МЕЛІТОПОЛЬСЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОГДАНА ХМЕЛЬНИЦЬКОГО

Факультет інформатики, математики та економіки

Кафедра інформатики і кібернетики

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти «магістр»

на тему **«Розробка системи керування доступом до захисних укриттів на основі пристроїв Akuvox»**

Виконав: здобувач вищої освіти
групи М314-і
спеціальність 122 Комп'ютерні науки
ОПП Комп'ютерні науки
Близнюк Олександр Ігорович

Керівник: кандидат педагогічних наук
Конюхов Сергій Леонідович

Рецензент: директор ТОВ «Тіанді»
Данилюк Вікторія Михайлівна

Запоріжжя – 2025 року

БЛИЗНЮК ОЛЕКСАНДР ІГОРОВИЧ

РОЗРОБКА СИСТЕМИ КЕРУВАННЯ ДОСТУПОМ ДО ЗАХИСНИХ УКРИТТІВ НА ОСНОВІ ПРИСТРОЇВ AKUVOX

Кваліфікаційна робота спрямована на розробку програмного комплексу, призначеного для віддаленого керування доступом до захисних укриттів, а також забезпечення автоматичного відчинення або зачинення входів залежно від сигналів тривоги або відбою. В умовах регулярних повітряних тривог постає потреба в надійних і доступних укриттях з можливістю централізованого керування. Традиційні механічні системи керування доступом не завжди забезпечують достатню швидкість, надійність і гнучкість, що зумовлює необхідність їхньої модернізації та цифровізації.

Об'єкт дослідження: веборієнтовані системи з можливістю керування віддаленими фізичними пристроями.

Предмет дослідження: система керування доступом до захисних укриттів.

Мета дослідження: спроєктувати та розробити систему керування доступом до захисних укриттів на основі пристроїв Akuvox.

Теоретичне значення дослідження полягає в аналізі сучасного стану й підходів до створення системи захисних укриттів у різних країнах, аналізі сучасних підходів до вирішення завдань контролю й керування доступом до приміщень.

Практичне значення дослідження полягає в тому, що розроблено програмний комплекс «Система керування доступом до захисних укриттів на основі пристроїв Akuvox», який складається з програми для пристрою інтерком-контролю доступу, що забезпечує керування відчиненням та зачиненням дверей відповідно до оповіщень тривоги або відбою тривоги, клієнтської частини – вебінтерфейсу оператора системи та серверної частини, яка забезпечує керування системою. Програмний комплекс доступний для придбання зацікавленими сторонами, наприклад житлово-експлуатаційними компаніями, які мають у керування захисні укриття.

Ключові слова: цивільний захист, керування доступом, стек технологій, Laravel, PHP, MySQL.

BLYZNIUK OLEKSANDR

DEVELOPMENT OF AN ACCESS CONTROL SYSTEM TO PROTECTIVE SHELTERS BASED ON AKUVOX DEVICES

The qualification work is aimed at developing a software package designed for remote control of access to protective shelters, as well as ensuring automatic opening or closing of entrances depending on alarm signals or deadlock. In conditions of regular air alarms, there is a need for reliable and accessible shelters with the possibility of centralized control. Traditional mechanical access control systems do not always provide sufficient speed, reliability and flexibility, which necessitates their modernization and digitalization.

Object of research: web-based systems with the ability to control remote physical devices.

Subject of research: access control system to protective shelters.

Purpose of research: to design and develop an access control system to protective shelters based on Akuvox devices.

The theoretical significance of the study is the analysis of the current state and approaches to creating a system of protective shelters in different countries, the analysis of modern approaches to solving the problems of controlling and managing access to premises.

The practical significance of the study is that the software package "System of access control to protective shelters based on Akuvox devices" has been developed, which consists of a program for an intercom access control device that provides control of opening and closing doors in accordance with alarm notifications or alarm reset, the client part - the web interface of the system operator and the server part that provides system management. The software package is available for purchase by interested parties, for example, housing and operating companies that manage protective shelters.

Keywords: civil protection, access control, technology stack, Laravel, PHP, MySQL.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ....3
ВСТУП....4
РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ....9
1.1. Аналіз сучасного стану системи захисних укриттів....9
1.2. Керування доступом до приміщень....19
1.3. Обґрунтування доцільності розробки програмного комплексу....26
РОЗДІЛ 2. ПРОЄКТУВАННЯ СИСТЕМИ КЕРУВАННЯ ДОСТУПОМ ДО ЗАХИСНИХ УКРИТТІВ НА ОСНОВІ ПРИСТРОЇВ AKUVOX....37
2.1. Огляд аналогів....37
2.2. Технічне завдання на розробку системи керування доступом до захисних укриттів на основі пристроїв Akuvox....44
2.3. Вибір засобів розробки....56
РОЗДІЛ 3. ОПИС СИСТЕМИ КЕРУВАННЯ ДОСТУПОМ ДО ЗАХИСНИХ УКРИТТІВ НА ОСНОВІ ПРИСТРОЇВ AKUVOX....65
3.1. Технічний опис системи....65
3.1.1. Базова структура Laravel-проєкту....65
3.1.2. Опис класів програмної реалізації....68
3.2. Користувацький опис....73
3.3. Модульне та інтеграційне тестування системи....80
ВИСНОВКИ....84
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ....89
ДОДАТОК....96

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БД	База даних
ДСНС	Державна служба України з надзвичайних ситуацій
ОМС	Органи місцевого самоврядування
СКБД	Система керування базами даних
ABAC	Attribute-Based Access Control
ACID	Atomicity, Consistency, Isolation, Durability
ACL	Access Control List
API	Application Programming Interface
CapBAC	Capability-Based Access Control
CBRN	Chemical, Biological Radiological, Nuclear
CRM	Customer Relationship Management
CRUD	Create, Read, Update, Delete
DAC	Discretionary Access Control
ERP	Enterprise Resource Planning
GIS	Geographic Information System
HTTP	HyperText Transfer Protocol
IoT	Internet of Things
JSON	JavaScript Object Notation
LCD	Liquid Crystal Display
MAC	Mandatory Access Control
MVCC	Multi-Version Concurrency Control
NFC	Near-Field Communication
NVR	Network Video Recorder
OLAP	Online Analytical Processing
ORM	Object-Relational Mapping
OWASP	Open Worldwide Application Security Project
PIN	Personal Identification Number
RBAC	Role-Based Access Control
REST	Representational State Transfer
RFID	Radio-Frequency Identification
SQL	Structured Query Language
SWOT	Strengths, Weaknesses, Opportunities, and Threats
UCON	Usage Control
UI	User Interface
WAF	Web Application Firewall
WAL	Write-Ahead Logging

ВСТУП

В сучасних умовах перед українським суспільством постає безліч завдань, що стосуються усіх сфер його функціонування. Найбільшу значущість має створення умов для захисту життя та здоров'я людини або принаймні зниження відповідних ризиків. Важливим засобом для цього є обладнані захисні укриття, в яких люди можуть перебувати достатньо довго. Вирішення цього завдання передбачає комплекс заходів, частину яких можна буде реалізувати лише в повоєнний період, наприклад, будівництво мережі захисних укриттів сучасного типу. Разом із тим, окремі заходи можуть бути вжиті вже зараз для підвищення доступності відповідних приміщень для громадян та покращання комфортності перебування в них.

Актуальність дослідження визначається комплексом безпекових, технічних і соціальних чинників. В умовах регулярних повітряних тривог постає потреба в надійних і доступних укриттях з можливістю централізованого керування. Об'єктивна складність полягає в тому, що такі приміщення розташовані далеко не всюди, а ті, що функціонують, часто мають багато недоліків, зокрема в аспекті доступності. Традиційні механічні системи керування доступом не завжди забезпечують достатню швидкість, надійність і гнучкість, що зумовлює необхідність їх модернізації та цифровізації.

Світова тенденція впровадження «розумних» технологій у критично важливу інфраструктуру сприяє переходу до автоматизованих та інтелектуальних систем керування. Пристрої Akuvox, які поєднують можливості відеодомофонії, контролю доступу, віддаленого керування та автоматизованої ідентифікації, дозволяють створити сучасну мережеву систему керування захисними укриттями. Завдяки інтеграції цих пристроїв можна підвищити рівень безпеки громадян, забезпечити фіксацію та аналіз подій, контролювати доступ лише авторизованих осіб, координувати дії персоналу в реальному часі тощо.

Додаткової значущості дослідженню надає можливість поєднувати систему на основі Akuvox з іншими засобами безпеки (системами оповіщення, пожежною сигналізацією, аварійним освітленням та резервним енергопостачанням). Це створює передумови для створення комплексної, масштабованої та відмовостійкої інфраструктури цивільного захисту. Важливим є й те, що захисні укриття мають працювати автономно навіть у випадку порушення основних мереж, а сучасні IP-пристрої дозволяють реалізувати такі сценарії.

Створення та підтримка функціонування захисних укриттів різних типів нині є предметом наукових досліджень. У наукових публікаціях висвітлено різні аспекти зазначеної проблеми, зокрема: підходи до створення системи захисних укриттів у різних країнах (С. Малліані та О. Слєпцов [17], A. Jörgen, J.F. Łątka, R. Tarczewski, Z. Szcześniak, B. Pieńko, M. Morales-Beltran, D. Gromek та L. Kosztołowicz [42], K. Kaczmarek [43]); стан та проблеми функціонування мережі захисних укриттів (В. Іваненко [9], С. Малліані та О. Слєпцов [17], Г. Олійник [20], В. Шумакова, В. Абракітов [30], A. Galkin, G. Samchuk, S. Lyfenko, A. Botsman, N. Braterska, O. Hriekova, Y. Drobotova та I. Tolmachov [39], H. Jiao та S. Feng [41]); створення автономних та інтегрованих захисних укриттів (О. Вертелецький, Т. Нікіфорова [4], Б. Коваль, О. Співак, О. Козленко та О. Климук [14], N. Kwon, J. Cho, Y. Ahn, J. Kim та Y.-J. Park [44]); проєктування внутрішнього середовища захисних споруд (Р. Михайлова, І. Антоненко та С. Рябова [19], М. Помазан, С. Іщенко [21], С. Рябова, Т. Струмінська та І. Антоненко [23]); автоматизація та цифровізація захисних укриттів (Є. Мартин, С. Лясковська та Н. Тарапата [18], X. Wu, F. Sun, X. Zhang та W. Wang [61]) тощо. Практичні аспекти створення, облаштування та забезпечення функціонування захисних укриттів розкрито в нормативних документах [7], науково-технічних і навчально-методичних публікаціях [3; 8; 11; 24; 29].

Апаратно-технічний та програмний аспекти автоматизації контролю та керування доступом до приміщень різного призначення розглянуто у працях О. Айко, О. Василенко та В. Степаненко [1], А. Казаряна, В. Теслюка та

В. Коваля [13], Л. Рибака та П. Кравця [22], В. Тітової, Ю. Кльоца, С. Мостового, В. Колісника [26], О. Юдіна та О. Весельської [31], S. Ameer, J. Benson та R. Sandhu [34], Z.N. Mohammad, F. Farha, A.O.M. Abuassba, S. Yang та F. Zhou [48], C. Stolojescu-Crisan, C. Crisan та B.-P. Butunoi [57], М. Василенка та А. Загорної [60] та інших науковців. Слід зауважити, що в цих публікаціях зроблено акцент на способах обмеження доступу до виробничих приміщень або його надання певним особам, а також керування доступом у системі «розумний будинок». Тобто можна стверджувати, що проблеми керування доступністю захисних укриттів є недостатньо дослідженими.

Отже, незважаючи на наявність наукових публікацій, проблеми автоматизації та цифровізації керування захисними укриттями, зокрема з використанням конкретних технологічних рішень, наразі недостатньо досліджені й потребують подальшого опрацювання як у теоретичному, так і у практичному аспектах.

Таким чином, соціальна та зокрема безпекова значущість розглянутої проблеми зумовлює вибір теми дослідження «Розробка системи керування доступом до захисних укриттів на основі пристроїв Akuvox».

Об’єкт дослідження: веборієнтовані системи з можливістю керування віддаленими фізичними пристроями.

Предмет дослідження: система керування доступом до захисних укриттів.

Мета дослідження: спроєктувати та розробити систему керування доступом до захисних укриттів на основі пристроїв Akuvox.

Для досягнення поставленої мети дослідження необхідно виконати такі завдання:

1) Проаналізувати інформаційні джерела (нормативні документи, науково-технічні та навчально-методичні публікації, відкриті Інтернет-ресурси) та вивчити предметну область дослідження.

2) Обґрунтувати доцільність розробки програмного комплексу.

3) Розробити технічне завдання на розробку системи керування доступом до захисних укриттів на основі пристроїв Akuvox та обрати засоби реалізації проєкту.

4) Розробити систему керування доступом до захисних укриттів на основі пристроїв Akuvox, а також документацію до неї.

5) Виконати тестування розробленої системи та виправити недоліки у випадку їх виявлення.

Для виконання поставлених завдань використано такі методи дослідження:

- *теоретичні*: аналіз інформаційних джерел – для вивчення предметної області дослідження; узагальнення і систематизація – для формування теоретичного підґрунтя дослідження; методи економічної діагностики та стратегічного аналізу (SWOT-аналіз, аналіз за моделлю п'яти сил Портера, аналіз ризиків, аналіз зацікавлених сторін) для попереднього визначення доцільності розробки програмного комплексу та його конкурентоспроможності, а також груп учасників, які мають вплив на проєкт або залежать від його результатів; моделювання – для розробки технічного завдання;

- *емпіричні*: розробка інтерфейсу користувача; розробка програмного забезпечення; тестування програмного забезпечення.

Теоретичне значення дослідження полягає в аналізі сучасного стану й підходів до створення системи захисних укриттів у різних країнах, аналізі сучасних підходів до вирішення завдань контролю й керування доступом до приміщень.

Практичне значення дослідження полягає в тому, що розроблено програмний комплекс «Система керування доступом до захисних укриттів на основі пристроїв Akuvox», який складається з програми для пристрою інтерком-контролю доступу, що забезпечує керування відчиненням та зачиненням дверей відповідно до оповіщень тривоги або відбою тривоги, клієнтської частини – вебінтерфейсу оператора системи та серверної частини,

яка забезпечує керування системою. Програмний комплекс доступний для придбання зацікавленими сторонами, наприклад житлово-експлуатаційними компаніями, які мають у керування захисні укриття.

Апробацію результатів дослідження здійснено шляхом участі у II Всеукраїнській науково-практичній конференції «Всесвітній день інформації» (27.11.2025 р.).

Структура кваліфікаційної роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел (62 найменування, зокрема 30 англійською мовою) й одного додатку. Робота містить 6 таблиць, 20 рисунків. Загальний обсяг роботи – 98 сторінок, з них – 88 сторінок основного тексту.

Вступ містить загальну характеристику кваліфікаційної роботи: обґрунтовано актуальність дослідження, визначено методологічний апарат (об’єкт, предмет, мета, завдання, методи дослідження), схарактеризовано теоретичне і практичне значення, наведено відомості про апробацію. В першому розділі наведено результати аналізу предметної області (сучасного стану й підходів до створення системи захисних укриттів, підходів до вирішення завдань контролю й керування доступом до приміщень), а також обґрунтовано доцільність виконання проєкту. У другому розділі наведено результати проєктування системи керування доступом до захисних укриттів на основі пристроїв Akuvox: схарактеризовано деякі аналоги, подано технічне завдання, обґрунтовано вибір засобів розробки проєкту. У третьому розділі подано опис розробленої системи. У висновках сформульовано теоретичні і практичні висновки з проведеного дослідження.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Аналіз сучасного стану системи захисних укриттів

В умовах війни з Росією дуже гостро постала проблема захисту цивільного населення від повітряних збройних атак. Для його забезпечення призначені захисні споруди, які створюють з метою виключення або мінімізації впливу надзвичайних ситуацій та застосування зброї різного виду.

У Кодексі цивільного захисту України [15] визначено такі види захисних споруд:

1) сховище – герметична споруда для перебування та захисту людей протягом не менш як 48 годин;

2) протирадіаційне укриття – негерметична споруда для перебування та захисту людей протягом не менш як 48 годин;

3) споруди подвійного призначення – будівлі, споруди або їх окремі частини, спроєктовані так, що в умовах надзвичайних ситуацій, воєнних дій або терористичних актів забезпечують захист населення, а в інший час використовуються для забезпечення суспільних або господарських потреб;

4) первинне (мобільне) укриття – технічний виріб, наприклад блок-модульного типу, призначений для короткострокового (до 4 годин) захисту населення;

5) найпростіше укриття – цокольне або підвальне приміщення, інша споруда підземного простору, де створено умови для тимчасового перебування людей протягом не менш як 48 годин.

Вимоги до проєктування сховищ, протирадіаційних укриттів та споруд подвійного призначення наведено у Державних будівельних нормах В.2.2-5:2023 [7].

Згідно з аналітичними документами в Україні на 2024 рік було 61803 споруди цивільного захисту, з яких 9% – сховища, 23% – протирадіаційні укриття, 68% – найпростіші укриття та споруди подвійного призначення. Разом із тим, близько 23% з наявних споруд непридатні для використання [29, с. 5-6].

З огляду на сучасні небезпеки, що постають у різних країнах світу, науковці приділяють увагу дослідженню проблем розбудови системи захисту населення, формуванню стратегічних та тактичних рекомендацій для їх вирішення, а також розробці технічних рішень.

Науковці С. Малліані та О. Слєпцов у праці [17] систематизували найбільш поширені обставини загибелі та поранення цивільних під час російських ракетних і дронових атак та виявили три ситуації підвищеної вразливості: удар по житловій забудові, ураження відкритих міських просторів та атаки на громадські будівлі з великим скупченням людей. Ці сценарії стали основою для оцінювання того, наскільки наявна в Україні система захисних споруд відповідає реальним потребам захисту населення.

Порівняння українських норм із фінською та ізраїльською моделями показало, що Україна має суттєві концептуальні прогалини. Зокрема, українська номенклатура не містить рішень, здатних ефективно забезпечити безпечний простір у житловій забудові. На противагу цьому, в Ізраїлі захисні приміщення розміщено безпосередньо у квартирах і на поверхах, завдяки чому забезпечується миттєвий доступ до укриття. Запровадження подібних конструктивно інтегрованих укриттів могло б суттєво підвищити рівень захисту українського населення. В Україні немає регламентованих і легко доступних наземних модульних укриттів, які могли б забезпечувати захист на відкритих територіях. Натомість у Фінляндії (тип S2) та Ізраїлі (тип Мамах) такі структури є обов'язковим елементом міського середовища та розміщуються у межах 50–100 метрів від місць масового перебування людей. Отже, для України надзвичайно важливо розробити та впровадити такі компактні, швидкодоступні й вибухостійкі укриття. Українські нормативи

також не враховують ризику одночасної загибелі великої кількості людей в єдиному великому просторі у разі прямого влучання. На відміну від цього, у Фінляндії та в Ізраїлі великі укриття обов'язково розділяються на менші ізольовані модулі. Такий підхід знижує масштаб можливих втрат і його запровадження в Україні є необхідним для підвищення безпеки громадських об'єктів.

Підсумовуючи, автори підкреслюють, що українська система цивільного захисту має потенціал для модернізації, однак потребує глибокого оновлення. Першочерговими напрямами є формування нових типів житлових укриттів, скорочення радіусів доступності, впровадження наземних модулів для відкритих просторів, а також структуризація великих укриттів на менші ізольовані блоки. Така модернізація дозволить адаптувати захисну інфраструктуру до трьох основних сценаріїв ураження та підвищить безпеку цивільного населення України в умовах довготривалої воєнної загрози [17].

Ґрунтовний аналіз стану укриттів для цивільного населення в умовах сучасних військових загроз, із акцентом на Польщу та порівняльним оглядом міжнародних практик проведено авторами дослідження [42]. Актуальність теми автори обґрунтовують зростанням кількості конфліктів у світі, насамперед війною Росії проти України, а також ескалацією на Близькому Сході та в інших регіонах. Показано, що понад 30 років у Європі цивільні сховища не розглядалися як пріоритет, що призвело до деградації інфраструктури. Зокрема не оцінювалася реальна придатність укриттів, тому «номінальна» місткість не дорівнює «фактичній» готовності.

На основі аналізу міжнародних практик розгортання системи захисних укриттів [42, с. 92-94] автори доводять, що підходи до створення та утримання укриттів у світі суттєво різняться, оскільки їх формували історичний досвід, рівень загроз, законодавча база та політика національної безпеки. Наведемо основні характеристики систем укриттів окремих країн:

1) США. Укриття розвивалися переважно під впливом природних катастроф, а не військових загроз. Для країни характерні: широка доступність

інформації та інструкцій; система публічних укриттів, часто створених на базі шкіл, громадських центрів, спортивних споруд; наявність масштабних стратегічних об'єктів, що забезпечують захист від високотехнологічних ударів, ядерного вибуху та проникаючої радіації. Укриття для цивільних рідко бувають герметичними чи розрахованими на CBRN-захист (хімічні, біологічні, радіаційні та ядерні загрози), оскільки країна не має постійної загрози ракетних ударів.

2) Швейцарія має найрозвинутішу систему укриттів у світі, що забезпечує майже 100% населення місцями в укриттях. Її характерні риси: багаторівнева мережа приватних та публічних бункерів; суворі стандарти герметичності, захисту від вибухової хвилі та радіації; інтеграція укриттів у житлові будинки; наявність складної інфраструктури тунелів та гірських сховищ. Така система є результатом багаторічної оборонної доктрини «всеохопного захисту».

3) Швеція. Укриття розраховані на 81% населення, будуються переважно як частина громадських будівель і житла, передбачають подвійне призначення (спортзали, паркування, склади тощо).

4) Фінляндія. Укриття забезпечують 70% населення, активно використовуються в мирний час під комерційні і соціальні функції (спортивні центри, паркінги, культурні простори), стандарти вимагають забезпечення 1м² на людину. Більшість сховищ – це підземні бетонні споруди високої стійкості.

5) Чехія. Чеська система укриттів сформувалася під впливом оборонної політики 1935-1989 років. Її особливості: укриття спочатку призначалися для захисту від авіаударів, а згодом від зброї масового ураження; після 1990 року будівництво нових сховищ практично припинилося; наявні укриття мають місткість приблизно 1,35 млн. осіб; сьогодні уряд акцентує увагу на імпровізованих укриттях, зокрема адаптації транспортної інфраструктури; для населення створено цифрову карту укриттів.

6) Німеччина. Після об'єднання країни у 1990 році програма укриттів була фактично згорнута. Характерні риси: існує близько 579 публічних

укриттів; укриттями забезпечено менше 0,6% населення; більшість укриттів проєктувалися для захисту від звичайних засобів ураження, а не сучасних високоточних боєприпасів; суттєве недофінансування та відсутність нових нормативів. Німеччина є одним із найслабших прикладів сучасної готовності до цивільної оборони в Європі.

7) Ізраїль. Країна має унікальну, найбільш «бойову» модель цивільного захисту, а саме: укриттями забезпечено приблизно 66% населення; поширені міклатим – публічні та приватні бомбосховища; з 1992 р. у кожній новій будівлі обов'язкова захищена кімната (мамад), герметична, з фільтровентиляцією; конструкції розраховані на ракетні удари та обвали уламків; особлива увага приділяється швидкій доступності укриттів (до 15–60 секунд у прикордонних містах).

8) Туреччина. Укриття призначені для захисту не лише від військових загроз, а й від природних катастроф, особливо землетрусів. Основні особливості: укриття часто розташовані в підвалах громадських будівель, шкіл, лікарень; існує чітка класифікація: спеціальні (для установ, підприємств, житлових будинків), загальні (для публічного користування); виділяють два типи захисту – від ударної хвилі та від радіоактивного випадіння; технічні вимоги закріплені в нормативних документах Міністерства громадських робіт.

На основі проведеного аналізу авторами розроблено рекомендації з проєктування сучасних захисних укриттів для Польщі та України [42, с. 94-97], зокрема:

1) Виокремлення чотирьох ключових функціональних зон укриття:

- вхідно-комунікаційна зона: шлюзи, тамбури, санітарні вузли для деконтамінації;
- базова житлова зона: зал очікування, місця для сидіння та сну;
- соціальна зона: кухня, санвузли, медичний пункт, кімнати відпочинку;
- технічна зона: фільтровентиляційні агрегати, генераторна, резервуари.

2) Основні технічні вимоги:

- герметичність;

- три режими вентиляції: звичайний, фільтровентиляція, повна ізоляція;
- автономне електро- та водопостачання;
- захист від накопичення вуглекислого газу;
- температурний контроль (максимальна температура не повинна перевищувати 29–30°C);
- наявність резервних евакуаційних виходів.

3) Зауваження щодо організації внутрішнього розпорядку: змінність циклу «сон – сидіння – робота»; необхідність чіткого керівництва для уникнення паніки.

Науковець K. Kaczmarek у праці [43] виконав комплексний аналіз системи безпеки Фінляндії як унікальної моделі довгострокової національної оборони та цивільної готовності, що може служити прикладом для країн Центральної та Східної Європи. Автор наголошує на історично зумовленій постійній готовності Фінляндії до воєнних і невоєнних загроз, особливо з боку Російської Федерації, що сформувало в країні цілісну систему державної та суспільної стійкості. Отже, в умовах повномасштабного вторгнення Росії в України врахування досвіду Фінляндії є актуальним для усіх країн Європи.

Важливою складовою цієї системи є наявність захисних укриттів. Фінляндія має одну з найбільших у світі мереж захисних споруд: укриття можуть розмістити 4,8 млн. людей з 5,5 млн. населення; понад 90% укриттів захищають від артилерійських/ракетних ударів, понад 80% – забезпечують захист від газових атак та радіації. Тобто система охоплює майже всю країну, і більшість місць проживання обладнані засобами захисту [43, с. 134].

Система будівництва та функціонування укриттів у Фінляндії регулюється Законом про порятунок 2011 року. Цей закон зобов'язує власників нових будівель створювати цивільні захисні укриття для мешканців або користувачів об'єктів. Будівництво укриттів є вимогою для: житлових будинків із великою кількістю квартир; шкіл, дитячих закладів; лікарень, соціальних установ; торгових центрів площею понад 400 м²; ресторанів на понад 50 місць; промислових і складських будівель площею понад 1500 м²;

місць масового перебування людей; об'єктів культурної спадщини; великих робочих місць (понад 50 осіб); тунелів громадського транспорту довжиною понад 100 метрів. Укриття повинні забезпечувати захист від вибухів, артилерійських та ракетних атак, від руйнування будівлі, від іонізуючого випромінювання, від токсичних та хімічних речовин, належний мікроклімат (температура, вентиляція), достатній рівень санітарії та гігієни. [43, с. 135-136].

Автор робить висновок, що досвід Фінляндії може бути надзвичайно цінним для країн Європи, однак його адаптація потребує підвищення суспільної обізнаності, політичної волі, формування культури безпеки та впровадження концепції всеохопної оборони на рівні держави й громадян.

Науковці H. Jiao та S. Feng [41] провели дослідження, присвячене оптимізації розміщення укриттів та побудові «життєвих кіл запобігання лихам» у малих міських поселеннях за допомогою методів геоінформаційного аналізу. Автори показали, що малі та середні міста мають найбільшу вразливість унаслідок нерівномірного розвитку, застарілої інфраструктури та обмежених ресурсів. Вони проаналізували просторові ризики, пов'язані з підвищеною сейсмічністю, підтопленнями та старою забудовою, що створює значні бар'єри для евакуації населення. Використовуючи наукові методи, автори визначили оптимальну мережу укриттів для короткострокового та середньострокового перебування людей та сформували трирівневу систему «життєвих кіл запобігання лихам», яка охоплює великі життєві кола для постійного проживання та локальні кола екстреної евакуації, для окремого регіону Китаю. Отримані результати та розроблені авторами методологічні підходи можуть бути використані як методична основа для модернізації систем укриттів у малих та середніх містах, а також адаптовані до українського контексту, зокрема в умовах підвищеної небезпеки воєнних і техногенних загроз.

У статті [44] підіймається проблема захисту населення Південної Кореї від повітряних військових загроз. Для протидії цим загрозам Південна Корея

покладається на активні стратегії протиповітряного захисту, які можуть давати позитивні результати, але мають обмеження щодо забезпечення безпеки населення. Показано, що Швеція, Швейцарія та Фінляндія надають пріоритет будівництву покращених захисних споруд. Тому для створення більш ефективної системи безпеки та керування надзвичайними ситуаціями важливо впроваджувати та вдосконалювати оборонні укриття, системи оповіщення та навчання. Автори доводять, що наявні захисні укриття, зокрема метро й паркінги, мають недостатні можливості для протидії хімічним, біологічним, радіологічним і ядерним атакам. Крім того, важливо враховувати витрати на будівництво таких захисних споруд. Науковці розробили модель, що оцінює економічну доцільність будівництва захисних споруд із урахуванням таких факторів, як збільшення коефіцієнта поверховості, операційний прибуток і збільшення кількості житлових одиниць. Запропонована модель не обмежується лише захисними спорудами, а може бути універсально застосована для широкого спектра оцінок доцільності, включно з керуванням безпекою та готовністю до надзвичайних ситуацій у будівлях різних країн, зокрема в Україні.

Автори праці [61] зосередили увагу на автоматизації та віддаленому керуванні функціонуванням захисних укриттів. Показано, що в екстремальних умовах високогір’я, крижаних регіонів, пустель та віддалених прикордонних районів суворі природні умови, незручність транспортування та високі витрати на інфраструктурне будівництво створюють значні труднощі для розгортання захисних укриттів. Традиційні системи з людським моніторингом мають проблеми низької ефективності, високих витрат і суттєвих ризиків для безпеки. Внутрішнє середовище таких укриттів є критично важливим для стабільної роботи та безпеки персоналу, тому надзвичайно важливим є моніторинг у реальному часі. Необслуговувані укриття можуть значно зменшити трудове навантаження на персонал. Завдяки інтеграції інтелектуальних та автоматизованих технологій такі системи можуть долати обмеження довкілля, забезпечуючи цілодобовий моніторинг і керування

ресурсами. Авторами розроблено систему моніторингу параметрів середовища в укритті. Завдяки встановленню датчиків температури, вологості, диму та контролю відкриття дверей оператори укриттів можуть у реальному часі відстежувати інформацію про параметри внутрішнього середовища. Одночасно система взаємодіє із зовнішнім обладнанням для контролю даних від кондиціонерів та дизель-генераторів. Так досягається інтелектуальне керування середовищем необслуговуваних укриттів.

У статті [39] розглядається малодосліджена проблема вразливості пасажирів громадського транспорту під час раптових повітряних атак. На відміну від традиційних моделей евакуації, що орієнтуються на населення у стаціонарних локаціях (житло, місце роботи та ін.), автори зосереджують увагу на мобільних групах громадян. На прикладі Харкова автори демонструють, що традиційні підходи до транспортного планування й моделі розміщення захисних укриттів існують окремо та не враховують вразливість людей у момент пересування або очікування транспорту. Науковці пропонують комплексну методику, яка об'єднує GIS-аналіз, ізохронне моделювання та класифікацію простору за поєднанням щільності зупинок і доступних укриттів. Метод враховує три критичні часові пороги (2, 5 та 15 хвилин), що відповідають «вікнам безпеки» для різних типів загроз (від балістичних ракет до повільних ударних дронів). Дослідження показало, що до початку війни лише біля 30% території Харкова були в межах 15-хвилинної доступності до укриття. Після розгортання мережі нових укриттів та модифікації транспортної системи цей показник зріс до 85–90 %, також зменшилась кількість зупинок, що не мають доступного укриття.

Більшість даних про укриття автори статті [39] отримали з офіційного ресурсу «Smart City GeoPortal», але вони не могли перевірити їхній фактичний стан. Якість укриття (вхід, місткість, герметичність) часто важливіша за його наявність, тому отримані результати можуть завищувати реальний рівень захищеності. Також відсутні дані про пасажиропотоки, тобто які зупинки мають високий ступінь ризику через концентрацію людей. Хоча загальний

рівень доступності укриттів зріс, навіть у центрі міста залишаються вразливі ділянки, особливо на трамвайних та автобусних маршрутах, периферійні ж райони Харкова відрізняються низькою доступністю як транспорту, так і укриттів, відповідно й більшою небезпекою для мешканців. Отже, міська безпека є просторово асиметричною й потребує диференційованих рішень, а не лише розширення міських укриттів. Також концепція обмежена відсутністю емпіричних спостережень реальної поведінки людей під час повітряних тривог, оскільки паніка, натовпи, темний час доби, небезпека уламків або зруйновані тротуари можуть значно зменшити радіус безпечної доступності. Як результат науковці пропонують тактичні і стратегічні кроки для зменшення ризиків, зокрема розміщення мобільних укриттів, інтеграцію транспортних і захисних норм у міське планування. Водночас варто зауважити, що більшість рекомендацій потребують значних інвестицій, стабільного енергопостачання та координації між відомствами, що в умовах війни є складним.

Отже, проведений аналіз наукових публікацій засвідчує, що нині існує доволі багато досліджень, в яких розглядаються проблеми проєктування, створення та підтримки функціонування захисних укриттів. Актуальність цих розвідок пов’язана зі збільшенням військової напруги у світі загалом, численними війнами та збройними конфліктами, техногенними катастрофами та природними катаклізмами. Науковці вивчають досвід країн, які приділяють увагу розбудові системи безпеки цивільного населення (наприклад, Швейцарія та Фінляндія), та на цій основі пропонують рекомендації для інших країн. Загалом, можна стверджувати, що така система повинна бути динамічною, достатньо гнучкою та оновлюваною для досягнення необхідного рівня безпеки в умовах нових загроз.

Стосовно системи захисних укриттів в Україні слід відзначити, що вона є недостатньо розгалуженою. Приміщення, споруджені у 20-му сторіччі не забезпечують належного рівня захисту від сучасної зброї, а в багатьох випадках знаходяться у стані, що не дозволяє їх експлуатувати. Отже, проблема оновлення цієї системи є надзвичайно актуальною.

1.2. Керування доступом до приміщень

Для вирішення завдань дослідження необхідно проаналізувати сучасні підходи до контролю й керування доступом до приміщень і на цій основі обрати варіант, який буде реалізовано як складову програмного комплексу. З цією метою нами вивчено наукові публікації, в яких розглядаються відповідні проблеми.

Контроль доступу є ефективним механізмом для розв'язання проблем приватності, безпеки та порушень доступу до приміщень. Його головна мета в системах типу «розумний будинок» – гарантувати, що ресурси доступні лише для авторизованих користувачів, даних і сервісів. Контроль доступу захищає систему, обмежуючи доступ легітимних користувачів відповідно до їхніх привілеїв та запобігаючи доступу неавторизованих осіб.

Існує декілька моделей контролю доступу, які можна застосувати в розумних будинках. Розглянемо їх [48, с. 909-910]:

1) Список контролю доступу (Access Control List, ACL).

Матриця контролю доступу була однією з перших технік керування доступом: її стовпці й рядки представляли об'єкти та суб'єкти, а кожен запис містив набір прав доступу для відповідного суб'єкта. Згодом був розроблений ACL – набір конкретних ресурсів, доступних лише визначеним користувачам згідно з їхніми привілеями.

2) Дискреційний контроль доступу (Discretionary Access Control, DAC).

Модель розроблена для систем і баз даних із багатокористувацьким середовищем. Доступ надається залежно від ідентичності користувача. Весь контроль над системою належить її власнику, який може надавати права іншим користувачам. Основний недолік – можливість отримання доступу нелегітимними користувачами.

3) Мандатний контроль доступу (Mandatory Access Control, MAC).

Кожен об'єкт має мітку, що визначає рівень його привілеїв, а кожен суб'єкт – мітку, що вказує, до яких об'єктів він має доступ. Користувачі мають

доступ лише до ресурсів відповідно до своїх службових обов'язків. Через статичність модель є недостатньо гнучкою та непридатною для динамічних середовищ, таких як розумні будинки.

4) Рольовий контроль доступу (Role-Based Access Control, RBAC).

Модель часто використовується в організаціях різного масштабу. Доступ до ресурсів ґрунтується на ролях користувачів. Доступні чотири ключові елементи: суб'єкти (користувачі), об'єкти (ресурси), ролі (набори дозволів) та операції (дії над ресурсами). Дозволи прив'язані до ролей, а користувачі отримують права відповідно до ролей, а не ідентичностей. Хоча користувач може мати декілька ролей, ця модель погано підходить для розумних будинків через брак контекстної обізнаності та динамічності.

5) Контроль доступу на основі можливостей (Capability-Based Access Control, CapBAC).

Модель реалізує децентралізований підхід, в якому рішення приймаються без залежності від центрального пристрою. Може працювати на достатньо потужних пристроях, але розумні будинки містять переважно ресурсообмежені пристрої, тому модель малопридатна.

6) Контроль використання (Usage Control, UCON).

Моделі ABAC та RBAC можуть змінювати атрибути тільки до або після запиту доступу, але не під час виконання доступу. UCON забезпечує більшу гнучкість завдяки додаванню обов'язкових умов, зовнішніх умов і змінних атрибутів, що можуть змінюватися під час використання ресурсу. Завдяки безперервній оцінці політик UCON може зупинити доступ у процесі його виконання, якщо права перестають бути чинними.

7) Контроль доступу на основі атрибутів (Attribute-Based Access Control, ABAC).

Це гнучкий, динамічний механізм, рішення в якому ґрунтується на атрибутах суб'єкта, об'єкта, ресурсів та контексту. Це дозволяє будувати складні, ситуаційно залежні правила. Завдяки гнучкості та контекстній

чутливості ABAC є найбільш придатною моделлю для авторизації в розумних будинках порівняно з традиційними рольовими підходами.

Дослідники М. Василенко та А. Загорна розробили комплексну систему безпеки офісного приміщення з використанням сучасних інформаційних технологій. У дослідженні [60] автори наводять опис інтегрованої моделі, що поєднує відеоспостереження, охоронну сигналізацію, контроль доступу та резервне живлення. Вони підкреслюють зростання ролі офісної безпеки у зв'язку зі зростанням загроз фізичного й кібернетичного характеру. Автоматизовані системи знижують рівень людських помилок та забезпечують можливість реагування в режимі реального часу. Розвиток відеоаналітики, біометрії та віддаленого доступу є ключовим чинником підвищення ефективності сучасних систем керування доступом.

Система організована так, щоб забезпечити автономність функціонування навіть при збоях основного електропостачання. До її складу входять такі компоненти [60, с. 64]:

1) Охоронна сигналізація: магнітні датчики, інфрачервоні сенсори, мікропроцесорна система, сирена.

2) Відеоспостереження: камери, сервер первинної обробки й детекції руху.

3) Контроль доступу: RFID-читачі, контролер замків, електромагнітні замки.

4) Резервне живлення: акумулятор, система управління літієвими батареями.

5) Головний сервер: ядро системи, що забезпечує централізоване керування та збір інформації.

Основні етапи функціонування системи [60, с. 66]:

1) Первинна перевірка стану датчиків вікон.

2) Автоматичне зачинення вікон за допомогою сервоприводів при ввімкненні охорони.

3) Перехід у режим охорони після підтвердження зачинення всіх вікон і дверей.

4) Реакція на будь-яке спрацювання датчиків руху або магнітних сенсорів: генерація сигналу тривоги; передача повідомлення на центральний сервер і до служби безпеки.

5) Безперервний відеозапис із зберіганням архіву за останній тиждень.

6) Перемикання на резервне живлення та повідомлення серверу про зміну стану.

Автори роблять висновок, що запропонована система забезпечить комплексний захист офісу, дозволить інтегрувати фізичні та інформаційні компоненти безпеки, підвищить надійність захисту завдяки резервному живленню, зменшить залежність від людського фактору.

Науковці Л. Рибак та П. Кравець у статті [22] досліджують шляхи вирішення проблеми підвищення ефективності систем контролю доступу в умовах розширення ринку «розумних» технологій та зростання потреби у надійних засобах захисту приміщень. На основі аналізу популярних систем SmartLock та Schlage Sense Smart Lock виявлено їхні недоліки, а саме: складність, висока вартість, уразливість до кібератак, залежність від сторонніх сервісів. Це дало підстави для формування вимог до нової системи, орієнтованої на автономність і підвищений рівень безпеки. Авторами розроблено інтелектуальну інформаційну систему «Розумний замок», засновану на технологіях розпізнавання облич та модульній архітектурі, придатній до інтеграції у сучасні системи «розумного дому». Програмний модуль розпізнавання облич реалізовано на основі бібліотек face_recognition та OpenCV. Серверна частина побудована з використанням фреймворку Flask і забезпечує обробку запитів, конфігурування пристрою та взаємодію з базою даних SQLite. Для апаратної реалізації системи застосовано одноплатний комп’ютер Raspberry Pi з під’єднаною камерою та електронним замком. Автори доводять, що запропоноване рішення може бути використане у

приватних домогосподарствах, офісах та підприємствах, а також у дослідницьких цілях – для тестування алгоритмів біометричної ідентифікації.

У статті [48] розглядається проблема контролю доступу в розумних будинках – динамічних, гетерогенних, багатокористувацьких системах, що містять різноманітні IoT-пристрої. Автори підкреслюють, що помилки авторизації можуть спричинити серйозні порушення приватності, витоки даних та небажане втручання. Сучасні огляди IoT безпеки рідко детально аналізують саме механізми доступу для смарт-домів, тому ця робота заповнює важливу прогалину.

Автори подають архітектуру розумного будинку у вигляді чотиришарової моделі: 1) фізичний рівень (датчики, актуатори, камери, замки, хаби); 2) мережевий рівень (канали зв'язку та протоколи); 3) проміжний рівень (шлюзи, обробка даних, маршрутизація); 4) прикладний рівень (сервіси та застосунки для користувача) [48, с. 908]. На основі аналізу основних моделей контролю доступу (ACL, DAC, MAC, RBAC, CapBAC, UCON, ABAC) вони роблять висновок, що ABAC та частково UCON є найбільш придатними для розумних домів завдяки гнучкості, контекстній обізнаності та можливості динамічної зміни політик. Науковці підсумовують, що сучасні моделі контролю доступу ще не здатні повністю задовольнити потреби розумних будинків, тому дослідження повинні зосередитися на створенні адаптивних і контекстно-обізнаних систем, мультикористувацьких і багатопристроєвих моделей, підтримці роботів та автоматизованих агентів, створенні гнучких фреймворків, що поєднують ABAC, UCON та сучасні технології (edge-cloud, blockchain, trust-based рішення).

Науковці S. Ameer, J. Benson та R. Sandhu [34] досліджують проблему побудови безпечних і гнучких механізмів контролю доступу в системах розумного будинку, де взаємодіють численні пристрої Інтернету речей, що використовуються різними категоріями користувачів. Вони доводять, що традиційні підходи до авторизації, зокрема ABAC та RBAC, є недостатньо адаптивними через високу динамічність домашнього середовища, змінні

контексти та різноманітні соціальні взаємозв'язки між користувачами. Автори пропонують нову модель атрибутивного контролю доступу HABACα, спеціально орієнтовану на пристрої IoT у системі розумного будинку. Модель використовує атрибути користувачів, пристроїв, операцій та станів середовища, що дає можливість формувати логічно складні, дрібнозернисті правила доступу. HABACα підтримує як статичні, так і динамічні атрибути, що дозволяє враховувати часові зміни, поведінкові параметри, місцеперебування та інші контекстуальні фактори.

У статті [36] наведено результати розробки та впровадження автоматизованої системи контролю доступу, що базується на технології розпізнавання облич та апаратному забезпеченні Arduino. Автори пропонують технічне рішення для вирішення проблеми некоректного контролю доступу в установах з кількома входами, зокрема в університетському середовищі. Дослідження зосереджене на побудові інтелектуальної біометричної системи, здатної автономно ідентифікувати осіб та керувати відкриттям дверей.

Автори виділили декілька проблем, що можуть бути вирішені завдяки впровадженню системи, а саме: фальсифікація документів, видавання себе за інших осіб, складність перевірки оплати академічних внесків, людський фактор і помилки при ручних перевірках [36, с. 12].

Дослідники виконали моделювання проєкту, створивши діаграму вимог, діаграму варіантів використання, діаграму підсистем, діаграму внутрішньої взаємодії блоків і потоків даних. На основі моделювання вони розробили програмну систему, яка складається з трьох модулів: підсистема біометричної реєстрації; підсистема верифікації (перевірки) особи; програма Arduino, що забезпечує фізичне відчинення / зачинення дверей на основі сигналів з комп'ютера.

Автори дослідження [38] розробили систему контролю доступу до приміщень на основі біометричної ідентифікації за відбитками пальців. Вони пропонують технічне рішення, що поєднує мікроконтролер, модуль сканування відбитків, систему оповіщення, індикаторний дисплей і

механізований дверний привід. Система реалізує автоматичне розпізнавання користувача, прийняття рішення щодо доступу та генерування сигналу тривоги у випадку виявлення неавторизованої спроби входу. Система об'єднує апаратні компоненти (трансформатор, випрямляч, реле, транзисторні ключі, Arduino/ATmega) та програмні модулі, що керують LCD-дисплеєм і біометричним датчиком. Отримані результати підтверджують працездатність та ефективність запропонованого прототипу, який може бути застосований для підвищення безпеки в житлових, офісних та промислових приміщеннях.

Науковці C. Stolojescu-Crisan, C. Crisan та B.-P. Butunoi у праці [57] досліджують застосування технологій Інтернету речей у розумних будинках та розглядають два рішення для автоматизації й безпеки: qToggle та MotionEyeOS. Автори наголошують, що зростання кількості IoT-пристроїв зробило розумні системи доступнішими, а потреба у віддаленому контролі, керуванні доступом і відеоспостереженні стала життєво важливою.

Рішення qToggle – це універсальна IoT-платформа для керування пристроями на базі ESP8266 і Raspberry Pi. Вона дозволяє відчиняти ворота й гараж, керувати сигналізацією та іншими системами через вебдодаток, що працює на будь-якому пристрої. Система легко розширюється, а її інсталяція не вимагає складної інфраструктури [57, с. 2-5]. Рішення MotionEyeOS – це операційна система для відеоспостереження, що перетворює Raspberry Pi на NVR-сервер або мережеву камеру, підтримує кілька сценаріїв розгортання і працює як із локальними, так і з IP-камерами. Система має зручний вебінтерфейс, підтримує детекцію руху, збереження відео та віддалений перегляд [57, с. 5-6]. Результати дослідження засвідчують, що бюджетні апаратні платформи можуть забезпечити надійне відеоспостереження, контроль доступу та домашню автоматизацію.

Отже, наразі є актуальним створення інтелектуальних систем безпеки, здатних поєднувати апаратні та програмні компоненти в єдиний комплекс, що працює автономно та забезпечує високу точність ідентифікації користувача. Вирішенню цього завдання присвячено багато публікацій українських і

закордонних науковців. У межах нашого дослідження поставлено інше завдання – автоматично надавати цивільному населенню доступ до захисних укриттів у випадку повітряної тривоги та автоматично зачиняти двері після того, як тривога скінчилася і приміщення звільнено. Його вирішення також потребує використання концепції Інтернету речей, оскільки також передбачається віддалене керування пристроями через мережу Інтернет.

1.3. Обґрунтування доцільності розробки програмного комплексу

Для вирішення завдань дослідження пропонується розробити програмний комплекс «Система керування доступом до захисних укриттів на основі пристроїв Akuvox», який складається з таких частин:

1) програма для пристрою інтерком-контролю доступу, що забезпечує керування відчиненням та зачиненням дверей відповідно до оповіщень тривоги або відбою тривоги, а також розсилку через телеграм-бот тимчасових PIN-кодів для відкриття дверей у випадку необхідності;

2) клієнтська частина – вебінтерфейс оператора системи для централізованого керування пристроями Akuvox;

3) серверна частина – програми та база даних, що забезпечують функціонування системи.

Проведемо *SWOT-аналіз* для оцінки доцільності розробки системи. Теоретичні основи та методику використання цього методу наведено у працях [5; 6; 10; 25]. Він призначений для аналізу внутрішнього (сильні й слабкі сторони) й зовнішнього (можливості та загрози) середовища досліджуваної системи, узагальнення наявної інформації та формування підґрунтя для подальшого прийняття управлінських рішень [6, с. 62].

В нашому випадку розглядається програмний комплекс і необхідно зробити висновок про доцільність його розроблення

1) Внутрішнє середовище:

1.1) Сильні сторони (S – Strengths):

- Система забезпечує швидке відчинення та зачинення дверей укриттів залежно від сигналів тривоги чи відбою повітряної тривоги без присутності персоналу. Це значно скорочує час доступу цивільного населення до укриття.

- Пристрої Akuvox мають стабільні інтерфейси API, підтримують сучасні протоколи безпеки та добре інтегруються в розподілені системи.

- Наявність вебінтерфейсу для оператора дозволяє централізовано керувати доступом, відстежувати статус укриттів, фіксувати події та здійснювати обслуговування.

- Наявність клієнтської (операторської) та серверної частини із системою ролей забезпечує контрольований доступ і захищеність.

- Автоматична розсилка тимчасових PIN-кодів підвищує гнучкість доступу, розвантажує персонал та мінімізує людський фактор.

- Серверна частина дозволяє масштабувати систему на необмежену кількість укриттів, зберігаючи централізоване управління.

1.2) Слабкі сторони (W – Weaknesses):

- Система прив’язана до конкретного виробника апаратури, що може бути обмежувальним фактором у закупівлях або модернізації.

- Робота системи залежить від наявності Інтернет-зв’язку та локальної мережі укриттів.

- Обмежена функціональність апаратних засобів Akuvox. Деякі сценарії взаємодії можуть бути обмежені API виробника, що потребуватиме додаткових обхідних рішень.

- Для високої надійності системи потрібні регулярні оновлення, аудит безпеки та резервування.

- Інтеграція багатьох компонентів (інтерком, сервер, Telegram-бот) може ускладнювати первинне впровадження.

2) Зовнішнє середовище:

2.1) Можливості (O – Opportunities):

- Через постійну потребу у швидкому доступі до укриттів система може стати стандартом для громадської безпеки.

- Можливе додавання відеоверифікації, журналів доступу з аналітикою, розпізнавання облич, інтеграції з міськими системами оповіщення.

- Створення українського програмного забезпечення зменшує залежність від іноземних продуктів і підтримує національну кібербезпеку.

- Рішення може стати продуктом для бізнесу: офіси, виробництва, освітні заклади, житлові комплекси тощо.

- Можливість інтеграції з іншими системами цивільного захисту.

2.2) Загрози (T – Threats):

- Як система критичної інфраструктури, вона може бути ціллю хакерських атак, тому потребує посиленого захисту.

- Зміни у протоколах або підтримці пристроїв можуть спричинити несумісність або потребу доробок.

- Відсутність живлення або Інтернету може блокувати роботу системи.

- На ринку вже є комерційні рішення, які можуть впроваджувати подібні системи, що створює конкурентний тиск.

SWOT-аналіз показує, що розробка програмного комплексу є доцільною, оскільки спрямована на вирішення актуального завдання оперативного та автоматизованого доступу до захисних укриттів, підвищує безпеку людей та знижує ризики, пов’язані з людським фактором. Сильні сторони та перспективи розвитку переважають слабкі місця, які здебільшого технічні й можуть бути усунуті або мінімізовані. Завдяки можливостям масштабування та інтеграції система має потенціал для впровадження в інфраструктуру цивільного захисту на місцевому та державному рівнях.

Аналіз стратегічних поєднань внутрішніх та зовнішніх факторів (табл. 1.1) показав, що система керування доступом до захисних укриттів на основі пристроїв Akuvox має значний потенціал для практичного застосування та подальшого розвитку.

Таблиця 1.1

Матриця SWOT-аналізу

	O – Можливості	T – Загрози
S – Сильні сторони	*SO-стратегії (використання сильних сторін для реалізації можливостей):* 1) Використовуючи автоматизовану реакцію на тривоги та масштабованість системи, впроваджувати рішення у громадах як частину цивільного захисту. 2) Завдяки інтеграції з Telegram та сучасному API Akuvox розширювати продукт аналітичними модулями та відеоверифікацією. 3) Завдяки модульній архітектурі пропонувати систему як комерційний продукт для бізнесу й житлового господарства.	*ST-стратегії (використання сильних сторін для мінімізації загроз):* 1) Використовувати захищені канали зв'язку та можливості обладнання Akuvox для зменшення ризиків кібератак. 2) Завдяки модульності швидко адаптувати систему до можливих змін API або політики виробника. 3) Забезпечити резервні сценарії роботи (локальний доступ, аварійні коди) використовуючи програмовані функції системи. 4) Підвищувати конкурентоспроможність через унікальні функції: Telegram-бот, аналітика доступу, централізований моніторинг.
W – Слабкі сторони	*WO-стратегії (усунення слабких сторін через використання можливостей):* 1) Використати підтримку громад та муніципалітетів для покращення інфраструктури зв'язку. 2) Розширювати власний модуль логіки для часткової компенсації обмежень обладнання Akuvox. 3) Залучати комерційні впровадження для фінансування технічної підтримки та оновлень. 4) Спрощувати початкове налаштування через створення інсталяторів, документації та автоматизованих конфігурацій.	*WT-стратегії (мінімізація слабких сторін та загроз одночасно):* 1) Впровадження резервних каналів зв'язку та кешування для зменшення залежності від мережі під час кризових ситуацій. 2) Розробка універсального проміжного шару, щоб уникнути прямої залежності від потенційно змінного API Akuvox. 3) Регулярний аудит безпеки та моніторинг для зменшення ризиків кібератак попри слабкі місця архітектури. 4) Автоматизація технічного обслуговування, щоб мінімізувати вплив людського фактору та потребу у ручному супроводі.

Комбінація сильних сторін із наявними можливостями свідчить про здатність системи ефективно масштабуватися, інтегруватися з іншими елементами інфраструктури цивільного захисту та перетворюватися на повноцінний інструмент забезпечення безпеки населення. Поєднання сильних сторін із потенційними загрозами демонструє, що система здатна мінімізувати ризики завдяки використанню захищених протоколів, можливості реалізації

резервних сценаріїв роботи та гнучкій адаптації до змін у політиці або API виробника обладнання. Це підвищує стійкість рішення у довгостроковій перспективі. Аналіз слабких сторін показує, що наявні обмеження можуть бути частково або повністю подолані завдяки використанню зовнішніх можливостей, зокрема шляхом поліпшення цифрової інфраструктури, розширення власної логіки керування та впровадження інструментів автоматизації конфігурації та технічного супроводу. Поєднання слабких сторін і загроз вказує на необхідність удосконалення безпекових та архітектурних аспектів: реалізації резервних каналів зв'язку, підвищення автономності роботи, впровадження регулярного аудиту безпеки та створення проміжного програмного шару для зменшення прив'язки до конкретного виробника. Такі заходи підвищать надійність системи в умовах зовнішніх ризиків.

Загалом, розробка є доцільною, обґрунтованою та здатною до масштабування. Наявні сильні сторони переважають слабкі, а запропоновані заходи дозволять успішно використовувати зовнішні можливості та ефективно протидіяти потенційним загрозам.

Проведемо *аналіз системи за моделлю п'яти сил Портера* [32; 53]. Модель дозволяє оцінити конкурентоспроможність програмного комплексу. Для системи, орієнтованої на автоматизоване керування доступом до укриттів, ключовими факторами є технологічні можливості, сумісність із обладнанням та відповідність актуальним безпековим потребам.

1) Сила конкуренції серед наявних компаній (інтенсивність конкуренції на ринку подібних програмних продуктів).

На ринку вже існують рішення з контролю доступу до приміщень (див. п. 2.1). Багато з них є комплексними та пропрієтарними, що включають як апаратне забезпечення, так і закрите програмне забезпечення. Однак спеціалізованих систем саме для автоматизації доступу до захисних укриттів майже немає, що створює конкурентну перевагу для даної розробки. Основні конкуренти – це інтегратори систем безпеки та виробники обладнання, які можуть запропонувати комплексні апаратно-програмні рішення. Проте такі

системи часто дорогі, недостатньо гнучкі та не орієнтовані безпосередньо на цивільний захист. Отже, ця сила має середній рівень впливу.

2) Загроза появи нових гравців.

Поріг входу у розробку програмного забезпечення відносно невисокий. Разом із тим, створення стабільних, надійних та сумісних з обладнанням рішень для критичної інфраструктури потребує глибокої експертизи. Наявність специфічного досвіду роботи з пристроями Akuvox та системами оповіщення про повітряні тривоги забезпечує додатковий захист від нових конкурентів. Однак зростання попиту на подібні системи може стимулювати появу інших розробників. Отже, рівень впливу: середній–високий.

3) Сила постачальників (вплив, який мають постачальники необхідних компонентів).

Ключовим постачальником у системі є виробник обладнання Akuvox. Залежність від їхніх інтеркомів, API та оновлень прошивок є суттєвим фактором ризику. Якщо політика компанії зміниться або підтримка API буде обмежена, це вплине на весь програмний комплекс. Також можливі перебої поставок обладнання через логістичні обмеження, зміни цін та ін. Висока залежність від одного постачальника збільшує вплив даної сили. Отже, рівень впливу: високий.

4) Сила покупців.

Кінцевими споживачами системи можуть бути органи місцевого самоврядування, заклади освіти, медичні та державні установи, приватні об’єкти з укриттями та ін. Ці споживачі зацікавлені у підвищенні безпеки, оперативному доступі до укриттів та автоматизації процесів. Їхня сила впливу помірна, оскільки альтернативні спеціалізовані рішення відсутні, але існують загальні системи контролю доступу, які можуть частково замінити функції комплексу. Однак споживачі часто мають обмежені бюджети, що робить більш привабними спеціалізовані рішення для конкретних задач. Отже, рівень впливу: середній.

5) Загроза товарів-замінників (наскільки легко клієнт може перейти на подібний продукт конкурента).

Існують альтернативні способи організації доступу до укриттів: ручне відкривання/замикання, системи контролю доступу інших виробників, механічні рішення без автоматизації. Однак вони не інтегруються з сигналами тривоги, мають більший вплив людського фактора, не забезпечують централізоване керування, не дають журналювання подій. Прямі замінники саме автоматизованої системи для укриттів практично відсутні, тому загроза помірна. Отже, рівень впливу: середній.

Таким чином, аналіз за моделлю Портера показує, що розробка має гарні перспективи для впровадження та розвитку, оскільки конкуренція у вузькому сегменті невисока, існує суспільна потреба в автоматизації доступу до укриттів, наявні аналоги мають іншу функціональність, система створює унікальну цінність за рахунок інтеграції з тривожними оповіщеннями та пристроями Akuvox. Водночас основними викликами залишаються залежність від постачальника обладнання та потенційна поява нових гравців на ринку.

Далі виконаємо *аналіз зацікавлених сторін (стейкголдерів)* для визначити всіх груп учасників, які мають вплив на проєкт або залежать від його результатів.

Основні групи стейкголдерів, що беруть участь у розробці, впровадженні та експлуатації системи:

1) Органи місцевого самоврядування (ОМС): відповідають за організацію цивільного захисту у громаді; зацікавлені в надійному доступі до укриттів та автоматизації процесів.

2) Керівники об’єктів (шкіл, лікарень, підприємств та ін.): приймають рішення щодо впровадження системи на локальному рівні; потребують інструменту для контролю доступу та безперебійної роботи укриттів.

3) Оператори системи (працівники, які взаємодіють із вебінтерфейсом): відповідають за моніторинг, ручне керування та контроль подій; зацікавлені у простоті інтерфейсу та мінімальному навантаженні під час тривог.

4) Технічні фахівці та ІТ-відділ: виконують налаштування обладнання Akuvox, інтеграцію та підтримку; зацікавлені у стабільності API, чіткій документації та зрозумілому логуванні.

5) Громада / користувачі укриттів: зацікавлені в гарантованому доступі до укриттів і відчутті безпеки.

6) Виробник обладнання Akuvox: постачає інтеркоми та API для їх керування; має вплив на технічні можливості та сумісність системи.

7) Розробники програмного комплексу: проєктують, реалізують та забезпечують розвиток системи; зацікавлені у зрозумілих вимогах і стабільному доступі до інфраструктури.

8) Державні служби цивільного захисту: можуть брати участь у координації оповіщення про тривоги; зацікавлені в інтеграції системи зі стандартами безпеки.

Для кожного стейкголдера визначено можливий рівень впливу на систему та зацікавленості в її використанні (табл. 1.2).

Таблиця 1.2

Оцінка рівня впливу та зацікавленості стейкголдерів

Стейкголдер	Рівень впливу	Рівень зацікавленості	Тип взаємодії з системою
Органи місцевого самоврядування	Високий	Високий	Керування, ухвалення рішень
Керівники об'єктів	Середній	Високий	Координація, впровадження
Оператори системи	Низький	Високий	Щоденна робота
Технічні фахівці та ІТ-відділ	Середній	Середній	Налаштування, підтримка
Громада / користувачі укриттів	Низький	Високий	Отримувачі послуг
Виробник обладнання Akuvox	Високий	Середній	Поставки, технічна сумісність
Розробники програмного комплексу	Високий	Високий	Реалізація та розвиток
Державні служби цивільного захисту	Середній	Середній	Потенційна інтеграція

На основі табл. 1.2 побудовано карту стейкголдерів за ступенем впливу на систему та зацікавленості в її використанні (рис. 1.1).

		Вплив		
		високий	**середній**	**низький**
Зацікавленість	**висока**	• Органи місцевого самоврядування • Розробники програмного комплексу	• Керівники об'єктів	• Оператори системи • Громада / користувачі укриттів
	середня	• Виробник обладнання Akuvox	• Технічні фахівці та IT-відділ • Державні служби цивільного захисту	
	низька			

Рис. 1.1. Карта стейкголдерів

Виходячи з цього, можна запропонувати таку стратегію взаємодії зі стейкголдерами:

1) Активно залучати органи місцевого самоврядування та керівників об'єктів до використання системи шляхом презентацій, тестування функціоналу, погодження вимог.

2) Забезпечувати технічну координацію роботи технічних фахівців, IT-відділів, розробників програмного комплексу шляхом надання технічної документації, протоколів інтеграції, рев'ю.

3) Забезпечувати інформаційну підтримку операторів системи шляхом навчання, підтримки, надання інструкцій.

4) Проводити моніторинг очікувань громади / користувачів укриттів шляхом забезпечення доступності укриттів.

5) Забезпечувати підтримку сумісності системи з обладнанням Akuvox шляхом узгодження API, тестування оновлень прошивок.

Отже, проведений аналіз засвідчує, що проєкт має широке коло зацікавлених сторін із різним рівнем впливу та потреб. Найбільший вплив на успіх системи мають органи місцевого самоврядування та керівники об'єктів, тоді як ключовими кінцевими бенефіціарами є громада / користувачі укриттів. Система повинна задовольняти вимоги технічних спеціалістів та бути сумісною з обладнанням Akuvox, що визначає стратегічні напрями її розвитку.

Проведемо *аналіз ризиків*, які можуть виникати у процесі експлуатації програмного комплексу та відповідно впливати на його конкурентоспроможність та затребуваність н ринку програмного забезпечення.

У процесі аналізу виокремлено 12 ключових ризиків (табл. 1.3), які можна об'єднати в такі групи: технічні ризики; інфраструктурні та експлуатаційні ризики; кібербезпекові ризики; організаційні ризики; правові та регуляторні ризики; ризики, пов'язані з постачальником обладнання.

Таблиця 1.3

Основні ризики системи та шляхи їх мінімізації

Ризик	Опис	Заходи з мінімізації
1) Втрата зв'язку з інтернетом або локальною мережею	Система може тимчасово не отримувати команди або дані	Локальні сценарії, резервні канали зв'язку, автономні таймери
2) Нестабільна робота API Akuvox або зміни в ньому	Оновлення прошивок, зміна протоколів	Постійне тестування, адаптивні інтеграційні модулі, контрактне API
3) Відключення електроенергії	Пристрої, інтеркоми та сервери втрачають живлення	Використання автономних джерел живлення, дублювання
4) Атаки на API чи сервер	Система може бути недоступною або скомпрометованою	Захист OWASP, WAF, шифрування, аудит безпеки
5) Несанкціонований доступ до укриттів або налаштувань	Зловмисник може відкрити двері або змінити конфігурацію	Мультифакторна автентифікація, ролі, логування дій
6) Збої в роботі серверної частини	Помилки програм, недостатнє тестування	Автоматичні тести, моніторинг, резервний сервер
7) Недостатня кваліфікація операторів	Помилки при роботі з вебінтерфейсом	Навчання, інструкції, спрощені UI-рішення
8) Збої пристроїв Akuvox	Несправність, деградація апаратної частини	Регламентне обслуговування, резервні пристрої
9) Витік персональних даних	Доступ до логів, користувачів, журналів	Шифрування бази даних, доступи по ролях, аудит
10) Невідповідність законодавству щодо цивільного захисту	Неправильна обробка тривог або доступів	Узгодження з нормами ДСНС, періодична перевірка
11) Кіберризики тривожних систем (фейкові тривоги)	Автоматичне відкриття укриттів за підробленим сигналом	Перевірка джерел сигналу, цифрові підписи
12) Людський фактор у конфігурації або експлуатації	Неправильні налаштування, несвоєчасне оновлення	Документація, інструкції, регламент управління змінами

На основі табл. 1.3 побудовано матрицю ризиків за ступенем ймовірності реалізації події та впливом на функціонування та використання програмного комплексу (рис. 1.2).

		Вплив		
		високий	**середній**	**низький**
Ймовірність	**висока**	• Відключення електроенергії.		
	середня	• Втрата зв'язку з інтернетом або локальною мережею. • Нестабільна робота API Akuvox або зміни в ньому. • Атаки на API чи сервер. • Несанкціонований доступ до укриттів або налаштувань	• Недостатня кваліфікація операторів. • Людський фактор у конфігурації або експлуатації.	
	низька	• Збої в роботі серверної частини. • Витік персональних даних. • Кіберризики тривожних систем (фейкові тривоги).	• Збої пристроїв Akuvox. • Невідповідність законодавству щодо цивільного захисту.	

Рис. 1.2. Матриця ризиків системи

Аналіз ризиків демонструє, що програмний комплекс працює в умовах підвищеної важливості та залежить як від технічної інфраструктури, так і від якісної експлуатації. Найбільш критичними є ризики, пов'язані з електропостачанням, мережами та стабільністю API. Усі ці ризики можуть бути зменшені шляхом резервування, кіберзахисту, правильної експлуатації та документованих процедур.

Отже, результати SWOT-аналізу, аналізу за моделлю п'яти сил Портера, аналізу зацікавлених сторін та аналізу ризиків дозволяють стверджувати, що розробка та впровадження системи керування доступом до захисних укриттів на основі пристроїв Akuvox є актуальною та доцільною. Очікується, що програмний комплекс буде затребуваний громадами, органами місцевого самоврядування, а також підприємствами та установами, які мають на утриманні захисні укриття, оскільки дозволить автоматизувати процеси керування доступом до укриттів у періоди повітряних тривог та без них.

РОЗДІЛ 2
ПРОЄКТУВАННЯ СИСТЕМИ КЕРУВАННЯ ДОСТУПОМ ДО ЗАХИСНИХ УКРИТТІВ НА ОСНОВІ ПРИСТРОЇВ AKUVOX

2.1. Огляд аналогів

У процесі дослідження проаналізовано програмні продукти, які можна розглядати як аналоги системи, що підлягає розробці. Зауважимо, що повних аналогів нами не було виявлено у відкритих Інтернет-джерелах.

Система керування дверима ZKBioBL (компанія ZKTeco, Китай) дозволяє контролювати і адмініструвати доступ до приміщень за допомогою мобільного додатку.

Основні можливості програми: відчинення / зачинення дверей через мобільний додаток; керування користувачами (додавання / видалення користувачів, редагування прав, створення груп, налаштування часових обмежень доступу для груп або окремих користувачів); перегляд історії (хто, коли, яким методом відчиняв / зачиняв); підтримка пароля без необхідності Bluetooth-ідентифікації; захист додатку через пароль суперкористувача. Рішення може використовуватися власниками приватних помешкань, бізнес-приміщень, малим бізнесом або організаціями, де потрібне просте рішення з керуванням доступом до дверей без складних систем контролю [28].

Рішення має обмеження, які слід враховувати при його виборі для обладнання приміщень, зокрема: залежність від смартфона (якщо немає телефону або зарядного пристрою, можуть виникнути ускладнення); потрібно виконувати налаштування, що потребує часу й уваги; безпека (потрібно дбати про надійні паролі, оновлення додатку, безпечні мережі тощо); інтеграція (якщо в будівлі вже встановлена система контролю доступу, потрібна додаткова інтеграція або апаратна підтримка) [28].

Програмне забезпечення BAS-IP Link (BAS-IP Ltd., Велика Британія) є серверною платформою для централізованого управління домофонним і контрольним обладнанням BAS-IP. Система забезпечує віддалену конфігурацію пристроїв, адміністрування доступу користувачів, обробку ідентифікаторів, журналювання подій і телефонію. Продукт призначений для житлових комплексів, бізнес-центрів, котеджних містечок та інших об'єктів з розгалуженою інфраструктурою доступу. [2].

Основні можливості рішення: система користувачів з ролями (адміністратор, менеджер, мешканець), кожна з яких має свій набір прав; керування об'єктами (комплексами), створення груп, призначення прав для різних груп користувачів; гнучке налаштування правил доступу (розклади, часові обмеження, прив'язка до користувачів); гостьовий доступ (мешканець або адміністратор може дати доступ гостю на певний час або кількість проходів); підтримка ідентифікаторів, зокрема фото мешканців; серверне керування допуском (панель виклику не зберігає дані локально, а звертається до сервера); централізоване керування пристроями (додавання, налаштування, оновлення, резервне копіювання); вбудований сервер телефонії для відеодзвінків, відчинення замків, телефонної книги, переадресації викликів; журнали та аудит (фіксація всіх подій) [2].

До переваг рішення можна віднести універсальність (підтримується робота на різних пристроях); масштабованість; безпека (реалізовані резервне копіювання, централізоване керування, серверне керування); простота для мешканців; адміністрування й контроль (система логування дозволяє відстежувати всі дії). Разом із тим, рішення має й обмеження, які слід враховувати: система передбачає певний рівень технічної підготовки, що для невеликих об'єктів може бути надлишковим; потрібно чітко прописати ролі, щоб уникнути помилок у доступі; система підтримує гостьовий доступ, але керування ним може потребувати додаткових процедур [2].

Отже, BAS-IP Link – це потужне рішення для комплексного керування системами доступу та домофонією, що особливо підходить для житлових

комплексів, які прагнуть цифровізувати контроль доступу. Платформа технічно зріла, масштабована, дозволяє детально контролювати всі події й доступи, забезпечує безпеку та зручність адміністрування. Водночас її повноцінне використання потребує якісної інфраструктури та кваліфікованого обслуговування.

Застосунок TTLock (Hangzhou Sciener Smart Technology Co., Китай) – це програмне рішення для комплексного керування інтелектуальними електронними замками різних типів, зокрема дверними, навісними, сейфовими, велосипедними та паркувальними. Програма забезпечує обмін даними між мобільним пристроєм та замком через Bluetooth, а за наявності шлюзу також через мережу Wi-Fi.

Після встановлення та реєстрації користувач отримує доступ до персонального облікового запису, який захищається за допомогою верифікації та секретних запитань. Додавання замка до системи здійснюється в безпосередній близькості до нього, після чого користувач набуває прав адміністратора. Адміністратор має можливість оновлювати прошивку замка, проводити діагностику, калібрувати час, керувати налаштуваннями та передавати права доступу іншим користувачам.

TTLock дозволяє створювати та надсилати електронні ключі із різними типами обмежень (постійні, тимчасові, разові та циклічні). Система підтримує роботу з кодовими паролями різних типів і призначення, включно з паролями очищення та індивідуальними, а також дає змогу додавати й використовувати IC-картки та відбитки пальців (за наявності відповідних модулів замка).

Функціонал розблокування включає відкриття дверей через мобільний застосунок, дотиком до клавіатури замка або віддалено через шлюз. Для бізнес-середовища передбачено модуль керування відвідуваністю, який дозволяє обліковувати прихід і вихід співробітників, налаштовувати робочі графіки, а також переглядати детальну статистику та звіти.

У системних налаштуваннях користувач може організовувати групи ключів, налаштовувати розблокування дотиком, переглядати інформацію про

застосунок та отримувати клієнтську підтримку. Окремим блоком передбачено управління шлюзами, через які забезпечується інтеграція замків у мережеву інфраструктуру та реалізується дистанційне керування, читання історії подій і передавання прав доступу.

Загалом TTLock надає широкий спектр інструментів для централізованого, безпечного та гнучкого керування смарт-замками, що робить його придатним як для побутового використання, так і для корпоративних та орендних систем доступу [27].

Schlage Home App (Schlage, США) – це мобільний застосунок, призначений для віддаленого керування розумними замками Schlage. Він дозволяє користувачу контролювати стан дверей, замикати чи відмикати їх у будь-який момент через смартфон, а також отримувати сповіщення про всі події, пов'язані з доступом. Додаток підтримує створення та керування індивідуальними кодами доступу, зокрема тимчасовими або періодичними. Усі дії фіксуються в журналі подій, завдяки чому власник може бачити, хто саме користувався замком і коли. Застосунок працює з різними моделями Wi-Fi та Bluetooth замків Schlage і може бути інтегрований з різними платформами розумних будинків. Керування кількома замками або кількома об'єктами здійснюється з єдиного інтерфейсу, що робить систему гнучкою і масштабованою. Загалом, Schlage Home App забезпечує сучасний підхід до домашньої безпеки, дозволяючи керувати доступом без фізичних ключів, отримувати актуальні сповіщення та налаштовувати зручні сценарії використання за допомогою смартфона [56].

Рішення Akuvox Smart Access (Akuvox, Китай) для малого та середнього бізнесу – це хмарна система контролю доступу, яка поєднує функціональність корпоративного рівня з простотою впровадження та обслуговування. Платформа дозволяє централізовано керувати доступом до дверей, приміщень і окремих об'єктів у реальному часі без потреби у власних серверах або складній IT-інфраструктурі.

Система підтримує різні методи ідентифікації: мобільний доступ, NFC/RFID-карти, Bluetooth, QR-коди та розпізнавання обличчя. Управління здійснюється через вебінтерфейс або мобільний застосунок, де адміністратор може додавати користувачів, налаштовувати права доступу та переглядати події. Платформа добре масштабована: до неї легко підключати нові пристрої, двері або локації. Завдяки хмарній архітектурі система отримує автоматичні оновлення та не потребує постійного втручання технічних фахівців.

Рішення орієнтоване на різні типи комерційних об'єктів (офіси, магазини, навчальні заклади, медичні установи, склади, коворкінги). Використання обладнання Akuvox забезпечує стабільну роботу, сучасний дизайн пристроїв та високий рівень безпеки. Отже, Akuvox Smart Access надає доступ до гнучкої, надійної та економічно вигідної системи контролю доступу з можливістю повного дистанційного керування та швидкого розширення у випадку зростання потреб [33].

Узагальнимо наведену вище інформацію (табл. 2.1).

Таблиця 2.1

Порівняння програмних рішень за функціональністю

Функція	ZKBioBL [28]	BAS-IP Link [2]	TTLock [27]	Schlage Home App [56]	Akuvox Smart Access [33]
Відкриття дверей через смартфон	Bluetooth / Wi-Fi	Bluetooth / інтерком	Bluetooth / Wi-Fi	Wi-Fi / Bluetooth	Bluetooth / NFC / хмара
Генерація тимчасових кодів	+	-	+	+	+ (переважно цифрові ключі)
Віддалене управління через хмару	Частково	+ (через сервер)	+ (через шлюз)	+	+ (повноцінно)
Підтримка домофону / інтеркому	-	+ (повноцінно)	-	-	+ (повноцінно)
Відеодзвінки з панелі	-	+	-	-	+
Управління кількома дверима	+	+	+	Обмежено	+ (масштабовано до бізнес-рівня)
Логи подій (історія відкриттів)	+	+	+	+	+ (деталізовано)
Розподіл прав доступу	Базово	Ролі, різні рівні	Гостьовий доступ	Гостьові коди	Гнучкі ролі, групи

Продовження табл. 2.1

Функція	ZKBioBL [28]	BAS-IP Link [2]	TTLock [27]	Schlage Home App [56]	Akuvox Smart Access [33]
API / інтеграції	Обмежені	API через Link Server	API в деяких моделях	Обмежено	+ (відкриті API для інтеграції)
Пуш-сповіщення	+	+	+	+	+
Робота з офлайн-замками	+ (Bluetooth)	Частково	+ (Bluetooth)	+ (Bluetooth)	Частково
Масштабованість (будинок → бізнес)	Низька – середня	Середня	Середня	Низька	Висока

Джерело: [2; 27; 28; 33; 56].

Наведемо порівняльну характеристику розглянутих платформ для організації систем електронного доступу:

1) Призначення та область застосування:

- ZKBioBL – мобільний застосунок для замків і контролерів компанії ZKTeco, що орієнтується переважно на невеликі об’єкти та індивідуальних користувачів. Система забезпечує базові функції керування доступом та генерування тимчасових кодів, але має обмежену масштабованість, характерну для рішень, прив’язаних до конкретної лінійки обладнання.

- BAS-IP Link призначений для комплексних систем домофонії та контролю доступу. Рішення орієнтовано на житлові комплекси, офісні будівлі та комерційні об’єкти, де використовується багатокомпонентна інфраструктура (інтерком, викликові панелі, контролери, Bluetooth-модулі).

- TTLock – універсальна комерційна платформа, що підтримує широкий спектр Bluetooth- та Wi-Fi-замків різних виробників. Система підходить як для приватного використання, так і для малих комерційних об’єктів.

- Schlage Home App – це фірмовий застосунок для розумних замків бренду Schlage. Платформа орієнтована на приватний житловий сектор і пропонує розширений функціонал для індивідуальних користувачів, але не призначена для масштабного корпоративного адміністрування.

- Akuvox Smart Access – хмарна платформа для бізнес-рівня та житлових комплексів. Система підтримує інтерком, смартфонний доступ,

цифрові ключі, віддалене хмарне адміністрування та інтеграцію з іншими компонентами систем безпеки. Має високий потенціал масштабування.

2) Функціональні можливості:

Усі системи забезпечують виконання базових операцій: відчинення дверей зі смартфона та перегляд історії подій. Відмінність між платформами полягає у рівні гнучкості та наборах додаткових функцій.

- ZKBioBL підтримує Bluetooth-відкриття, створення тимчасових кодів доступу, передачу «мобільних ключів» і базове управління користувачами. Функціонал призначений для замків ZKTeco та не передбачає глибоких інтеграцій з домофонними системами.

- BAS-IP Link забезпечує розширений функціонал, включно з прийомом відеовикликів, керуванням інтеркомом, відчиненням замка по Bluetooth та інтелектуальним маршрутом виклику. Додаток працює у зв'язці з Link-сервером і інтегрується з усіма пристроями BAS-IP.

- TTLock дозволяє створювати гостьові, періодичні, одноразові та офлайн-коди доступу. Платформа має вебпанель, API, а також можливість керування багатьма незалежними замками.

- Schlage Home App забезпечує керування замками, створення постійних і тимчасових кодів, інтеграцію з платформами «розумного дому». Функціонал обмежений контролем дверей у житлових приміщеннях.

- Akuvox Smart Access включає хмарне налаштування користувачів, цифрові ключі, QR-доступ, інтеграцію з домофонією, ведення журналів, управління кількома об'єктами та адміністрування великої кількості дверей. Платформа підтримує API і легко інтегрується у складні інженерні системи.

3) Інфраструктура та вимоги до розгортання:

- Schlage Home App та TTLock є найпростішими у впровадженні – вони не потребують серверів та працюють напряму з Wi-Fi/Bluetooth-замками.

- ZKBioBL також використовує безпосередній зв'язок із замками, але його розгортання залежить від конкретних моделей обладнання ZKTeco та їхньої конфігурації.

- BAS-IP Link вимагає встановлення Link-сервера, що забезпечує маршрутизацію викликів та управління домофонною інфраструктурою. Такий підхід підвищує функціональність, але потребує системного адміністрування.

- Akuvox Smart Access працює у хмарному середовищі та потребує підключення пристроїв Akuvox до мережі з доступом до Інтернету. Окремий сервер на об'єкті не потрібен, проте потрібне комплексне налаштування інфраструктури.

4) Масштабованість та можливість інтеграції:

- Akuvox Smart Access та BAS-IP Link мають найвищий потенціал масштабування, оскільки забезпечують централізоване керування десятками або сотнями точок доступу та підтримують інтерком.

- TTLock пропонує середній рівень масштабованості, орієнтований на невеликі готельні мережі або приватні об'єкти з багатьма замками.

- ZKBioBL обмежується масштабуванням у межах лінійки ZKTeco.

- Schlage Home App не передбачає корпоративного адміністрування й підходить лише для індивідуального користування.

Отже, усі розглянуті програмні рішення пропонують засоби для керування доступом до приміщень і можуть бути використані на об'єктах різного рівня. Проте, вони не вирішують завдань, поставлених у нашому дослідженні, а саме керування доступом до захисних укриттів на основі даних про повітряні тривоги.

2.2. Технічне завдання на розробку системи керування доступом до захисних укриттів на основі пристроїв Akuvox

І. Загальна інформація про проєкт.

Назва проєкту: Система керування доступом до захисних укриттів на основі пристроїв Akuvox.

Мета проєкту: Розробити веборієнтовану систему з централізованим керуванням захисними укриттями.

Галузь застосування: система використовується диспетчерськими та оперативними службами, що здійснюють контроль доступу до укриттів, обладнаних пристроями Akuvox.

Система повинна виконувати такі основні функції:

- відчиняти та зачиняти двері захисних укриттів через API пристроїв Akuvox;
- реагувати на сигнали повітряної тривоги та відбою тривоги;
- керувати доступом користувачів згідно з ієрархією ролей;
- вести журнал подій;
- надсилати повідомлення через Telegram;
- здійснювати моніторинг стану пристроїв та вчасно вирішувати проблеми, що виникають.

II. Архітектура системи.

Система складається з таких частин (рис. 2.1):

1) програма для пристрою інтерком-контролю доступу, що забезпечує керування відчиненням та зачиненням дверей відповідно до оповіщень тривоги або відбою тривоги, а також розсилку через телеграм-бот тимчасових PIN-кодів для відкриття дверей у випадку необхідності;

2) клієнтська частина – вебінтерфейс оператора системи для централізованого керування пристроями Akuvox;

3) серверна частина – програми та база даних, що забезпечують функціонування системи.

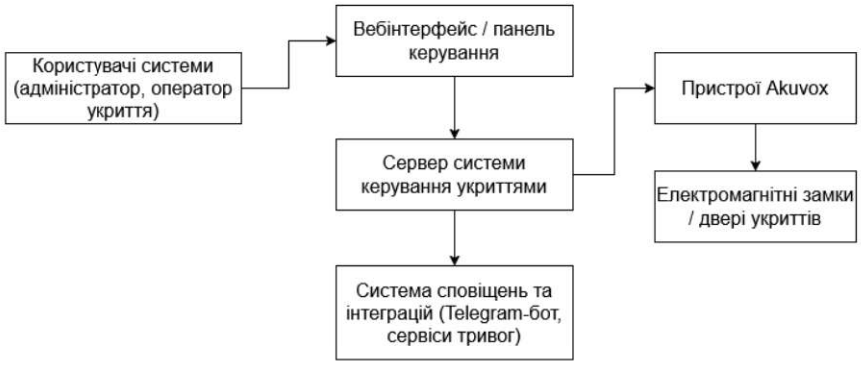


Рис. 2.1. Діаграма взаємодії системи керування доступом до захисних укриттів з пристроями Akuvox

Розробка та функціонування системи забезпечується використанням стеку технологій:

- серверна частина (backend): фреймворк Laravel 9 (PHP 8.1);
- клієнтська частина – вебінтерфейс оператора системи (frontend): адаптивна верстка, стек HTML / CSS / JavaScript;
- зберігання даних: СКБД MySQL 8 для основних даних; FileDB для логування понад 5 ГБ;
- Telegram Bot API – для розсилки повідомлень через Telegram бота;
- Akuvox API (через HTTP GET-запити) – для керування пристроями Akuvox.

Компоненти системи взаємодіють таким чином (рис. 2.2). З вебінтерфейсу оператора системи відправляються запити до серверної частини, яка взаємодіє з Akuvox API, СКБД MySQL та Telegram Bot API. Через Akuvox API реалізується збирання інформації про поточний стан входів до укриттів (відчинено / зачинено / наявні проблеми) для відображення у вебінтерфейсі та відправлення інформації про події до бази даних. З бази даних до Telegram Bot API відправляються тимчасові PIN-коди доступу, а також повідомлення про стан пристрою (онлайн / офлайн). Журнал подій формується на основі інформації з БД MySQL і зберігається у файловій базі даних FileDB.

III. Функціональні вимоги до системи керування доступом до захисних укриттів через пристрої Akuvox.

Вимоги до модулю авторизації та доступу:

- система повинна підтримувати авторизацію користувачів через токени сесії (Laravel Sanctum);
- система повинна здійснювати автентифікацію за логіном та паролем;
- система повинна реалізовувати рольову модель доступу (RBAC) з трьома рівнями ролей: супер-адміністратор, адміністратор, користувач;

- система повинна здійснювати перевірку прав доступу до дій і ресурсів через політики (UserPolicy, DevicePolicy);

- користувачі з нижчими ролями не повинні мати можливості виконувати дії, заборонені їхнім рівнем доступу.

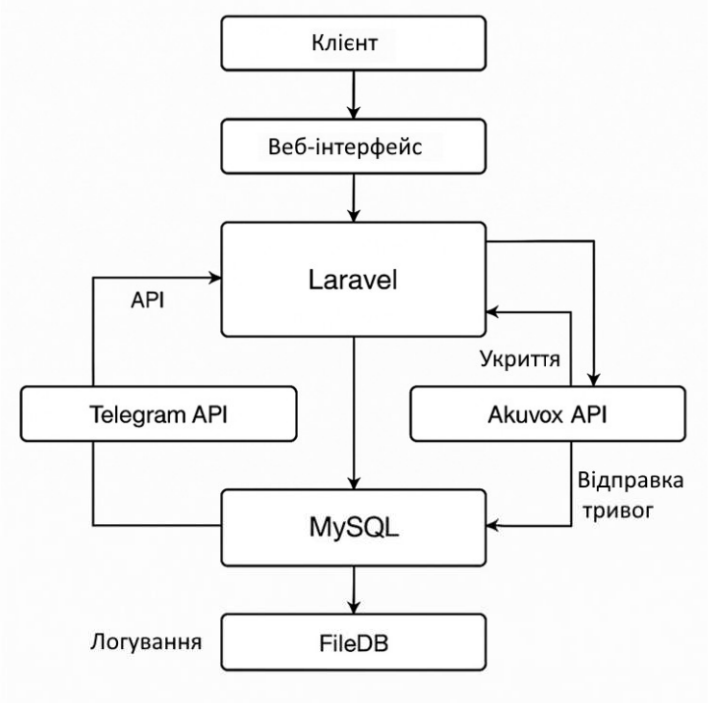


Рис. 2.2. Блок-схема взаємодії компонентів системи

Вимоги до модулю керування користувачами:

- система повинна забезпечувати CRUD-функціональність для керування користувачами;

- інформація про користувачів повинна зберігатися в таблиці бази даних з полями: name (ім’я користувача); email (адреса електронної пошти); password_hash (пароль); role (права); creator_id (ідентифікатор адміністратора, який створив запис); notes (додаткова інформація); created_at (дата і час створення запису);

- система повинна дозволяти супер-адміністратору й адміністратору створювати нових користувачів;

- система повинна забезпечувати зміну ролей користувачів відповідно до ієрархії;

- система повинна вести журнал створення та змін користувачів.

Вимоги до модулю керування пристроями Akuvox:

- система повинна забезпечувати CRUD-функціональність для пристроїв;

- інформація про пристрої повинна зберігатися в таблиці бази даних з полями: http_api (рядок для підключення до пристрою за допомогою API); type (тип укриття); location (адреса укриття); housing_office (власник укриття); provider (постачальник послуг Інтернет); contract; phone; admin_id (ідентифікатор адміністратора укриття);

- система повинна забезпечувати можливість надсилання команд на пристрої через Akuvox API (HTTP GET);

- система повинна відображати актуальний статус пристроїв (онлайн / офлайн);

- при переході пристрою в офлайн система повинна надсилати відповідне повідомлення в Telegram.

Вимоги до модуля тривог:

- система повинна приймати сигнали тривоги через webhook від зовнішнього сервісу тривог;

- після отримання сигналу тривоги система повинна автоматично: відчиняти двері укриттів, надсилати відповідні сповіщення в Telegram, фіксувати подію в журналі.

- система повинна підтримувати автоматичне зачинення дверей після скасування тривоги;

- вебінтерфейс оператора системи має відображати статус «тривога / відбій» у режимі реального часу.

Вимоги до модулю логування:

- система повинна вести два типи логів: журнали подій користувачів (у MySQL), журнали доступу та станів пристроїв (у FileDB, формат JSON);

- система повинна забезпечувати можливість перегляду логів у вебінтерфейсі оператора системи;

- логи повинні містити: час події, тип події, суб'єкт події (користувач / пристрій), результат операції;

- система повинна підтримувати зберігання великих обсягів логів (понад 5 ГБ) через FileDB;

- система має запобігати видаленню логів без прав супер-адміністратора.

Вимоги до Telegram-модуля:

- система повинна надсилати тимчасовий PIN-код доступу до укриття користувачам з використанням Telegram-бота при активації тривоги на випадок, якщо двері не було відчинено автоматично;

- система має надсилати службові повідомлення в Telegram, зокрема: пристрій перейшов у стан онлайн; пристрій перейшов у стан офлайн; відчинення / зачинення дверей;

- Telegram-бот повинен працювати як на основному сервері, так і на резервному.

IV. Вимоги до резервування та відмовостійкості.

Архітектура системи оповіщення про повітряні тривоги з резервуванням на основі двох серверів (рис. 2.3):

1) Система повинна підтримувати роботу двох серверів: головного та резервного.

2) Загальний сервер повітряних тривог відправляти команди на обидва сервери одночасно.

3) Головний сервер обробляє команди в нормальному режимі.

4) Якщо головний сервер не відповідає або неактивний, резервний сервер виявляє проблему (через «перевірку стану»). Далі активується резервне реагування й резервний сервер бере на себе контроль всіх операцій.

5) Перемикання на резервний сервер має виконуватися без втрати критичної функціональності.

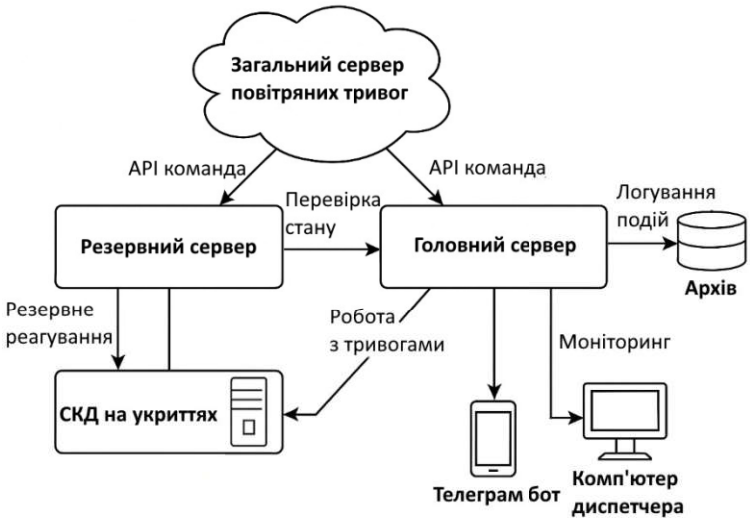


Рис. 2.3. Архітектура системи оповіщення про повітряні тривоги з резервуванням на основі двох серверів

V. Інтеграційні вимоги:

- система повинна працювати з Akuvox API через HTTP GET-запити;
- система повинна інтегруватися з Telegram Bot API;
- система повинна приймати тривожні сигнали від зовнішнього API через webhook;
- система повинна підтримувати внутрішній API для взаємодії між серверами.

VI. Вимоги до клієнтської частини системи.

Призначення вебінтерфейсу оператора системи:

- моніторинг технічного стану укриттів у режимі реального часу;
- супроводження процесу усунення проблем.

Основні функції вебінтерфейсу оператора системи:

- керування користувачами та пристроями;
- відображення станів у вигляді інтерактивної карти-сітки за кольоровою моделлю;
- пошук укриттів;
- ручне взяття проблем у роботу;
- відображення технічних даних щодо кожного входу в укриття;

- відображення журналу подій.

Користувачі системи: адміністратори укриттів – оператори системи.

Обмеження та залежності:

- система залежить від актуального каналу зв'язку з пристроями Akuvox;
- частота оновлення даних визначається API серверної частини;
- функціонування системи вимагає постійного Інтернет-з'єднання.

Вимоги до панелі керування користувачами:

1) Панель призначена для перегляду списку користувачів та інформації про одного користувача, створення та редагування записів користувачів.

2) Панель повинна містити поле для пошуку користувача за іменем.

3) Панель повинна містити список користувачів у форматі таблиці з полями:

- Ім'я – прізвище, ім'я та, батькові користувача;
- Права – показує тип прав «Користувач» або «Адміністратор»;
- Дата створення – дата створення облікового запису;
- Створив – інформація про користувача, який створив цей обліковий запис;
- Пристрої – інформація про доступні для цього облікового запису пристрої;
- Примітка – додаткова інформація про користувача (не обов'язково);
- Кнопки керування записом: відобразити / приховати, редагувати, видалити.

4) Панель повинна містити кнопку «Додати користувача або адміна», яка відкриває сторінку для створення облікового запису нового користувача.

Вимоги до панелі керування пристроями:

1) Панель призначена для перегляду списку пристроїв та інформації про обраний пристрій, а також створення й редагування записів пристроїв.

2) Панель повинна містити таблицю з полями:

- http_api – рядок для підключення до пристрою за допомогою API;

- Розташування – адреса фізичного розташування пристрою;
- Дата створення – дата додавання пристрою до системи моніторингу;
- Адмін – адміністратор, який може керувати цим пристроєм;
- Кнопки керування записами: редагувати, видалити.

3) Панель повинна містити поле для пошуку пристрою за розташуванням.

4) Панель повинна містити та кнопку «Додати пристрій», яка відкриває сторінку для занесення інформації про новий пристрій з такими полями:

- http_api – рядок для підключення до пристрою за допомогою API;
- Тип укриття – інформація про тип укриття;
- Адреса пристрою – інформація про фізичне розташування пристрою;
- ЖЕК – заповнюється, якщо пристрій перебуває на балансі ЖЕКу;
- Провайдер – інформація про провайдера, що надає доступ до Інтернету для вибраного пристрою;
- Договір – номер договору з провайдером Інтернету;
- Номер телефону – номер телефону технічної підтримки Інтернет провайдера
- Адміністратор – можливість вибрати користувача, що може керувати цим пристроєм.

Вимоги до головного екрану.

Головний екран повинен містити:

1) Поле «Пошук» – для пошуку потрібного пристрою у списку за розташуванням.

2) Список пристроїв у системі з можливістю прокрутки.

3) Рядок «Тривога» або «Відбій» в залежності від наявності або відсутності повітряної тривоги.

4) Рядок «Оператор», де вказано поточного користувача системи.

5) Поле «Журнали» з індикацією:

- «Червоний дзвінок» та «Червоний замок» разом означають, що розпочалася повітряна тривога, але двері укриття не були успішно відчинені;

- «Червоний дзвінок» та «Зелений замок» разом означають, що розпочалася повітряна тривога, двері укриття були успішно відчинені;

- «Зелений дзвінок» та «Зелений замок» разом означають, що повітряна тривога закінчилася, двері укриття були успішно зачинені;

- «Зелений дзвінок» та «Червоний замок» разом означають, що повітряна тривога закінчилася, але двері укриття не були успішно зачинені;

- «Зелена галочка» означає, що пристрій онлайн та все працює нормально;

- «Червоний хрестик» означає, що пристрій не онлайн та з ним втрачено зв'язок.

6) Список «Проблемні укриття» для відображення пристроїв, що недоступні, з можливістю прокрутки. При натисканні на проблемне укриття відобразити на центральному екрані цей пристрій.

7) Полотно для відображення всіх укриттів у вигляді кіл:

7.1) Кожне коло відповідає одному укриттю.

7.2) Коло автоматично змінює колір в залежності від таких факторів:

- Червоний колір – пристрій недоступний, PIN-код недійсний;
- Фіолетовий колір – пристрій взято в роботу;
- Помаранчевий колір – пристрій недоступний, PIN-код дійсний;
- Зеоений колір – все добре.

8) Кнопки керування укриттями:

- «Відкрити» – ручне відкриття дверей укриття з інтерфейсу програми;
- «Закрити» – ручне закриття дверей укриття з інтерфейсу програми;
- «Взяти в роботу» – при недоступності пристрою оператор може викликати спеціалістів для усунення несправностей, натиснувши цю кнопку. Дія записується в логах;
- «Перевірка» – перевірити доступність пристрою з інтерфейсу програми.

9) Панель «Показники обраного укриття», де відображуються характеристики укриття при натисканні на відповідне коло: Тип укриття;

Адреса; Відповідальний; Провайдер; Поточний стан; Пін-код панелі; Взяв в роботу.

Макет інтерфейсу головного екрану наведено на рис. 2.4.

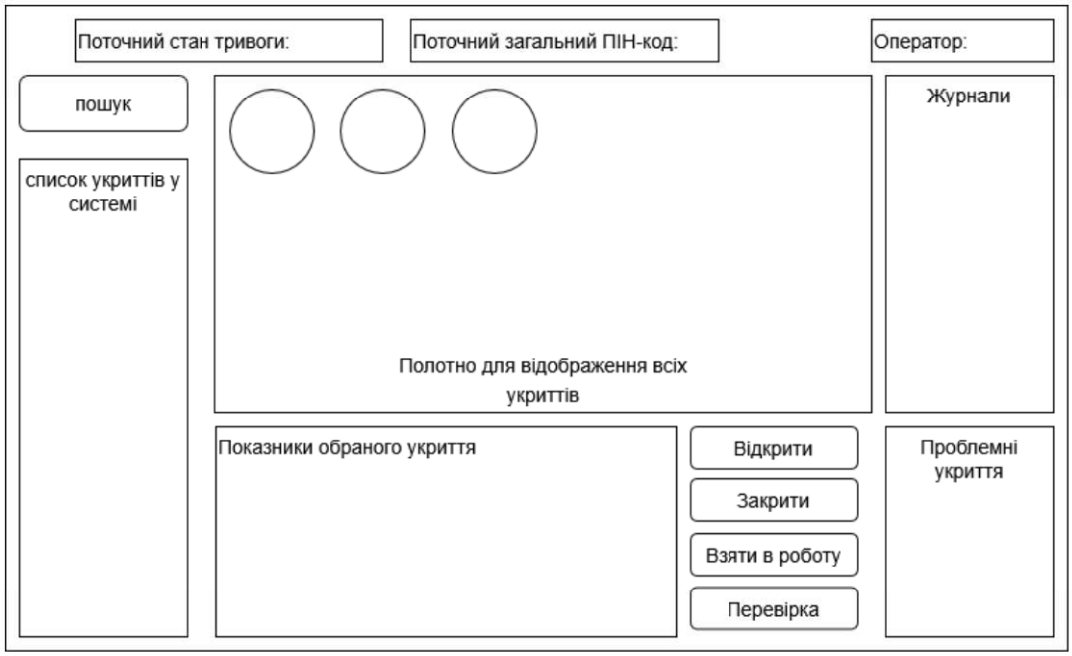


Рис. 2.4. Макет головного екрану вебінтерфейсу оператора системи

Вимоги до розділу «Журнали».

Розділ призначений для відображення логування стану пристрою. Зберігається лог 1 місяць. Назва розділу – Журнал роботи реле та PIN.

Вікно журналу повинно містити такі елементи:

- поле «Дата» – для вибору дати пошуку логування;
- поле «Час початку» – для вибору часу, з якого відображувати логування;
- поле «Час кінця» – для вибору часу, до якого відображувати логування;
- кнопка «Показати журнал» – для активації пошуку.

Результати пошуку відобразити в форматі таблиці з полями: Пристрій (поточна назва пристрою); Тривога (наявність або відсутність тривоги); Статус ПІН (PIN-код, що був активний на пристрої в заданий час); Доступність

пристрою (пристрій був доступний або недоступний); Реле (було успішне або неуспішне відкриття укриття); Дата та час (точний час та дата подій).

Вимоги до розділу «В роботі».

У цьому розділі відображується повне логування пристроїв, що були вибрані оператором для виправлення проблем. Зберігається лог 1 місяць.

Вікно журналу повинно містити такі елементи:

- поле «Пристрій» – поточна назва пристрою;
- поле «Оператор» – прізвище, ім’я та по батькові оператора, який взяв пристрій в обробку;
- поля «Дата та час початку» та «Дата та час початку» – визначають період, протягом якого відбувалися роботи.

Вимоги до продуктивності:

1) Система повинна оновлювати стани пристроїв із затримкою не більш як 2-5 секунд (залежить від бекенд-сервісів).

2) Інтерфейс повинен працювати без зависань при кількості сот до 500.

Вимоги до надійності:

1) Система повинна коректно обробляти відсутність мережі.

2) Усі зміни статусів зберігаються на сервері.

Вимоги до юзабіліті:

1) Інтерфейс має бути адаптивним та підтримувати масштабування елементів.

2) Кольорові стани мають бути інтуїтивно зрозумілими.

Вимоги до безпеки:

1) Необхідно забезпечити обов’язкову авторизацію користувачів.

2) Доступ до обробки тривог має бути обмежений роллю адміністратора.

Наведений документ докладно описує вимоги до всіх компонентів програмного комплексу «Система керування доступом до захисних укриттів на основі пристроїв Akuvox». Він є основою для розробки програмного забезпечення.

2.3. Вибір засобів розробки

У процесі розробки програмного проєкту використано стек технологій, наведений у технічному завданні (п. 2.1): мова програмування PHP 8.1, фреймворк Laravel 9; HTML / CSS / JavaScript, адаптивна верстка; СКБД MySQL 8, FileDB; Telegram Bot API; Akuvox API. Схарактеризуємо причини вибору цих технологій.

Вибір мови програмування для розробки серверної частини системи.

До числа популярних та широко використовуваних мов серверної веброзробки належать, зокрема C#, JavaScript та PHP. Розглянемо їх як альтернативи для виконання проєкту.

C# разом із платформою .NET Core характеризується високою продуктивністю, статичною типізацією та широкими архітектурними можливостями. Завдяки JIT-компіляції та розвиненій моделі багатопоточності ASP.NET Core здатний забезпечувати як високу пропускну здатність вебсервера, так і ефективну роботу з ресурсоємними алгоритмами. Це робить його одним із найкращих рішень для корпоративних систем із складною бізнес-логікою, високими вимогами до безпеки та інтеграції з іншими сервісами. Крім того, він органічно поєднується з інфраструктурою Microsoft, що робить його оптимальним вибором для фінансових, логістичних та державних систем [35].

JavaScript у середовищі Node.js ґрунтується на однопотоковій подієвій моделі з неблокуючим введенням-виведенням, що робить цю мову програмування ефективною в розв’язанні задач, пов’язаних з обробкою великої кількості паралельних з’єднань. У системах реального часу (чати, стрімінгові платформи, інтерактивні вебдодатки та ін.) Node.js демонструє високу продуктивність і здатність масштабуватися без значних витрат ресурсів. Його екосистема, побудована навколо менеджера пакетів npm, забезпечує швидкий старт проєктів і широкий вибір готових модулів, хоча водночас потребує високої дисципліни в керуванні залежностями. У складних

обчислювальних задачах JavaScript поступається більш продуктивним платформам, оскільки однопотокове виконання вимагає винесення ресурсомістких процесів у мікросервіси. Попри це, в типових веб-додатках з інтенсивним мережевим трафіком JavaScript є одним із найефективніших рішень [50].

Мова програмування PHP зорієнтована на класичну модель веброзробки, де кожен HTTP-запит обробляється окремим процесом. Такий підхід забезпечує передбачувану поведінку, просту масштабованість через збільшення кількості процесів та ізоляцію станів між запитами. З появою PHP версій 7 і 8 мова отримала суттєве зростання продуктивності та розширені можливості типізації, що підвищило її надійність у великих проєктах. PHP зберігає статус найбільш ефективного рішення для розробки традиційних CRUD-орієнтованих застосунків, корпоративних сайтів, інтернет-магазинів та API середньої складності. Фреймворки Laravel і Symfony дозволяють досягати високої швидкості розробки завдяки готовим інструментам для роботи з базами даних, автентифікацією, чергами та обробкою подій. При цьому PHP менш зручний для розробки систем реального часу [52].

Для вирішення завдань нашого дослідження можна використати будь-яку з розглянутих мов програмування, оскільки специфічних вимог серверна частина системи не висуває. З огляду на це, обираємо мову PHP, яка наразі залишається одним з найпоширеніших засобів розробки серверних застосунків завдяки гнучкості, широкій інфраструктурі та великій кількості фреймворків.

Вибір PHP фреймворку.

Нині для розробки програмних проєктів найчастіше використовуються фреймворки – набори спеціалізованих програмних інструментів, бібліотек, стандартів, які надають структуру проєкту та засоби розробки, що дозволяє стандартизувати архітектурний підхід, підвищити безпеку, зменшити час розробки та забезпечити масштабованість системи. Вибір фреймворку визначається вимогами до масштабованості, продуктивності, архітектурної

строгості проєкту, а також наявними ресурсами команди й характером проєкту.

У процесі вибору фреймворку для створення проєкту з використанням мови програмування PHP було проаналізовано офіційну документацію поширених фреймворків CodeIgniter [37], Laminas Project [45], Laravel [46], Phalcon [51], Symfony [58], Yii [62]. Результати проведеного аналізу за критеріями продуктивності, складності використання, архітектурної гнучкості, наявності ORM та типових сфер застосування представлено в табл. 2.2.

Таблиця 2.2

Порівняння фреймворків

Фреймворк	Продуктивність	Складність використання	Архітектурна гнучкість	Наявність ORM	Типові сфери застосування
Laravel	Середня	Низька	Гнучка	Eloquent	Веб-сервіси, CRM, REST API
Symfony	Середня / висока	Висока	Дуже гнучка	Doctrine	Корпоративні системи, мікросервіси
Yii	Висока	Середня	Структурована	ActiveRecord	Панелі керування, CRUD-системи
CodeIgniter	Висока	Низька	Проста	Немає	Прості веб-додатки
Phalcon	Дуже висока	Середня	Оптимізована	Власна ORM	Високонавантажені системи
Laminas Project	Середня / висока	Висока	Дуже формальна	Doctrine	Enterprise-платформи

Розглянуті фреймворки належать до різних сегментів PHP-екосистеми:

- Laravel позиціонується як фреймворк для максимально швидкої та комфортної розробки. Він має виразний синтаксис та розвинену екосистему.

- Symfony – це високорівнева платформа з модульною структурою, що застосовується в масштабованих корпоративних системах. Фреймворк характеризується суворою архітектурною дисципліною та гнучкістю конфігурацій.

- Yii орієнтований на продуктивність та строгішу структурність. Завдяки вбудованим інструментам швидкої генерації CRUD-функціоналу підходить для класичних інформаційних систем.

- CodeIgniter є мікрофреймворком, який забезпечує мінімальний поріг входження й високу швидкодію, проте має обмежений набір інструментів для розробки великих систем.

- Phalcon виконаний у вигляді PHP-розширення, написаного на C, що забезпечує найвищу продуктивність серед розглянутих фреймворків.

- Laminas Project – це набір компонентів корпоративного рівня, орієнтований на створення складних високонадійних платформ.

Стосовно продуктивності фреймворків можна зробити висновок, що найвищу продуктивність демонструє Phalcon, який працює на рівні розширення PHP. Yii та CodeIgniter також забезпечують високу швидкодію завдяки оптимізованому ядру. Laravel та Symfony, хоча й мають більшу складність абстракцій, залишаються достатньо продуктивними для більшості веб-систем.

Найнижчий поріг входження має Laravel, що забезпечується зрозумілим синтаксисом, наявністю численних вбудованих інструментів та ґрунтовної документації. CodeIgniter також вирізняється простотою, хоча має менший функціональний набір. Symfony та Laminas вимагають значно більше зусиль на конфігурацію, але відзначаються високою стабільністю.

Максимально гнучку модульну структуру мають Symfony та Laminas, що робить їх придатними для побудови корпоративних систем із тривалим життєвим циклом. Laravel забезпечує компроміс між гнучкістю та простотою, тоді як Yii дотримується більш класичного підходу до архітектури.

Laravel використовує ORM Eloquent, орієнтовану на Active Record-підхід. Symfony та Laminas традиційно працюють із Doctrine ORM, яка підтримує Data Mapper-архітектуру і краще підходить для великих проєктів. Yii пропонує власний Active Record. У CodeIgniter немає повноцінного ORM, а Phalcon має власну високу продуктивну ORM-реалізацію.

Отже, кожний із розглянутих фреймворків орієнтований на специфічну нішу. Laravel доцільно застосовувати в системах, де важлива швидкість розробки та наявність великої кількості готових рішень. Symfony та Laminas

Project є оптимальними для корпоративних високонавантажених платформ з високими вимогами до архітектури. Yii поєднує продуктивність і структурованість, що робить його ефективним для класичних адміністративних та інформаційних систем. CodeIgniter рекомендується для невеликих застосунків або проєктів із жорсткими обмеженнями. Phalcon є оптимальним вибором для систем, де критичною є продуктивність і мінімальні накладні витрати.

Враховуючи зазначене, для розробки системи керування доступом до захисних укриттів на основі пристроїв Akuvox обрано фреймворк Laravel.

Вибір СКБД для зберігання основних даних системи.

Основним способом зберігання даних у сучасних інформаційних системах різного призначення, зокрема веборієнтованих, є бази даних. Тому необхідно обрати СКБД, яка буде використовуватись у нашому проєкті.

Фреймворк Laravel підтримує популярні реляційні системи керування базами даних, надаючи широкий набір функціональних можливостей через ORM Eloquent та механізм міграцій. До складу Laravel входять драйвери для таких СКБД, як MySQL/MariaDB (драйвер pdo_mysql), PostgreSQL (драйвер pdo_pgsql), SQLite (драйвер pdo_sqlite), Microsoft SQL Server (драйвер pdo_sqlsrv), що забезпечує гнучкість при виборі технологічної платформи [46].

Схарактеризуємо коротко зазначені СКБД.

СКБД MySQL набула популярності завдяки простоті, швидкодії та широкій підтримці. Це серверна СКБД із можливістю використання різних механізмів зберігання даних, серед яких основним є InnoDB. Цей механізм забезпечує підтримку ACID-властивостей, транзакційність, багатоверсійність та блокування на рівні рядків, що дозволяє досягти високої конкурентності при роботі багатьох клієнтів. MySQL демонструє високу продуктивність під час виконання типових вебнавантажень, добре масштабується та підтримує реплікацію різних типів. Типовими сферами її використання є вебсайти, REST-сервіси, CRM-системи та інші рішення з високою інтенсивністю дрібних транзакцій [49].

СКБД MS SQL Server належить до класу корпоративних СКБД із розвинутими засобами забезпечення надійності, безпеки та інтеграції з інфраструктурою підприємств. Система має складну багатокомпонентну архітектуру, що включає засоби оброблення транзакцій, інструменти для інтеграції даних, аналізу, побудови OLAP-сховищ та засоби формування звітів. Головною мовою програмування на стороні сервера є T-SQL, що суттєво розширює стандарт SQL та дозволяє реалізовувати складну бізнес-логіку у вигляді збережених процедур, тригерів і функцій. MS SQL Server забезпечує високу продуктивність на великих і навантажених системах, активно використовує паралельну обробку та має ефективний оптимізатор запитів. Система підтримує реплікацію даних, кластери високої доступності та засоби автоматичного керування ресурсами. Вона є частиною Windows-екосистеми та Active Directory, що робить її одним із головних виборів для великих підприємств. Недоліком є висока вартість ліцензій, а також певна залежність від середовища Microsoft. Найчастіше MS SQL Server використовується в корпоративних ERP-, банківських та аналітичних системах [47].

СКБД SQLite створена для вбудованих сценаріїв використання. На відміну від серверних систем, SQLite працює як бібліотека, вбудована у програму, і не потребує окремого сервера або мережевої взаємодії. Усі дані зберігаються в одному файлі, що робить цю систему легкою, мобільною та зручною для розгортання. SQLite використовує механізм журнального запису WAL, але не підтримує складних механізмів масштабування та має значні обмеження щодо конкурентного доступу, оскільки блокування відбувається на рівні файлу. Підтримка SQL у SQLite дещо обмежена, але достатня для більшості задач локального зберігання даних. Її продуктивність є дуже високою в умовах локальних операцій без одночасного доступу кількох клієнтів, але вона не підходить для серверних рішень із високим навантаженням. SQLite масово використовується у мобільних додатках, десктопних застосунках, IoT-пристроях, ігрових рушіях та інших системах, де важлива компактність і простота зберігання даних [55].

СКБД PostgreSQL є однією з найпотужніших об'єктно-реляційних систем керування базами даних із відкритим кодом. Архітектура PostgreSQL базується на механізмі MVCC, який забезпечує відсутність блокувань читання, а також на журнальному записі WAL, що гарантує відновлення даних у випадку збою. Перевагами PostgreSQL є розширюваність та одна з найповніших реалізацій SQL-стандарту. Продуктивність PostgreSQL особливо висока у випадку складних запитів, багаторівневих JOIN, аналітики та операцій над великими обсягами даних. Система підтримує фізичну та логічну реплікацію. PostgreSQL найчастіше використовується у фінансово-технологічних системах, аналітичних платформах, логістичних рішеннях, системах з високими вимогами до надійності та складних бізнес-правил [54].

Отже, вибір конкретної СКБД залежить від вимог до продуктивності, масштабованості, складності бізнес-логіки, середовища розгортання та бюджету проєкту. Враховуючи це, для нашого випадку оптимальним рішенням буде використання СКБД MySQL.

Вибір способу зберігання логів.

Вибір FileDB як сховища для логів зумовлений функціональними особливостями журналювання в системі, а також вимогами до продуктивності та обсягів даних.

Логи доступу пристроїв і станів реле мають характер потокових, переважно додаткових даних, які рідко змінюються та читаються здебільшого послідовно за часовими інтервалами. Для такого типу навантаження використання класичної реляційної СКБД є менш ефективним: великі таблиці логів призводять до зростання розміру індексів, уповільнення складних запитів та ускладнення резервного копіювання. FileDB, як файлова БД із зберіганням записів у структурованому форматі, краще відповідає сценарію лінійного нарощування даних та архівування.

Розділення зберігання операційних даних та логів великого обсягу дає змогу розвантажити MySQL і забезпечити стабільну роботу транзакційної

частини системи. Усі критично важливі для бізнес-логіки дані залишаються в реляційній БД, а великий масив журналів виноситься у FileDB.

FileDB спрощує реалізацію архівування та довгострокового зберігання логів. Оскільки логи зберігаються у файловій структурі, їх можна легко: архівувати за періодами, переносити на окремі носії, очищувати старі журнали без втручання в структуру реляційної БД.

Комбінація MySQL та FileDB узгоджується з вимогами до масштабованості, продуктивності та надійності: MySQL використовується для транзакційних операцій і критичних даних, FileDB оптимізована для швидкого запису великого обсягу логів, їх гнучкого зберігання та подальшої обробки у відповідних розділах вебінтерфейсу.

Окрім використання файлової бази даних FileDB для зберігання великих обсягів логів, було розглянуто альтернативні підходи – зберігання журналів в окремих таблицях MySQL та застосування документоорієнтованих БД (наприклад, MongoDB). Реляційні рішення забезпечують зручність SQL-запитів, але при зростанні обсягів логів призводять до суттєвого збільшення індексів та ускладнення резервного копіювання. Використання NoSQL бази даних також є гарним рішенням для великих обсягів даних, що часто додаються та рідше змінюються. Проте це додаткова технологія, що вимагає додаткової інфраструктури й ускладнює супровід системи. З огляду на це, для розробки даного проєкту обрано FileDB як компромісне рішення, що поєднує простоту впровадження, високу швидкість додавання записів і гнучкість структури даних при зберіганні логів великого обсягу.

Вибір API.

Вибір API для взаємодії системи з пристроями, встановленими в укриттях, визначається їхнім типом і відповідно це Akuvox HTTP API.

Akuvox HTTP API – це інтерфейс для керування домофонними панелями через HTTP(S). Він дозволяє інтегрувати пристрої з системами автоматизації, безпеки, моніторингу та сторонніми сервісами. Обмін даними здійснюється у форматі JSON, а низка операцій передбачає роботу з файлами. API підтримує

методи GET та POST, де POST використовується для передачі структурованих параметрів у полі data [40].

Akuvox HTTP API – це великий набір REST-подібних ендпоінтів, який дає змогу повністю керувати домофонною панеллю. Наведемо перелік ендпоінтів Akuvox HTTP API, що безпосередньо стосуються відчинення дверей (табл. 2.3).

Таблиця 2.3

Ендпоінти Akuvox HTTP API для керування дверима

Ендпоінт	Метод	Призначення
/api/relay/trig	GET / POST	Основна функція для відкривання дверей (тригер реле A/B/C).
/api/relay/status	GET / POST	Отримання поточного стану реле (відкрито/закрито).
/api/relay/get	GET / POST	Читання налаштувань реле (типи контактів, затримки).
/api/relay/set	POST	Налаштування параметрів реле (затримки, типи).
/api/input/status	GET / POST	Статус дверних датчиків (Input A/B/C). За потреби контроль стану дверей.
/api/input/set	POST	Прив'язка реакції на датчик (наприклад, автоматичне відкриття реле).
/api/privatekey/get	GET / POST	Отримання списку приватних кодів доступу (PIN-коди).
/api/privatekey/ add	POST	Додавання PIN-кодів з прив'язкою до дверей (DoorNum).
/api/privatekey/del	POST	Видалення PIN-кодів доступу.
/api/doorlog/get	GET / POST	Лог доступу: події відкриття/помилки.
/api/doorlog/clear	GET / POST	Очистка журналу відкривань дверей.

Вибір Telegram Bot API також обумовлений конкретним завданням – необхідністю розсилки повідомлень через месенджер Telegram.

Telegram Bot API – це офіційний HTTP-інтерфейс, який дозволяє розробникам створювати та керувати ботами Telegram через надсилання звичайних HTTPS-запитів. Він забезпечує механізм обміну даними між ботом та користувачами, каналами, групами й іншими елементами API працює за принципом REST-подібних викликів: кожен метод – це окремий HTTPS-запит до сервера Telegram [59].

Отже, на основі аналізу технічної документації обґрунтовано вибір стеку технологій для розробки проєкту.

РОЗДІЛ 3
ОПИС СИСТЕМИ КЕРУВАННЯ ДОСТУПОМ ДО ЗАХИСНИХ УКРИТТІВ НА ОСНОВІ ПРИСТРОЇВ AKUVOX

3.1. Технічний опис системи

3.1.1. Базова структура Laravel-проєкту

Структура проєкту відповідає вимогам технічного завдання та забезпечує розділення компонентів системи керування доступом до захисних укриттів на основі пристроїв Akuvox. Основою системи є типовий каркас Laravel, у межах якого виокремлено модулі авторизації, керування користувачами, взаємодії з пристроями Akuvox, обробки тривог, логування, Telegram-інтеграції та механізм резервування з використанням двох серверів (рис. 3.1).

- 🗀 `app/`
  - `Models/` – моделі домену (користувачі, пристрої, тривоги, журнали тощо).
  - `Http/`
    - `Controllers/` – REST API, веб-контролери панелей.
    - `Middleware/` – аутентифікація, авторизація, перевірка ролей.
    - `Requests/` – валідація вхідних даних.
    - `Resources/` – API-ресурси (форматування JSON-відповідей).
  - `Policies/` – політики доступу (UserPolicy, DevicePolicy).
  - `Services/` – інтеграції й бізнес-логіка (Akuvox, Telegram, FileDB, AlarmService).
  - `Events/`, `Listeners/` – реакція на тривоги, зміну стану пристроїв, відправку повідомлень.
  - `Jobs/` – черги (надсилання Telegram, оновлення статусів, збереження логів у FileDB).
  - `Console/Commands/` – крон-задачі: перевірка серверів, опитування пристроїв.
- 🗀 `routes/`
  - `api.php` – API для фронтенду, вебхуків тривог, внутрішнього API між серверами.
  - `web.php` – вебінтерфейс оператора.
- 🗀 `database/`
  - `migrations/` – створення таблиць.
  - `seeders/` – базові ролі, супер-адмін, тестові пристрої.
- 🗀 `config/`
  - `services.php` – конфіг для Telegram, зовнішнього сервісу тривог, Akuvox.
  - `logging.php` – канал під FileDB (JSON-файли).
- 🗀 `storage/app/filedb/` – FileDB для логів пристроїв.
- 🗀 `resources/views/` – шаблони для інтерфейсу оператора.
- 🗀 `public/` – статика (css, js, іконки статусів).

Рис. 3.1. Фізична структура проєкту

Кожний функціональний блок реалізовано у вигляді окремого підмодуля з власними моделями, контролерами, сервісами та допоміжними класами.

Проєкт розроблено з дотриманням принципів розділення відповідальності:

- моделі (Models) відповідають за структуру даних та взаємодію з БД;
- контролери (Controllers) реалізують приймання запитів і виклик бізнес-логіки;
- сервіси (Services) інкапсулюють бізнес-процеси;
- події та слухачі (Events, Listeners) забезпечують реактивну обробку змін у системі;
- завдання та черги (Jobs) використовуються для асинхронних операцій.

Модуль авторизації та ролей. Система має три рівні користувачів: супер-адміністратор, адміністратор і звичайний користувач. Модулі авторизації реалізовано через Laravel Sanctum, що дозволяє забезпечити захист API-інтерфейсу токен-аутентифікацією.

Політики доступу визначають, які дії доступні кожному рівню ролей. Це забезпечує контроль над створенням, редагуванням та видаленням користувачів, переглядом журналів та інтерактивною взаємодією з пристроями.

Модуль керування користувачами. Структура включає вебконтролери для вебінтерфейсу оператора. Передбачено реєстрацію, редагування та видалення користувачів з урахуванням ієрархії ролей. Модуль забезпечує пошук та відображення списку користувачів, зміну ролей, ведення журналу дій користувачів.

Модуль роботи з пристроями Akuvox. Для кожного пристрою зберігається його конфігурація: URL API, тип, локація, підрядник, телефон, відповідальний адміністратор тощо. Комунікація з пристроями реалізована через окремий сервіс AkuvoxClient, який інкапсулює HTTP-запити для відкриття, закриття та перевірки стану дверей. Сервіс DeviceStatusService відстежує зміни стану (online/offline) та генерує відповідні події.

Модуль обробки тривог. Однією з ключових частин системи є автоматична реакція на сигнали тривог, які надходять через webhook. Модуль включає модель AlarmEvent для фіксації фактів надходження сигналів та сервіс AlarmService, який відкриває всі укриття у разі тривоги, закриває їх після отримання сигналу відбою, надсилає сповіщення у Telegram, записує відповідні події в журнали. Це забезпечує повністю автоматизований режим реагування на критичні події.

Модуль логування. Система використовує дві технології зберігання логів: MySQL для важливих подій (дії користувачів, робочі записи, ключові події системи); FileDB (JSON-файли) для масових логів пристроїв, обсяг яких може перевищувати 5 ГБ. Файли структуруються по пристроях і містять записи про стани реле, помилки, PIN-коди та інші технічні дані. Запис у FileDB виконується сервісом FileDbLogger, а читання та фільтрація – сервісом LogQueryService, який підтримує опції фільтрування за датою, часом, пристроєм та типом події.

Інтеграція з месенджером Telegram. Модуль відповідає за відправку тимчасових PIN-кодів, надсилання службових повідомлень, оповіщення про технічний стан пристроїв. Сервіс TelegramBotService виконує надсилання повідомлень.

Система резервування та внутрішній API. Оскільки система передбачає безперервну роботу, реалізовано архітектуру з двома серверами: основним та резервним. Кожен сервер може опитувати інший через внутрішній API та визначати його стан. Сервіс ServerHealthService здійснює регулярні перевірки доступності основного сервера, а InternalApiClient забезпечує взаємодію між вузлами. У випадку відмови основного сервера резервний автоматично перебирає функції керування на себе.

Веб-інтерфейс оператора. Відображує всі основні функції системи: поточний стан тривоги (тривога/відбій); список пристроїв із кольоровими індикаторами; дані оператора; кнопки керування дверима (відкрити/закрити);

розділи «В роботі», «Журнали», «Користувачі», «Пристрої». Контролер DashboardController об’єднує дані з різних модулів і подає їх у зручній формі.

Отже, структура Laravel-проєкту побудована так, щоб чітко розділяти логіку між модулями, забезпечувати масштабування та доповнення функціоналу, гарантувати безпеку та жорстке управління ролями, швидко реагувати на події тривоги, зберігати журнали подій, підтримувати резервування та відмовостійкість системи, надавати оператору інтуїтивно зрозумілий інтерфейс.

3.1.2. Опис класів програмної реалізації

Наведемо опис основних класів програмної реалізації системи керування доступом до захисних укриттів на базі пристроїв Akuvox.

Доменні класи.

1) Клас User. Представляє зареєстрованого користувача системи. Зберігає основні облікові дані та роль користувача. Додатково зберігається ідентифікатор користувача, який створив поточного, що дає змогу відслідковувати адміністративну ієрархію.

Основні функції класу: автентифікація користувача через механізми Laravel; надання інформації про роль та права доступу; зв’язок з пов’язаними журналами дій (UserActionLog) та записами в розділі «В роботі» (WorkLog).

2) Клас Device. Моделює пристрій Akuvox, що використовується для керування дверима укриття. Відповідає за збереження конфігураційної інформації про пристрій, зв’язки з журналами роботи (WorkLog), PIN-кодами (PinCode) та подіями тривог (AlarmEvent), використання у сервісах, які безпосередньо виконують керування дверима через HTTP API.

3) Клас AlarmEvent. Описує факт надходження сигналу тривоги чи відбою від зовнішньої системи. Основні поля включають тип події (тривога/відбій), джерело повідомлення та момент спрацювання. Основні функції: реєстрація кожного сигналу тривоги у БД; надання вхідних даних для

сервісу обробки тривог (AlarmService); використання у внутрішньому API при передачі подій між основним і резервним сервером.

4) Клас PinCode. Використовується для представлення тимчасових PIN-кодів, що надсилаються через Telegram для доступу до певних укриттів. Він зберігає значення PIN-коду, прив'язаний пристрій, час закінчення дії та статус (дійсний/недійсний).

5) Клас UserActionLog. Фіксує дії, які виконують користувачі в системі. Атрибути включають ідентифікатор користувача, текстовий опис дії та часову мітку. Клас використовується для аудиту безпеки, формування звітів щодо роботи операторів, аналізу помилок та інцидентів у системі.

6) Клас WorkLog. Реалізує записи розділу «В роботі». Зберігає прив'язку до пристрою, оператора, опис проблеми чи завдання, а також статус. Основні функції: ведення переліку поточних задач, пов'язаних з укриттями та пристроями; відображення у вебінтерфейсі для планування та контролю виконання робіт.

Класи авторизації та ролей:

1) Клас UserPolicy. Містить набір методів для перевірки прав користувача на виконання дій із сутністю User. Політика враховує роль користувача, а також ієрархію.

2) Клас DevicePolicy. Визначає, хто і в яких межах може працювати з об'єктами Device. Політика враховує роль користувача.

3) Програмний шар EnsureUserHasRole. Застосовується до маршрутів веб- та API-інтерфейсу для перевірки, чи належить поточний користувач до однієї з дозволених ролей.

Класи роботи з пристроями, тривогами та Telegram:

1) Клас сервісу AkuvoxClient. Інкапсулює логіку HTTP-взаємодії з пристроями Akuvox. Надає методи: openDoor(device) – запит на відкриття дверей; closeDoor(device) – запит на закриття дверей; checkStatus(device) – отримання поточного стану пристрою. Сервіс ізолює низькорівневі мережеві

виклики від іншої частини системи, що спрощує тестування та подальшу заміну/розширення API.

2) Клас сервісу AlarmService. Відповідає за бізнес-логіку обробки сигналів тривоги та відбою. На вхід він отримує об'єкти AlarmEvent і виконує відчинення дверей укриттів через AkuvoxClient при надходженні сигналу тривоги, зачинення дверей після завершення тривоги, оновлення глобального стану системи (тривога/відбій) для головного екрану, формування записів у журналах, відправку сповіщень через TelegramBotService.

3) Клас сервісу TelegramBotService. Реалізує інтеграцію системи з Telegram. Основні функції: відправка PIH-кодів; надсилання службових повідомлень операторам.

4) Клас сервісу TelegramPinService. Відповідає за життєвий цикл тимчасових PIN-кодів: генерація нового PIN-коду для конкретного пристрою; валідація отриманих PIN-кодів; надсилання PIN-коду через TelegramBotService. Завдяки цьому сервісу забезпечується безпечний, тимчасовий доступ до укриттів за допомогою керованих PIN-кодів.

Класи журналів та резервування:

1) Клас сервісу FileDbLogger. Реалізує запис великих обсягів технічних логів пристроїв у файлову структуру. Основні функції: логування подій у файли формату JSON; структуризація логів за пристроями та часом; запис службових повідомлень про помилки.

2) Клас сервісу LogQueryService. Забезпечує зручний доступ до журналів FileDB. Він надає методи підготовки даних для відображення у веб-інтерфейсі розділу «Журнали».

3) Клас ServerNode. Моделює вузли кластеру (основний та резервний сервери). Він містить такі дані: назву/тип вузла; базову адресу; ознаку активності; час останнього сигналу життєздатності. Вони використовуються для моніторингу доступності сервера та переключення ролей.

4) Клас сервісу ServerHealthService. Виконує періодичну перевірку стану основного сервера. Виконує функції: опитування вузлів ServerNode через

внутрішній API; фіксація результатів перевірок; ініціація процедури переходу на резервний сервер, якщо основний вузол недоступний.

5) Клас сервісу InternalApiClient. Інкапсулює звернення до внутрішнього API іншого сервера: отримання статусу; пересилання подій тривог, якщо необхідно дублювати обробку на резервному вузлі. Він дозволяє ізолювати логіку HTTP-взаємодії між вузлами від решти системи.

Представимо структуру основних компонентів системи керування доступом до захисних укриттів, а також взаємозв'язки між класами у форматі UML-діаграм: діаграма основних доменних класів системи (рис. 3.2); діаграма авторизації та ролей (рис. 3.3); діаграма взаємодії пристроїв, тривог та Telegram-модуля (рис. 3.4).

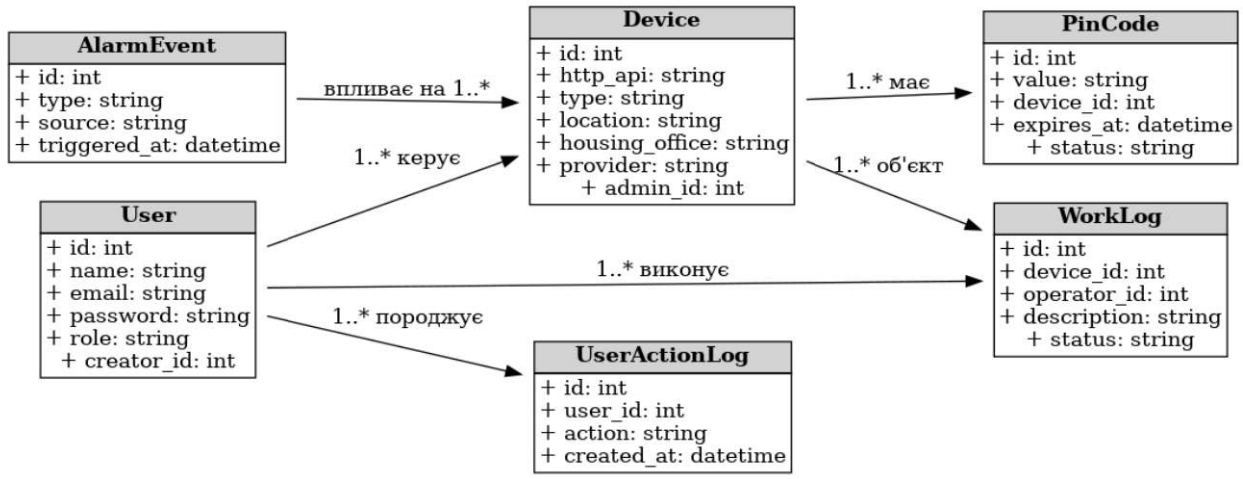


Рис. 3.2. UML-діаграма основних доменних класів системи

На рис. 3.2 зображено ключові сутності доменної моделі: User, Device, AlarmEvent, PinCode, UserActionLog та WorkLog. Діаграма демонструє, що: користувач може керувати багатьма пристроями; кожен пристрій має власні журнали роботи та PIN-коди; тривожні події впливають на стан пристроїв; усі дії користувачів фіксуються в журналі. Ця модель становить основу загальної логічної структури системи.

Діаграма (рис. 3.3) описує підсистему авторизації, яка включає: клас User (джерело ролей і прав доступу); політики доступу UserPolicy та DevicePolicy; програмний шар EnsureUserHasRole, що здійснює перевірку прав

під час доступу до маршрутів системи. Діаграма ілюструє механізм керування доступом та ієрархію ролей: користувач взаємодіє з політиками, а програмний шар блокує або дозволяє доступ залежно від ролі.

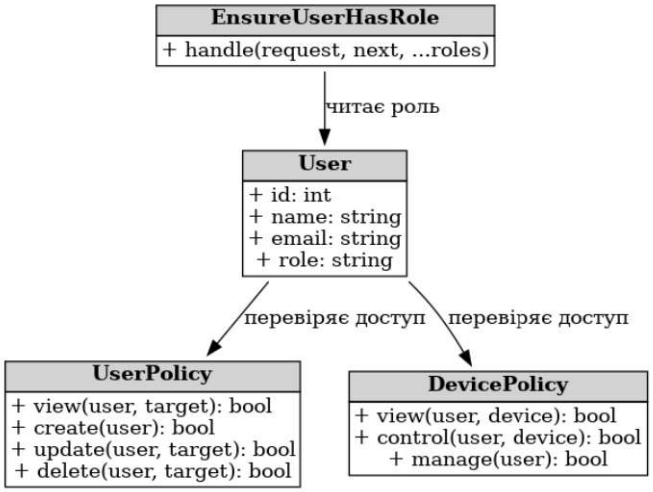


Рис. 3.3. UML-діаграма авторизації та ролей

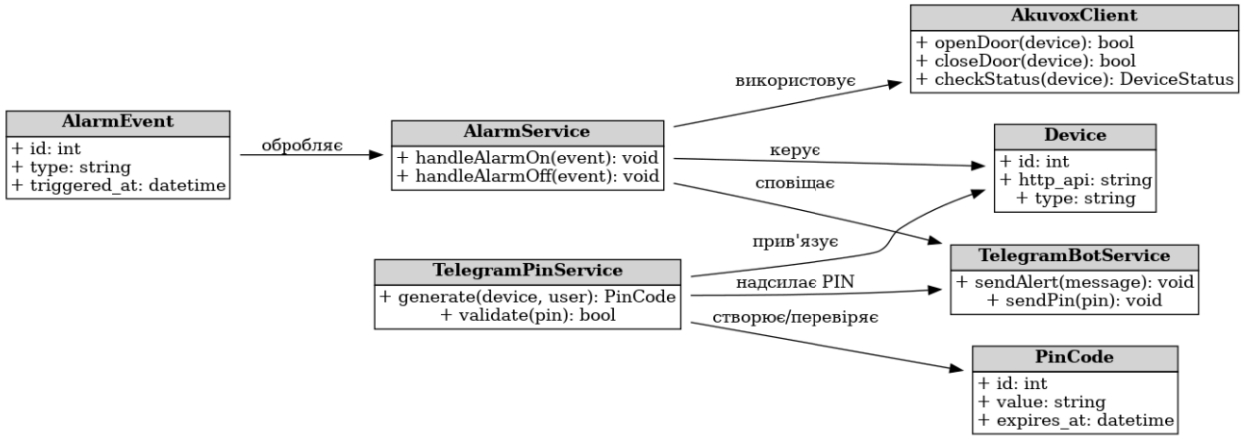


Рис. 3.4. UML-діаграма взаємодії пристроїв, тривог та Telegram-модуля

На діаграмі (рис. 3.4) зображено класи, що реалізують технічну взаємодію з пристроями Akuvox, а також обробку тривог і керування Telegram-повідомленнями. Включено такі служби: AkuvoxClient – API-взаємодія з пристроями (відчинити, зачинити, перевірити); AlarmService – логіка обробки тривоги, зміна станів дверей та формування сповіщень; TelegramBotService – відправка службових повідомлень; TelegramPinService – генерація й перевірка PIN-кодів; класи Device, AlarmEvent і PinCode, які

використовуються цими сервісами. Діаграма демонструє, як система реагує на подію тривоги, керує пристроями та сповіщає користувачів через Telegram.

Розгортання системи:

- операційна система: Ubuntu 22.04 LTS;
- вебсервер: Apache 2.4;
- мова програмування: PHP 8.1;
- база даних: MySQL 8;
- фреймворк: Laravel.

3.2. Користувацький опис

Відповідно до завдань дослідження система представляє собою програмний комплекс, який вирішує два основні завдання: 1) автоматичне відчинення та зачинення дверей з використанням інтеркомів Akuvox; 2) віддалене централізоване керування мережею таких пристроїв.

Компонент системи, розміщений в укриттях, працює так:

1) Всі входи в укриття обладнуються інтерком-контролем доступу, який має електромагнітний замок з датчиком стану дверей, безконтактною кнопкою для виходу, пристроєм аварійного доступу для відчинення входу фізичним ключем.

2) Всередині укриття встановлюється комутаційний вузол та безперебійний блок живлення, до якого підключаються всі компоненти системи. Всі пристрої мають бути об’єднані в локальну мережу.

3) Для забезпечення віддаленого керування пристроями в укритті необхідно передбачити доступ до Інтернету через енергонезалежний канал зв’язку.

4) Програма керування пристроєм отримує повідомлення про оголошення повітряної тривоги з вебсервісу, до якого підключена. Після цього автоматично відмикається замок і додатково телеграм-ботом розсилаються

тимчасові пін-коди. Такий пін-код діє протягом усього часу тривоги і є резервним способом доступу до укриття.

5) Після відбою тривоги пристрій закриває замок та змінює PIN-код.

Використання вебінтерфейсу оператора системи керування доступом до захисних укриттів.

Для входу в систему необхідно пройти процедуру авторизації, для чого у відповідній формі (рис. 3.5) ввести електронну пошту та пароль користувача.

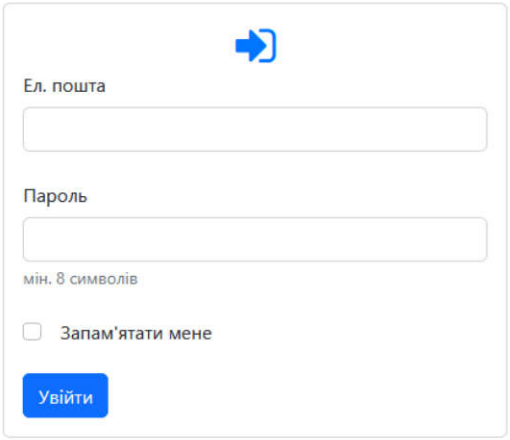


Рис. 3.5. Сторінка авторизації користувача

Після авторизації відкривається сторінка панелі керування (рис. 3.6). Відповідно до технічного завдання в системі передбачено три ролі: супер-адміністратор, адміністратор та користувач. Залежно від того, хто пройшов авторизацію, панель керування буде мати певні обмеження функціоналу.

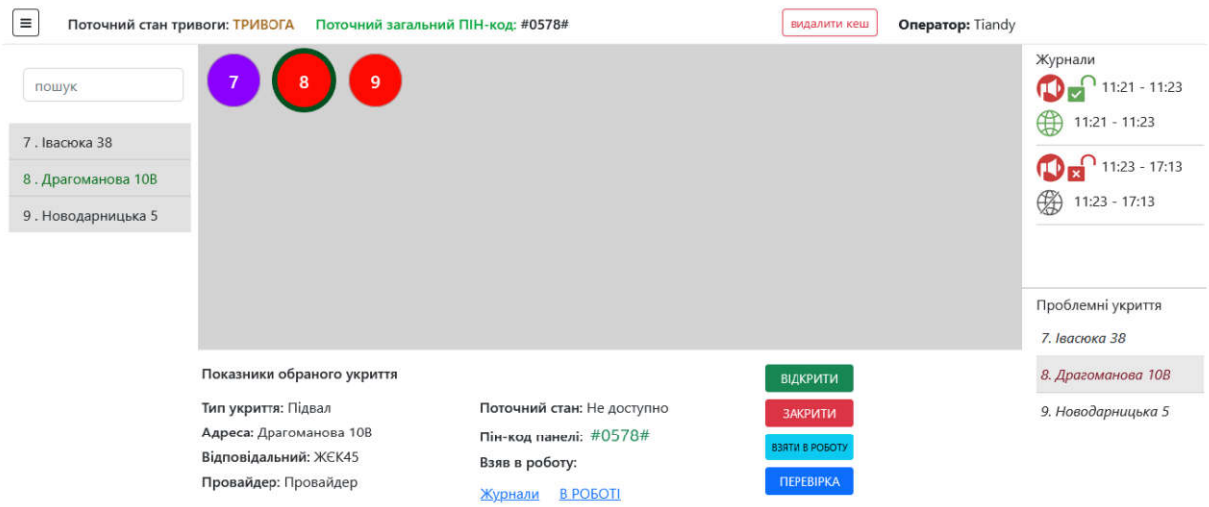
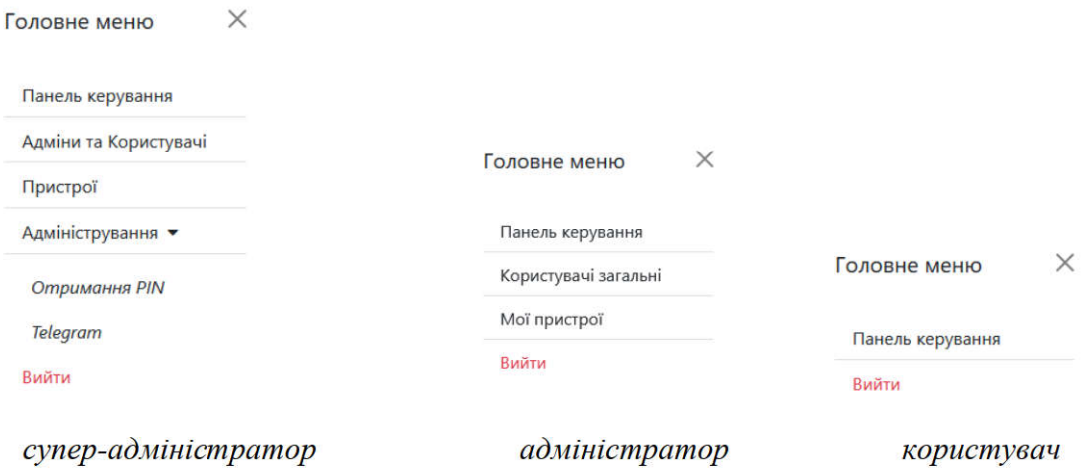


Рис. 3.6. Головний екран вебінтерфейсу

У лівому верхньому куті знаходиться кнопка для відкриття меню, яке містить пункти: Панель керування; Адміни та Користувачі; Пристрої; Адміністрування; Вийти. Зазначені пункти доступні, якщо користувач має роль супер-адміністратора. Якщо користувач має роль адміністратора, то йому доступні панель керування, а також перегляд пристроїв, за які він відповідає, та списку звичайних користувачів. Якщо користувач має роль користувача, то йому доступна лише панель керування. Варіанти меню для різних ролей наведено на рис. 3.7.



супер-адміністратор *адміністратор* *користувач*

Рис. 3.7. Меню системи для різних ролей

Більшу частину екрану Панелі керування займає полотно для відображення укриттів. Укриття представлено у вигляді кіл – кожне коло відповідає одному укриттю. Колір кола залежить від поточного стану укриття змінюється автоматично: червоний (пристрій недоступний, PIN-код недійсний); фіолетовий (пристрій взято в роботу); помаранчевий колір (пристрій недоступний, PIN-код дійсний); зелений (все добре).

При виборі кола в панелі «Показники обраного укриття» відображується інформація про відповідне укриття, а саме: тип укриття; його адреса; відповідальний (організація, на балансі якої знаходиться укриття); провайдер послуг Інтернет; поточний стан; PIN-код панелі; дата і час взяття пристрою в

роботу у випадку проблем. Окрім того, в панелі «Журнали» відображується поточний стан укриття за допомогою спеціальних індикаторів:

- разом «Червоний дзвінок» та «Червоний замок»: розпочалася повітряна тривога, але двері укриття не були успішно відчинені;
- разом «Червоний дзвінок» та «Зелений замок»: розпочалася повітряна тривога, двері укриття були успішно відчинені;
- разом «Зелений дзвінок» та «Зелений замок»: повітряна тривога закінчилася, двері укриття були успішно зачинені;
- разом «Зелений дзвінок» та «Червоний замок»: повітряна тривога закінчилася, але двері укриття не були успішно зачинені;
- «Зелена галочка»: пристрій онлайн, все працює нормально;
- «Червоний хрестик»: пристрій офлайн та з ним втрачено зв'язок.

Для вибору укриття також можна використати список, розташований з лівого боку панелі керування. Якщо список великий і відображується з прокручуванням, можна скористатися полем «Пошук» для пошуку укриття за адресою.

Окремо з правого боку панелі створено список «Проблемні укриття», де відображується список укриттів, які потребують втручання оператора або ремонту.

Для ручного керування призначені кнопки, при натисканні на які виконується відповідна операція, а також виводиться повідомлення про результат операції, наприклад «Помилка пристрою!»:

- «Відкрити» – відчинення дверей укриття;
- «Закрити» – зачинення дверей укриття;
- «Взяти в роботу» – виклик спеціалістів для усунення несправностей при недоступності пристрою. Відповідне повідомлення виводиться в полі «Взяв в роботу» на панелі «Показники обраного укриття»;
- «Перевірка» – перевірка доступності пристрою.

Для перегляду логів призначені посилання «Журнали» та «В роботі».

Натискання на посилання «Журнали» відкриває спливаюче вікно «Журнал роботи реле та PIN» (рис. 3.8). В ньому відображується журнал подій поточного укриття (обраного на полотні). Для відбору необхідних даних слід вказати дату, час початку та час кінця періоду логування та натиснути кнопку «Показати журнал». Журнал відображується у форматі таблиці з полями: пристрій, тривога, статус ПІН, доступність пристрою, реле, дата та час.

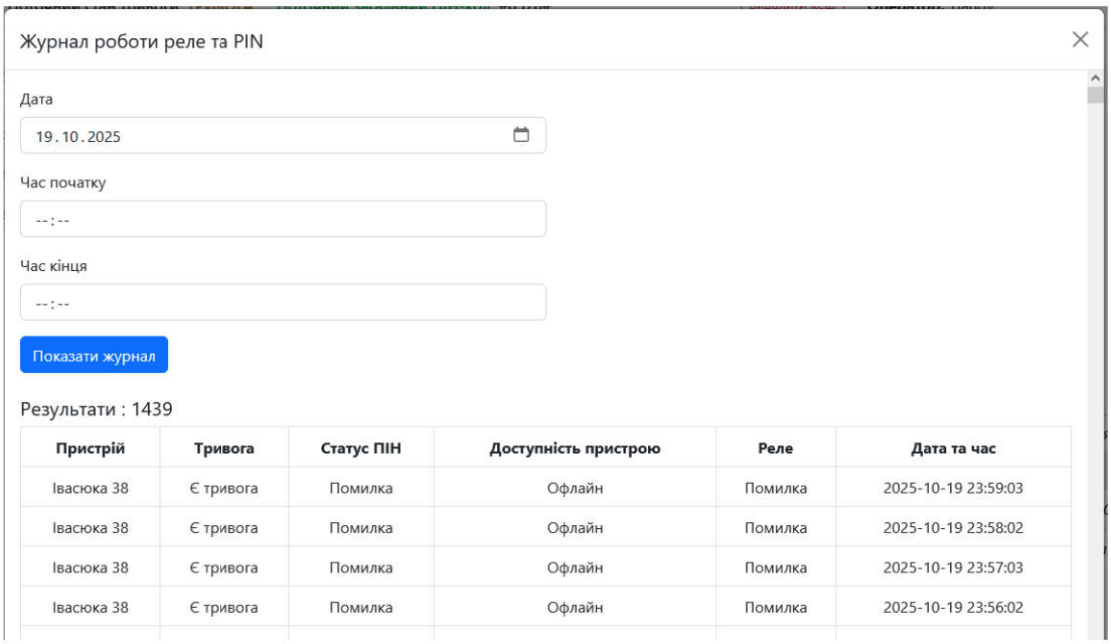


Рис. 3.8. Спливаюче вікно «Журнал роботи реле та PIN»

Натискання на посилання «В роботі» відкриває спливаюче вікно «Журнал робіт» (рис. 3.9). В ньому відображується журнал робіт з технічного обслуговування поточного укриття (обраного на полотні). Журнал відображується у форматі таблиці з полями: пристрій, взяв у роботу, дата та час початку, дата та час кінця.

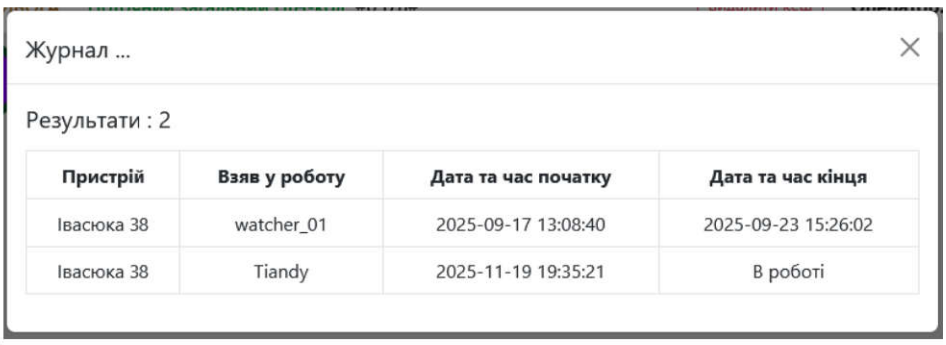


Рис. 3.9. Спливаюче вікно «Журнал робіт»

Для керування обліковими записами користувачів слід у меню обрати пункт «Адміни та Користувачі». Після цього відкривається відповідна сторінка (рис. 3.10).

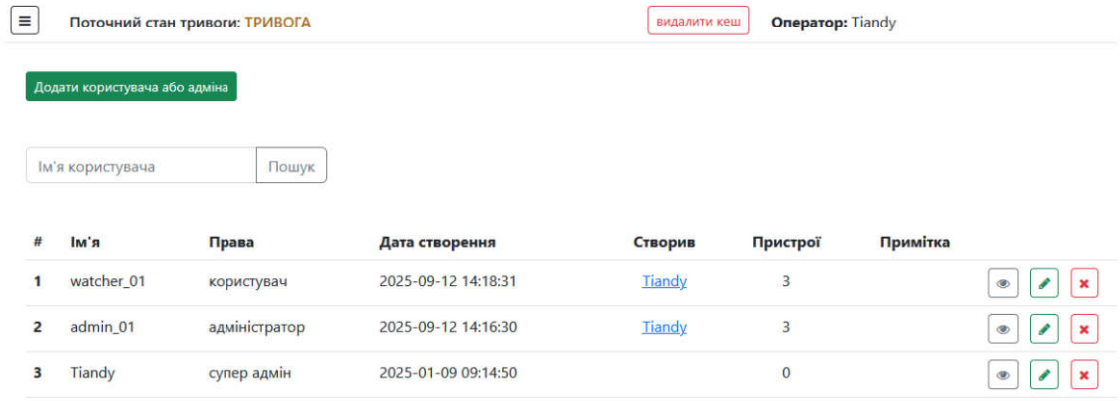


Рис. 3.10. Головна сторінка розділу керування користувачами

Сторінка містить список користувачів у форматі таблиці з полями: Ім’я; Права; Дата створення; Створив; Пристрої; Примітка; кнопки керування записом (відобразити / приховати, редагувати, видалити). Для пошуку користувача у списку за іменем призначене поле «Пошук». Для створення нового облікового запису призначена кнопка «Додати користувача або адміна». Після її натискання відкривається сторінка з формою додавання (рис. 3.11).

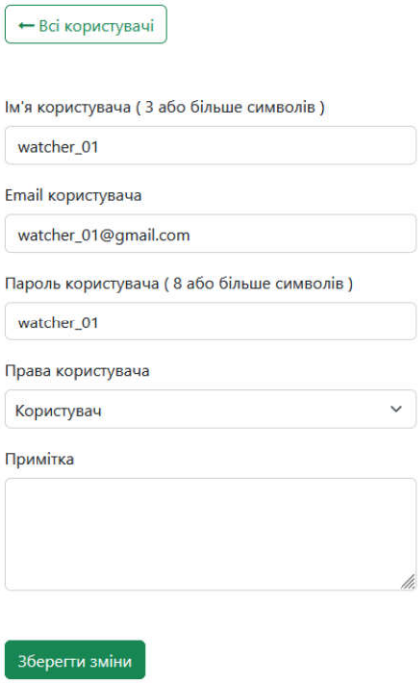


Рис. 3.11. Форма для додавання або редагування користувача

Для керування пристроями слід у меню обрати пункт «Пристрої». Після цього відкривається відповідна сторінка (рис. 3.12).

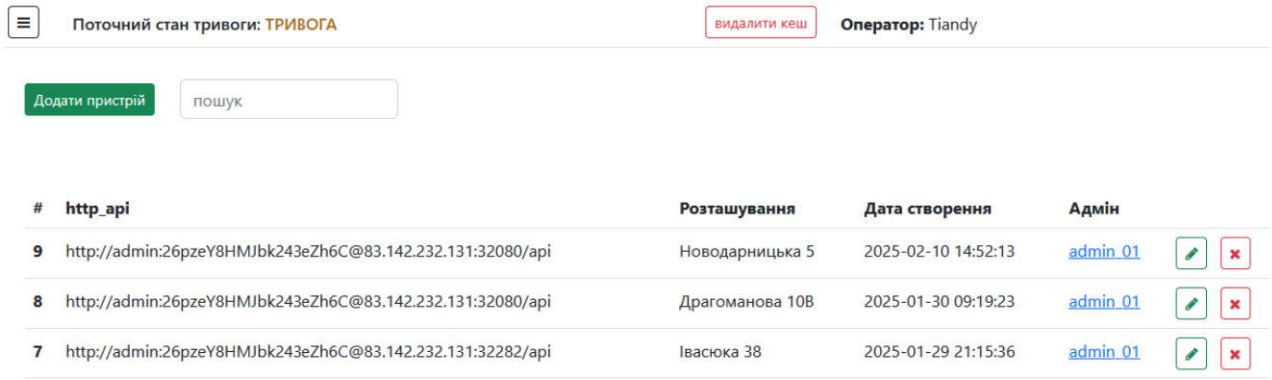


Рис. 3.12. Головна сторінка розділу керування пристроями

Сторінка містить список пристроїв у форматі таблиці з полями: http_api; Розташування; Дата створення; Адмін; кнопки керування записом (редагувати, видалити). Для пошуку пристрою у списку за адресою призначене поле «Пошук». Для створення нового запису призначена кнопка «Додати пристрій». Після її натискання відкривається сторінка з формою додавання (рис. 3.13).

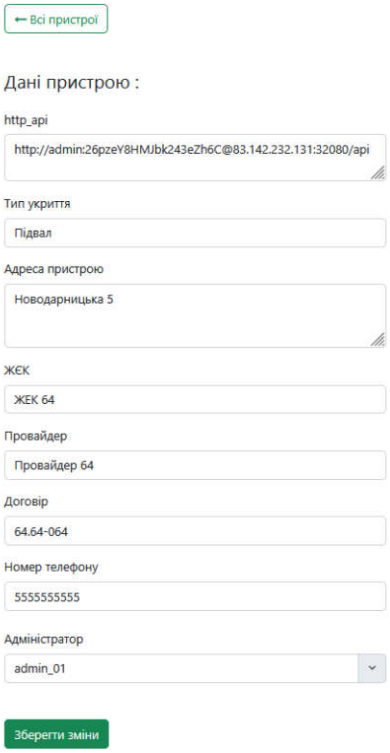


Рис. 3.13. Форма для додавання або редагування пристрою

Пункт меню «Адміністрування» містить два пункти:

1) Отримання PIN. Відкриває сторінку, де можна вказати URL адресу для отримання PIN-коду пристрою.

2) Telegram. Відкриває сторінку, де відображується список Telegram-каналів для відправлення повідомлень.

Калькулювання собівартості та розрахунок бюджету проєкту виконано на основі підходу, описаного Н. Кудлаєвою та С. Круцем [16]. Для розрахунку використано дані про заробітну плату розробників програмного забезпечення в Україні у 2025 році за даними редакції DOU [12]. Розрахунки наведено в Додатку. Прийнято до уваги, що у виконанні такого проєкту можуть взяти участь 5 розробників різного рівня кваліфікації: програміст, керівник групи; програміст-верстальник; вебдизайнер; програміст пристроїв Akuvox; тестувальник. Загалом, бюджет проєкту склав 820217,30 грн. за 740 людино-годин з урахуванням прибутку 25% від собівартості продукту.

3.3. Модульне та інтеграційне тестування системи

Відповідно до завдань дослідження у процесі розробки системи проводилось модульне та інтеграційне тестування за допомогою PHPUnit.

Метою тестування програмного забезпечення є перевірка коректності реалізації функціональних вимог технічного завдання, а також оцінка надійності, відмовостійкості та безпечності розробленої системи.

Основні завдання тестування: перевірка роботи механізмів автентифікації та авторизації з урахуванням ролей користувачів; перевірка коректності бізнес-логіки обробки тривог та відбоїв; валідація генерації й використання тимчасових PIN-кодів; тестування взаємодії з API пристроїв Akuvox; підтвердження коректної роботи підсистеми журналювання; перевірка механізму резервування та перемикання між основним і резервним серверами; тестування ключових HTTP-маршрутів (API логіну, webhook тривог); перевірка правильності функціонування вебінтерфейсу оператора системи.

Скрипти з тестами знаходяться в каталозі tests (рис. 3.14), який в Laravel містить дві папки:

- папка Feature – призначена для інтеграційних тестів, які перевіряють взаємодію компонентів проєктів;
- папка Unit – призначена для модульних тестів, які перевіряють невеликі ізольовані частини коду (наприклад, функції).

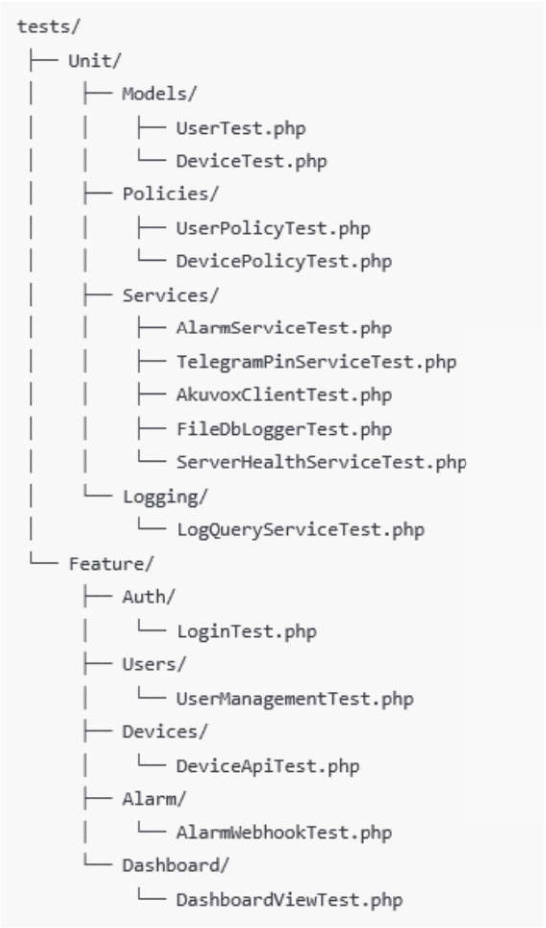


Рис. 3.14. Фізична структура папки з тестами

Наведемо призначення розроблених тестів.

UserPolicyTest.php. Мета: перевірити, що політика UserPolicy коректно реалізує правила доступу до операцій над користувачами відповідно до ролей.

DevicePolicyTest.php. Мета: переконатися, що політика DevicePolicy коректно обмежує доступ до операцій керування пристроями.

AlarmServiceTest.php. Мета: перевірити, що при надходженні сигналу тривоги всі потрібні пристрої відчиняються, при відбої – зачиняються, викликається TelegramBotService, створюються записи в логах.

TelegramPinServiceTest.php. Мета: перевірити, що PIN-код генерується, зберігається в БД, має коректний час дії.

AkuvoxClientTest.php. Мета: перевірити, що клієнт коректно формує HTTP-запит до пристрою та інтерпретує успішну відповідь.

FileDbLoggerTest.php. Мета: перевірити формування та збереження логів пристроїв у файловій структурі FileDB.

ServerHealthServiceTest.php. Мета: переконатися, що при недоступності основного сервера відбувається автоматичне перемикання на резервний.

LoginTest.php. Мета: перевірити коректність виконання авторизації користувача.

AlarmWebhookTest.php. Мета: переконатися, що система правильно приймає сигнали тривоги та ініціює подальшу обробку.

DashboardViewTest.php. Мета: перевірити правильність роботи вебінтерфейсу оператора системи. Тест має підтвердити, що сторінка доступна лише авторизованому користувачу, сторінка правильно відображається, у відповіді присутні необхідні елементи інтерфейсу, дані з моделі успішно передаються до шаблону, відсутній доступ для гостей (неавторизованих користувачів).

У результаті проведення модульного та інтеграційного тестування було перевірено коректність роботи основних компонентів системи керування доступом до захисних укриттв на базі пристроїв Akuvox. Тестування охопило моделі даних, сервіси бізнес-логіки, політики доступу, HTTP-маршрути API, обробку тривог, генерацію PIN-кодів, журнали подій, а також механізм резервування серверів. Проведені тести підтвердили: стабільність доменної моделі (всі моделі коректно взаємодіють між собою, правильно відображають структуру бази даних та забезпечують коректне виконання CRUD-операцій); правильність роботи механізмів авторизації та ролей (доступ до критичних функцій надається виключно відповідним ролям); коректність бізнес-логіки обробки тривог (система належним чином реагує на сигнали тривоги та відбою, викликає необхідні сервіси та виконує керування пристроями); надійність механізму тимчасових PIN-кодів (PIN-коди генеруються, зберігаються, відправляються та валідуються згідно з вимогами безпеки); коректну взаємодію з API пристроїв Akuvox (клієнтські запити формуються правильно, а помилки зовнішнього API належним чином обробляються);

якісну роботу підсистеми журналювання (логи користувачів та пристроїв записуються в MySQL і FileDB, формати даних відповідають визначеним правилам, збереження великих обсягів даних працює коректно); надійність механізму резервування серверів (при недоступності основного сервера ініціюється перемикання на резервний вузол); стабільність API-маршрутів (ключові точки повертають коректні статуси та стабільно виконують необхідні дії); вебінтерфейс оператора системи доступний для авторизованих користувачів, недоступний для гостей, правильно відображується з усіма елементами інтерфейсу.

Загалом, результати тестування свідчать про те, що система працює стабільно, відповідає функціональним вимогам та може бути використана у промисловій експлуатації. Тести підтвердили правильність реалізації бізнес-логіки та відповідність архітектурних рішень вимогам технічного завдання.

ВИСНОВКИ

У процесі дослідження було досягнуто поставлену мету – спроєктовано та розроблено систему керування доступом до захисних укриттів на основі пристроїв Akuvox. Система забезпечує автоматичне (без присутності людини) відчинення та зачинення дверей захисних укриттів на основі даних про повітряні тривоги, а також централізований моніторинг мережі таких пристроїв, розміщених у різних укриттях, для своєчасного вирішення наявних проблем.

Відповідно до поставлених завдань сформульовано такі висновки.

У процесі виконання *першого завдання* проаналізовано інформаційні джерела (нормативні документи, науково-технічні та навчально-методичні публікації, відкриті Інтернет-ресурси) та вивчено предметну область дослідження, пов’язану з функціонуванням захисних укриттів, їхньою інфраструктурою, вимогами до безпеки, а також сучасними підходами до контролю доступу й автоматизації подібних систем.

Аналіз засвідчує, що система захисних укриттів в Україні потребує суттєвої модернізації, оскільки має значні структурні й нормативні недоліки: відсутність інтегрованих житлових укриттів, недостатній розвиток наземних модульних захисних споруд, застарілість багатьох сховищ і низька фактична готовність значної частини інфраструктури. Досвід Фінляндії, Ізраїлю, Швейцарії та інших країн показує, що лише систематична робота з удосконалення стандартів безпеки, розбудови системи укриттів, покращання їхньої доступності, розміщення та технічного оснащення дозволить ефективно захистити цивільне населення в умовах військових дій.

Проаналізовані наукові публікації демонструють низку актуальних світових тенденцій: інтеграція укриттів у житлові й громадські будівлі, що забезпечує швидкий доступ; використання модульних наземних споруд у місцях масового перебування людей; геоінформаційне моделювання

доступності укриттів, зокрема з урахуванням мобільності населення; автоматизація та моніторинг середовища укриттів, що дозволяє зменшити потребу у персоналі; розвиток систем контролю доступу, орієнтованих на безпечну ідентифікацію користувачів, багаторівневі політики авторизації та інтеграцію з IoT-пристроями.

Аналіз моделей контролю доступу (ACL, RBAC, ABAC, UCON, CapBAC) дозволяє зробити висновок, що найбільш перспективними для динамічних середовищ, до яких належать захисні укриття, є контекстно-орієнтовані та атрибутивні моделі, що дозволяють реалізувати гнучкі правила доступу залежно від ролей, станів середовища та зовнішніх подій (зокрема сигналів повітряної тривоги).

З огляду на розширення загроз у світі, інтенсивність збройних конфліктів і низьку фізичну готовність багатьох укриттів, система доступу до захисних споруд має не лише технічну, а й соціальну важливість. Актуальність теми підтверджується як сучасним станом цивільного захисту України, так і міжнародним досвідом, що наголошує на необхідності децентралізованих, автоматизованих і високотехнологічних рішень для захисту населення. Автоматизація доступу до укриттів є логічним етапом розвитку систем цивільного захисту, а розробка відповідного програмного комплексу відповідає сучасним підходам, міжнародним практикам і нагальним потребам українського суспільства.

У процесі виконання *другого завдання* обґрунтовано доцільність розробки програмного комплексу.

Аналіз внутрішніх і зовнішніх факторів (SWOT-аналіз), оцінка ринкового середовища за моделлю п’яти сил Портера, а також аналіз зацікавлених сторін та ризиків підтверджують, що розробка програмного комплексу «Система керування доступом до захисних укриттів на основі пристроїв Akuvox» є доцільною. Система має значний потенціал завдяки сильним сторонам – автоматизації доступу до укриттів, використанню стабільних API пристроїв Akuvox, можливості централізованого керування,

масштабованості, наявності вебінтерфейсу та інтеграції з Telegram-ботом. Ці властивості формують конкурентну перевагу на тлі загальних систем контролю доступу, які не орієнтовані на специфіку цивільного захисту або вирішення вузьких завдань. Разом із тим, виявлено слабкі сторони, зокрема залежність від обладнання конкретного виробника, вимоги до стабільного інтернет-з'єднання, потребу в регулярному технічному обслуговуванні та безпекових аудитах. Ці недоліки можуть бути значною мірою компенсовані використанням зовнішніх можливостей: розширенням інфраструктури зв'язку, удосконаленням внутрішньої логіки системи, підвищенням автономності її компонентів та залученням підтримки органів місцевого самоврядування. Оцінка ринку засвідчує, що конкурентний тиск у вузькому сегменті систем для доступу до укриттів є низьким, а ризик появи прямих замінників – помірний, оскільки увага розробників переважно спрямована на комплексні рішення. Зростання суспільної потреби у швидкому та безпечному доступі до укриттів стимулює формування попиту на такі програмні рішення. Аналіз ризиків демонструє, що основні загрози (збої зв'язку, проблеми з електроживленням, кіберризики, зміни в API) можуть бути ефективно мінімізовані через резервування, використання захищених протоколів, підвищення стійкості архітектури та впровадження регламентованих процедур експлуатації.

Можна стверджувати, що програмний комплекс є конкурентоспроможним і здатним зайняти власну нішу у сфері автоматизованих систем цивільного захисту. Він має перспективи масштабування, інтеграції з іншими елементами інфраструктури безпеки та подальшого функціонального розвитку. Отже, розробка системи є доцільною та відповідає сучасним вимогам до цифрових рішень у сфері захисту населення під час надзвичайних ситуацій.

У процесі виконання *третього завдання* проведено комплексний аналіз сучасних програмних рішень у сфері електронного керування доступом до приміщень, сформульовано технічне завдання на розробку системи керування доступом до захисних укриттів, а також обґрунтовано вибір технологічного

стеку для реалізації проєкту. Розгляд наявних аналогів показав, що попри високий рівень розвитку комерційних систем контролю доступу, жодна з них не забезпечує необхідної для проєкту функціональності, пов'язаної з автоматичним реагуванням на сигнали повітряної тривоги та централізованим керуванням укриттями. Системи ZKBioBL, BAS-IP Link, TTLock, Schlage Home App та Akuvox Smart Access відзначаються високим ступенем технологічності, проте створені для інших сценаріїв використання й не враховують специфічних потреб цивільного захисту населення.

На основі виявлених вимог було сформульовано детальне технічне завдання, яке охоплює архітектуру системи, функціонал окремих модулів, вимоги до продуктивності, безпеки, відмовостійкості та інтеграційних механізмів. Особлива увага приділена організації реагування на тривожні сигнали, підтримці резервних серверів, журналюванню подій, керуванню користувачами й пристроями, а також роботі з Telegram-ботом і Akuvox API. Запропонована архітектура забезпечує комплексність, масштабованість і відповідність вимогам оперативного керування захисними укриттями.

Аналіз варіантів засобів розробки показав, що серед доступних мов програмування та вебфреймворків оптимальним рішенням з урахуванням специфіки проєкту є комбінація PHP 8.1 та Laravel 9, що забезпечує баланс між продуктивністю і зручністю розробки. Як основну СКБД обрано MySQL, яка відповідає вимогам до надійності, транзакційності, швидкодії та витримує типові вебнавантаження. Для зберігання журналів подій обрано файлову базу даних File DB. Для взаємодії із зовнішніми системами використано Akuvox HTTP API та Telegram Bot API, які повністю відповідають функціональним потребам створюваного комплексу. Для розробки клієнтської частини проєкту використано стек HTML / CSS / JavaScript, який є стандартом для створення вебінтерфейсів.

Відповідно до *четвертого завдання* розроблено систему керування доступом до захисних укриттів на основі пристроїв Akuvox, а також документацію до неї. Структура проєкту відповідає вимогам технічного

завдання та забезпечує розділення компонентів системи керування доступом до захисних укриттів на основі пристроїв Akuvox. Основою системи є типовий каркас Laravel, у межах якого виокремлено модулі авторизації, керування користувачами, взаємодії з пристроями Akuvox, обробки тривог, логування, Telegram-інтеграції та механізм резервування з використанням двох серверів. Також розроблено технічний і користувацький опис системи.

Додатково проведено калькулювання собівартості та розрахунок бюджету проєкту. Розрахунковий бюджет проєкту склав 820217,30 грн. за 740 людино-годин з урахуванням залучення п’яти виконавців різного рівня кваліфікації та прибутку 25% від собівартості продукту.

Відповідно до *п’ятого завдання* виконано модульне та інтеграційне тестування розробленої системи з використанням Laravel PHPUnit та виправлено недоліки, виявлені під час тестування. Метою тестування була перевірка коректності реалізації функціональних вимог технічного завдання, оцінка надійності, відмовостійкості та безпечності розробленої системи. Під час тестування було перевірено роботу механізмів автентифікації та авторизації, коректність бізнес-логіки обробки тривог та відбоїв, валідацію генерації й використання тимчасових PIN-кодів, взаємодію з API пристроїв Akuvox, коректність роботи підсистеми журналювання, механізм резервування та перемикання між основним і резервним серверами, ключові HTTP-маршрути, правильність роботи вебінтерфейсу оператора системи. Результати тестування свідчать про те, що система працює стабільно, відповідає функціональним вимогам та може бути використана у промисловій експлуатації.

Отже, поставлені завдання дослідження виконано в повному обсязі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Айко О.В., Василенко О.Д., Степаненко В.М. Системи автоматизації контролю доступу на об'єкти. *Теоретичні і прикладні проблеми фізики, математики та інформатики*: матеріали XXII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених, [Київ], 13−17 травня 2024 р. КПІ ім. Ігоря Сікорського. Київ, 2024. С. 106-108. URL: https://ela.kpi.ua/handle/123456789/67096.

2. BAS-IP Link – програмне забезпечення для віддаленого керування всім функціоналом пристроїв BAS-IP! *basIP*. URL: https://www.bas-ip.com.ua/articles/bas-ip-link-po-dlya-udalyonnogo-upravleniya-vsem-funktsionalom-ustrojstv-bas-ip/.

3. Вареник С.І. Приведення в готовність захисних споруд цивільного захисту з урахуванням умов особливого періоду: навчально-методичний посібник. Кропивницький: НМЦ ЦЗ та БЖД Кіровоградської області, 2023. 72 с.

4. Вертелецький О.О., Нікіфорова Т.Д. Інтегровані захисні укриття цивільного захисту. *Матеріали V науково-практичної конференції студентів, аспірантів і молодих вчених*, (25−26 квітня 2024, Дніпро) : зб. тез. Дніпро: ПДАБА, 2024. С. 123-125. URL: http://srd.pgasa.dp.ua:8080/xmlui/handle/123456789/14971.

5. Гарастовська А.В., Пєтухова О.В. Формування маркетингових стратегій розвитку підприємств молочної галузі за допомогою SWOT-аналізу та PEST-аналізу. *Економіка та суспільство*. 2023. № 57. https://doi.org/10.32782/2524-0072/2023-57-56.

6. Дикань В.Л., Токмакова І.В., Овчиннікова В.О., Корінь М.В., Толстова А.В. Економічна діагностика: Підручник. Харків: УкрДУЗТ, 2022. 284 с.

7. Захисні споруди цивільного захисту. ДБН В.2.2-5:2023. Київ: Міністерство розвитку громад, територій та інфраструктури України, 2023. 131 с.

8. Забезпечення доступності споруд цивільного захисту для маломобільних груп населення. Методичний посібник / Упоряд.: Т. Жидкова, Я. Грибальський. Київ: Національна Асамблея людей з інвалідністю України, 2023. 40 с. URL: https://naiu.org.ua/wp-content/uploads/2023/03/NAIU_AvailabilityOfCivilProtectionStructuresUA_v04.pdf.

9. Іваненко В.С. Захисні споруди: реальний захист населення. *Стратегія розвитку міст: молодь і майбутнє (інноваційний ліфт): поствоєнна розбудова*: матеріали міжнародної науково-практичної конференції, квітень 2023 року. Харків: Харківський національний університет міського господарства імені О.М. Бекетова, 2023. С. 341-346. URL: https://dspace.mnau.edu.ua/jspui/handle/123456789/13726.

10. Іващенко М.В., Бикова Т.Б. SWOT-аналіз процесу впровадження змішаного навчання в закладах вищої освіти. *Електронне наукове фахове видання «Відкрите освітнє е-середовище сучасного університету»*. 2018. № 5. С. 107–115. https://doi.org/10.28925/2414-0325.2018.5.107115.

11. Ільченко М., Гвоздь В., Рудушко І., Бас О. Особливості конструктивних рішень захисних споруд цивільного захисту: Навч. посіб. Черкаси, 2022. 130 с.

12. Іполітова І. Зарплати українських розробників – літо 2025. *Редакція DOU*. 07.07.2025. URL: https://dou.ua/lenta/articles/salary-report-devs-summer-2025/.

13. Казарян А.Г., Теслюк В.М., Коваль В.Я. Використання функції розпізнавання облич для контролю доступу користувачів та автоматизованого управління налаштувань приладів «розумного» будинку. *Моделювання та інформаційні технології*. Вип. 83. С. 180-185.

14. Коваль Б.С., Співак О.А., Козленко О.В., Климук О.С. Мобільні бомбосховища. *Матеріали XV Міжнар. наук.-техн. конф. молодих вчених та*

студентів «Інновації молоді в машинобудуванні», м. Київ, 23 квіт. - 3 трав. 2024 р. Київ: КПІ імені Ігоря Сікорського, 2024. URL: https://imm-mmi.kpi.ua/imm2024/paper/view/30698/17610.

15. Кодекс цивільного захисту України. Відомості Верховної Ради (ВВР), 2013, № 34-35, ст.458. URL: https://zakon.rada.gov.ua/laws/show/5403-17.

16. Кудлаєва Н.В., Круць С.В. Особливості калькулювання собівартості програмного продукту. *Причорноморські економічні студії*. 2019. Вип. 47-2. С. 138-144. https://doi.org/10.32843/bses.47-60.

17. Малліані С.О., Слєпцов О.С. порівняльний аналіз архітектурно-просторових рішень захисних споруд цивільного призначення: досвід України, Фінляндії та Ізраїлю. *Архітектурний вісник КНУБА*. 2025. № 33. С. 121-133. https://doi.org/10.32347/2519-8661.2025.33.121-133.

18. Мартин Є.В., Лясковська С.Є., Тарапата Н.В. Програмне забезпечення для аналізу безпеки бомбосховищ. *Науковий вісник Таврійського державного агротехнологічного університету*. 2019. Т. 9, № 1. URL: https://oj.tsatu.edu.ua/index.php/visnik/article/view/210.

19. Михайлова Р., Антоненко І., Рябова С. Сучасне бомбосховище: актуальні завдання та модернізація. *Актуальні проблеми сучасного дизайну : збірник матеріалів V Міжнародної науково-практичної конференції*, м. Київ, 27 квітня 2023 року. У 2-х т. Т. 2. Київ : КНУТД, 2023. С. 217-220. URL: https://er.knutd.edu.ua/handle/123456789/24751.

20. Олійник Г. Формування архітектури дитячих дошкільних закладів з включенням в їх структуру споруд цивільного захисту. *Proceedings of the XII International Scientific and Practical Conference "New integrations of modern education in universities"* (December 05 - 08, 2023) Amsterdam, Netherlands. International Science Group. 2023. С. 27-31. http://doi.org/10.46299/ISG.2023.2.12.

21. Помазан М.Д., Іщенко С.С. Особливості вентиляції бомбосховищ. *Тиждень науки-2023. Факультет будівництва, архітектури та дизайну. Тези доповідей науково-технічної конференції*, Запоріжжя, 24-28 квітня 2023 р.

[Електронний ресурс]. Запоріжжя : НУ «Запорізька політехніка», 2023. С. 23-25. URL: https://zp.edu.ua/uploads/dept_s&r/2023/conf/4.1/TN_2023-FBAD.pdf.

22. Рибак Л.Я., Кравець П.О. Інтелектуальна інформаційна система «розумний замок» для захисту приміщень. *Вісник Національного університету «Львівська політехніка» «Інформаційні системи та мережі»*. 2019. Вип. 6. С. 41-51. https://doi.org/10.23939/sisn2019.02.041.

23. Рябова С.С., Струмінська Т.В., Антоненко І.В. Бомбосховище: особливості облаштування внутрішнього простору. *Інноватика в освіті, науці та бізнесі: виклики та можливості* : матеріали ІІІ Всеукраїнської конференції здобувачів вищої освіти і молодих учених, м. Київ, 17 листопада 2022 року. Т. 1. Київ: КНУТД, 2022. С. 207-213. URL: https://er.knutd.edu.ua/handle/123456789/22785.

24. Семко О., Філоненко О., Зигун А. Основи проектування захисних споруд цивільного захисту. Полтава: ПП «Астрая», 2024. 121 с.

25. Синчук І.В. Вплив SWOT-аналізу на прийняття управлінських рішень в умовах фінансової кризи. *Молодий вчений*. 2016. № 3(30). С. 174-178. URL: http://molodyvcheny.in.ua/files/journal/2016/3/41.pdf.

26. Тітова В., Кльоц Ю., Мостовий С., Колісник В. Система контролю та управління доступом на основі RFID-технологій. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2023. № 4. С. 44-48. https://doi.org/10.31891/2219-9365-2023-76-5.

27. TTLock. Керівництво користувача. URL: https://trinix.ua/wp-content/uploads/tt-lock_manual_ua.pdf.

28. Управління дверима із ZKBioBL. *ZKTeco Україна*. URL: https://zkteco.systems/ua/solution/door-management/.

29. Хвостенко В. Безпечне укриття: практичні аспекти та поради. Порадник для органів місцевого самоврядування. Київ, 2024. 26 с. URL: https://atilog.ua/wp-content/uploads/bezpechne_ukrittya_praktichni_aspekti_0.pdf.

30. Шумакова В., Абракітов В. Оптимізація розташування бомбосховищ для мирного населення України в житлових масивах населених

місць під час війни. *Наука про цивільний захист як шлях становлення молодих вчених* / Матеріали Всеукраїнської науково-практичної конференції курсантів, студентів, ад'юнктів (аспірантів). Черкаси: Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України, 2023. С. 102-104.

31. Юдін О.К., Весельська О.М. Аналіз та класифікація систем контролю та управління доступом на підприємстві. *Наукоємні технології*. 2018. Т. 38, № 2. С. 220–225. https://doi.org/10.18372/2310-5461.38.12830.

32. 5 сил Портера. *Дія Бізнес*. URL: https://business.diia.gov.ua/entrepreneur-handbook/item/5_syl_Portera.

33. Akuvox Smart Access. *Akuvox. Open A Smart World*. URL: https://www.akuvox.com/smart-access/smb-solution.

34. Ameer S., Benson J., Sandhu R. An Attribute-Based Approach toward a Secured Smart-Home IoT Access Control and a Comparison with a Role-Based Approach. *Information*. 2022. Vol. 13, No. 2. Art. 60. 33 p. https://doi.org/10.3390/info13020060.

35. Get started with ASP.NET Core. URL: https://learn.microsoft.com/en-us/aspnet/core/get-started?view=aspnetcore-10.0.

36. Boluma Mangata B., Mbambi K., Muamba K., Khalaba F. Modeling and implementation of an automatic Access control system for secure premises using facial recognition. *Journal of Computing Research and Innovation*. 2022. Vol. 7, No. 2. P. 11–22. https://doi.org/10.24191/jcrinn.v7i2.273.

37. CodeIgniter User Guide. *CodeIgniter*. URL: https://www.codeigniter.com/userguide3/.

38. Daniyan I.A., Daniyan O.L., Adeodu A.O., Ojaokomo F., Mpofu K. Development of Controlled Alert System for Human Access into Premises. *Journal of Emerging Trends in Engineering and Applied Science*. 2018. Vol. 9, No. 3. P. 140-149. URL: https://journals.co.za/doi/abs/10.10520/EJC-11a1782d58.

39. Galkin A., Samchuk G., Lyfenko S., Botsman A., Braterska N., Hriekova O., Drobotova Y., Tolmachov I. Planning passafeguard in conflict zones and assessment of public transport stop accessibility to shelters. *Transportation*

Research Part A: Policy and Practice. 2025. Vol. 201. Art. 104669. https://doi.org/10.1016/j.tra.2025.104669.

40. HTTP API manual for Akuvox Intercom. URL: https://data.nag.wiki/Akuvox/E12S/Documentation/Akuvox HTTP API Manual 20220610.pdf.

41. Jiao H., Feng S. Towards Resilient Cities: Optimizing Shelter Site Selection and Disaster Prevention Life Circle Construction Using GIS and Supply-Demand Considerations. *Sustainability*. 2024. Vol. 16, No. 6. Art. 2345. https://doi.org/10.3390/su16062345.

42. Jörgen A., Łątka J.F., Tarczewski R., Szcześniak Z., Pieńko B., Morales-Beltran M., Gromek D., Kosztołowicz L. Design of Shelters for Civilians in the Event of Armed Conflict: State of the Art and Contemporary Design Guidelines. *Środowisko Mieszkaniowe / Housing Environment*. 2025. No. 52. e2025019. P. 91-99. https://doi.org/10.2478/he-2025-0019.

43. Kaczmarek K. Finland's Security System: Lessons for Central and Eastern Europe. *Ius et Securitas*. 2024. No. 2. P. 133-142. URL: https://iusetsecuritas.pl/wp-content/uploads/2025/04/8_Krzysztof-Kaczmarek.pdf.

44. Kwon N., Cho J., Ahn Y., Kim J., Park Y.-J. Developing a Framework for Evaluating Project Feasibility of Disaster Management Facilities: Case Studies of Two Protective Shelters in South Korea. *Journal of Management in Engineering*. 2024. Vol. 41, Issue 1. https://doi.org/10.1061/JMENEA.MEENG-6067.

45. Laminas Documentation. Laminas Project. URL: https://docs.laminas.dev/.

46. Laravel. Official Documentation. URL: https://laravel.com/docs/12.x.

47. Microsoft Intelligent Data Platform. URL: https://www.microsoft.com/en-us/sql-server/.

48. Mohammad Z.N., Farha F., Abuassba A.O.M., Yang S., Zhou F. Access control and authorization in smart homes: A survey. *Tsinghua Science and Technology*. 2021. Vol. 26, No. 6. P. 906-917. https://doi.org/10.26599/TST.2021.9010001.

49. MySQL Documentation. URL: https://dev.mysql.com/doc/.

50. Node.js v25.2.1 documentation. URL: https://nodejs.org/docs/latest/api/.

51. Phalcon Framework: A PHP framework built as an extension for PHP. URL: https://docs.phalcon.io/5.9/introduction/.

52. PHP Manual. URL: https://www.php.net/manual/en/.

53. Porter M.E. The Five Competitive Forces That Shape Strategy. *Harvard Business Review*. 2008. P. 25-40. URL: https://piazza.com/class_profile/get_resource/iyd2tysc6fj5aa/iyxgbroqf172cb.

54. PostgreSQL Documentation. URL: https://www.postgresql.org/docs/.

55. SQLite Documentation. URL: https://sqlite.org/docs.html.

56. Stay connected with Schlage Home app. *Schlage*. URL: https://www.schlage.com/en/home/smart-locks/schlage-app.html.

57. Stolojescu-Crisan C., Crisan C., Butunoi B.-P. Access control and surveillance in a smart home. *High-Confidence Computing*. 2022. Vol. 2. Art. 100036. 9 p. https://doi.org/10.1016/j.hcc.2021.100036.

58. Symfony Documentation. URL: https://symfony.com/doc.

59. Telegram Bot API. URL: https://core.telegram.org/bots/api.

60. Vasylenko M.P., Zahorna A.R. Security System for Office Premises with Use of Modern Information Technologies. *Electronics and Control Systems*. 2025. Vol. 2, No. 84. P. 63-67. https://doi.org/10.18372/1990-5548.84.20195.

61. Wu X., Sun F., Zhang X., Wang W. Research and Design of an Unattended Shelter Environmental Parameter Monitoring System. *2025 IEEE 14th International Conference on Communications, Circuits and Systems (ICCCAS)*, Wuhan, China, 2025. Pp. 583-588. https://doi.org/10.1109/ICCCAS65806.2025.11102321.

62. The Definitive Guide to Yii 2.0. *Yii Framework*. URL: https://www.yiiframework.com/doc/guide/2.0/en.

ДОДАТОК

Розрахунок бюджету проєкту «Система керування доступом до захисних укриттів на основі пристроїв Akuvox»

Розрахунок бюджету проєкту виконано на основі підходу, описаного Н. Кудлаєвою та С. Круцем [16].

Таблиця 1

Пропозиції для меж коефіцієнта кваліфікації

Кваліфікація фахівця	Межа коефіцієнта кваліфікації
Senior	8–10
Intermediate	5–7
Junior	3–4
Trainee	1–2

Таблиця 2

Розрахунок базового окладу за одну годину роботи (у 2025 р.), USD

Посада	Кваліфікація фахівця	Норма годин за рік (40-годинний роб. тиждень)	Середня норма годин в 1 місяці	Оклад (USD)	Оклад за 1 годину роботи (USD)
Програміст, керівник групи	Senior	1993	166	4450	26,81
Програміст-верстальник	Junior	1993	166	950	5,72
Вебдизайнер	Trainee	1993	166	376	2,27
Програміст пристроїв Akuvox	Middle	1993	166	2400	14,46
Тестувальник	Middle	1993	166	2400	14,46

Таблиця 3

Розрахунок надбавки за складність виконуваних робіт, USD

Посада	Характер робіт	Різноманітність / комплексність робіт	Самостійність виконання робіт	Масштаб і складність керівництва	Додаткова відповідальність	Сумарний розрахунковий показник	Середній розрахунковий показник	Максимальна надбавка (USD)	Надбавка (USD)
Програміст, керівник групи	10	10	10	10	10	50	10	110	110
Програміст-верстальник	4	3	2	3	3	15	3	110	33
Вебдизайнер	3	2	1	2	2	10	2	110	22
Програміст пристроїв Akuvox	7	6	6	6	5	30	6	110	66
Тестувальник	6	5	7	5	4	27	5,4	110	59,4

Таблиця 4

Розрахунок доплати за кваліфікацію ІТ-фахівця (за кваліфікаційними характеристиками)

Доплата за кваліфікацію працівника	Коефіцієнт кваліфікації	Сума доплати (USD)
Максимальний розрахунковий коефіцієнт	10	120
Програміст, керівник групи	10	120
Програміст-верстальник	3	36
Вебдизайнер	2	24
Програміст пристроїв Akuvox	6	72
Тестувальник	5,4	64,8

Таблиця 5

Бюджет на оплату послуг ІТ-фахівців

Посада	Кваліфікація фахівця	Оклад за 1 годину роботи (USD)	Надбавка за складність робіт (USD)	Доплата за кваліфікацію працівника (USD)	Кількість годин	Оклад (USD)	Оплата за послуги фахівців (USD)	Оплата за послуги фахівців (грн.)
Програміст, ке-	Senior	26,81	110	120	290	7774,9	8004,9	337726,73

рівник групи								

Продовження табл. 5

Посада	Кваліфікація фахівця	Оклад за 1 годину роботи (USD)	Надбавка за складність робіт (USD)	Доплата за кваліфікацію працівника (USD)	Кількість годин	Оклад (USD)	Оплата за послуги фахівців (USD)	Оплата за послуги фахівців (грн.)
Програміст-верстальник	Junior	5,72	33	36	210	1201,2	1270,2	53589,74
Вебдизайнер	Trainee	2,27	22	24	100	227	273	11517,87
Програміст пристроїв Akuvox	Middle	14,46	66	72	100	1446	1584	66828,96
Тестувальник	Middle	14,46	59,4	64,8	40	578,4	702,6	29642,69
Бюджет за послуги з програмування	-	-	**290,4**	**316,8**	**740**	**11227,5**	**11834,7**	**499305,99**

Таблиця 6

Розрахунок ліквідаційної вартості та амортизаційних відрахувань

Показник	Розрахунок	Вартість за 1 одиницю (грн.)	Сума за 5 одиниць (грн.)
Вартість ноутбука	-	36000,00	180000
Ліквідаційна вартість	1% від вартості	360	1800
Амортизація за 1 рік	(вартість – ліквідаційна вартість) / 3 роки	11880	59400
Амортизація за період розробки (740 год.)	(амортизація за 1 рік – норма годин на рік) * кількість годин роботи	4411,039	22055,19

Таблиця 7

Калькулювання собівартості програмного продукту

Показник	Розрахунок собівартості програмного продукту, грн.
Фонд оплати праці	499306
ЄСВ (22%)	109847,3
Військовий збір (5%)	24965,3
Амортизація	22055,19
Собівартість	656173,8
Прибуток, 25%	164043,5
Бюджет проєкту	**820217,3**