іншими системами безпеки, наприклад, відеоспостереженням чи пожежною сигналізацією. Такі системи здатні аналізувати поведінку користувачів, адаптуватися до змін і навіть виявляти підозрілу активність. Інтелектуальні СКУД, засновані на технологіях штучного інтелекту, стають основою для побудови концепції «розумних будівель» [9].

У підсумку, вибір методу реалізації СКУД залежить від багатьох факторів: масштабу об'єкта, бюджету, вимог до безпеки та технологічних можливостей. Кожен із описаних методів має свої переваги та обмеження, тому важливо проводити детальний аналіз перед впровадженням системи на конкретному об’єкті.

1.3 Аналіз існуючих реалізацій пристроїв

У даному підрозділі буде розглянуто готові пристрої, які використовуються для реалізації систем контролю та управління доступом (СКУД). Порівняння та аналіз таких пристроїв є дуже важливими для потенційної розробки нових рішень у цій галузі. Кожен тип СКУД має свої переваги та недоліки, які залежать від методів ідентифікації, умов експлуатації та специфіки об'єкта. Далі розглянемо приклади пристроїв, що представляють різні типи СКУД, з детальним аналізом їхніх характеристик.

Біометричні СКУД – біометричні пристрої забезпечують високий рівень безпеки завдяки використанню унікальних фізіологічних або поведінкових характеристик людини. Для прикладу було взято біометричний автономний замок ZKTeco L7000 [10].

ZKTeco L7000 – це автономний замок, призначений для використання в міжкімнатних дверях. У замку обладнана надійний захист від злому. Потрапити в приміщення можна за відбитком пальця, після введення 4-х значного коду з клавіатури або за допомогою механічного ключа. Не потрібно носити ключ, просто помістіть палець на датчик читання, і двері розблокується протягом 1 секунди після перевірки. Замок має візуальний OLED-дисплей. Завдяки одній конструкції засувки, цей замок може замінити замок циліндричної ручки, не змінюючи ваші двері. Шаблони відбитків залишаються неушкодженими після збою живлення. Корпус замка виконаний зі сплаву цинку, який досить міцний, щоб захистити систему від будь-якого значного зовнішнього впливу. Блокування живиться чотирма лужними 1,5 батареями великої місткості, які можуть витримувати до 5000 операцій розблокування. На дисплеї OLED буде відображатися стан рівня потужності батареї. Ви можете відкрити двері за допомогою аварійного механічного ключа (рис 1.1).

Рисунок 1.1 – ZKTeco L7000

З опису маємо, що ZKTeco L7000 є надійним автономним замком з кількома рівнями захисту, що робить його хорошим вибором для міжкімнатних дверей, де важлива безпека і швидкість доступу. Завдяки можливості використовувати три способи доступу, замок підходить для різних сценаріїв. Однак його залежність від батарей та можливі проблеми з поломкою електронних компонентів можуть бути важливими факторами, які слід враховувати при виборі. Для застосувань у домашніх або офісних умовах, де доступ до приміщення не потребує частих змін, замок є дуже зручним і безпечним варіантом. Схема роботи спристрою (рис 1.2).

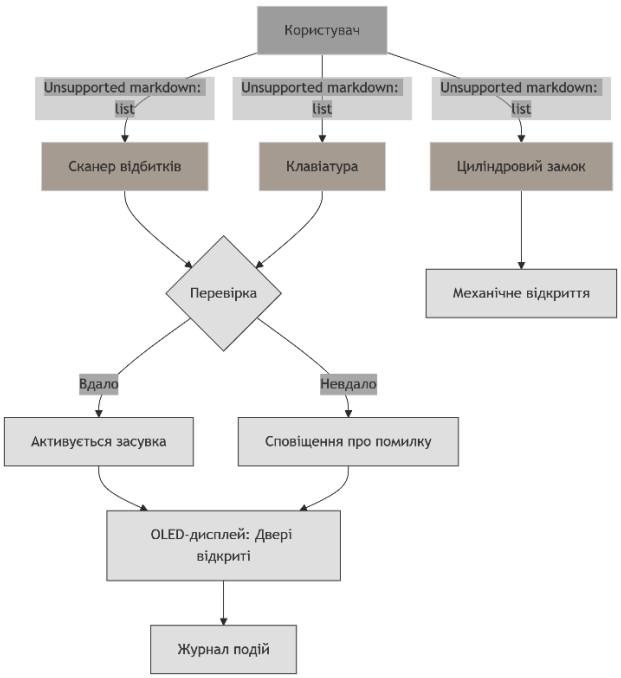


Рисунок 1.2 – Схема роботи пристрою ZKTeco L7000

Карткові СКУД - карткові системи доступу є традиційними, але все ще популярними завдяки простоті використання та відносно невисокій вартості.

HID Global Proximity Cards - це один із найпоширеніших варіантів карткових систем доступу. Картки оснащені безконтактними чипами, які забезпечують швидку ідентифікацію. Вони часто використовуються в офісах і на промислових підприємствах [11].

До переваг можна віднести легкість використання, надійність, доступна ціна, а до недоліків можливість втрати картки або передачі іншій людині. Для опрацювання даної картки компанія пропонує – ZKTeco RFID Readers.

ZKTeco RFID Readers – це сучасний зчитувач, який підтримує RFID-технологію. Пристрій сумісний із картками та брелоками, що робить його універсальним вибором для житлових комплексів і готелів .

Підсумовуючи, варто зазначити, що також існує пристрій, який поєнує в собі ці технології та формує повноцінну СКУД, а саме пропускна система ZKTeco через ітурнікети дійсно використовує картки для входу. В основі цієї системи лежить зчитувач карток EM-Marin, який ідентифікує користувача за допомогою його персональної картки (рис 1.2).

Рисунок 1.3 – Пропускна система за картами через турнікет ZKTeco

Система розрахована на ефективний контроль доступу, забезпечуючи автоматизацію процесу входу через турнікети, і чудово підходить для офісів, підприємств або інших об'єктів із великим потоком людей. Схема роботи пристрою (рис 1.4).

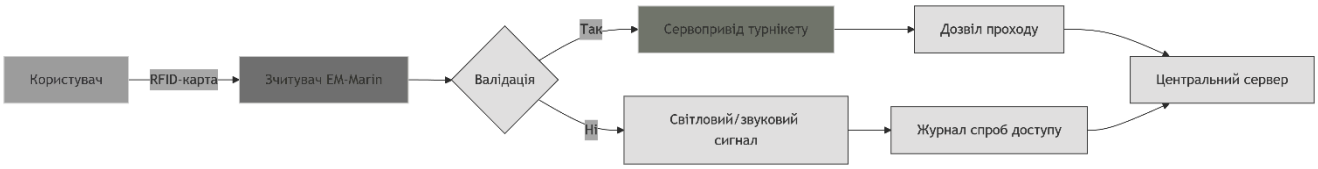


Рисунок 1.4 – Схема роботи пристрою турнікет ZKTeco

Бездротові СКУД – бездротові системи доступу активно розвиваються, пропонуючи інноваційні рішення для сучасних офісів і житлових будівель.

Для прикладу розглянемо пристрій INLock_street [12]. Бездротовий біометричний комплект контролю доступу INLock_street – це сучасне рішення для захисту приміщень, що забезпечує багатофункціональність і зручність використання. Його можна встановлювати на вулиці, оскільки пристрій витримує атмосферні впливи. До комплекту входять бездротова кодова клавіатура, електромеханічний замок і пульт дистанційного управління. Система підтримує кілька способів доступу: за допомогою відбитка пальця, ПІН-коду, RFID-карт, Bluetooth або Wi-Fi (рис 1.5).

Рисунок 1.5 – Бездротовий біометричний комплект контролю доступу INLock_street

Основною перевагою пристрою є автономність – живлення від батарей забезпечує тривалий термін роботи (до року) при частому використанні. Матеріали корпусу (метал і гартоване скло) додають надійності. Пристрій також підтримує великий обсяг користувачів (900 ключів доступу та 100 відбитків пальців), що

робить його універсальним для застосування в різних умовах. Схема роботи пристрою (1.6)

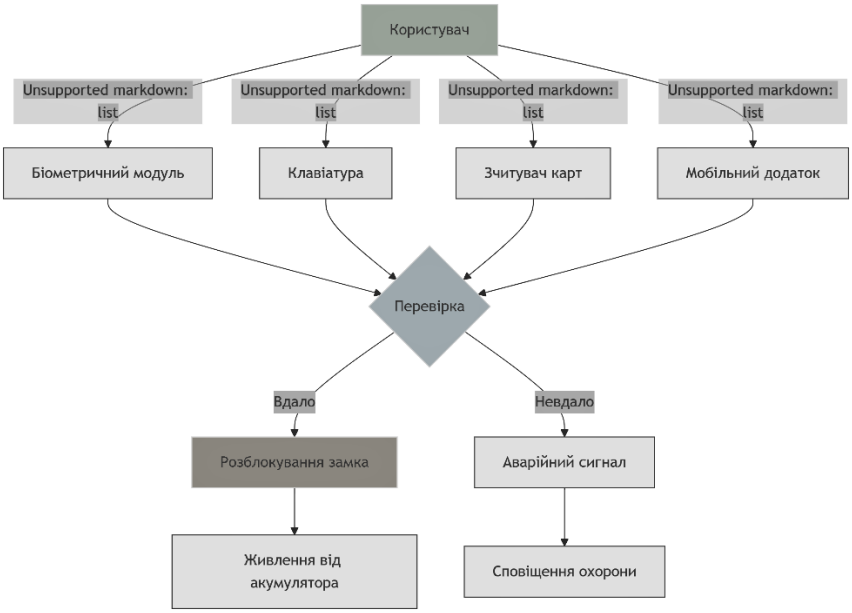


Рисунок 1.6 – Схема роботи пристрою INLock_street

Недоліком може бути залежність від батарейного живлення, що вимагає періодичної заміни батарей, особливо при інтенсивному використанні. Опційне підключення через Bluetooth і Wi-Fi потребує додаткового модуля, що може збільшувати витрати. Також використання бездротових пристроїв потенційно може бути вразливим до перешкод або зловмисного втручання. INLock_street підходить для приватних і комерційних об'єктів, забезпечуючи високий рівень безпеки та зручності управління доступом.

Маємо наступні переваги та недоліки систем контролю та управління доступом: Модель **ZKTeco L7000** – це біометричний автономний замок для внутрішнього використання. Його перевага – підтримка кількох способів доступу (відбиток, PIN, ключ), автономність і простота встановлення. Він зберігає до 500 відбитків і 30 000 подій, що підходить для офісів і квартир. Недоліком є залежність від батарей та відсутність мережевої інтеграції.

ZKTeco RFID Reader – турнікетна система з RFID і біометрією, призначена для об'єктів із великим потоком людей. Відзначається високою пропускною здатністю (до 30 осіб/хв), міцною конструкцією та довгим ресурсом роботи (до 1

млн циклів). Водночас потребує постійного живлення, складний у встановленні та не є автономним.

INLock_street – бездротовий біометричний комплект, що поєднує PIN, RFID, відбитки, Bluetooth і Wi-Fi. Він придатний для зовнішнього використання, автономний (до 1 року роботи) і підтримує до 900 користувачів. Його слабке місце – залежність від додаткових модулів та потенційна вразливість до завад у бездротовому середовищі.

Порівняння характеристик пристроїв наведено у таблиці 1.1.

Таблиця 1.1 – Порівняльна характеристика систем контролю та управління доступом

Критерій	ZKTeco L7000 (Біометричний замок)	HID + ZKTeco RFID Reader (Карткова система)	INLock_street (Бездротова біометрична система)
Тип СКУД	Біометрична	Карткова	Бездротова біометрична
Спосіб ідентифікації	Відбиток пальця, PIN-код, механічний ключ	Картка (RFID)	Відбиток пальця, PIN-код, RFID, Bluetooth, Wi-Fi
Автономність	Так (працює від батарей)	Так (залежить від живлення зчитувача)	Так (до 1 року автономної роботи від батарей)
Місце встановлення	Внутрішні двері	Приміщення (офіси, підприємства)	Приміщення і вулиця

Виходячи з порівняльної характеристики розуміємо, що для кожної системи контролю та управління доступом є потреби та сценарії в яких вони повинні працювати, а саме:

ZKTeco L7000 – це оптимальне рішення для організації контролю доступу у внутрішніх просторах з помірними вимогами до безпеки. Його зручно встановлювати у невеликих офісах, кімнатах для персоналу, архівах, комірках або технічних приміщеннях. З огляду на автономне живлення, замок не потребує підключення до мережі або складного монтажу.

ZKTeco RFID Reader – доцільно використовувати у зонах з високою інтенсивністю переміщення персоналу чи відвідувачів, де потрібен не тільки контроль доступу, але й обмеження фізичного проходу. Це типово для входів у виробничі приміщення, бізнес-центри, банки, школи. Турнікетна система дозволяє чітко фіксувати кожен прохід, інтегрується з RFID або біометричними зчитувачами, забезпечуючи надійну ідентифікацію та реєстрацію подій у реальному часі. Такі системи також можуть бути частиною загального комплексу СКУД, працюючи разом із відеонаглядом або охоронною сигналізацією.

INLock_street – призначений для універсального застосування в умовах, де важлива автономність, гнучкість та стійкість до зовнішніх впливів. Його часто використовують у приватних будинках, майстернях або офісах малого бізнесу, що розташовані у віддалених або відкритих локаціях. Завдяки бездротовому зв’язку та живленню від батарей, пристрій не потребує прокладки кабелів, що значно спрощує монтаж. При цьому підтримка кількох методів автентифікації (біометрія, PIN, RFID, Bluetooth, Wi-Fi) дозволяє адаптувати систему до потреб різних категорій користувачів – від мешканців і технічного персоналу до гостей.

При впровадженні систем контролю та управління доступом є також ключовим кількісна характеристика.

Порівняння кількісних характеристик наведено у таблиці 1.2.

Таблиця 1.2 – Кількісна характеристика систем контролю та управління доступом.

Параметр	ZKTeco L7000	ZKTeco RFID Reader (турнікет)	INLock_street (бездротовий замок)
Тип СКУД	Біометричний автономний замок	Карткова + біометрична турнікет-система	Бездротова біометрична система
Матеріал корпусу	Сплав цинку	SUS304 нержавіюча сталь	Метал + гартоване скло
Кількість користувачів	500 відбитків пальців	До 25/30 осіб/хв (швидкість проходження)	900 ключів доступу, 100 відбитків пальців
Кількість паролів	100	Не зазначено	До 900 PIN-кодів (4–6 символів)
Тип автентифікації	Відбиток пальця, PIN, механічний ключ	RFID, відбиток пальця	Відбиток, PIN, RFID, Bluetooth, Wi-Fi, радіопульт
Кількість подій в пам’яті	30 000	Не зазначено	Не зазначено
Зв’язок / зчитування	USB-флеш	Вбудований RFID, біометрія	Біометрична клавіатура, Bluetooth, Wi-Fi (опція)
Робоча температура (°C)	0 – 45	-28 – +60	-10 – +50 (типово для подібних пристроїв)
Живлення	4 × AA батарейки	AC 110/220 В, 50/60 Гц	Батарейки (ресурс – до 1 року або 16 000 відкриттів)
Аварійне відкриття	Механічний ключ, 9В батарея	Так	Радіобрелок, механізм на корпусі

Товщина дверей / смуга руху (мм)	35–55 (стандарт), 55–75 (опція)	600 мм смуга руху	Універсальна, встановлення на двері
Розміри (мм)	Стандартна ручка	480×280×1008	Стандартне накладне виконання
MCBF (середній ресурс)	~100 000 циклів	1 000 000 циклів	~16 000 циклів на батареях
Потужність споживання	Низьке (від батарей)	Очікування: 6 Вт / Робота: 18 Вт	Автономне живлення
Світлодіодний індикатор	Так	Так	Так
Вага (нетто / з упаковкою)	~1.5 кг	31 кг / 45 кг	~2.0–2.5 кг з кріпленням
Захист від зовнішнього середовища	Ні (використання всередині)	Так (якщо турнікет під навісом)	Так (придатний для вулиці)
Рівень безпеки	Середній	Середній	(мультирежимний контроль доступу)

Отже, кожен із розглянутих типів СКУД має свої переваги та недоліки. Біометричні системи забезпечують високий рівень безпеки, але залежать від стабільного живлення та можуть мати обмеження в умовах зовнішнього впливу. Карткові рішення залишаються простими та зручними у використанні, проте схильні до компрометації через втрату або передачу карток. Бездротові системи є сучасними та гнучкими, однак вимагають додаткового захисту від зловмисного втручання. Проведений аналіз підтверджує необхідність створення вдосконаленої багатофункціональної системи доступу, здатної ефективно працювати в складних умовах та забезпечувати високий рівень захисту.

1.4 Висновок до розділу 1 та постановка задачі

На основі проведеного аналізу можна зробити висновок, що системи контролю та управління доступом (СКУД) є критично важливим елементом

забезпечення безпеки сучасних об’єктів. Різноманітні моделі контролю доступу, такі як RBAC, MAC, DAC та їх варіації, мають свої переваги й обмеження, що визначають їх ефективність залежно від специфіки об'єкта. Біометричні технології та інтеграція IoT, хмарних рішень і штучного інтелекту відіграють ключову роль у розвитку СКУД, дозволяючи автоматизувати процеси ідентифікації й управління доступом [13].

Основними викликами залишаються забезпечення захисту даних користувачів, підвищення стійкості систем до електромагнітних завад та інших зовнішніх впливів, а також висока вартість впровадження складних рішень. Аналіз методів і пристроїв реалізації СКУД, таких як біометричний замок ZKTeco L7000, карткові зчитувачі ZKTeco RFID Readers та бездротовий комплект INLock_street, показав, що кожен із цих пристроїв має свої обмеження. Зокрема, проблеми включають залежність від живлення, чутливість до зовнішніх впливів і відсутність універсальності.

Враховуючи недоліки розглянутих пристроїв, основним завданням є створення багатофункціонального рішення, яке об'єднає переваги наявних технологій і забезпечить максимальний комфорт, зручність і захищеність. Майбутня розробка має врахувати сучасні виклики і запропонувати інноваційний підхід до контролю доступу.

Постановка задачі:

– інтегрувати функцію адаптивного екранування для захисту від електромагнітних завад і зловмисного зовнішнього втручання;

– використати біометричні технології для точності ідентифікації та зниження ризиків, пов’язаних із фізичними носіями (картки, ключі);

– забезпечити універсальність через інтеграцію з IoT-пристроями і алгоритмами штучного інтелекту для адаптивного управління доступом;

– реалізувати механізми енергоефективності для автономних пристроїв, що зменшить залежність від джерел живлення;

– врахувати ергономіку й зручність використання пристрою для мінімізації складності його налаштування і експлуатації.

2 ПРОЄКТУВАННЯ ТА РОЗРОБКА АЛГОРИТМІВ РОБОТИ ЗАХИЩЕНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

У сучасному світі системи контролю доступу мають вирішальне значення для забезпечення безпеки на критичних об'єктах. Вони мають важливі функції, такі як запобігання несанкціонованому доступу, моніторинг руху персоналу та інтеграція з іншими системами безпеки. Зважаючи на постійні загрози, зокрема електромагнітні перешкоди, такі системи повинні бути адаптовані до складних умов. Технології адаптивного екранування забезпечують додаткову захист, дозволяючи ефективно протистояти зовнішнім впливам та зберігати високу надійність роботи навіть у несприятливих умовах.

2.1 Обґрунтування та опис удосконалення пристрою

Удосконалення пристрою, розробленого для багатофункціональної системи контролю доступу, обґрунтоване необхідністю підвищення його захищеності, функціональності та адаптивності до сучасних викликів безпеки. Такі виклики виникають у ситуаціях, коли традиційні СКУД не справляються з новітніми типами загроз – зокрема, несанкціонованим проникненням на об’єкти критичної інфраструктури, відсутністю постійного моніторингу приміщень або порушенням роботи систем під впливом електромагнітних завад. У таких умовах потрібен пристрій, здатний не лише забезпечити точну ідентифікацію, а й реагувати на нетипову поведінку після доступу.

Варто наголосити, що цей пристрій проєктується спеціально для об'єктів критичної інфраструктури – таких як енергетичні вузли, дата-центри, телекомунікаційні хаби, військові або урядові об'єкти – де вкрай важливими є високий рівень захисту, стійкість до зовнішніх впливів та недопущення витоку даних. Завдяки використанню екрануючих тканин і спеціальної фарби, пристрій буде ефективно захищений від електромагнітних випромінювань, що унеможливлює його застосування в умовах із типовим побутовим або офісним навантаженням. Тому його використання у звичайних школах, архівах,

комунальних установах або малих офісах є недоцільним – як через надлишкову складність, так і через економічну необґрунтованість такого рівня захисту.

По-перше, вдосконалення зумовлене обмеженнями сучасних СКУД. Карта, PIN-код або навіть автономна біометрія не гарантують повної безпеки у випадках, коли після легального входу в приміщення відбувається вторинне проникнення (наприклад, співробітник залишається після закриття, або його супроводжує стороння особа). Такі ситуації критичні саме для об’єктів з обмеженим або секретним доступом, де контроль має здійснюватися не лише на етапі входу, а й упродовж перебування всередині.

По-друге, технічне вдосконалення спрямоване на підвищення ефективності й розширення функціональності пристрою. Установка соленоїдного замка забезпечить фізичну фіксацію дверей із високою механічною надійністю, що є важливим у зонах з підвищеним ризиком фізичного втручання. Мікропроцесор ESP32, який підтримує Wi-Fi і Bluetooth, забезпечує можливість віддаленого адміністрування, логування подій та обміну даними з іншими захисними системами, що критично важливо для об'єктів з великою територією або обмеженим доступом фізичного персоналу.

Ключове вдосконалення – інтеграція лазерної сітки – реалізує контроль простору за дверима після авторизованого доступу. Ця функція є актуальною саме для приміщень, де важливо знати, чи залишився хтось після завершення доступу, зокрема в серверних зонах, системних відсіках або архівах, що обслуговуються вахтовим персоналом.

Також застосування Touch ID забезпечить високоточну біометричну автентифікацію з неможливістю передачі доступу третім особам, що особливо необхідно у сферах із підвищеною вимогою до персоналізованого контролю. Це знижує ризики компрометації системи за рахунок використання чужих карток або зламу кодів.

Функція журналювання через ESP32 забезпечить контроль усіх подій доступу з можливістю створення звітів та інтеграції з хмарними або локальними системами

безпеки – те, що критично для державних або стратегічно важливих об’єктів, де аудит доступу є частиною вимог безпеки.

Захист пристрою від електромагнітних завад, реалізований через внутрішнє екранування та екрануюче покриття корпусу, дозволяє йому стабільно функціонувати в умовах промислових перешкод, електромагнітного шуму або навмисного радіочастотного впливу. Ця особливість робить пристрій придатним для промислових об’єктів, транспортної інфраструктури, електростанцій та інших зон із високим рівнем техногенного навантаження.

Таким чином, запропоновані вдосконалення не лише посилюють технічні можливості системи, а й чітко орієнтовані на конкретні завдання в сфері критичної безпеки. Пристрій забезпечує підвищену стійкість, контроль, адаптивність та захищеність, але при цьому його застосування доцільне виключно у середовищах, де такі характеристики є обов’язковими, а не у звичайних навчальних, архівних чи адміністративних установах, де достатньо стандартних СКУД.

2.2 Обґрунтування вибору елементарної бази та мови розробки

Під час проєктування системи контролю і управління доступом (СКУД) було обрано елементну базу, що забезпечує базову та додаткову функціональність при збереженні невисокої вартості, компактності та простоти інтеграції. Основні вимоги до системи включали: ідентифікацію користувача, ведення обліку подій та підвищену захищеність від зовнішніх впливів, зокрема електромагнітних.

Центральним керуючим елементом є мікроконтролер ESP32 Development Board, який працює на двоядерному процесорі Tensilica з тактовою частотою до 240 МГц [14]. Модуль підтримує бездротові інтерфейси Wi-Fi та Bluetooth, а також містить велику кількість портів вводу/виводу, що дозволяє реалізувати як зчитування даних з датчиків, так і керування виконавчими пристроями (рис. 2.1).

Рисунок 2.1 – Мікроконтролер ESP32 Development Board

Технічні харктеристики ESP32 Development Board наведені в таблиці 2.1.

Таблиця 2.1 – Технічні характеристики ESP32 Development Board

Характеристика	**Значення**
Процесор	Двоядерний Tensilica LX6, до 240 МГц
Оперативна пам’ять	520 КБ SRAM
Flash-пам’ять	4 МБ SPI Flash
Інтерфейси	Wi-Fi 802.11 b/g/n, Bluetooth v4.2 BR/EDR та BLE
GPIO	До 40 цифрових входів/виходів
Аналогові входи	До 16 каналів ADC
PWM	До 19 каналів PWM
DAC	2 канали DAC
Інші інтерфейси	UART, SPI, I2C, I2S, SDIO, CAN, IR, сенсори дотику
Робоча напруга	3.3 В
Сумісність	Arduino IDE, MicroPython, LUA та інші

Для біометричної аутентифікації в системі використовується оптичний модуль зчитування відбитків пальців FPM10A (рис 2.2).

Рисунок 2.2 – Сканер відбитків пальців FPM10A

Даний сканер дозволяє швидко та точно ідентифікувати користувача за унікальним відбитком пальця. Це забезпечує високий рівень захисту доступу без

потреби у картках чи PIN-кодах [15]. Технічні характеристики сканеру висвітлені в таблиці 2.2.

Таблиця 2.2 – Технічні характеристики сканеру відбитку пальців

Характеристика	**Значення**
Тип	Оптичний біометричний сенсор
Інтерфейс	UART TTL
Робоча напруга	3.3 В
Робочий струм	< 120 мА
Пам’ять	Вбудована флеш-пам’ять для збереження шаблонів відбитків
Підтримка	Повна підтримка прошивки та програмного забезпечення для Windows
Застосування	Системи безпеки, ідентифікації, електронне голосування тощо

Для фізичного блокування доступу використовується електромагнітний замок (Solenoid Lock 12V 0.4A), який керується мікроконтролером та забезпечує утримання дверей у закритому стані до моменту авторизації (рис. 2.3). Завдяки простій конструкції, замок можна інтегрувати у різні типи дверей, шухляд або сейфів [16].

Рисунок 2.3 – Електромагнітний соленоїдний замок 12В 0.4А

Для виявлення присутності або наближення застосовується інфрачервоний PIR-датчик руху TZT HC-SR501, який фіксує зміну теплового фону у зоні дії [17]. У разі виявлення руху пристрій може активувати систему ідентифікації або ввімкнути підсвічування елементів керування. Також датчик може використовуватись як тригер для фіксації спроб несанкціонованого доступу (рис 2.4).

Рисунок 2.4 – Інфрачервоний PIR-датчик руху TZT HC-SR501

Живлення усієї системи здійснюється від стандартного джерела постійної напруги 5–12 В (акумулятор, блок живлення або Power Bank), а дані та логи подій зберігаються на SD Adapter Micro SD Storage Expansion Board, що підключається до ESP32 через SPI-інтерфейс [18]. Це дозволяє вести історію доступів, помилок та подій для подальшого аналізу без підключення до мережі.

Для швидкого та ефективного сповіщення було додатково додано логування у боті в месенджері, що дозволяє швидко в режимі реального часу спостерігати за записувати дії.

З метою забезпечення захисту пристрою від електромагнітного випромінювання в його конструкції застосовано спеціалізовані матеріали. Екрануюча тканина використовується для локального покриття електронних компонентів, зменшуючи їхню вразливість до зовнішніх полів. Екрануюча фарба наноситься на внутрішні поверхні корпусу, створюючи провідний шар, який поглинає або відбиває електромагнітні хвилі, що дозволяє знизити рівень впливу небажаного випромінювання на функціонування пристрою.

З програмної точки зору розробка пристрою здійснюється у середовищі Arduino IDE – популярному інструменті з відкритим кодом, який широко використовується для програмування мікроконтролерів, зокрема ESP32. Ця платформа забезпечує інтуїтивно зрозумілий інтерфейс, підтримує велику кількість бібліотек для роботи з DAC, PWM, GPIO, UART, таймерами, а також містить зручні засоби компіляції, відлагодження та завантаження прошивки

безпосередньо в мікроконтролер. Для ESP32 існує офіційна підтримка через бібліотеку esp32 by Espressif [19].

Основною мовою програмування в Arduino IDE є C++, що є ідеальним вибором для роботи з вбудованими системами. Ця мова дозволяє безпосередньо взаємодіяти з апаратними ресурсами мікроконтролера, включаючи роботу з регістрами, таймерами, внутрішніми шинами, механізмами переривань. Завдяки цьому можливо досягти високої точності в керуванні DAC-портами, а також у синхронізації процесів, зокрема під час генерації псевдовипадкових сигналів або шуму.

C++ забезпечує ефективне використання обмежених апаратних ресурсів ESP32 – зокрема оперативної пам’яті, що є критично важливим у малоресурсних пристроях [20]. Мова дозволяє оптимізувати розмір прошивки, уникати надмірного використання динамічної пам’яті, застосовувати покажчики, статичні змінні, inline-функції тощо, що позитивно впливає на продуктивність та стабільність роботи системи.

Крім того, C++ підтримує об’єктно-орієнтований підхід, що дозволяє структурувати проєкт на окремі логічні компоненти: модуль керування доступом, модуль сенсорного контролю, логування подій тощо. Така архітектура спрощує модифікацію, розширення та тестування проєкту, а також полегшує додавання нових функцій, як-от сенсорні елементи, зміну частот генерації сигналу або інтеграцію з мережевими сервісами.

Широка база відкритих бібліотек, таких як ArduinoRandom, ESP-DAC, Audio та інші, значно прискорює розробку: замість створення функцій з нуля можна використати перевірені компоненти з активної спільноти. Це зменшує кількість помилок, полегшує пошук рішень у разі виникнення труднощів і підвищує надійність загальної системи.

Отже, поєднання Arduino IDE та мови програмування C++ є обґрунтованим вибором для реалізації програмної частини пристрою. Такий підхід відкриває широкі можливості для керування апаратними ресурсами ESP32, забезпечує високу

продуктивність і масштабованість, а також дозволяє легко адаптувати систему до змін та нових вимог [21].

Усі обрані елементи відповідають вимогам до енергоефективності, зручності інтеграції та інформаційної безпеки. Завдяки цьому пристрій забезпечує надійний контроль доступу, автоматичне логування подій і виявлення несанкціонованих проникнень без потреби в постійному нагляді з боку користувача.

Використання мови програмування C++ у середовищі Arduino IDE дозволяє ефективно працювати з апаратними ресурсами ESP32, забезпечуючи точне керування модулями сканування, датчиками руху та логуванням подій. Це створює гнучку, масштабовану та продуктивну систему, придатну як для домашнього використання, так і для об’єктів з підвищеними вимогами до захисту.

2.3 Принцип дії пристрою та загальна схема роботи

Робота пристрою побудована на багаторівневій логіці контролю доступу та виявлення несанкціонованого проникнення. Центральним елементом є сканер відбитків пальців, який виконує ідентифікацію користувача. Сценарій перший має наступну послідовність: після прикладання пальця здійснюється перевірка наявності відповідного відбитка у системній базі даних.

Якщо збіг підтверджено, пристрій активує соленоїдний замок і дозволяє вхід до приміщення, фіксуючи подію в журналі подій. У випадку відсутності збігу доступ не надається, і спроба також реєструється. Для виходу з приміщення передбачено кнопку керування: натискання на неї деактивує замок, дозволяючи відчинити двері. Після їх закриття система автоматично активує лазерний датчик руху, що переходить у режим моніторингу (рис 2.5).

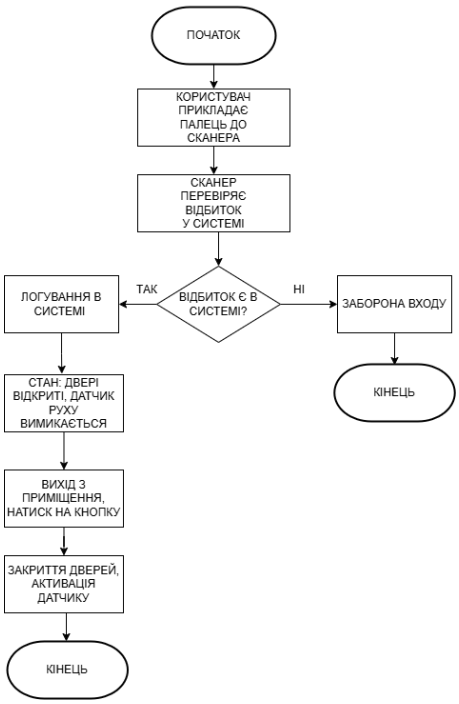


Рисунок 2.5 – Структурна схема роботи пристрою за першим сценарієм

Сценарій другий: у разі несанкціонованого проникнення в приміщення в обхід основного входу – наприклад, через вікно або інший альтернативний шлях – датчик руху фіксує присутність об’єкта. У відповідь на це система генерує сигнал тривоги та здійснює запис інциденту в лог-файл для подальшого аналізу (рис 2.6).

Рисунок 2.6 – Структурна схема роботи пристрою за другим сценарієм

Система контролю та управління доступом працює за наступним алгоритмом:

Крок 1 – Користувач підходить до пристрою контролю доступу та прикладає палець до сканера відбитків пальців.

Крок 2 – Сканер здійснює перевірку відбитка у базі даних.

Крок 3 – Якщо відбиток є у системі, користувач отримує дозвіл на вхід, замок розблоковується, подія входу фіксується у журналі, а лазерний датчик руху автоматично вимикається, щоб уникнути помилкового спрацювання під час перебування людини всередині приміщення.

Крок 4 – Для виходу користувач натискає кнопку, що ініціює процедуру виходу з приміщення.

Крок 5 – Після зачинення дверей система автоматично активує лазерний датчик руху, переводячи систему в режим охорони.

Крок 6 – Якщо хтось намагається проникнути до приміщення несанкціоновано, минаючи сканер і двері (наприклад, через вікно чи інші отвори), датчик фіксує рух.

Крок 7 – У випадку такого спрацювання система реєструє інцидент у логах та подає сигнал тривоги, інформуючи про потенційне порушення периметру безпеки.

Система контролю доступу функціонує на базі вбудованої структури даних, яка зберігається у flash-пам’яті або на microSD через SPI-інтерфейс. Вона реалізує мінімальну, але достатню структуру для забезпечення точного логування доступів, контролю користувачів і аналітики подій. В свою чергу база даних має наступну структуру (рис 2.7).

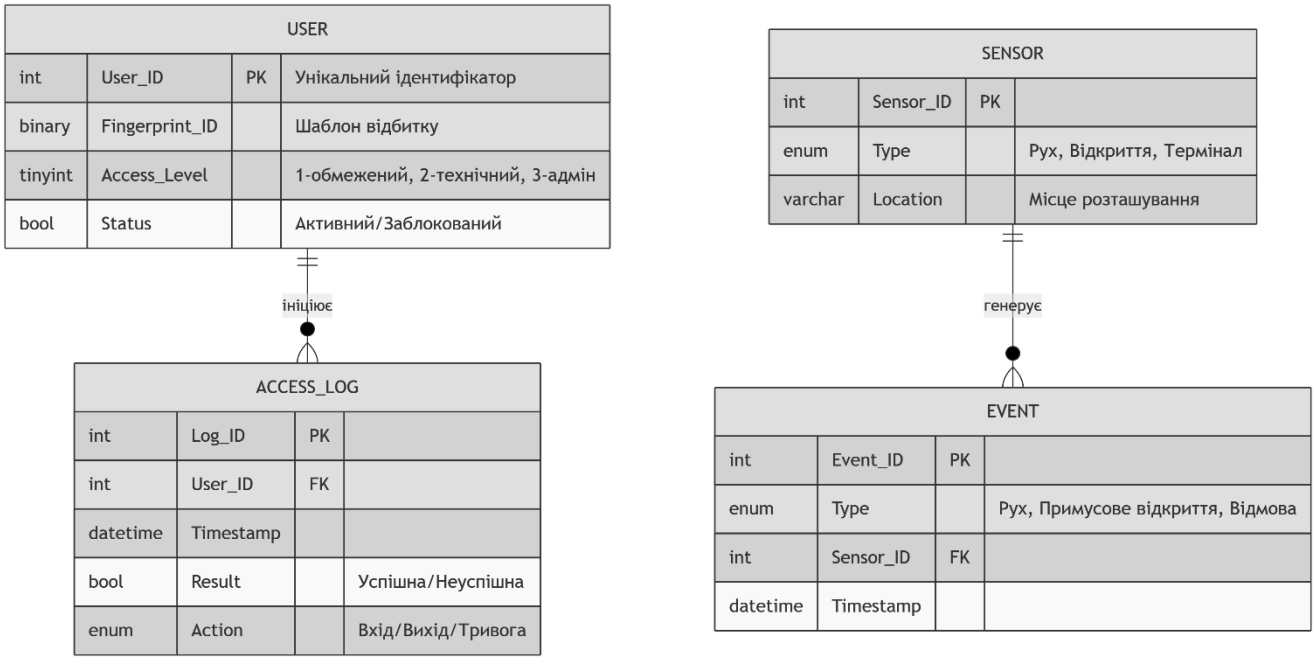


Рисунок 2.7 – ER-модель бази даних системи контролю доступу

1. Сутність User (Користувач)

Ця сутність відповідає за збереження інформації про користувачів системи, їх ідентифікацію та рівень доступу.

– User_ID (PK) – унікальний ідентифікатор користувача, що забезпечує однозначну ідентифікацію в системі;

– Fingerprint_ID – біометричний шаблон відбитку пальця, що використовується для аутентифікації користувача;

– Access_Level – рівень доступу користувача, який визначає права та обмеження в системі (1– обмежений доступ, 2 – технічний персонал, 3 – адміністратор);

– Status – статус облікового запису користувача, який визначає його активність у системі (Активний / Заблокований).

2. Сутність Access_Log (Журнал подій доступу)

Дана сутність фіксує всі події, пов’язані зі спробами користувачів отримати доступ до контрольованих об’єктів.

– Log_ID (PK) – унікальний ідентифікатор запису журналу подій.

– User_ID (FK) – зовнішній ключ, що посилається на користувача, який ініціював подію.
– Timestamp – точний час і дата події доступу.
– Result – результат спроби доступу (успішна / неуспішна).
– Action – тип дії, що виконувалася: вхід, вихід, або сигнал тривоги.

3. Сутність Event (Події безпеки)

Ця сутність відповідає за збереження інформації про інциденти безпеки, які відстежуються системою за допомогою сенсорів.

– Event_ID (PK) – унікальний ідентифікатор події безпеки.– Type – категорія події (наприклад: рух, примусове відкриття, відмова датчика).

– Sensor_ID (FK) – зовнішній ключ, що посилається на сенсор, який зафіксував подію.

– Timestamp – дата і час виникнення події.

4. Сутність Sensor (Сенсор)

Сутність, що містить інформацію про сенсори, встановлені для контролю фізичного стану об’єктів та приміщень.

– Sensor_ID (PK) – унікальний ідентифікатор сенсора;

– Type – тип сенсора (наприклад: датчик руху, датчик відкриття, датчик температури тощо);

– Location – фізичне розташування сенсора в межах контрольованого об’єкта.

Зв’язок між сутностями User і Access_Log є відношенням типу «один-до-багатьох» (1:N). Це означає, що кожен користувач може мати множину записів у журналі подій доступу. Зв’язок реалізується через зовнішній ключ Access_Log.User_ID, який посилається на унікальний ідентифікатор користувача User.User_ID.

Аналогічно, зв’язок між сутностями Sensor і Event також має тип «один-до-багатьох» (1:N). Кожен сенсор може породжувати багато подій безпеки, що відображається у множині записів у таблиці Event. Цей зв’язок реалізовано через

зовнішній ключ Event.Sensor_ID, який посилається на унікальний ідентифікатор сенсора Sensor.Sensor_ID.

Додаткові зауваження

– User – ключова сутність, що відповідає за ідентифікацію, аутентифікацію та авторизацію користувачів у системі.

– Access_Log служить для точного журналювання спроб доступу, що необхідно для аудиту і розслідування інцидентів безпеки.

– Event фіксує всі події, пов’язані із сенсорними системами безпеки, що дозволяє оперативно реагувати на потенційні загрози.

– Sensor – відображає фізичні пристрої, які моніторять стан об’єкта, забезпечуючи автоматизований збір інформації про події безпеки.

Таким чином, запропонований пристрій реалізує сучасний підхід до контролю доступу та базової охорони приміщень. Його принцип роботи ґрунтується на використанні біометричної автентифікації за відбитком пальця, що забезпечує високий рівень захисту від несанкціонованого доступу. У разі успішного розпізнавання, користувач отримує дозвіл на вхід, а система фіксує цю дію у журналі подій. Після виходу з приміщення, натискання кнопки ініціює зміну стану системи, і після зачинення дверей активується лазерний датчик руху. Якщо в подальшому виявлено рух за відсутності дозволеного входу через сканер, система спрацьовує на тривогу та реєструє інцидент.

Перевагами даного технічного рішення є автономність, низьке енергоспоживання, простота експлуатації та встановлення, а також можливість застосування в умовах обмеженого простору. Пристрій не потребує складного обслуговування та легко адаптується до будь-якого типу дверного отвору.

У подальшому розвиток пристрою може включати інтеграцію з мобільними додатками, що дозволить миттєво інформувати користувача про тривоги чи спроби доступу. Також можлива передача логів у централізовану охоронну систему для аналітики та прийняття рішень на вищому рівні.

Серед обмежень слід відзначити чутливість до обхідних шляхів проникнення (наприклад, через технічні отвори, вікна або вентиляцію), а також відсутність

резервних механізмів сповіщення при повній втраті зв’язку. Незважаючи на це, пристрій забезпечує ефективний базовий рівень безпеки і може стати частиною більш масштабної системи охорони в критично важливих або ізольованих об’єктах.

Загалом, система демонструє високу ефективність у межах своєї функціональності та має значний потенціал для подальшого розвитку з урахуванням потреб користувача та вимог до безпеки.

2.4 Висновок до розділу 2

У даному розділі було обґрунтовано необхідність удосконалення багатофункціональної системи контролю доступу для забезпечення підвищеного рівня безпеки на критичних об’єктах. Запропоновані технічні рішення, зокрема використання мікроконтролера ESP32, біометричної ідентифікації через Touch ID, соленоїдного замка та лазерної сітки для контролю простору, суттєво розширюють функціональність та підвищують надійність системи. Особлива увага приділена захисту пристрою від електромагнітних завад шляхом застосування екрануючих матеріалів та фарби, що забезпечує стабільність роботи навіть в умовах інтенсивних зовнішніх впливів.

Обґрунтування вибору елементної бази та мови програмування підтвердило доцільність використання Arduino IDE та мови C++ для забезпечення високої продуктивності, гнучкості та масштабованості системи. Розроблений алгоритм роботи пристрою передбачає багаторівневий контроль доступу та ефективний моніторинг приміщення, що дозволяє своєчасно виявляти несанкціоновані проникнення.

Отже, запропоноване удосконалення відповідає сучасним вимогам безпеки, підвищує функціональні можливості та надійність системи контролю доступу, що є важливим кроком для захисту критичних об’єктів від сучасних загроз.

3. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ БАГАТОФУНКЦІОНАЛЬНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ПІДВИЩЕНОЇ ЗАХИЩЕНОСТІ ДО КРИТИЧНИХ ОБ'ЄКТІВ ВІД ЕЛЕКТРОМАГНІТНИХ ЗАВАД І ФУНКЦІЄЮ АДАПТИВНОГО ЕКРАНУВАННЯ

У цьому розділі представлено процес розробки та реалізації програмно-апаратного комплексу системи контролю та управління доступом (СКУД), що поєднує сучасні технології безпеки та автоматизації. Розглянуто архітектуру системи, яка включає мікроконтролер ESP32, біометричний сканер відбитків пальців FPM10A, електромагнітний замок, інфрачервоний датчик руху HC-SR501 та модуль зберігання даних на microSD-карті та паралельне оперативне логування у боті в месенджері. Описано особливості підключення та взаємодії компонентів, а також представлено програмне забезпечення, що забезпечує їхню координацію.

Особливу увагу приділено процесу тестування системи: описано методику перевірки, зафіксовано результати тестів та проаналізовано ефективність роботи пристрою в реальних умовах.

3.1 Програмна реалізація для системи контролю доступу

У цьому розділі описано процес практичної реалізації запропонованої системи контролю та управління доступом на базі мікроконтролера ESP32. Розглянуто особливості взаємодії апаратних компонентів, таких як біометричний сканер, електромагнітний замок, датчики руху та засоби виводу інформації.

Наведено фрагменти програмного коду, що забезпечують обробку подій, прийняття рішень щодо надання доступу та реєстрацію подій у пам'яті пристрою. Особливу увагу приділено забезпеченню автономної роботи системи, а також можливості її використання в реальних умовах, де важливими є надійність, безперервність контролю та фіксація подій.

Ця частина програмної реалізації відповідає за підключення всіх необхідних бібліотек та підготовку графічного елементу, який буде відображатись на OLED-дисплеї.

Підключення бібліотек:

```
include <Adafruit_Fingerprint.h>   // Бібліотека для роботи зі сканером відбитків пальців
include <HardwareSerial.h>        // Для роботи з апаратним UART
include <Adafruit_GFX.h>          // Графічна бібліотека для дисплея
include <Adafruit_SSD1306.h>      // Бібліотека для OLED-дисплея SSD1306
include <SPI.h>
include <Wire.h>
```

Ці бібліотеки дозволяють використовувати OLED-дисплей і сканер відбитків пальців, а також серійне з’єднання. SPI та Wire – стандартні бібліотеки для обміну даними по SPI/I2C.

Конфігурація дисплея

```
SCREEN_WIDTH 128 // Ширина OLED-дисплея в пікселях
SCREEN_HEIGHT 64 // Висота OLED-дисплея в пікселях
OLED_RESET     -1 // Якщо дисплей не має окремого RESET-піна
Adafruit_SSD1306 display(SCREEN_WIDTH, SCREEN_HEIGHT, &Wire, OLED_RESET);
```

Тут створюється об’єкт display, який використовує I2C-з'єднання для керування дисплеєм розміром 128x64 пікселі.

Значок сканера відбитків

```
LOGO_HEIGHT   64
LOGO_WIDTH    128
static const unsigned char PROGMEM logo_bmp[] = { ... }
```

Це масив байтів, що зберігає зображення (іконку відбитка пальця) у форматі **bitmap**, яке буде відображене на дисплеї. Воно визначається вручну у форматі монохромного зображення (1 біт на піксель), закодованого у HEX.

Функція setup() – початкова ініціалізація

```
void setup() {
  Serial.begin(9600);
  while (!Serial);
```

Ініціалізується серійний порт зі швидкістю 9600 бод. Команда while (!Serial); чекає, поки з'єднання з комп'ютером буде встановлене (актуально для Arduino з USB).

```
 display.begin(SSD1306_SWITCHCAPVCC, 0x3C);
display.clearDisplay();
display.drawBitmap(0, 0, logo_bmp, LOGO_WIDTH, LOGO_HEIGHT, WHITE);
display.display();
delay(2000);
```

Ініціалізується OLED-дисплей за адресою 0x3C. Очищається попереднє зображення. Потім на дисплей виводиться логотип (відбиток пальця) з масиву logo_bmp. Затримка 2 секунди дозволяє користувачу побачити заставку.

```
 finger.begin(57600);
if (finger.verifyPassword()) {
 Serial.println("Found fingerprint sensor!");
} else {
 Serial.println("Did not find fingerprint sensor :(");
 while (1) { delay(1); }
}
```

Ініціалізується з'єднання зі сканером відбитків пальців через finger.begin(). Потім перевіряється пароль для підтвердження, що модуль сканера працює правильно. Якщо не знайдено – програма зупиняється в нескінченному циклі.

Додаткові налаштування

```
 finger.getTemplateCount();
Serial.print("Sensor contains "); Serial.print(finger.templateCount); Serial.println(" templates");
```

Виводиться кількість зареєстрованих у сканері відбитків. Це важливо для логіки авторизації – система має знати, чи є вже зареєстровані користувачі.

```
 pinMode(LOCK_PIN, OUTPUT);
digitalWrite(LOCK_PIN, LOW); // Початково замок замкнено
```

Налаштовується пін, який керує електромагнітним замком. LOW – замок зачинений.

Основний цикл loop()

```
int getFingerprintIDez() {
 uint8_t p = finger.getImage();
 if (p != FINGERPRINT_OK) return -1;
```

```
  p = finger.image2Tz();
  if (p != FINGERPRINT_OK) return -1;

  p = finger.fingerFastSearch();
  if (p != FINGERPRINT_OK) return -1;

  return finger.fingerID;
 }
```

Функція getFingerprintIDez():

- Зчитує зображення пальця;
- Перетворює його в шаблон;
- Порівнює з базою зареєстрованих відбитків.

Якщо знайдено збіг – повертає ID користувача. Інакше повертає -1.

Основний цикл loop() (продовження)

```
void loop() {
  int id = getFingerprintIDez(); // Отримуємо ID користувача
```

(або -1, якщо невідомий)

Зчитується відбиток пальця. Якщо знайдено збіг – змінна id містить номер користувача.

```
  if (id >= 0) {
    display.clearDisplay();
    display.setTextSize(1);
    display.setTextColor(WHITE);
    display.setCursor(0,0);
    display.println("Access granted!");
    display.println("Welcome, User ");
    display.print(id);
    display.display();
```

Якщо користувача розпізнано:

- Дисплей очищується.
- Виводиться повідомлення про успішну аутентифікацію.
- Вказується номер користувача (ID).

```
    digitalWrite(LOCK_PIN, HIGH); // Відкриваємо електрозамок
    delay(5000);              // Тримати замок відкритим 5 секунд
    digitalWrite(LOCK_PIN, LOW); // Знову зачинити замок
```

Електромагнітний замок відкривається на 5 секунд, після чого автоматично зачиняється.

Лазерний сенсор або PIR – сигналізація несанкціонованого доступу

```
 int motion = digitalRead(PIR_PIN); // Зчитування стану PIR-датчика
if (motion == HIGH) {
 Serial.println("ALERT: Motion or laser breach detected!");
```

Перевіряється, чи було виявлено рух або перетин лазерного променя:

- Якщо сигнал високий (HIGH), тобто датчик спрацював – це означає несанкціонований доступ.
- У серійну консоль виводиться тривожне повідомлення.

```
  display.clearDisplay();
 display.setTextSize(1);
 display.setCursor(0,0);
 display.setTextColor(WHITE);
 display.println("ALERT!");
 display.println("Unauthorized access");
 display.display();
 //  додано керування сиреною, сповіщенням
}
```

На дисплей виводиться попередження про тривогу. Це допомагає локально оповістити про загрозу. У цьому місці додати вмикається сигналізація.

Ініціалізація SD-картки (в setup())

```
#include <SD.h>
#define CS_PIN 5 //
void setup() {
 Serial.begin(9600);
 if (!SD.begin(CS_PIN)) {
  Serial.println("SD init failed!");
  return;
 }
 Serial.println("SD init success.");
}
```

Підключаємо бібліотеку SD та ініціалізуємо картку пам’яті. Якщо SD не виявлено – виводиться помилка.

Логування доступу в loop() після успішного зчитування:

```
if (id >= 0) {
 File logFile = SD.open("access.log", FILE_WRITE);
 if (logFile) {
  logFile.print("User ID: ");
  logFile.print(id);
  logFile.print(" - Time: ");
  logFile.println(millis()); // Можна замінити на RTC-час, якщо є модуль
  logFile.close();
 } else {
  Serial.println("Error opening access.log");
 }
}
```

Створюється або відкривається файл access.log на SD-карті, до якого додається запис:

- ID користувача
- Час (у мілісекундах з моменту запуску; для реального часу краще використовувати RTC-модуль)

Логування несанкціонованих спроб (перетин лазера / невідомий відбиток):

```
if (motion == HIGH || id == -1) {
 File logFile = SD.open("access.log", FILE_WRITE);
 if (logFile) {
  logFile.println("ALERT: Unauthorized access attempt");
  logFile.close();
 }
}
```

При фіксації руху або якщо відбиток не розпізнано, також ведемо запис до лог-файлу.

Логування та передання даних у бот:

```
void sendTelegram(String message)
```

Це функція, яка викликається щоразу, коли потрібно надіслати повідомлення в бота.

```
Serial.println("Sending message: " + message);
```

Цей рядок виводить у серійний монітор (Serial Monitor) текст, який буде надіслано в бот. Це корисно для налагодження – проглядається, що саме надсилається.

```
bot.sendMessage(CHAT_ID, message, "Markdown");
```

bot – об'єкт класу UniversalTelegramBot, який використовується для взаємодії з API месенджера**.**

sendMessage – метод для надсилання повідомлень.

Параметри:

CHAT_ID – ID користувача або групи, куди буде надіслано повідомлення. У твоєму випадку це**:**

```
const char* CHAT_ID = "601532377";
```

Приклад вмісту access.log після кількох подій:

```
User ID: 2 - Time: 125300
User ID: 3 - Time: 221950
ALERT: Unauthorized access attempt
User ID: 1 - Time: 405000
```

У результаті реалізації цього розділу було створено повнофункціональний програмний прототип системи контролю та управління доступом, що поєднує сучасні апаратні та програмні рішення. Система забезпечує надійну ідентифікацію користувачів за відбитками пальців, керує електромагнітним замком для фізичного блокування доступу, а також реагує на несанкціоновані дії за допомогою PIR-датчика руху та лазерного променя. Важливою особливістю реалізованої системи є можливість ведення журналу подій на SD-картці, що дозволяє зберігати інформацію про всі спроби доступу, включно з тривогами у випадку перетину охоронної зони або невдалих спроб авторизації. Вся взаємодія відображається на OLED-дисплеї, що робить систему зручною у використанні.

3.2 Апаратна реалізація системи контролю та управління доступом

Реалізація апаратної частини розробленої системи контролю та управління доступом ґрунтується на використанні мікроконтролера ESP32 Development Board, що виступає центральним елементом керування і забезпечує взаємодію всіх

компонентів системи. Було створено функціональну програмну реалізацію призначений для організації надійного доступу до приміщення з біометричною ідентифікацією, реєстрацією подій та функцією захисту від вторгнень. Розроблена схема дозволяє візуалізувати вигляд приладу, а також спрощує процес фізичної збірки компонентів. Для наочності та спрощення процесу збірки були спроектовані схеми, які зображені на рисунку 3.1 та 3.2.

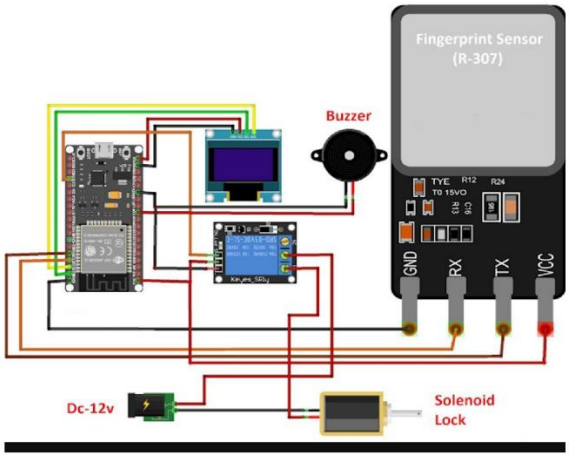


Рисунок 3.1 – Схема системи контролю та управління доступом

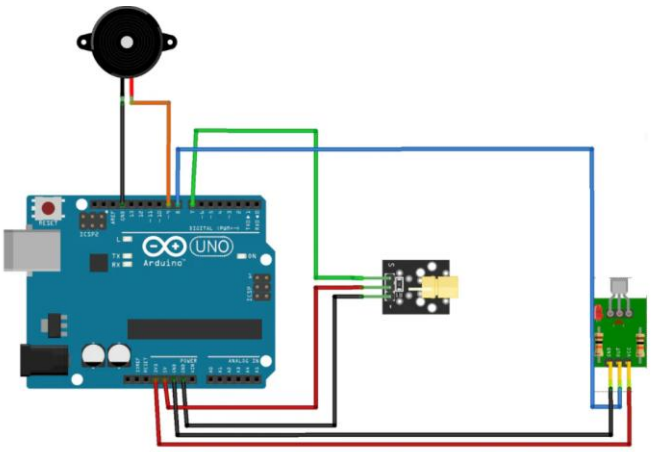


Рисунок 3.2 – Схема системи контролю та управління доступом

До складу пристрою входять наступні основні компоненти:

– ESP32 Development Board – двоядерний мікроконтролер з інтегрованими інтерфейсами Wi-Fi та Bluetooth. Він обробляє сигнали з датчиків, приймає рішення щодо дозволу доступу, керує замком та відповідає за запис логів подій на SD-карту;

– біометричний сканер відбитків пальців FPM10A – здійснює автентифікацію користувачів. У разі успішного зчитування відбитка надається дозвіл на відкриття електромагнітного замка. Усі спроби (успішні та невдалі) записуються на SD-картку з часовою міткою;

– електромагнітний замок Solenoid Lock 12V – фізичний виконавчий елемент, що утримує або розблоковує двері. Замок підключений через транзисторний ключ, який керується ESP32;

– PIR-датчик руху HC-SR501 – визначає наявність руху перед зоною входу, активуючи сканер і готуючи систему до авторизації. Це підвищує енергоефективність та безпеку;

– лазерний бар'єр і фотодатчик – формують невидимий промінь, що перетинається при вході або спробі проникнення. У разі спрацювання бар'єра, коли система озброєна, генерується запис у лог про тривожну подію;

– кнопка відкриття зсередини (Push Button) – встановлена біля виходу (з внутрішньої сторони дверей), дозволяє безперешкодно розблокувати замок зсередини без біометричної авторизації. Це необхідно для дотримання норм безпеки та евакуації;

– SD Adapter Micro SD Storage Module – зберігає журнали доступу, включаючи дату, час, результат ідентифікації, спрацювання лазера, а також використання кнопки відкриття. Це дозволяє забезпечити повний аудит подій системи;

– екрануючі матеріали – в конструкції пристрою застосовані тканини та покриття для захисту від електромагнітних завад, що забезпечує стабільну роботу електроніки навіть у складних умовах.

Підключення основних елементів зображено в таблиці 3.1.

Таблиця 3.1 – Підключення елементів схеми

Компонент	Пін/Контакт	Підключення до ESP32 / живлення
Сканер відбитків FPM10A	TX	RX ESP32
	RX	TX ESP32
	VCC	3.3V
	GND	GND

PIR-датчик HC-SR501	VCC	5V
	GND	GND
	OUT	GPIO25
Електромагнітний замок	"+"	12V зовнішнє джерело
	"–"	Транзистор, керований від GPIO
Лазер	VCC	5V
	GND	GND
Фотодатчик	OUT	GPIO32
	GND	GND
Кнопка відкриття	Один контакт	GND
	Інший контакт	GPIO33 (режим INPUT_PULLUP)
SD Adapter	CS	GPIO5
	MOSI	GPIO23
	MISO	GPIO19
	SCK	GPIO18
	VCC	3.3V
	GND	GND

При створені пристрою важливо було враховувати живлення для роботи схеми, для цього виокремлено:

Мікроконтролер та лазер живляться від 5В через стабілізатор або PowerBank. Замок потребує окремого 12В джерела живлення. Для стабільної роботи SD-карти та лазерного бар’єра застосоване фільтраційне розгалуження живлення із конденсаторами.

У результаті реалізації апаратної частини отримано автономну багатофункціональну систему доступу з біометричною автентифікацією, можливістю виходу зсередини, , а також надійним збереженням усіх подій у базі на SD-картці та логуванням у режимі реального часу у боті в месенджері. Такий пристрій підходить для використання в офісах, лабораторіях та інших критичних об'єктах, де потрібен підвищений рівень захисту.

3.3 Прототип системи управління та контролю доступом

Завершено етап проєктування пристрою та написання програмного коду. Наступним кроком є реалізація прототипу системи контролю та управління доступом, що дозволить перейти до практичного впровадження та тестування розробленого пристрою.

При активації пристрою надсилається повідомлення у бот, що почалась робота пристрою (рис 3.3).

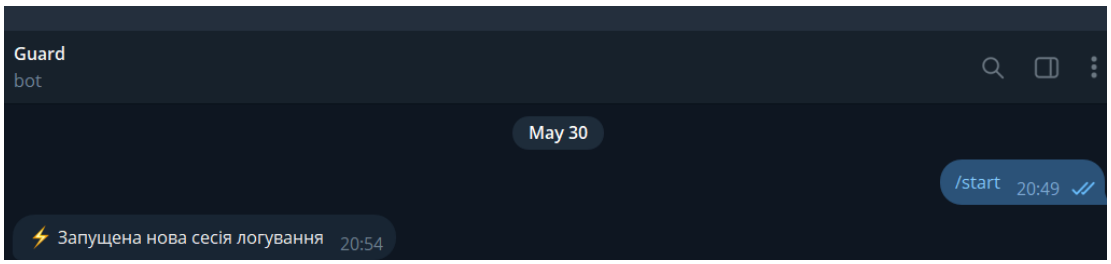


Рисунок 3.3 – Початок логування подій

Перша частина пристрою включає інфрачервоний датчик руху (PIR) для виявлення присутності в зоні контролю, а також кнопку, яка використовується для виходу з приміщення шляхом ручного відкриття замка . Ці елементи забезпечують додатковий рівень функціональності та зручності у користуванні системою. Коли у зоні видимості датчику відбувається рух, з’являється відповідне повідомленя у боті (рис 3.4).

Рисунок 3.4 – Внутрішня частина пристрою та логування у боті

Основна частина пристрою, яка містить сканер відбитків пальців, що відповідає за ідентифікацію користувача, та OLED-дисплей. На екрані відображається поточний стан системи: відкритий або закритий замок, а також повідомлення про відмову у доступі у випадку, якщо відбиток не розпізнано. Цей

блок забезпечує візуальний зворотний зв’язок і є ключовим елементом для реалізації біометричного контролю доступу. Логування події передається у бот в месенджер з відповідним повідомленням, що замок зачинено. Випадок коли замок зачинено зображено на рисунку 3.5.

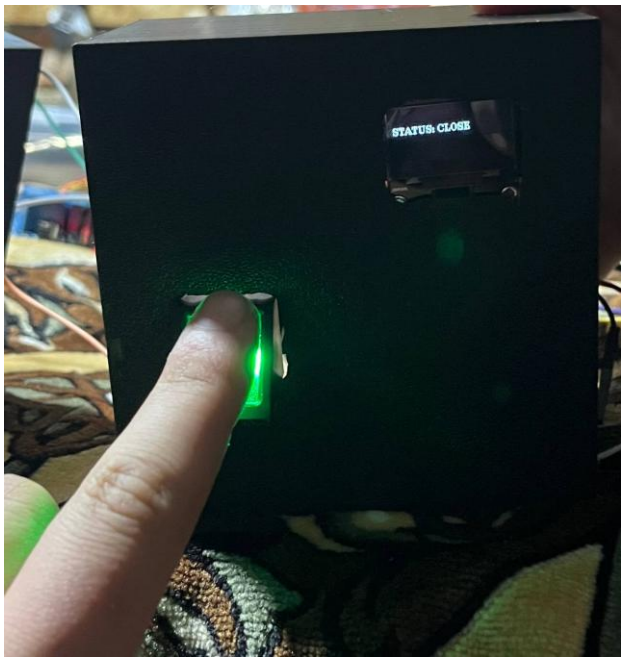


Рисунок 3.5 – Вигляд зачиненого замка

У випадку коли відбиток пальцю розпізнано, з’являється повідомлення на дисплеї, що замок відчинено. Логування події передається у бот в месенджер з відповідним повідомленням, що замок відчинено, результат зображений на рисунку 3.6.

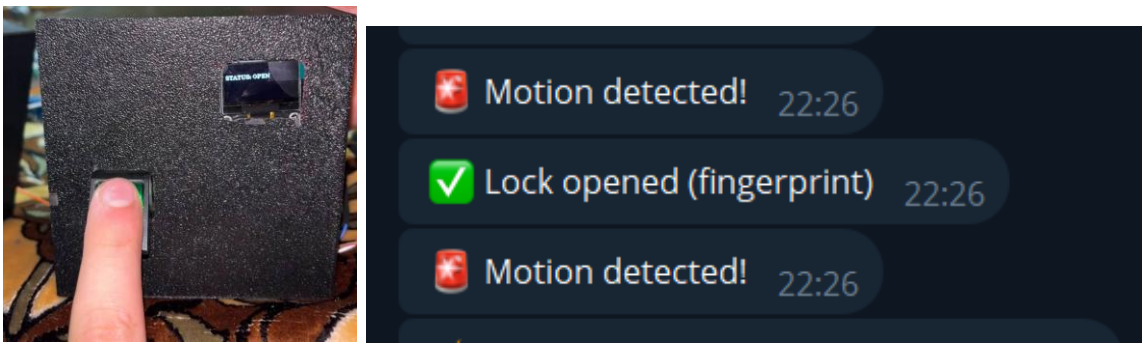


Рисунок 3.6 – Вигляд відчиненого замка та логування відкриття

У випадку коли відбиток не знайдено, на екран виводиться відповідне повідомлення та відбувається логування даної події (рис 3.7)

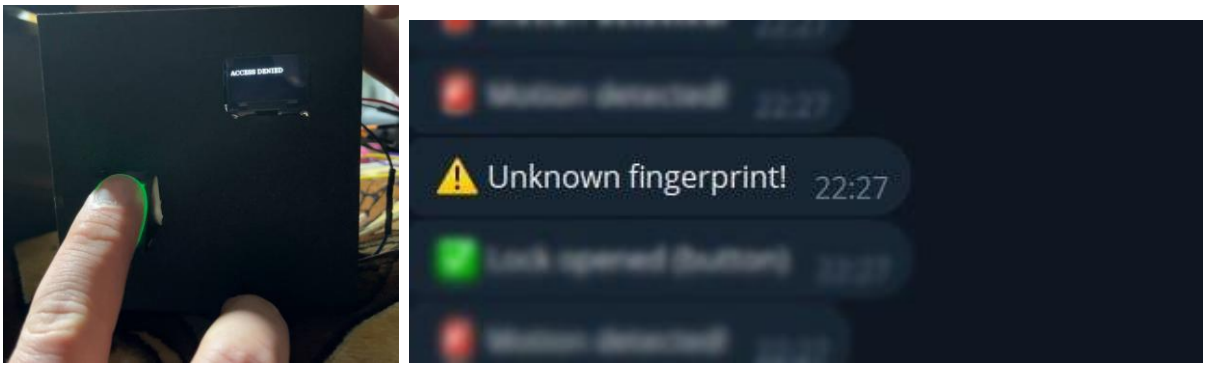


Рисунок 3.7 – Вигляд нерозпізнаного відбитку та логування

Відкривання замку за допомогою кнопки дозволяє відкрити замок з середини, відповідно дана подія записується у боті (рис 3.8).

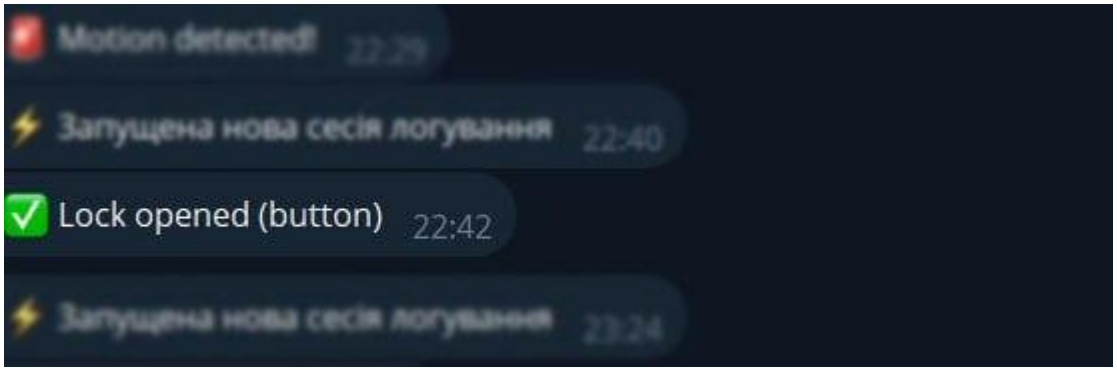


Рисунок 3.8 – Логування відкриття замка

Успішний вхід через відбиток пальця або через кнопку відчиняють соленоїдний замок, відкритий та закритий замок зображено на рисунку 3.9.

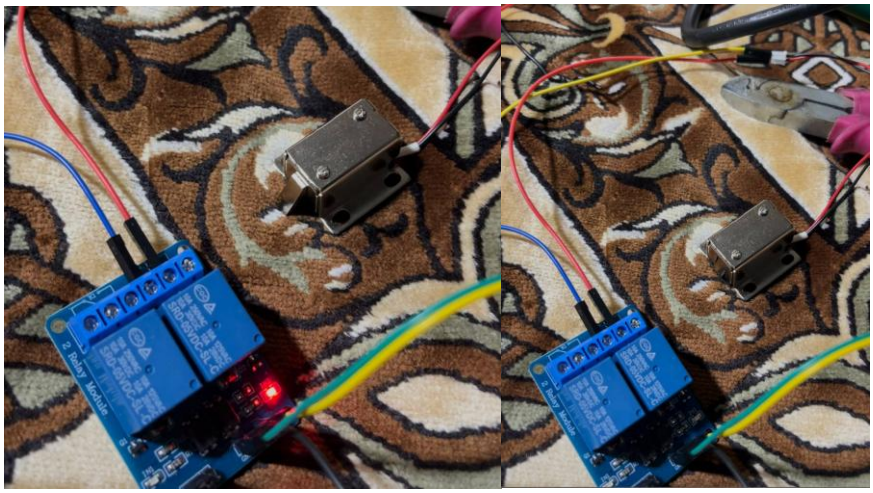


Рисунок 3.9 – Вигляд відчиненого та зачиненого замка

У результаті тестування було підтверджено повну працездатність розробленого пристрою: система стабільно підключається до Wi-Fi-мережі, коректно реагує на вхідні події, включаючи розпізнавання відбитків пальців, фіксацію руху та

натискання кнопки виходу. Усі дії супроводжуються миттєвим інформуванням користувача через бота. Робота датчиків, виконавчих і індикаційних елементів є узгодженою та повністю відповідає закладеному алгоритму роботи системи контролю та управління доступом.

3.4 Висновок до розділу 3

У цьому розділі було здійснено повноцінну реалізацію програмно-апаратного комплексу системи контролю та управління доступом (СКУД) із підвищеним рівнем захисту на базі мікроконтролера ESP32. Основна мета полягала в розробці пристрою, здатного забезпечити надійне фізичне обмеження доступу до об’єктів критичної інфраструктури, із врахуванням сучасних загроз інформаційній безпеці.

Було використано кілька ключових апаратних компонентів, кожен з яких виконує свою роль у загальній архітектурі захисту. Біометричний модуль FPM10A відповідає за автентифікацію користувачів за відбитками пальців, що дозволяє значно знизити ризик несанкціонованого доступу у порівнянні з традиційними методами (наприклад, картками або PIN-кодами). PIR-датчик руху забезпечує пасивний моніторинг зони контролю, виявляючи присутність навіть без спроби автентифікації, що підвищує рівень фізичної безпеки.

OLED-дисплей використовується як інтерфейс взаємодії з користувачем, дозволяючи оперативно інформувати про статус пристрою, результати перевірки доступу або сповіщення про події. Система також оснащена електрозамком, який забезпечує фізичне блокування або розблокування доступу в залежності від результату перевірки користувача.

Особливу увагу приділено логуванню подій. Використання SD-картки дозволяє зберігати детальні журнали всіх дій: спроб входу, результатів автентифікації, подій руху, часу тощо. Це дає змогу здійснювати ретроспективний аналіз подій безпеки, виявляти аномалії у поведінці користувачів та своєчасно реагувати на потенційні інциденти.

Програмна частина була реалізована на мові C++ із використанням бібліотек Arduino IDE, що забезпечує гнучкість у модифікації та масштабуванні системи. Архітектура коду дозволяє легко додавати нові функції, зокрема підключення до Wi-Fi, хмарні сервіси для резервного копіювання логів, або інтеграцію з мобільними застосунками.

У результаті тестування система показала стабільну роботу, високу точність розпізнавання відбитків пальців, швидке реагування на події, а також зручність у взаємодії. Усі функціональні блоки були успішно синхронізовані, що дозволило досягти поставленої мети – створення ефективного засобу контролю фізичного доступу, який відповідає сучасним вимогам інформаційної безпеки та може бути адаптований до умов конкретного об'єкта.

Таким чином, реалізований пристрій підтвердив можливість побудови надійної та гнучкої системи контролю доступу на основі недорогих і доступних компонентів, що робить його перспективним для застосування в освітніх установах, лабораторіях, офісах або інших об'єктах з підвищеними вимогами до безпеки.

ВИСНОВОК

У ході виконання бакалаврської кваліфікаційної роботи було здійснено повний цикл розробки багатофункціональної системи контролю та управління доступом (СКУД) підвищеного рівня захисту для критичних об’єктів, з урахуванням сучасних загроз та вимог до інформаційної та фізичної безпеки. На основі проведеного аналізу існуючих підходів, методів та пристроїв СКУД, було визначено ключові недоліки типових рішень: недостатній захист від електромагнітних завад, низька гнучкість, обмежена автономність, залежність від фізичних носіїв і відсутність можливості адаптації до змін середовища.

У результаті була розроблена і реалізована система на базі мікроконтролера ESP32, що включає біометричну ідентифікацію за відбитком пальця (модуль

FPM10A), сенсори руху (PIR), OLED-дисплей для зворотного зв’язку з користувачем, SD-картку для логування подій, електрозамок для фізичного обмеження доступу та елементи адаптивного екранування для захисту від електромагнітного впливу. Програмна частина була реалізована мовою C++ з використанням Arduino IDE, що забезпечило простоту модифікації, розширюваність та можливість інтеграції з IoT-інфраструктурою.

Під час тестування пристрій показав стабільну та надійну роботу, високу точність автентифікації, стійкість до зовнішніх впливів і зручність користування. Всі функціональні блоки успішно синхронізовані, що дозволяє говорити про досягнення поставлених цілей – створення захищеної, гнучкої та масштабованої СКУД для застосування в умовах підвищених вимог до безпеки.

Таким чином, результати дипломної роботи підтверджують практичну доцільність реалізації сучасної СКУД на основі доступних апаратних рішень, із можливістю подальшої модернізації, зокрема через підключення до хмарних сервісів, використання мобільних застосунків та впровадження штучного інтелекту [22].

Запропонована система є перспективною для впровадження в державних установах, лабораторіях, офісах та інших об’єктах критичної інфраструктури.

ПЕРЕЛІК ПОСИЛАНЬ

1. Shilpi Harnal1, R.K. Chauhan; "Flexible Role-Based Access Control: A Survey and Research Challenges 18 November 2019 (дата звернення: 25.05.2025).

2. Nastaran Farhadighalati, Luis A. Estrada-Jimenez, Sanaz Nikghadam-Hojjati, Jose Barata; "A Systematic Review of Access Control Models: Background, Existing Research, and Challenges"; IEEE Access, Volume: 13, Page(s): 17777 - 17806; 23 January 2025 (дата звернення: 20.05.2025).

3. Рейценштейн К.С. Методи обходу дискреційної політики управління доступом Windows шкідливим ПЗ. Дипломна робота. Київ 2021 (дата звернення: 16.05.2025).

4. Vanesa Watson, Jochen Sassmannshausen, Karl Waedt; "Secure Granular Interoperability with OPC UA"; Draude, Lange, Sick (Hrsg.): INFORMATIK 2019 Workshops, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2019; 309 (дата звернення: 16.05.2025).

5. Захаров, В. П., Рудешко, В. І. (2015). Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. – 2-ге вид., доп. Львів: ЛьвДУВС. 492 с. (дата звернення: 16.05.2025).

6. Алгоритми штучного інтелекту: Все, що потрібно знати. URL: https://undetectable.ai/blog/uk/ (дата звернення: 17.05.2025).

7. Контроль доступу – все що вам потрбно знати про біометрію. URL: https://worldvision.com.ua/articles/kontrol-dostupa-vse-chto-vam-nuzhno-znat-o-biometricheskoy-zashchite?srsltid=AfmBOopn81OFY7gJgsrfJ81w-5Zk8tY7O0y-INB4UgkDZp5gUU2ryDNi (дата звернення: 16.05.2025).

8. Мобільні технології у СКУД. URL: https://salto.com.ua/news/mobile_technologie_in_access_control/ (дата звернення: 17.05.2025).

9. Управління доступом (система контролю доступу - СКУД). URL: https://softtim.com.ua/rishennya/informatsijna-bezpeka/upravlinnya-dostupom (дата звернення: 17.05.2025).

10. Замок L7000. URL: https://zktecoua.com/ua/products/zamok-l7000/ (дата звернення: 18.05.2025).

11.RFID Reader . URL: https://www.zkteco.com/en/RFIDReader (дата звернення: 18.05.2025).

12. INLock_street. URL: https://www.zamokcity.com.ua/product/ (дата звернення: 18.05.2025).

13. Comprasions of RBAC, DAC, MAC.URL https://www.researchgate.net/figure/Comparisons-of-RBAC-DAC-and-MAC_fig2_325117644 (дата звернення: 18.05.2025).

14. ESP32. URL: https://www.espressif.com/en/products/socs/esp32/resources (дата звернення: 18.05.2025).

15. Fingerprint Reader Sensor Module Optical Fingerprint for Arduino Loc F9V6. URL: https://www.amazon.in/Fpm10A-Fingerprint-Reader-Optical-Arduino/dp/B0D2HXDS43 (дата звернення: 18.05.2025).

16. Електромеханічний соленоїдний замок електрозамок засувка. URL: https://evse.com.ua/elektromekhanicheskij-solenoidnyj-zamok-elektrozamok-zaschelka-mini (дата звернення: 17.05.2025).

17. Інфрачервоний датчик руху HC-SR501 для Arduino . URL: https://evse.com.ua/infrakrasnyj-datchik-dvizheniya-hc-sr501-dlya-arduino?utm_source=google&utm_campaign=16015167765&utm_medium=cpc&gclid=Cj0KCQjw_8rBBhCFARIsAJrc9yDNR9IUGIOCDXzwEr91KDBSEBDY823u1aS7BOK_F2xDtzHJ8LtshboaAixQEALw_wcB (дата звернення: 17.05.2025).

18. SPI інтерфейс. URL: https://itmaster.biz.ua/directory/standarts/spi.html (дата звернення: 17.05.2025).

19. ESP-IDF Programming Guide. URL: https://docs.espressif.com/projects/esp-idf/en/stable/esp32/get-started/index.html (дата звернення: 17.05.2025).

20. News, Status & Discussion about Standard C++ . URL: https://isocpp.org/ (дата звернення: 17.05.2025).

21. Arduino IDE 2.3.6 . URL: https://www.arduino.cc/en/software/ (дата звернення: 17.05.2025).

22. Римаренко М.В. Використання штучного інтелекту та технології блокчейн для підвищення безпеки системи управління доступом. КОНФЕРЕНЦІЇ ВНТУ електронні наукові видання. URL: https://conferences.vntu.edu.ua/index.php/mn/mn2025/paper/viewFile/24590/20351(дата звернення: 17.05.2025).

ДОДАТКИ

Додаток А. Технічне завдання

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

ЗАТВЕРДЖУЮ
Голова секції "Управління інформаційною безпекою" кафедри МБІС
д.т.н., професор
_____ Юрій ЯРЕМЧУК
" 20 " березня 2025 р.

ТЕХНІЧНЕ ЗАВДАННЯ

до бакалаврської кваліфікаційної роботи на тему:
Розробка багатофункціональної системи контролю доступу підвищеної захищеності до критичних об'єктів від електромагнітних завад і функцією адаптивного екранування
08-72.БДР.012.00.058 ТЗ

Керівник бакалаврської кваліфікаційної роботи
к.т.н., доц., зав. каф. МБІС
Карпінець В. В.
"20" березня 2025 р

Вінниця – 2025 р.

1. Найменування та область застосування

Розробка багатофункціональної системи контролю доступу підвищеної захищеності до критичних об’єктів від електромагнітних завад і функцією адаптивного екранування.

2.Підстава для розробки

Розробка виконується на основі наказу ректора ВНТУ № 97 від 20.03.2025 р.

3. Мета та призначення розробки

3.1 Мета розробки: розробка багатофункціональної системи контролю доступу підвищеної захищеності до критичних об’єктів від електромагнітних завад і функцією адаптивного екранування

3.2 Призначення: система забезпечує захист від несанкціонованого доступу з оповіщенням про інцидент, логуванням подій та біометричним доступом.

4. Джерела розробки

4.1 Shilpi Harnal1, R.K. Chauhan; "Flexible Role-Based Access Control: A Survey and Research Challenges 18 November 2019 (дата звернення: 25.05.2025).

4.2 Nastaran Farhadighalati, Luis A. Estrada-Jimenez, Sanaz Nikghadam-Hojjati, Jose Barata; "A Systematic Review of Access Control Models: Background, Existing Research, and Challenges"; IEEE Access, Volume: 13, Page(s): 17777 - 17806; 23 January 2025 (дата звернення: 20.05.2025).

4.3 Рейценштейн К.С. Методи обходу дискреційної політики управління доступом Windows шкідливим ПЗ. Дипломна робота. Київ 2021 (дата звернення: 16.05.2025).

4.4 Vanesa Watson, Jochen Sassmannshausen, Karl Waedt; "Secure Granular Interoperability with OPC UA"; Draude, Lange, Sick (Hrsg.): INFORMATIK 2019 Workshops, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2019; 309 (дата звернення: 16.05.2025).

4.5 Захаров, В. П., Рудешко, В. І. (2015). Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. – 2-ге вид., доп. Львів: ЛьвДУВС. 492 с. (дата звернення: 16.05.2025).

5. Вимоги до програми

5.1 Вимоги до функціональних характеристик:

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

5.1.2 Реалізація програмно-апратної системи не повина містити дорогих компонетів;

5.1.3 Програмний засіб повинен виконувати процес реєстрації та перевірки користувачів у системі.

5.2 Вимоги до надійності:

5.2.1 Програмно-апаратний засіб повинен працювати без помилок, у випадку виникнення критичних ситуацій необхідно передбачити контрольований пропуск у приміщення;

5.2.3 Програмно-апаратний засіб повинен виконувати свої функції.

6. Вимоги до програмної документації

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

7. Вимоги до технічного захисту інформації

7.1 Необхідно забезпечити захист розроблюваного програмно-апаратного засобу від несанкціонованих змін;

7.2 Неможливість отримання доступу до керування системою контролю та управління доступом.

8. Техніко-економічні показники

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

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

9. Стадії та етапи розробки

№ з/п	Назва етапів бакалаврської кваліфікаційної роботи	Початок	Закінчення
1.	Визначення напрямку бакалаврської роботи, формулювання теми	11.03.2025	17.03.2025
2.	Аналіз предметної області обраної теми	21.03.2025	16.04.2025
3.	Розробка алгоритму роботи	13.05.2025	21.05.2025
4.	Написання бакалаврської роботи на основі розробленої теми	21.05.2025	23.05.2025
5.	Передзахист бакалаврської кваліфікаційної роботи	23.05.2025	24.05.2025
6.	Виправлення, уточнення, корегування бакалаврської кваліфікаційної роботи	26.05.2025	28.05.2025
7.	Захист бакалаврської кваліфікаційної роботи	10.06.2025	11.06.2025

10. Порядок контролю та прийому

10.1 До приймання бакалаврської кваліфікаційної роботи надається:

– ПЗ до бакалаврської кваліфікаційної роботи;

- демонстрація результату бакалаврської кваліфікаційної роботи;
- презентація;
- відзив керівника роботи;
- відзив рецензента

Технічне завдання до виконання прийняв _____ Римаренко М.В.

Додаток Б. Лістинг програмного коду

```
#include <Adafruit_Fingerprint.h>
#include <HardwareSerial.h>
#include <U8g2lib.h>
#include <Wire.h>
#include <WiFi.h>
#include <WiFiClientSecure.h>
#include <UniversalTelegramBot.h>

#define RELAY_PIN    15  // Реле для замка
#define BUTTON_PIN    4  // Кнопка відкриття
#define PIR_PIN      18  // Датчик руху

const char* ssid = "ASUS";
const char* password =
const char* BOT_TOKEN = "7657726344:AAHoVK0ZfkzDa9ooS_ZzyliyAdah-eDsnOY";
const char* CHAT_ID = "601532377";

// OLED: SDA = GPIO21, SCL = GPIO22
U8G2_SSD1306_128X64_NONAME_F_HW_I2C oled(U8G2_R0, U8X8_PIN_NONE);

// UART2 для R307 (TX = 17, RX = 16)
HardwareSerial mySerial(2);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

WiFiClientSecure secured_client;
UniversalTelegramBot bot(BOT_TOKEN, secured_client);

// Для контролю частоти повідомлень про рух
unsigned long lastMotionTime = 0;
const unsigned long motionCooldown = 10000; // 10 секунд

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

```
// Підключення до Wi-Fi
WiFi.begin(ssid, password);
oled.begin();
oled.clearBuffer();
oled.setFont(u8g2_font_ncenB08_tr);
oled.drawStr(0, 24, "Connecting to WiFi...");
oled.sendBuffer();

while (WiFi.status() != WL_CONNECTED) {
  delay(500);
  Serial.print(".");
}
Serial.println("\nWiFi connected!");
oled.clearBuffer();
oled.drawStr(0, 24, "WiFi connected");
oled.sendBuffer();

secured_client.setInsecure();  // Вимикаємо SSL перевірку

// Ініціалізація UART для сканера відбитків
mySerial.begin(57600, SERIAL_8N1, 16, 17);
finger.begin(57600);
if (finger.verifyPassword()) {
  Serial.println("Fingerprint sensor found!");
} else {
  Serial.println("Fingerprint sensor error :(");
  oled.clearBuffer();
  oled.drawStr(0, 24, "Sensor error");
  oled.sendBuffer();
  while (true) delay(1);  // Зупинка програми, якщо сенсор не знайдено
}

pinMode(RELAY_PIN, OUTPUT);
digitalWrite(RELAY_PIN, LOW);
pinMode(BUTTON_PIN, INPUT_PULLUP);
```

```
 pinMode(BUZZER_PIN, OUTPUT);
 digitalWrite(BUZZER_PIN, LOW);
 pinMode(PIR_PIN, INPUT);

 showStatus(false); // Відобразити закритий стан
 delay(2000);
 sendTelegram("⚡ Запущена нова сесія логування");
}

void loop() {
 getFingerprintID();

 // Обробка кнопки
 if (digitalRead(BUTTON_PIN) == LOW) {
  Serial.println("Button pressed — opening lock");
  openLock();
  sendTelegram("✅ Lock opened (button)");
  delay(500); // антидребезг
 }

 // Перевірка PIR-сенсора
 detectMotion();

 delay(50);
}

void getFingerprintID() {
 uint8_t p = finger.getImage();
 if (p != FINGERPRINT_OK) return;

 p = finger.image2Tz();
 if (p != FINGERPRINT_OK) return;

 p = finger.fingerSearch();
```

```
  if (p == FINGERPRINT_OK) {
    Serial.println("Fingerprint recognized!");
    sendTelegram("✅ Lock opened (fingerprint)");
    openLock();
  } else {
    Serial.println("Unknown fingerprint!");
    sendTelegram("⚠️ Unknown fingerprint!");
    showError();
  }
}

void openLock() {
  digitalWrite(RELAY_PIN, HIGH);
  showStatus(true);
  delay(3000);
  digitalWrite(RELAY_PIN, LOW);
  showStatus(false);
}

void showStatus(bool unlocked) {
  oled.clearBuffer();
  oled.setFont(u8g2_font_ncenB08_tr);
  if (unlocked) {
    oled.drawStr(0, 24, "STATUS: OPEN");
  } else {
    oled.drawStr(0, 24, "STATUS: CLOSE");
  }
  oled.sendBuffer();
}

void showError() {
  oled.clearBuffer();
  oled.setFont(u8g2_font_ncenB08_tr);
  oled.drawStr(0, 24, "ACCESS DENIED");
  oled.sendBuffer();
```

```
  for (int i = 0; i < 3; i++) {
    digitalWrite(BUZZER_PIN, HIGH);
    delay(100);
    digitalWrite(BUZZER_PIN, LOW);
    delay(100);
  }

  showStatus(false);
 }

 void detectMotion() {
  if (digitalRead(PIR_PIN) == HIGH) {
    unsigned long now = millis();
    if (now - lastMotionTime > motionCooldown) {
      lastMotionTime = now;
      Serial.println("Motion detected!");
      sendTelegram("🚨 Motion detected!");
      // Можна додати додаткові реакції тут
    }
  }
 }

 void sendTelegram(String message) {
  Serial.println("Sending message: " + message);
  bot.sendMessage(CHAT_ID, message, "Markdown");

    }

#include <Wire.h>

#define SCREEN_WIDTH 128 // OLED display width, in pixels
#define SCREEN_HEIGHT 64 // OLED display height, in pixels

// Declaration for an SSD1306 display connected to I2C (SDA, SCL pins)
#define OLED_RESET     -1 // Reset pin # (or -1 if sharing Arduino reset pin)
```

```
Adafruit_SSD1306 display(SCREEN_WIDTH, SCREEN_HEIGHT, &Wire, OLED_RESET);

// Icon of Fingerprint
#define LOGO_HEIGHT   64
#define LOGO_WIDTH    128
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&Serial2);

int relayPin = 15;
int buzzerPin = 23;

void setup()
{
 pinMode(relayPin, OUTPUT);
 pinMode(buzzerPin, OUTPUT);

 digitalWrite(relayPin, LOW);
 digitalWrite(buzzerPin, LOW);

 Serial.begin(57600);
 Serial2.begin(115200);

if(!display.begin(SSD1306_SWITCHCAPVCC, 0x3C))
{
   Serial.println(F("SSD1306 allocation failed"));
   for(;;); // Don't proceed, loop forever
 }

 while (!Serial);
 delay(100);

 display.clearDisplay();
 display.drawBitmap(0, 0, logo_bmp, LOGO_WIDTH, LOGO_HEIGHT, 1);
 display.display();

 Serial.println("Fingerprint Door Lock");
```

```
delay(3000);
display.clearDisplay();

// set the data rate for the sensor serial port
finger.begin(57600);

if (finger.verifyPassword())
{
  Serial.println("Fingerprint Sensor Connected");
  display.clearDisplay();
  display.setTextSize(2);            // Normal 1:1 pixel scale
  display.setTextColor(SSD1306_WHITE);       // Draw white text
  display.setCursor(25, 0);           // Start at top-left corner
  display.println(("Sensor"));
  display.setCursor(5, 35);
  display.println("Connected");
  display.display();
  delay(3000);
 // display.clearDisplay();
}

else
{
  display.clearDisplay();
  display.setTextSize(2);            // Normal 1:1 pixel scale
  display.setTextColor(SSD1306_WHITE);       // Draw white text
  display.setCursor(25, 0);           // Start at top-left corner
  display.println(("Sensor"));
  display.setCursor(5, 35);
  display.println("Not Found");
  display.display();

  Serial.println("Unable to find Sensor");
  delay(3000);
  Serial.println("Check Connections");
```

```
  while (1) {
    delay(1);
  }
 }
display.clearDisplay();
}

void loop()                    // run over and over again
{
 getFingerprintIDez();
 delay(50);            //don't need to run this at full speed.
}

// returns -1 if failed, otherwise returns ID #
int getFingerprintIDez()
{
 uint8_t p = finger.getImage();
 if (p != FINGERPRINT_OK)
 {

  display.clearDisplay();
  display.drawBitmap(0, 0, logo_bmp, LOGO_WIDTH, LOGO_HEIGHT, 1);
  display.display();
  Serial.println("Waiting For Valid Finger");
  return -1;
 }

 p = finger.image2Tz();
 if (p != FINGERPRINT_OK)
 {
  display.clearDisplay();
  display.setTextSize(2);             // Normal 1:1 pixel scale
  display.setTextColor(SSD1306_WHITE);        // Draw white text
  display.setCursor(0, 0);            // Start at top-left corner
```

```
  display.println(("Prateek Image"));
  display.setCursor(0, 35);
  display.println("Try Again");
  display.display();

  Serial.println("Prateek Image Try Again");
  delay(3000);
  display.clearDisplay();
  return -1;
}

p = finger.fingerFastSearch();
if (p != FINGERPRINT_OK)  {

  display.clearDisplay();
  display.setTextSize(2);           // Normal 1:1 pixel scale
  display.setTextColor(SSD1306_WHITE);       // Draw white text
  display.setCursor(20, 0);          // Start at top-left corner
  display.println(("Invalid"));
  display.setCursor(25, 20);
  display.println("Finger");
  display.setCursor(10, 40);
  display.println("Try Again");
  display.display();
  Serial.println("Not Valid Finger");
  delay(3000);
  display.clearDisplay();
  return -1;
}

// found a match!
  display.clearDisplay();
  display.setTextSize(2);           // Normal 1:1 pixel scale
  display.setTextColor(SSD1306_WHITE);       // Draw white text
  display.setCursor(40, 0);          // Start at top-left corner
```

```
  display.println(("Door"));
  display.setCursor(15, 20);          // Start at top-left corner
  display.println(("Unlocked"));
  display.setCursor(20, 40);
  display.println("Welcome");
  display.display();

  digitalWrite(relayPin, HIGH);
  digitalWrite(buzzerPin, HIGH);
 delay(6000);

  display.clearDisplay();
  display.setTextSize(2);           // Normal 1:1 pixel scale
  display.setTextColor(SSD1306_WHITE);       // Draw white text
  display.setCursor(20, 10);          // Start at top-left corner
  display.println(("Closing"));
  display.setCursor(20, 30);          // Start at top-left corner
  display.println(("the Door"));
  display.display();

  digitalWrite(relayPin, LOW);
  digitalWrite(buzzerPin, LOW);
  delay(3000);

  display.clearDisplay();

  Serial.println("Door Unlocked Welcome");

  return finger.fingerID;
}
```

Додаток В. Ілюстраційний матеріал

РОЗРОБКА БАГАТОФУНКЦІОНАЛЬНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ПІДВИЩЕНОЇ ЗАХИЩЕНОСТІ ДО КРИТИЧНИХ ОБ'ЄКТІВ ВІД ЕЛЕКТРОМАГНІТНИХ ЗАВАД І ФУНКЦІЄЮ АДАПТИВНОГО ЕКРАНУВАННЯ

Виконав: студент групи 2КІТС-21-Б Римаренко М.В.
Науковий керівник: к.т.н., доц., зав. каф. МБІС Карпінець В.В.

АКТУАЛЬНІСТЬ ТЕМИ

Сучасний розвиток технологій у сфері безпеки та контролю доступу вимагає впровадження нових або вдосконалених технічних рішень. Зростання загроз несанкціонованого доступу до критичних об'єктів зумовлює потребу у створенні багатофункціональних, захищених та адаптивних систем. Актуальним є розроблення рішень, що забезпечують надійну автентифікацію, стійкість до електромагнітних завад, зручне мобільне керування, підтримку двофакторної авторизації та інтеграцію з сучасною IT-інфраструктурою.

МЕТА РОБОТИ

Метою є розробка та створення прототипу багатофункціональної системи контролю і управління доступом, орієнтованої на використання у приміщеннях з підвищеними вимогами до захисту від електромагнітних випромінювань. Система забезпечує біометричну ідентифікацію користувача за відбитком пальця, індикацію стану замка на вбудованому екрані, локальне управління доступом за допомогою кнопки, а також миттєве інформування користувача про події через захищений канал у месенджері.

АНАЛІЗ ІСНУЮЧИХ АНАЛОГІВ

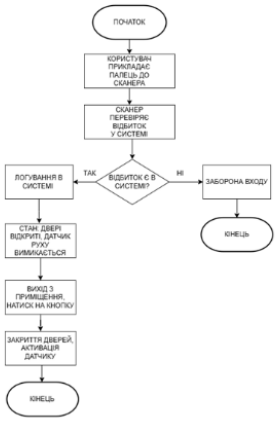
ZKTeco L7000 - біометричний замок з вбудованим сканером відбитків пальців.

ZKTeco RFID Reader - зчитувач карт доступу з підтримкою контролю проходу.

INLock_street – вулична система контролю доступу з металевим корпусом та RFID.

РОЗРОБКА СТРУКТУРНОЇ СХЕМИ

На цьому етапі було створено структурну схему пристрою, яка включає всі необхідні компоненти для контролю доступу та обробки даних. Розроблено блок-схему, яка дозволяє чітко уявити взаємодію між основними частинами пристрою.



АНАЛІЗ ІСНУЮЧИХ АНАЛОГІВ

ZKTeco L7000 - біометричний замок з вбудованим сканером відбитків пальців.

ZKTeco RFID Reader - зчитувач карт доступу з підтримкою контролю проходу.

INLock_street – вулична система контролю доступу з металевим корпусом та RFID.

ОБ’ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

Об’єкт дослідження - технічні засоби та інформаційні технології, що застосовуються у системах контролю доступу для захисту критично важливих об'єктів.
Предмет дослідження - процес розробки та функціонування багатофункціональної системи контролю доступу, яка поєднує мобільне керування, біометричну автентифікацію, лазерну детекцію, екранування від електромагнітних завад і логування подій.

ВИКОРИСТАНІ АПАРАТНІ ЗАСОБИ

ESP32 — мікроконтролер з вбудованим Wi-Fi та Bluetooth, що забезпечує обробку даних та керування пристроєм.
FPM10A — оптичний біометричний сканер відбитків пальців для ідентифікації користувача.
PIR-датчик — сенсор руху, що активує систему при виявленні присутності.
OLED-дисплей (0.96") — відображає повідомлення, статус системи та результати сканування.
Соленоїдний замок — виконавчий механізм для блокування або розблокування доступу.
Кнопка — використовується для виходу з приміщення.
Джерело живлення (5В) — забезпечує енергоживлення усіх компонентів пристрою.
Джерело живлення соленоїдного замка (12В) — забезпечує енергоживлення замка.

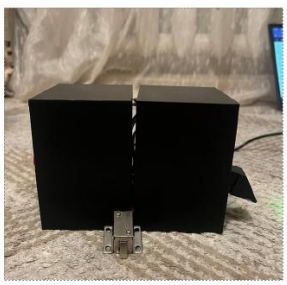
ВИКОРИСТАНІ ТЕХНОЛОГІЇ

- C++ (Arduino) — основна мова для програмування ESP32.
- Arduino IDE — середовище розробки для написання та прошивки коду.
- Wi-Fi (ESP32) — забезпечує бездротове з'єднання для передачі даних.
- HTTP/REST API — використовується для відправки логів на сервер або в хмару.
- Екранувальна тканина Фарадея - захист від електромагнітного впливу зсередини.
- Екранувальна фарба - захист від електромагнітного випромінювання зовні.

РЕАЛІЗОВАНИЙ ПРОТОТИП ПРОТОТИП

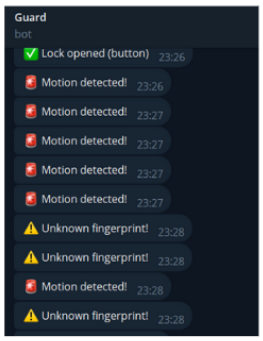
Сканування відбитку та результат сканування

Моніторинг руху лазерним дачиком та вихід кнопкою



Відкриття або закриття соленоїдного

ЗАПИС ПОДІЙ



Запис додається у випадку:

- початку роботи пристрою
- відкриття замка за допомогою відбитку пальця
- хибний відбиток пальця
- виявлений рух
- відкриття замка кнопкою

Висновок

У результаті виконання роботи було створено функціональний програмно-апаратний комплекс системи контролю та управління доступом, який поєднує в собі надійність, зручність та сучасні технології безпеки. Пристрій забезпечує біометричну ідентифікацію користувача, реагує на присутність за допомогою датчика руху, дозволяє відкривати двері як за відбитком пальця, так і за допомогою кнопки, фіксує події у режимі реального часу в боті у месенджері та надає візуальний зворотний зв’язок через OLED-дисплей. Завдяки підключенню до Wi-Fi і реалізації API, комплекс може працювати як автономно, так і у складі більшої мережі захисту об'єкта. Такий підхід дозволяє гнучко масштабувати систему відповідно до вимог конкретного середовища та завдань.

ДЯКУЮ ЗА УВАГУ!

ПРОТОКОЛ ПЕРЕВІРКИ НАВЧАЛЬНОЇ (КВАЛІФІКАЦІЙНОЇ) РОБОТИ

Назва роботи:

розробка багатофункціональної системи контролю доступу підвищеної захищеності до критичних об'єктів від електромагнітних завад і функцією адаптивного екранування

Тип роботи: бакалаврська кваліфікаційна робота

Підрозділ Кафедра менеджменту на безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
Гр. 2КІТС-216

Керівник доцент Карпінець В.В. _____

Показники звіту подібності

Strike Plagiarism	
Оригінальність	98%
Загальна схожість	2%

Аналіз звіту подібності (відмітити потрібне)

- ☒ **Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.**
- ☐ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її автора. Роботу направити на доопрацювання.
- ☐ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Заявляю, що ознайомлений (-на) з повним звітом подібності, який був згенерований Системою щодо роботи (додається)

Автор _____ Римаренко М.В.
(підпис) (прізвище, ініціали)

Опис прийнятого рішення

- ☒ **Допустити до захисту**

_____

_____

_____

_____

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