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

Пояснювальна записка

до магістерської кваліфікаційної роботи

на тему: «Система програмно-технічного захисту музейного виставкового експонату»

08-20.МКР.010.00.000 ПЗ

Виконав: студент 2 курсу, групи 1БС-18м
спеціальність 125 – Кібербезпека

_____ Мусійчук М.Т.

Керівник: к. т. н., доц. каф. ЗІ

_____ Куперштейн Л.М.

Рецензент
к. т. н., доц., доц. каф. ОТ

_____ Крупельницький Л.В.

Вінниця – 2019 року

АНОТАЦІЯ

В магістерській кваліфікаційній роботі було розроблено охоронну систему захисту музейного виставкового експонату, яка є стійкою до втручання зловмисників. Було проведено наукове-дослідне обґрунтування доцільності досліджень, аналіз існуючих систем захисту, а також розроблено структурну та електричну схему пристрою та розраховано надійність системи. Також був розроблений мобільний додаток для керування системою віддалено. В економічному розділі оцінено затрати на розробку та її доцільність.

ABSTRACT

At the comprehensive master's qualification work was considered the security system of protection the museum exhibit resistant to intruder intruders. The research substantiation of expediency of researches, analysis an existing protection systems were conducted, as well as the structural and electrical scheme of the device was developed and the system reliability was calculated. Also there was developed mobile application for managing system. The economic section evaluates the cost of development and her expediency.

ЗМІСТ

ВСТУП

Сьогодні питання із захищеності об'єкта стають все більш актуальними та користуються попитом для будь-якого об'єкта бізнесу, житла, виробництва, об'єктів соціального призначення та особистого життя. Охоронні системи захисту є одними з найбільш важливих напрямків у сфері безпеки. Вони забезпечують необхідний рівень захисту і значно зменшують втручання людей у вирішенні питань здійснення контролю за важливими об'єктами цілодобово.

Головне призначення охоронної системи полягає в оперативному і гарантованому сповіщенні правоохоронні служби про несанкціоноване втручання. Рішення даної задачі можливе тільки при правильному оснащенні об'єкта охорони сучасними високонадійними технічними засобами охоронної сигналізації.

В даний час розробники технічних засобів охорони працюють над впровадженням в системи методи машинного навчання і штучний інтелект. Спеціалізовані алгоритми оброблятимуть сигнали від датчиків і активовувати їх. Це знизить навантаження у співробітників, збільшить ефективність охорони.

Об’єктом магістерської кваліфікаційної роботи є процеси захисту музейного виставкового експонату від несанкціонованого доступу.

Предмет дослідження є системи захисту музейного виставкового експонату.

Метою магістерської кваліфікаційної роботи є покращення рівня захищеності музейного виставкового експонату від несанкціонованого доступу.

Для досягнення мети необхідно розв’язати такі задачі:

- дослідити та проаналізувати існуючі аналоги, зробити висновки щодо їхнього рівня захисту;
- провести техніко-економічне обґрунтування розробленого пристрою;
- розробити та обґрунтувати вибір апаратної складової;
- розробка програмної частини системи захисту;
- розрахувати затрати на реалізацію апаратної та програмної частини;
- виконати тестування коректності роботи програмно-технічної системи.

Наукова новизна. Запропоновано комбіновано модель системи захисту музейного виставкового експонату, яка відрізняється розширеними функціональними можливостями у вигляді комбінованих систем захисту об'єктів з додатковими сповіщеннями про фізичне втручання до об'єкту захисту, що дозволяє підвищити захищеність від несанкціонованого доступу.

Практична цінність полягає у тому, що розроблено систему захисту музейного виставкового експонату у вигляді програмно-апаратного комплексу на базі мікроконтролерної платформи Arduino.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Науково технічне обґрунтування проблеми

Музеї і галереї зіштовхують зі все більш складними завданнями у сфері безпеки в зв'язку зі зростанням кількості озброєних пограбувань за останні 10 років. Нажаль, але потрібно всього лише 58 секунд для викрадення картини. Охорона безцінних предметів є особливо важливим завданням для публічних музеїв та галерей. Ці установи зіштовхуються з дилемою: необхідно зберегти експонати у безпеці і в той ж час дати шанс мільйонам відвідувачів побачити їх.

Предметом захисту в музеї може бути будь-що: пам'ятки культури, об'єкти природи, твори всіх видів образотворчого і декоративного мистецтва, пам'ятки писемності, дорогоцінне каміння, картини, старовинний одяг тощо [1]. Для забезпечення захисту музейних установ та експонатів відносять такі заходи безпеки, які зображені на рис.1.1.

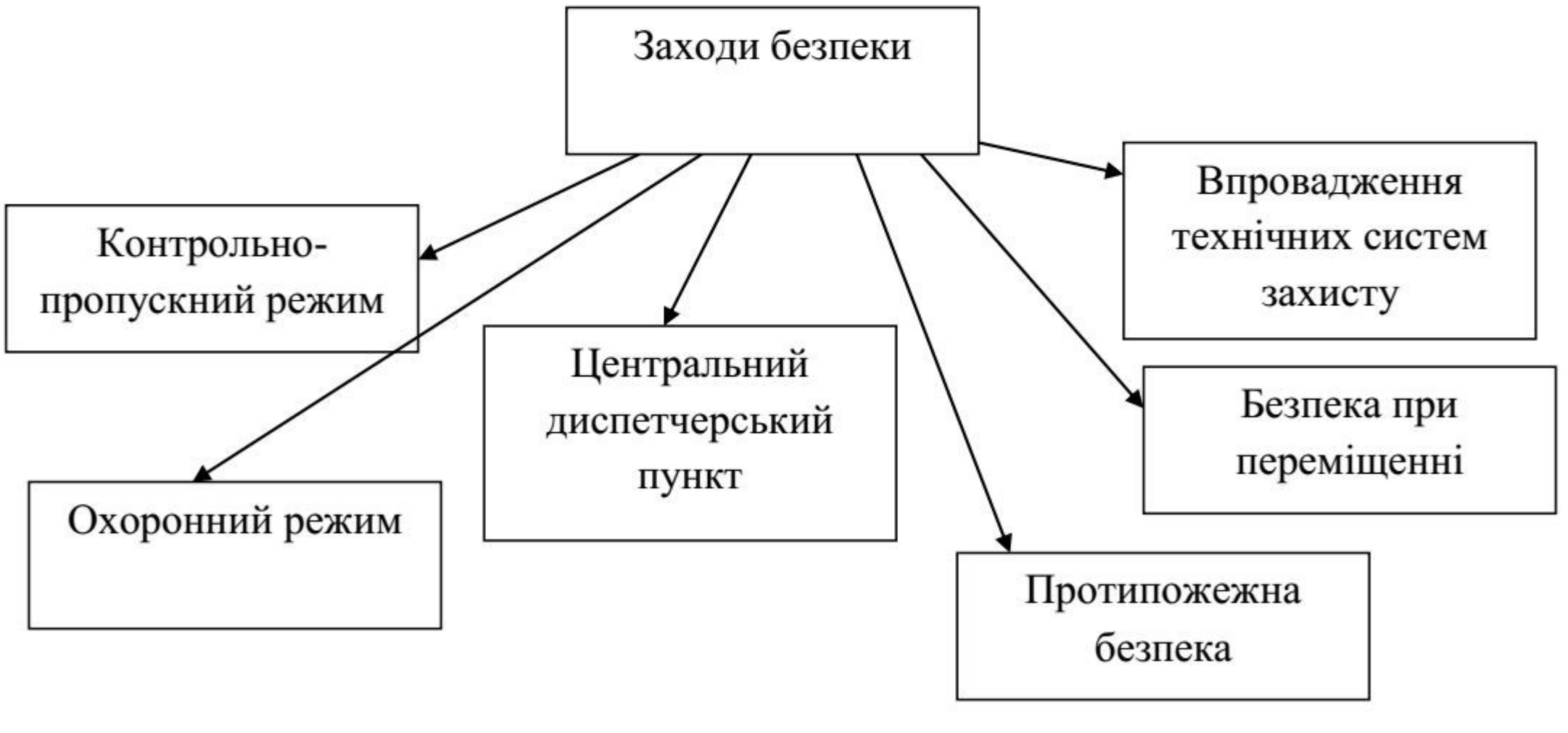


Рисунок 1.1 – Існуючі заходи безпеки музейних установ

Задачею охоронного режиму є забезпечення правопорядку, безперервне спостерігання за експонатами, забезпечення пропускного режиму, виклик групи

швидкого реагування, патрулювання території згідно з графіком, приймання та здача під охорону матеріальних цінностей, ключів.

Контрольно-пропускний режим встановлює порядок проходу громадян, проїзду транспортних засобів, переміщення культурних і матеріальних цінностей на територію музейних установ, оформлення пропусків і тощо.

Система заходів щодо забезпечення пожарної безпеки в установах складається з трьох основних груп заходів [2]:

- встановлення протипожежного режиму;
- підтримка належного протипожежного стану у всіх місця;
- контроль за виконанням правил пожежної безпеки при експлуатації, ремонту, обслуговування приміщень.

Небезпека музейних експонатів може відбутися при транспортуванні. До організації безпеки музейних експонатів при транспортуванні відносяться:

- спільне планування організації під'їздів, вантажно-розвантажувальних зон;
- організація перевезень дорогоцінних металів;
- дотримання правил упаковки та транспортування музейних експонатів;
- страхування музейних експонатів;
- маркування музейних експонатів з цілю подальшої ідентифікації.

Комплексна система безпеки музейного експонату являється складною інформаційною системою. Для досягнення ефективності функціонування таких систем потрібно відповідне обладнання збору інформації від різних засобів виявлення (сповіщення охороною, відеокамери, датчиків вологості і температури, тощо). Для цього в складовій системи повинні бути:

- системи передачі інформації;
- системи диспетчерського контролю і керування інженерними мережами музейного об'єкта, побудованими на базі програмно-технічних засобів;

– центрального диспетчерського пульта керування системою.

Оснащення музейних експонатів технічними системами безпеки має відбуватися комплексно в обов'язковому порядку на етапі робіт пов'язаних з створенням чи підсиленням захисту нерухомих пам'ятків історії чи культури.

За останні 10 років з музеїв, фондів, приватних колекцій поцупили в 10 разів більше культурних цінностей, ніж за попереднє десятиріччя, а кількість обікрадених музеїв зросла вдвічі. Об’єктами нападів стають невеликі музеї, розташовані в невеликих містах, селах, які мають статус народних музеїв і є муніципальними. Причиною тому є убоге фінансування, незахищеність, інколи навіть людська психологія [2].

За минулий рік в Україні було викрадено 56 музейних експонатів, з них 17 картин, інші – переважно нумізматика і це лише у двох областях. Серед викрадених картин: «Перебування Т. Г. Шевченка в науці у диякона Єфрема», «Портрет сестри Оксани» та «Портрет Агафії (Теренової Гапки)» 1895 року - автор І. Макушенка, «Колодязь» 2010 р. автор Ю. Іщенко, «Коліївщина» І. Губасного 1987 року, «Тиха вулиця» 1984 року І. Бондар та інші.

Серед зниклих експонатів в Україні також є дві монети римської імперії II-IV ст. до н. е., фрагмент лимісного динарія Андріана 138 р. н.е.; два півторагрошовика Сигізмунда III 1620-го та 1625 з дорогоцінного металу білону, дві мідні монети Російської імперії датовані 1753, шість швецьких солідів (золотих монет) Густава Адольфа 1631 року та інші нумізматичні предмети.

Проблемою є те що впровадження цих заходів не забезпечить повністю захист музейним експонатам. Таким чином розроблюваний пристрій в магістерській кваліфікаційній роботі набуває високої актуальності, оскільки сучасний стан захисту музейних виставкових експонатів є досить вразливим, а розроблювана система забезпечить максимально високу захищеність від несанкціонованого доступу.

1.2 Аналіз можливих загроз та факторів їх виникненняв музеях

Світовий досвід, створення систем безпеки для установ культури дозволяє виділити три основні елементи, що входять до складу будь-якої установи, і вимагають забезпечення їх безпеки і збереження [2]:

- люди (суб'єкти) – персонал і відвідувачі, співробітники служби безпеки і охорони;
- об'єкти, території, будівлі, споруди, інженерне обладнання матеріальні цінності, в першу чергу музейні експонати, колекції, що охороняються;
- інформаційно-комунікаційна система музею, база даних музею, інформація і канали її передачі та прийому.

Кожен з виділених елементів має свої особливості, які необхідно враховувати при визначенні можливих загроз.

Основні групи загроз групуються наступним чином:

- група загроз, пов'язана з порушенням режимів зберігання та експлуатації;
- група загроз кримінального і терористичного характеру (крадіжки, злодійство, вимагання, акти вандалізму, грабежі);
- група загроз пов'язана з порушенням правил безпеки (підпали, самозайманння з різних причин);
- група загроз техногенного характеру (протікання, відключення електрики, обвалення, ураження електричним струмом);
- група загроз стихійного характеру (урагани, повені, лісові пожежі).

Головною проблемою забезпечення безпеки музейних установ є відсутність своєчасного аналізу і прогнозу потенційних загроз. В основному служби безпеки музею реагують на те, що трапилося, тоді як необхідно прогнозувати заздалегідь усі можливі заходи захисту і запобігати потенційній загрозі.

Аналізуючи різні загрози як зовнішні (з боку відвідувачів, виходу з ладу обладнання, стихійних лих та ін.), так і внутрішні (з боку персоналу музею,

обслуговуючих організацій та ін.) необхідно розглядати різні моделі поведінки порушника. Під порушником в загальному вигляді можна розглядати особу або групу осіб, які в результаті навмисних або ненавмисних дій забезпечує реалізацію загроз безпеки музейного закладу [5]. Модель порушника визначає:

- категорії, які можуть впливати на об'єкт;
- цілі, які можуть переслідувати порушники кожної категорії, можливий кількісний склад, використовувані інструменти, приладдя, оснащення, зброю;
- типові сценарії можливих дій порушників, які описують послідовність дій груп та окремих порушників, способи їх дій на кожному етапі.

Для загроз порушення режимів збереження, характерні наступні моделі порушників (основними особами, які вчиняють порушення є співробітники музею):

- пошкодження збереження музейних предметів в слідстві порушення умов зберігання: температурно-вологісного режиму, світлового режиму;
- пошкодження стану будівель і ландшафтних територій в слідстві порушення режимів експлуатації;
- втрата стану музейних предметів, будівель, територій через відсутність своєчасного проведення реставраційних робіт;
- пошкодження матеріальних і культурних цінностей під час транспортування, вантажно-розвантажувальних роботах.

Для загроз кримінального та терористичного характерні наступні моделі порушників:

- організована, добре технічно-підготовлена група, що має чітко розроблений план розкрадання або грабежу дорогих музейних предметів, знайома з особливостями музейної установи, а також з використовуваними технічними засобами охорони, існуючим режимом охорони, використовуваному каналу передачі тривожних повідомлень

на пост охорони. Технічні засоби передбачуваного порушника можуть мати можливість глушіння GSM-каналу, прослуховування радіоканалу взаємодії постів охорони, що має в своєму складі зброю, сучасні технічні засоби злому елементів інженерної укріпленості. Наявність в складі групи порушників співробітників музею (в гіршому випадку співробітників служби безпеки або охорони) передбачає наявність безперешкодного доступу до місця розміщення головного обладнання технічних систем безпеки. Однак в даному випадку це не є важливим чинником, тому що передбачається, що технічне забезпечення та професійна підготовка порушника забезпечить виведення з ладу існуючі технічні засоби безпеки (або середовище їх передачі на пост охорони). До даної категорії порушників також відносяться і групи, націлені на вчинення терористичних актів на території музейних установ;

– організована злочинна група, що має своєю метою матеріальне збагачення за рахунок крадіжки наявних в музеї матеріально-культурних цінностей. Технічне оснащення і кваліфікацію порушника можна охарактеризувати як поганий або задовільний (тобто рівень оснащення не перевищує рівень існуючого обладнання системи безпеки, що не дозволить порушникові здійснити її злом і відключення). Найчастіше відсутність необхідного технічного забезпечення порушника в даному випадку компенсується залученням співробітників безпеки або охорони музейного установи, що дозволяє отримати порушнику безперешкодний доступ на пост охорони;

– випадковий, непідготовлений порушник, який вирішив скористатися зручним випадком в роботі персоналу музею або технічних систем безпеки для здійснення крадіжки; до цієї групи також

входять порушники, що мають на меті вчинення актів вандалізму (в першу чергу будівель і територій установи).

Найбільш складним з точки зору своєчасного виявлення є модель організованого, добре підготовленого порушника, при якій відбувається перенаправлення уваги служби безпеки музейного закладу на найбільш очікувану, але помилкову модель порушення [6].

Для загроз, пов'язаних з порушенням правил пожежної безпеки характерні такі моделі розвитку ситуації:

– загорання внаслідок незадовільного стану електропроводки будівлі;
– загорання внаслідок незадовільного стану елементів електроустановки будівлі (розподільні щити, вимикачі);
– загорання дерев'яних будівель і необмежене поширення вогню внаслідок відсутності системи захисту від блискавок;
– загорання, пов'язані з порушенням протипожежного режиму (куріння в не відведених місцях, порушення при організація вогневих робіт);
– загибель людей, в слідстві відсутності системи оповіщення при пожежі, відсутність необхідних евакуаційних шляхів, втрати матеріальнокультурних цінностей через невиконання планів евакуації при пожежі.

1.3 Аналіз існуючих охоронних систем захисту експонатів

Будь-який музейник експонат потребує захисту від зловмисників, саме тому охоронні системи захисту музейних експонатів мають неабияку цінність. І з кожним роком ці системи вдосконалюються, але крадіжок менше не стає. Розглянемо системи, які вже присутні на ринку.

Система UATAG (див. рис. 1.2) є визначною подією для музейної діяльності, бо дозволяє швидко та значно дешевше за експертизу, гарантовано ідентифікувати автентичність предметів та убезпечити їх від підміни [8], яка базується на:

- унікальних бирках із листового прозорого скла з непідробною фактурою тріщин (фізичний захист);
- розподіленій базі даних Blockchain (цифровий захист), захищеній від підробки та переробки;
- надійній підтримці переліку цифрових записів, що постійно зростають.

Рисунок 1.2 - UATAG – Вигляд скляного ідентифікатора справжності

Винайдена технологія ідентифікації автентичності предметів є надійною на підставі неповторності візерунка скляних тріщин, які є унікальним ідентифікатором конкретного предмета, забезпечує:

- неможливість повторного використання клейкої стрічки, якою бирка кріпиться до експоната;
- 100% гарантію захисту ексклюзивних предметів від підробок;
- миттєву візуальну перевірку оригінальності бирки, яку неможливо використати повторно;
- абсолютну неможливість підробки бирки, що гарантує недоторканість чи непідміну експоната.

Встановлення справжності певного об’єкта відбувається шляхом візуального порівняння унікального візерунка тріщин на прозорому склі бирки. Цей візерунок є

невід'ємною частиною пристрою для ідентифікації оригінальності предметів UATAG із його електронним відображенням із захищеної бази даних.

Застосування бирки ідентифікації автентичності предметів може бути надзвичайно широким – всюди, де існує теоретична можливість підміни оригінала на фальсифікат і де експертна перевірка оригінальності буде набагато дорожчою, ніж використання бирки ідентифікації. Наприклад, для музейних предметів (картин, посуду, одягу, предметів нумізматики, фалеристики, цінних документів) дії можуть бути такими: після висновку експерта бирка, яка закріплена за цим експертом, кріпиться на музейному експонаті відповідним чином (кріплення за допомогою клейкої стрічки, протягування нитки крізь отвори). В іншому разі, оригінальний музейний експонат, найретельніше перевірений групою експертів, за 5 хв. після перевірки може бути замінений перед експонуванням. При використанні запропонованих бирок такий ризик мінімізовано, бо в музейних працівників буде документ про його оригінальність.

Як працює система UATAG:

- бирка з унікальним "відбитком" тріщин на склі прикріпляється до предмета за допомогою невідривної стрічки (пломби);
- у разі виникнення сумнівів у автентичності походження предмета користувач сканує QR-код, нанесений на стрічку бирки, за допомогою будь-якого мобільному додатку для зчитування QR-кодів, і потрапляє на сторінку, де міститься інформація про бирку-ідентифікатор, предмет, якому вона належить, та власника або виробника цього предмету;
- користувач порівнює скляний візерунок бирки-ідентифікатора, що тримає в руках, із зображенням, яке видає захищена база даних методом накладання або співставлення. Це можливо без застосування жодних рідерів, сканерів та іншого технічного обладнання;

– якщо фактура тріщин бирки-ідентифікатора, яка прикріплена до предмета, матиме збіг із фактурою тріщин на фото, оригінальність (точніше – відсутність підміни предмету) буде підтверджена.

Загалом це дуже корисна система захисту, але вона не забезпечує безпеку музейному експонату, тому що коли експонат буде викрадено то вже не буде що перевіряти і дізнаватися чи це підробка чи ні.

Також музеї використовують таку систему, як Tecsar Alert Ward (див. рис. 1.3). Ця система - це комплект бездротової сигналізація для охорони дорогоцінних об’єктів [9]. Комплект призначений для самостійної установки.

Ця сигналізація може працювати в двох режимах:

– на охороні – виявивши вторгнення датчики передають сигнал по радіоканалу на центральний блок і він включає зовнішню звукову тривогу;

– знятий з охорони – сигналізація не реагує на сигнали датчиків, крім датчиків диму, газу, затоплення.

Рисунок 1.3 – Вигляд системи охорони Tecsar Alert Ward

Використання системи охорони Tecsar Alert Ward не передбачає абонплати охоронним службам. Єдиними можливими грошовими витратами, після покупки даної сигналізації, будуть поповнення sim-карти обраного оператора. Щомісячний внесок якої буде залежати від обраного користувачем тарифу та способу експлуатації.

Основними недоліками цієї системи є:

- швидко сідають батарейки в датчиків руху;
- хибне спрацювання датчиків;
- незручне користування;
- нечутлива клавіатура на пульті.

Охоронна система Alfa KS-SF05R (див. рис. 1.4) це незамінна, проста в обігу і ефективна система захисту експонатів економ класу [10]. Принцип роботи та налаштування є дуже простими. Для початку роботи досить встановити всі датчики в обраних вами місцях та після цього потрібно увімкнути в ятір сирену, яка є головним пристроєм приймачем, пульт, який знаходиться в комплекті виконує функцію підключення всіх датчиків з приймачем при наведенні на сирену при затиску червоної кнопки на 3-5 секунд. І після цього охоронна система готова до використання.

Рисунок 1.4 – Вигляд охоронної системи Alfa KS-SF05R

Використання так само просте і ефективне. Для постановки в режим охорони досить натиснути кнопку “ARM” на пульті, для зняття з охорони кнопка “DISARM”. При виявленні руху, або при розмиканні датчика відкриття спрацьовує гучна сирена, потужністю 70 дБ. Система Alfa KS-SF05R здатна надійно забезпечити охорону невеликих приміщень, наприклад, дача, будинок, квартира, склад, магазин, ларьок, торгова точка, гараж і т.д

Система Alfa KS-SF05R має такі недоліки як:

- замала гучність сирени;
- дуже мала перешкодозахищеність;
- відсутність сповіщення на центральний пульт;
- відсутність інтелектуальної частини в функціоналі пристрою.

Очевидно, що з безлічі сучасних охоронних систем неможливо виділити одну, яка була б універсальною і якнайкращою зі всіх аспектів. При виборі і проектуванні системи охорони необхідно враховувати безліч чинників, що безпосередньо впливають на роботу такої системи. Таким чином, після аналізу існуючих охоронних систем музейних експонатів можна відзначити деякі пункти, а саме те, що на ринку не представлено охоронної системи, яка могла б захистити експонати належним чином і з відповідним функціоналом і доступною ціною, тому доцільність розробленого пристрою не викликає сумніву.

1.4 Формалізація вимог та постановка задачі

Програмно-технічні системи захисту є досить надійними для охорони музейного виставкового експонату. В таких системах можна використовувати будь-який набір датчиків відповідно до цілей, яких потрібно досягти, що і є значною перевагою, а також можливість швидкодії сповіщення охорону чи власників при порушенні системи та простоті керування.

Підсумовуючи те що сказане, розроблювана система програмно-технічного захисту це ресурсоємкий процес розробки програмного та апаратного

забезпечення, але при правильній побудові програмно-технічної системи та розробці мобільного додатку, вона буде досить простою в користуванні та багатофункціональна одночасно і по доступній ціні.

Вимоги до роботи наступні:

- простота в користуванні системою;
- доступна ціна пристрою;
- можливіст керування системою віддалено;
- можливість сповіщення при порушенні захисту віддалено;
- можливість сповіщення за допомогою сирени;
- наявність захисту завдяки ультразвуковим датчикам;
- забезпечення надійності завдяку датчику руху та магнітогерконовому датчику;
- розробка мобільного додатку для керування системою захисту та збереження останніх повідомлень;
- можливість контролю безпеки за тиском.

Програмно-технічна система захисту повинна бути запрограмована таким чином, щоб при спрацюванні різних датчиків (ультразвуку, тиску, руху) сигналізація повідомила про це вповноважену особу та ввімкнулась сирена.

Для реалізації апаратної частини було обрано платформу Arduino, як систему управління (контролера), оскільки дана платформа дозволяє швидко та якісно створити пристрій з можливістю тестування в реальних умовах, а ціна системи буде значно нижча в порівнянні з конкурентами.

Мобільний додаток був реалізований за допомогою фреймворку React Native. Завдяки кроссплатформленості та набіром можливостей виконувати нативний функціонал, мобільний додаток покращить систему логувань та дозволить керувати прогрпмно-технічною системою з будь-якої віддаленої точки за допомогою мобільного телефона з операційною системою IOS чи Android.

Даний вибір компонентів дає змогу розробити програмно-технічну систему захисту на основі GSM-SIM800l, більш функціональною, ніж аналогічні системи на ринку, але значно зменшить її вартість та покращить швидкість передачі повідомлень завдяки їй.

В даному розділі було проведено аналіз існуючих охоронних систем. В результаті отримано вимоги до програмно-технічної системи захисту, обрано платформу та набір охоронних сповіщувачів для розробки для найбільш зручної та продуктивної функціональності пристрою.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ ЗАХИСТУ

2.1 Аналіз об’єкта захисту

Система програмно-технічного захисту музейного експонату, яка розробляється в магістерській роботі призначена для захисту дорогоцінних речей в музеях.

Основне призначення системи програмно-технічного захисту музейних експонатів – захист та виявлення зловмисників, які хочуть викрасти старовинні картини, дорогоцінні коштовності, монети, старовинну оздоблену дорогоцінним камінням зброю та багато інших витворів мистецтва. Багато систем забезпечує захист музейним експонатам від несанкціонованого доступу та цілісності музейним експонатам постійним наглядом та має можливість вмикати сигналізацію при різних порушенях:

- доторкання до об'єктів захисту;
- розбиття скла;
- відкриття дверей;
- рух біля об’єкту захисту;
- дуже голосного сповіщення;
- пересування або зміщення об'єкту захисту.

Дана система захисту, яка розроблена в магістерській кваліфікаційній роботі забезпечує захист експонатів за допомогою належного та комплексного розміщення датчиків навколо об’єкта захисту, що забезпечує захист експонатів з різних сторін та швидкісного сповіщення за допомогою мобільного додатку. Для зручного розташування експонатів був запропонований макет для об'єктів захисту, який зображений на рисунку 2.1.

На плані макету для об’єктів захисту розміщений маленький виступ на якому будуть знаходитися різні об’єкти захисту. Враховуючи особливість макету для об’єкту захисту було задане наступне розташування датчиків, для забезпечення

повної безпеки, яке зображено на рис. 2.2. Було запропоновано встановлення датчиків таким чином, що кожен номер датчика це:

1. Датчик ультразвуку.
2. Магнітогерконовий датчик.
3. Датчик тиску.
4. Датчик руху.

Датчик ультразвуку повинен розміщуватись навпроти об’єкту захисту для того, щоб у разі викрадення чи переміщення об’єкта він спрацював та включилася сирена. Датчик спрацьовує на зміну довжини дистанції між об’єктом та датчиком.

Магнітогерконовий датчик повинен розміщуватися зверху для контролю підняття чи опускання скла і у разі чого він спрацює та включиться сирена, ще перед тим як об’єкт буде викрадений, що завчасно запобігає планам зловмисників.

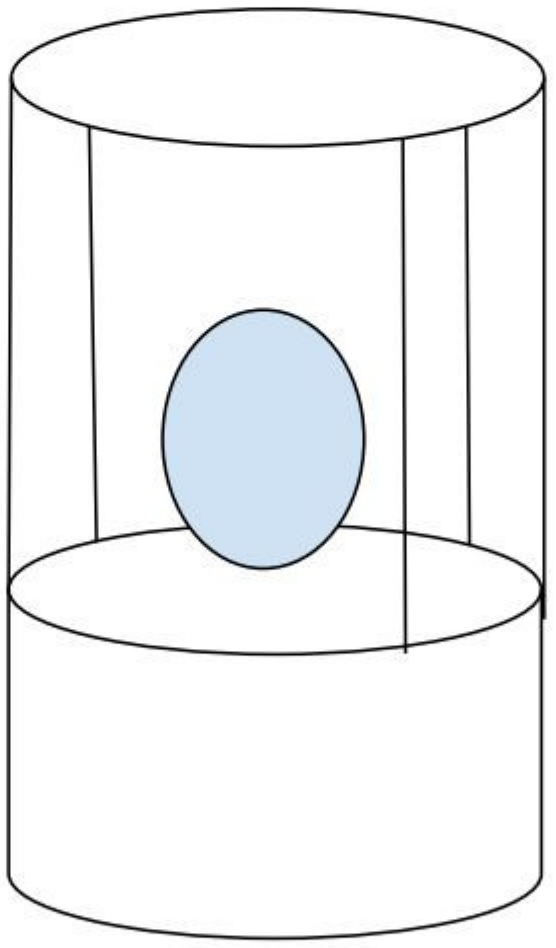


Рисунок 2.1 – Модель для об’єктів захисту

Датчик тиску повинен знаходитися під об’єктом і контролювати вагу покладену на нього. Якщо вага буде змінена, тобто об’єкт буде піднятий то спрацює датчик тиску, який відправить сигнал для увімкнення сигналізації та сповіщення охорони.

Датчик руху повинен розміщуватися зверху для контролю наближення будь-кого зі зловмисників до скла. Якщо датчик руху виявить якийсь рух, який відбувається зверху, тобто це означає що хтось наблизився та хоче підняти скло, то відправлятиметься сигнал попередження про небезпеку.

Завдяки такому розміщенню датчиків, можна з впевненістю задтвердити, що об’єкт захисту не буде викрадений непоміченим. При розташуванні належним чином визначається, що об’єкт захищений зі всіх сторін склом, а також оточений різними датчиками, які забезпечують огляд навколо. Зловмисник не зможе підійти близько до об’єкта непоміченим, тому що з кожної сторони і навіть зверху слідкують різні датчики захисту об’єкта.

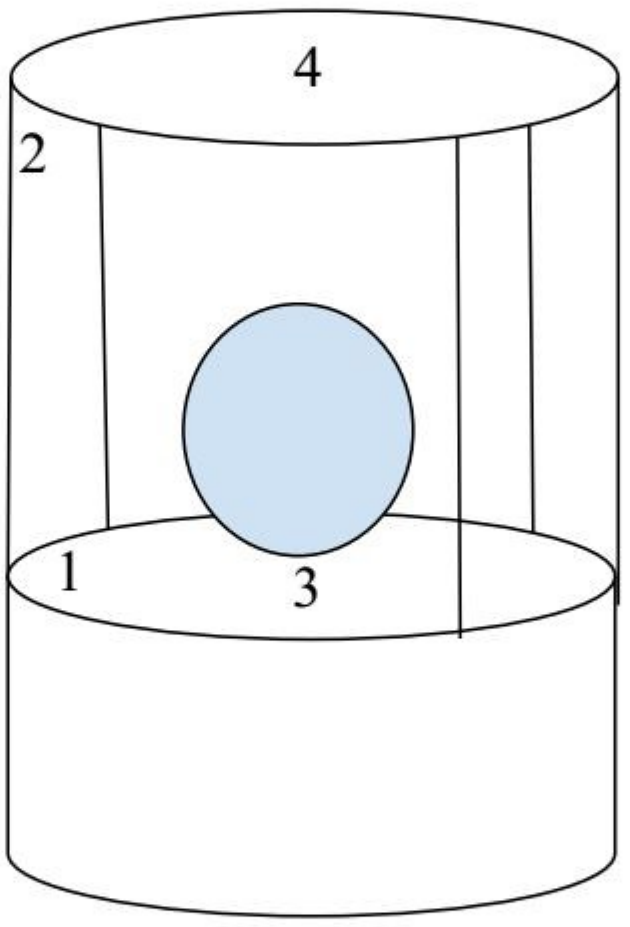


Рисунок 2.2 – Розміщення датчиків захисту виставкового експонату

Підсумовуючи вищесказане можна з впевненістю сказати що, завдяки такому розміщенню датчиків захисту, система забезпечує захист від несанкціонованого доступу до об'єкта захисту і також надає можливість повного сповіщення службу охорону про будь-які маніпуляції з цим об’єктом.

2.2 Розробка загальної структури апаратного засобу

Структура системи програмно-технічного захисту музейних експонатів розроблялася для забезпечення надійності і захисту на найвищому рівні експонатів від зловмисників і для досягнення цієї цілі знадобилися компоненти, які будуть забезпечувати безпеку експонатам:

- датчики ультразвуку;
- датчик тиску;
- GSM-модуль;
- Arduino Nano;
- автономний акумулятор;
- контролер напруги;
- магнітний датчик;
- датчик руху.

Слід зазначити, що перші два датчики, які наведені вище повністю впроваджують захист музейним експонатам, вони забезпечують захист об'єктам до яких буде неможливо пройти непомітно не заставивши їх спрацювати. Завдяки магнітному датчику та датчику руху буде також спрацьоване звукове сповіщення про небезпеку та надсилання застережливого повідомлення завдяки GSM-модуля та сповіщення на телефон у мобільний додаток в якому буде відбуватися логування про те що відбувається з експонатом у музеї.

Служба охорони або власник музею або музейних експонатів можуть слідкувати за своїми музейними експонатами через додаток у мобільному телефоні, в якому буде відбуватися запис дій, які відбуваються з музейним експонатом.

Взаємозв'язок апаратної частини з мобільним додатком відбувається за допомогою GSM-модуля. На апаратний пристрій приходить повідомлення з командою для увімкнення датчиків та запуску системи і коли якийсь з цих датчиків спрацював, то GSM-модуль відправляє у відповідь повідомлення, яка містить інформацію про те який датчик спрацював і що відбувається з системою.

Структурна модель системи програмно-апаратного засобу захисту зображено на рис. 2.3.

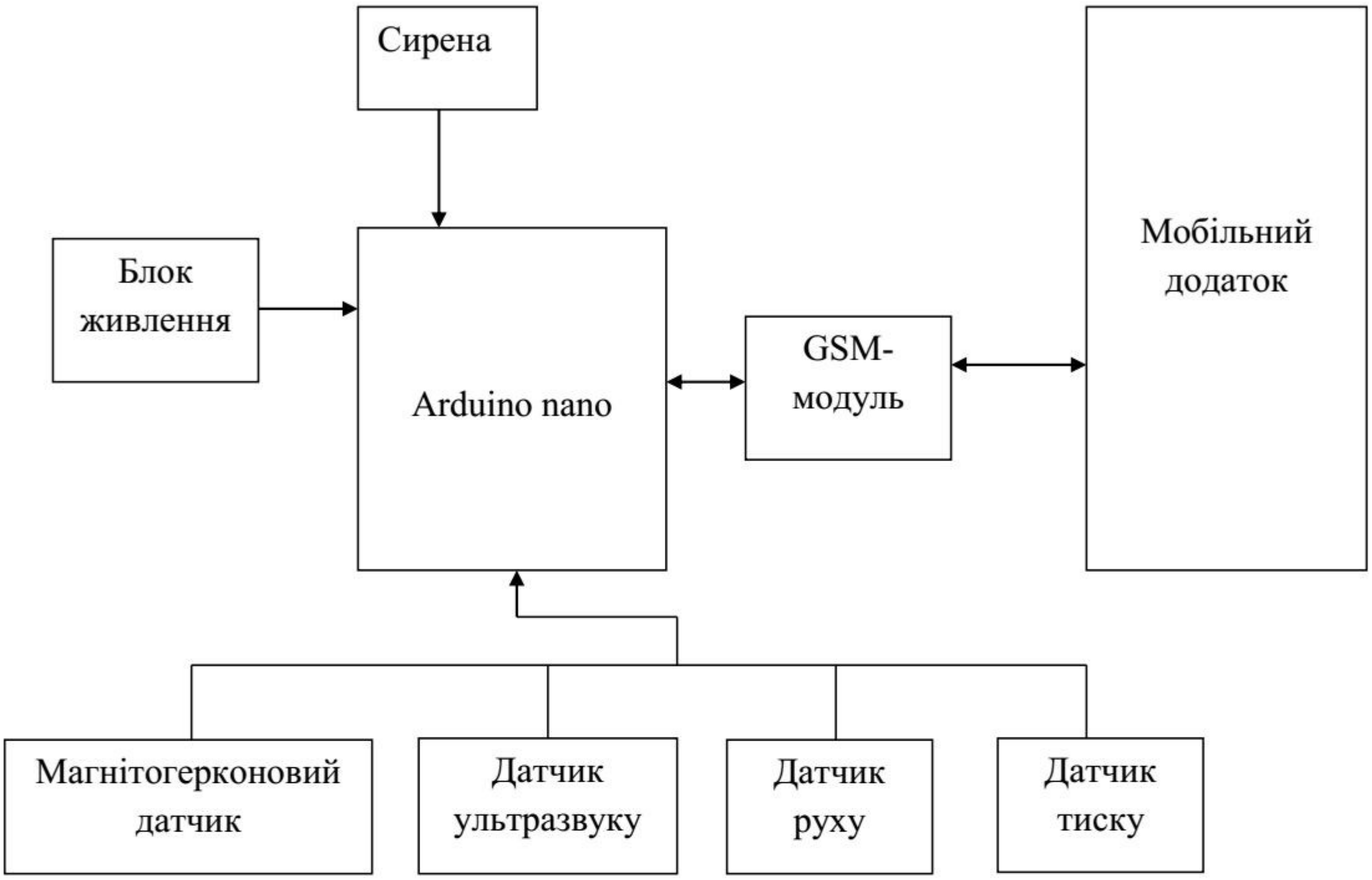


Рисунок 2.3 – Структурна модель системи програмно-апаратного захисту

Загальний алгоритм роботи апаратної частини системи програмно-технічного захисту зображено на рис. 2.4. За цим алгоритмом система повинна:

- при запуску системи захисту на GSM-модуль повинен прийти код, який активує систему та переведе усі датчики в активний режим;
- коли якийсь з активних датчиків спрацювали, то вмикається звукове сповіщення та відправляється повідомлення до служби охорони;
- якщо нічого не відбувається датчики залишаються в активному режимі і чекають на їхнє спрацювання.

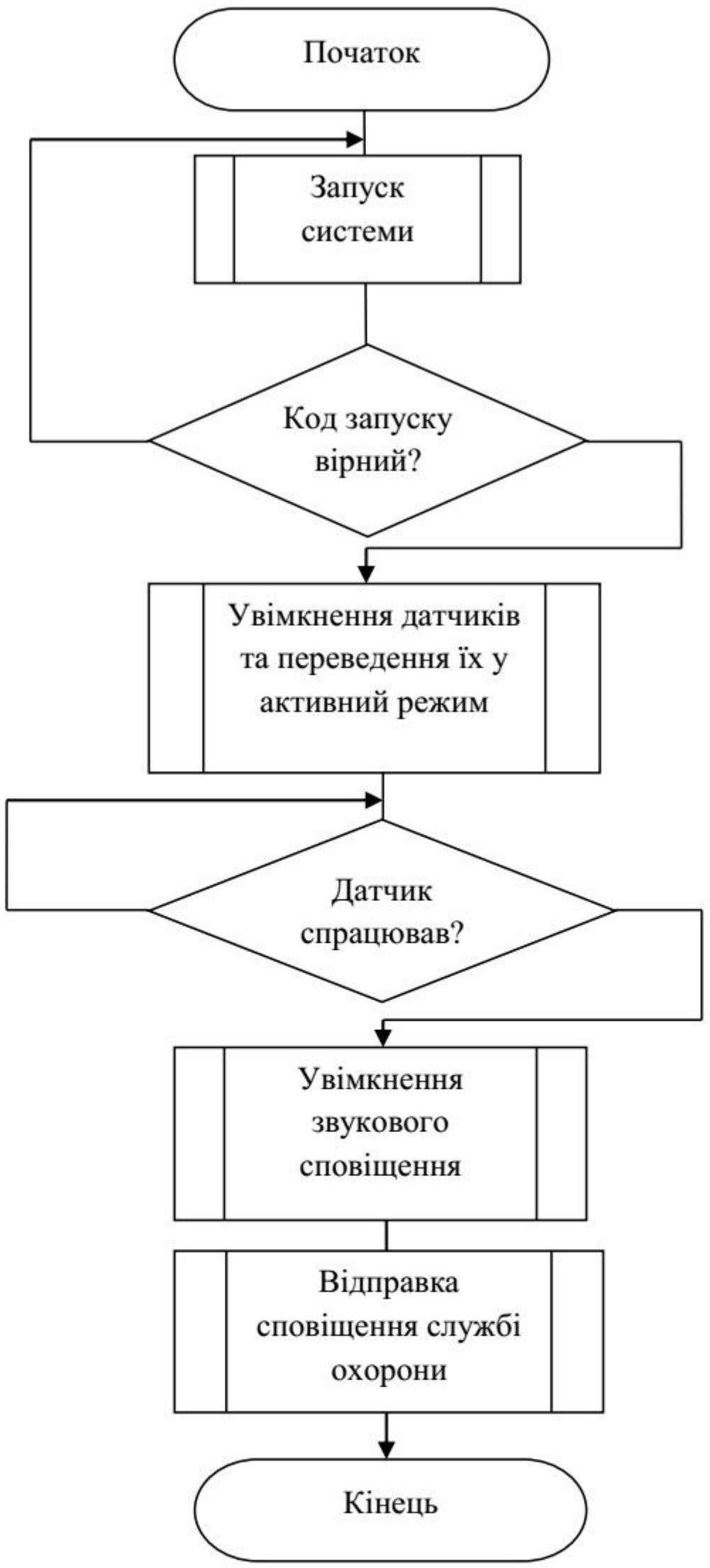


Рисунок 2.4 – Загальний алгоритм роботи апаратної частини

Завдяки розробленому алгоритму система програмно-технічного захисту музейних експонатів забезпечують захист від зловмисників та сповіщення про будь-який несанкціонований доступ до об'єкту захисту.

2.3 Обґрунтування вибору засобів розробки мобільного додатку

У магістерській комплексній роботі був також розроблений мобільний додаток для керування системою захисту музейних експонатів. Для розробки було обрано React Native [11].

React Native – це фреймворк для створення мобільних додатків для операційних систем IOS та Android, створений компанією Facebook.

Крім загальної кодової бази між декількома платформами, з'являється можливість повторного використання коду з веб-додатком. Це дійсно дуже цікавий наслідок, який скоротить як тимчасові витрати на розробку, так і кількість необхідних для розробки продукту інженерів.

Додатки React Native дозволяють використовувати нативні елементи інтерфейсів з операційної системи, одночасно підтримуючи парадигму React в JavaScript.

Те, що робить React Native дійсно функціональним, – той факт, що є можливість отримати доступ до всіх API через рідне середовище. Не потрібно додаткове зіставлення шарів, яке необхідно оновлювати.

Додатки на React Native пишуться на мові JavaScript – на одній з найпопулярніших мов програмування. Розробник пише основну частину коду на Javascript - спільною мовою для всіх платформ, а цей код взаємодіє з нативними компонентами операційних систем. В результаті ми отримуємо мобільні додатки, що працюють на всіх існуючих платформах (iOS, Android, Universal Windows Platform).

Кросплатформеність і простота розробки зменшують час, необхідне для реалізації проекту (якщо порівнювати з нативної розробкою). Додатково на терміни позитивно впливає підтримка з боку розвиненого спільноти розробників React: у відкритому доступі є велика кількість плагінів (модулів), які можна використовувати в React Native. Їх застосування також спрощує роботу розробника.

Додатки, розроблені на React Native, близькі до нативним судячи з поведінки і зовнішнього вигляду. Це реальні мобільні додатки, і вони відповідають очікуванням користувача, який звик використовувати Android або iOS. У певному сенсі React Native займає свою нішу в сфері мобільного розробки: він ідеально підходить для тих випадків, коли потрібна швидкість нативних додатків, але не потрібна їх складність (тобто для невеликих і середніх додатків).

Безсумнівною перевагою React Native є простота об'єднання з компонентами нативного коду програми (написаного на Objective C або Swift під iOS або на Java під Android). З одного боку, можна додавати нативні компоненти в додатки, розроблені на React Native, якщо, наприклад, потрібна більш висока продуктивність. З іншого боку, можна використовувати компоненти React Native в нативних додатках, щоб, наприклад, додати певні функції відразу на обидві платформи (як наприклад, в Instagram).

На даний момент існує достатньо фреймворків, які використовують JavaScript для створення iOS та Android додатків, таких як PhoneGap або Titanium. Проте React Native має перед ними ряд переваг [12]:

1. На відміну від PhoneGap, в React Native логіка додатка пишеться і працює на JavaScript, в той час як його інтерфейс залишається повністю нативним. Таким чином не потрібно ніяких компромісів, характерних для HTML5 UI.

2. На відміну від Titanium, React вводить новий оригінальний і вкрай ефективний підхід до створення призначених для користувача інтерфейсів. Якщо говорити коротко, UI додатки виражається як функція поточного стану програми.

Ключова особливість React Native в тому, що його розробники мають намір принести модель програмування React в сферу розробки мобільних додатків.

Якщо у вас є досвід створення програмного забезпечення на Objective-C або Swift, ви напевно не зрадієте ідеї переходу на JavaScript. Але разом з тим, другий пункт явно мав зацікавити Swift-розробників. Безсумнівно, працюючи зі Swift, вам доводилося вивчати багато нових і більш ефективних способів шифрування

алгоритмів, а також методик, що сприяють перетворенню і незмінності. Проте, спосіб побудови UI тут дуже схожий на той, що використовується при роботі з Objective-C: він теж грунтується на UIKit і є імперативним.

React за рахунок таких новітніх понять як Virtual DOM і узгодженню переносить функціональне програмування на шар призначений для інтерфейсу користувача.

Беручи до уваги усі вищесказані плюси обраного фреймворку, можна сказати що React Native чудово підходить для розроблюваного додатку, так як він використовує нативні елементи розробки, такі як зчитування та відправлення повідомлень, за допомогою яких відбуватиметься керуванням приладом. А також підтримка використання додатку на різних мобільних пристроях з операційними системами IOS та Android.

2.4 Обґрунтування вибору компонентів системи захисту

Програмно-технічна система захисту музейних експонатів від зловмисників, що виконувалася у магістерській кваліфікаційній роботі складається з наступних елементів:

- плата Arduino Nano;
- датчик ультразвуку HC-SR04;
- GSM модуль SIM 800L;
- автономний акумулятор;
- датчик тиску Sparkfun (DAT118);
- сирена SHD 4216;
- датчик руху DP-102;
- магнітний датчик DCS-40;

У якості плати для блоку обробки даних було обрано Arduino Nano [5], так як плата є компромісом ціна - якість, а портів для вводу даних та їх виводу вистачить для реалізації системи (рис 2.5).

Рисунок 2.5 – Плата Arduino Nano

Плата Arduino Nano - це повнофункціональний мініатюрний пристрій на базі мікроконтролера ATmega 328(Arduino 3.0) або ATmega 168 (Arduino Nano 2.x), адаптований для використання з макетної плати. Arduino Nano є дуже схожий за функціональністю на Arduino Duemilanove, але їх відмінність в тому що вони різні за розмірами та відсутністю роз'єму живлення, а також відрізняється за типом USB-кабелю(Mini-B) [9]. Також перевагою Arduino є низька ціна в порівнянні з більшістю подібних платформ та кросплатформленість. З нею можна працювати хоч з Windows, хоч з Mac OS. Характеристики даної плати:

- мікроконтролер - ATmega168 чи ATmega328;
- робоча напруга – 5В;
- рекомендована напруга живлення – 7-12В;
- гранична напруга живлення – 6-20В;
- цифрові входи / виходи – 14;
- аналогові входи – 8;
- Flash-память – 16 КБ чи 32 КБ;
- SRAM – 1 КБ чи 2 КБ;
- EEPROM – 512 Б чи 1 КБ;
- Тактова частота – 16 МГц;

Для звукового сповіщення про небезпеку був обраний модуль SHD 4216 (рис. 2.6). Даний модуль на основі п'єзоелектричного зумера використовується для подачі звукових сигналів [14]. Його гучність залежить від подачі напруги. Характеристики модуля звукового сповіщення:

- робоча напруга – 3-24 В;
- номынальна робоча напруга – 12 В;
- робочий струм – до 12 мА;
- гучність – 95 дБ;
- довжина проводів – 15 см;
- частота звуку - 3000 ± 500 Гц;
- розмір корпусу - 4.2 х 1.6 см;

Рисунок 2.6 – Вигляд модуля SHD-4216 для звукового сповіщення

Також у систему програмного-технічного захисту був доданий датчик руху DP-102 (рис. 2.7), який працює на основі інфрачервоного пасивного датчика і який має довгий термін роботи та легко підключається до плати Arduino [16]. Технічні характеристики модуля датчика руху:

- зона огляду – до 12 метрів;
- вага – 6 г;
- мінімальна кількість часу між показниками – 0.2 іс;
- область виявлення - 110° х 70°;

Основний недолік є те, що цей датчик унеможливлює калібрування від уникнення помилкових спрацювань, але у той ж час є нецмовірно чутливий до наближення різних об’єктів.

Рисунок 2.7 – Вигляд модуля датчика руху DP-102

Для підключення різних пристроїв до GSM мережі використовується модуль GSM SIM-800L (рис. 2.8) з можливістю легкого підключення, взаємодією з платою Arduino Nano, а також є можливість підключення додаткових антен для покращення якості сигналу [15]. Основні технічні відомості про модуль:

- GPRS class – 12;
- номінальна робоча напруга – 3.7 – 2.4 В;
- підтримка мережі – 4х діапазона мережа, 900/1800/1900 МГц;
- струм режиму очікування – 0.7 мА;
- максимальний струм – 500 мА;
- робоча температура – -30 до 75 градусів;
- розміри - 25х23мм;

Рисунок 2.8 – Вигляд модуля GSM SIM-800L

Для контролю стану відкриття використовується магнітогерконовий датчик DCS-40 (рис. 2.9), який є пластиковим та накладного типу [17]. Його основна перевага між іншими датчиками є різниця в ціні, так як його формування базується на простіших принципах розробки, які не поступаються іншим аналогам. Встановлення і перебування його непомітним для зловмисників відбувається завдяки його незначним розмірам.

Рисунок 2.9 – Вигляд модуля магнітогерконового датчика DCS-40

Ультразвуковий датчик відстані HC-SR04, призначений для вимірювання відстаней від 2 до 400 см, а межа його точності може досягати до 3 мм [18]. Модуль включає ультразвуковий передач, приймач і вузол контролю. На покази датчика практично не впливають сонячні промені та електромагнітні шуми.

Рисунок 2.10 – Вигляд ультразвукового датчика HC-SR04

Використовується ультразвуковий давай HC-SR04 за наглядом цінних об’єктів. Технічні характеристики ультразвукового датчика HC-SR04:

- робоча напруга – 3.8-5.5 В;
- робочий струм – 8 мА;
- мінімальна дистанція – 2 см;
- максимальна дистанція – 400 см;
- частота ультразвуку – 40kHz;
- кут зору – 30 градусів;

Для зміни свого опору в залежності від сили прикладеної до нього використовується датчик тиску DAT118 (рис. 2.11). Чим більший тиск на нього, тим менший його опір. Без тиску опору складає близько 1 мОм. Резистор може фіксувати вагу від 100 г до 10 кг, що чудово підходить під об'єкт захисту [19].

Рисунок 2.11 – Вигляд датчика тиску DAT118

Також у системі програмно-технічного захисту використовується акумулятор ємністю 18650 А, для його автономного використання у випадках відключення електроенергії.

На основі вищесказаних датчиків, в системі програмно-технічного захисту передбачено використання апаратного пристрою тому було розроблено схему електричну принципову. Дана схема зображена на рисунку 2.12.

Для забезпечення живлення всієї системи використовується два понижуючих конвертера D1, D2 для напруги 3.3В та 5В відповідно. Основна частина схеми живиться від напруги 5В, але так як нам необхідно забезпечити резистори для

підтяжок для цифрових ліній, то необхідно використати додатковий конвертер для 3,3В.

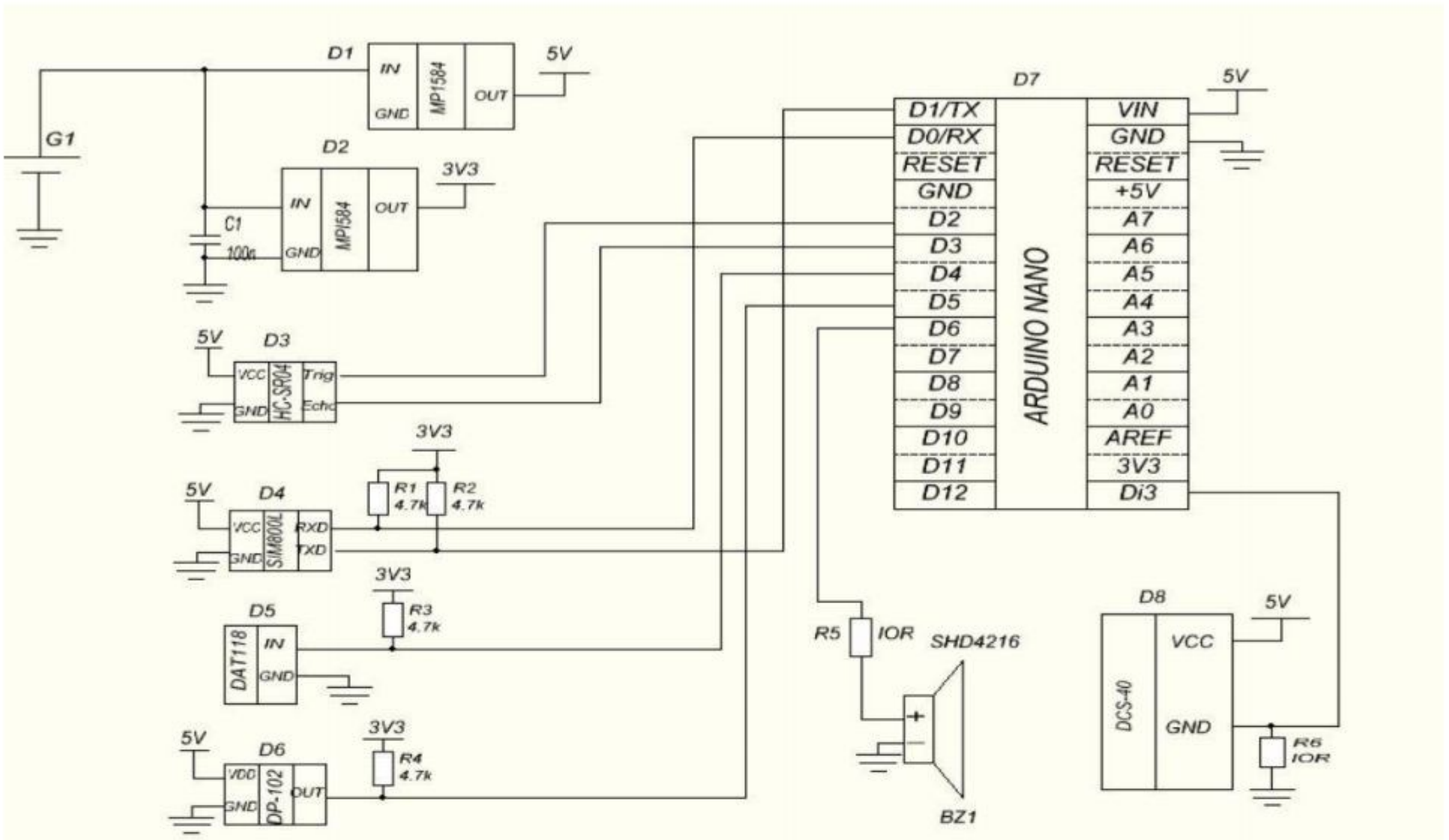


Рисунок 2.12 – Схема електрична принципова

Кожний з елементів схеми потрібно приєднати до головного модуля. Використовуючи інформаційні порти вводу/виводу D1-D13 в головному модулі D7 приєднуються всі інші компоненти схеми відповідно до кількості їхніх портів.

Наприклад інформаційні порти сенсора SIM800L приєднуються до портів D1, D0 модуля Arduino Nano, де ці зв’язки визначаються в прошивці для головного модуля, яка буде керувати всією системою.

Отже елементи апаратної частини наведені вище дозволять забезпечити захист музейним експонатам та реалізувати запланований функціонал в повній мірі та за низькою ціною.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ

3.1 Розробка програмного забезпечення для апаратної частини

Система програмно-технічного захисту музейних експонатів розроблялася за допомогою Arduino Nano для обробки даних. Система розроблялася в Arduino Studio (див. рис. 3.1.) за допомогою мови програмування C++. Arduino Studio це апаратна обчислювальна платформа для аматорського конструювання, основними компонентами якої є плата мікроконтролера з елементами вводу/виводу [20].

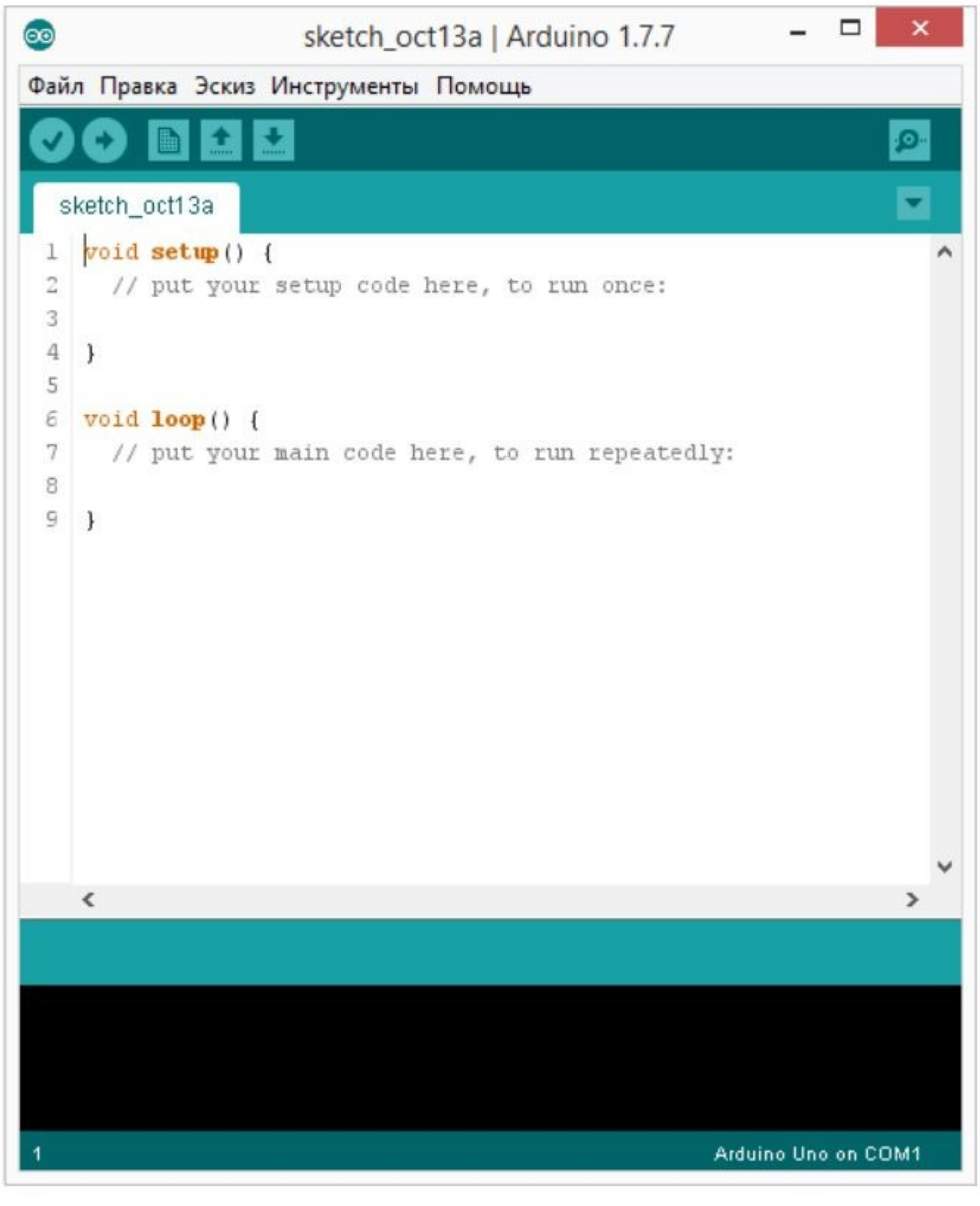


Рисунок 3.1 – Вигляд середовища програмування Android Studio

На початку виконання програмного коду ми ініцілізуємо датчики сенсору, ультразвуку, зумер, геркон, датчик тиску, а далі створюємо смс-повідомлення, які

будуть приходити при тій чи іншій команді, а також номер телефону на який будуть відправлятися повідомлення про викрадення, наближення тощо.

```
int moveSensor = 8;
int switchPin = 4; //Gercon
int trigPin = 2;
int echoPin = 3;
int zummerPin = 9;
int powerSensor = A0;

char smsbuffer[160];
char PowerOFF[] = "Sirena is off";
char sirena[] = "Sirena is on!";
char sms1[] = "Warning!!! Moving is detected";
char smsW[] = "Security is active!";
char sendsms[160];
String phoneNumber = "+380632754682";
```

За керуванням системою відповідає функція retrieveSms(), її логіка полягає в увімкненні система віддалено та її ввимкненні, за допомогою GSM-модуля, який приймає 0 або 1 і в залежності від команди відбувається та чи інша дія.

```
void retriveSMS()
{
    // Retrieve SMS value.
    uint16_t smslen;
    if (!fona.readSMS(1, replybuffer, 250, &smslen))
    {
        Serial.println("Failed!");
    }
    Serial.println(replybuffer);
    int command = atoi(replybuffer);
    if (command == 1)
    {
        sendMessage("Systema is working (1)");
        systemIsWork = true;
    }

    if (command == 0)
    {
        sendMessage("Systema is off (0)");
        isSrenaOn = false;
```

```
        systemIsWork = false;
    }

    fona.deleteSMS(1); }
```

А повідомлення відправляються за допомогою функції sendMessage(), в параметр яких приймаються, як стрічки, які потрібно відправити на телефон через GSM-пристрій.

```
void sendMessage(String text)
{
    char number[20];
    phoneNumber.toCharArray(number, 20);
    char sms[100];
    text.toCharArray(sms, 100);
    fona.sendSMS(number, sms);
    fona.deleteSMS(1);
}
```

Завдяки методам checkMoveSensor(), checkFSRSensor(), checkDistanceSensor() реалізовано спрацювання сигналізації при зміні руху біля об'єкту захисту, викрадення об'єкта захисту з датчика тиску, та зміна довжини за допомогою датчика ультразвуку, який вимірює зміни до об'єкта захисту.

```
        if (moveSensorData > 0)
        {
            isSrenaOn = true;
            sendMessage("Module of movement is working! HELP!!!");
        }

    if (fsrReading == 0)
        {
            isSrenaOn = true;
            sendMessage("Module of pressure is working HELP!!!");
        }

        if (abs(defaultDistance - distance_sm) > 10)
            {
                isSrenaOn = true;
                sendMessage("Module of ultrasound is working!!! HELP!!!")
;
            }
```

Спрацювання системи сповіщення відбувається завдяки реалізованій функції startSirena(), яка приймає параметри zummerPin та isSirenaOn та якщо параметр isSirenaOn має значення true, то система вмикається, а zummerPin дає змогу дізнатися, який датчик спрацював.

```
void startSirena()
{
    digitalWrite(zummerPin, isSirenaOn);
}
```

Отже, завдяки вищенаведеній програмній реалізації можна зрозуміти, як працює система програмно-технічного захисту, де задіяні усі датчики для підвищення захисту від несанкціонованого доступу та забезпечує надійність збереження об’єкта в цілісності.

3.2 Розробка мобільного додатку керування

В даному розділі було розроблено мобільний додаток та його тестування. Додаток буде використовуватися для віддаленого керування системою захисту музейних експонатів та зчитування повідомлень від системи.

У додатку використовувалася зовнішня бібліотека для отримання, зчитування та відправлення повідомлень. Назва бібліотеки – react-native-get-sms-android. Додаток має тільки одну панель керування системою захисту, що робить її дуже зручною для використання користувачам. Вигляд головної панелі мобільного додатку зображений на рис. 3.2.

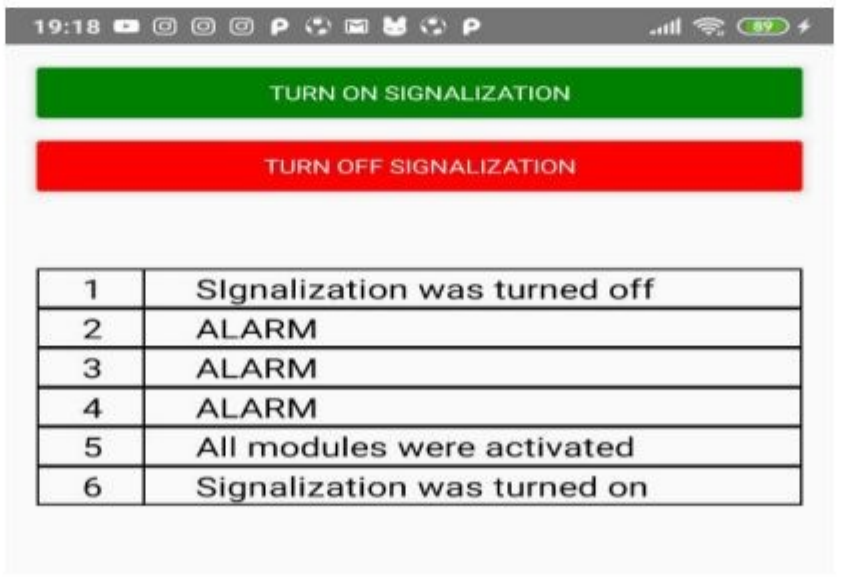


Рисунок 3.2 – Вигляд головної панелі мобільного додатку

За допомогою мобільного додатку користувач може віддалено увімкнути та ввимкнути сигналізацію за допомогою двох допоміжних кнопок на головному екрані, які знаходяться зверху. При натисканні на будь-яку з цих кнопок користувач додатку має можливість отримати повідомлення про успішне увімкнення або вимкнення сигналізації. Ці дані записуються у сховище для отримання детальної інформації, що відбувається із системою. А також за допомогою цього додатку користувач може бачити стан програмно-технічної системи захисту музейного експонату: увімкнена чи ввимкнена система, в якому стані знаходяться датчики системи і найголовніше користувач може бачити, що в систему міг проникнути зловмисник та побачити це у системі логування програмно-технічного засобу та те що сигналізація чи якісь з датчиків вже спрацювали.

За керуванням станом системи програмно-технічного захисту в мобільному додатку відповідає функція:

```
sendSms(command){
  SmsAndroid.autoSend(
    "+380632754682",
    command,
    (fail) => {
      console.log('Failed with this error: ' + fail);
    },
    (success) => {
      console.log('SMS sent successfully');
    },
  );
}
```

Завдяки цій функції користувач має можливість увімкнути систему захисту або ввимкнути її за допомогою параметру command, який містить статус, який потрібно відправити системі, і за яким вона зрозуміє, що саме потрібно зробити.

А також у додаток було впроваджено функцію життєвого циклу, яка відповідає за отримання оновлених повідомлень від системи захисту, яка кожну

секунду робить перевірку системних логів. Цей функціонал був реалізований за допомогою функції життєвого циклу componentDidMount:

```
componentDidMount(){
    setInterval(()=>this.getAllSms(), 1000);
    this.getAllSms();
  }
```

І для фільтрації повідомлень та номерів з яких повинні приходити дані був створений об'єкт у якому можна також відфільтрувати тему повідомлення. І завдяки цьому об'єкту користувач буде отримувати інформацію від системи.

```
var filter = {
  box: 'inbox', // 'inbox' (default), 'sent', 'draft',
'outbox', 'failed', 'queued', and '' for all
  // the next 4 filters should NOT be used together, they
are OR-ed so pick one
  // read: 0, 0 for unread SMS, 1 for SMS already read
  // _id: 1234, // specify the msg id
  address: '+380632754682', // sender's phone number
  body: 'Signalization Content', // content to match
  // the next 2 filters can be used for pagination
  indexFrom: 0, // start from index 0
  // maxCount: 10, // count of SMS to return each time
};
```

Отже підсумовуючи вищесказане можна зазаначити, що власник у будь-якому місці та у будь-який час буде повідомлений, про те що зловмисник намагався вкрасти його систему та знати, що саме було спрацьовано у системі захисту технічного засобу музейного-виставкового експонату за допомогою цього додатку.

3.3 Тестування системи програмного-технічного засобу

Тестування системи програмного-технічного засобу буде відбуватися за допомогою ручного тестування та системи логування, яка робить перевірки чи належним чином відпрацювала програма. За допомогою ручного тестування є можливість перевірити роботоздатність датчиків руху, магнітогерконового

датчика, ультразвукового датчика та датчика тиску та надійність об’єкту. Тестування програмної частини системи захисту відбувалося у компіляторі Arduino Studio. Вигляд системи програмного-технічного захисту зображено на рисунку 3.3.

Рисунок 3.3 – Вигляд системи програмного-технічного захисту

Для початку потрібно перевірити чи працює система захисту взагалі і для цього потрібно увімкнути автономне живлення і розібрати систему таким чином, щоб було видно умі датчики. Якщо світлодіоди на платі обробки даних Arduino та на GSM-модулю світяться червоним кольором, то це означає що система підключена до живлення. Вигляд системи в розібраному вигляді зображено на рисунку 3.4.

Рисунок 3.4 – Вигляд системи, що підключена до живлення

Як зображено вище зрозуміло, що система працює, так як горять світлодіоди.

Було проведено по 20 тестів на кожний датчик в системі, тестування проводилося з об’єктом захисту, вага якого була 700 г. При спрацюванні датчиків сирена вмикалася та відправляла повідомлення, у якому знаходяться результати роботи датчиків (див. рис. 3.5) та апаратного засобу в цілому.

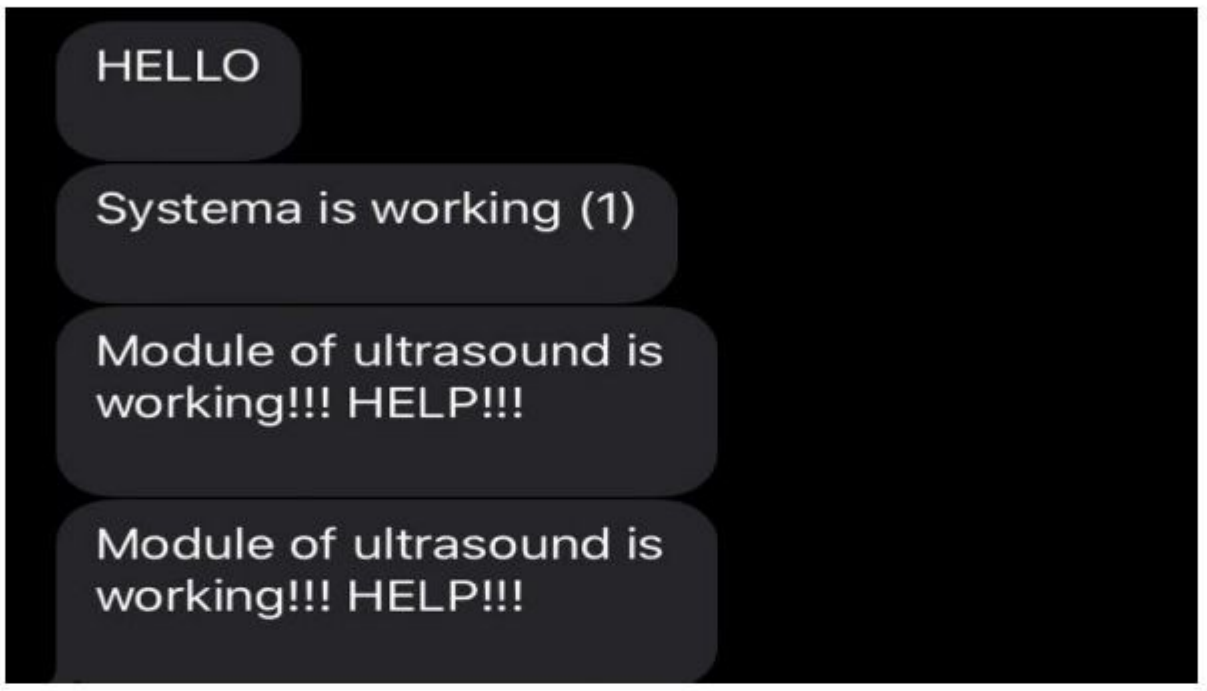


Рисунок 3.5 – Вигляд результатів роботи датчиків.

Якщо не приходять повідомлення від системи, але видно що всі датчики працюють у нормальному режимі, то потрібно поповнити рахунок сім-картки, яка вставлена в GSM-модуль (див. рис. 3.6).

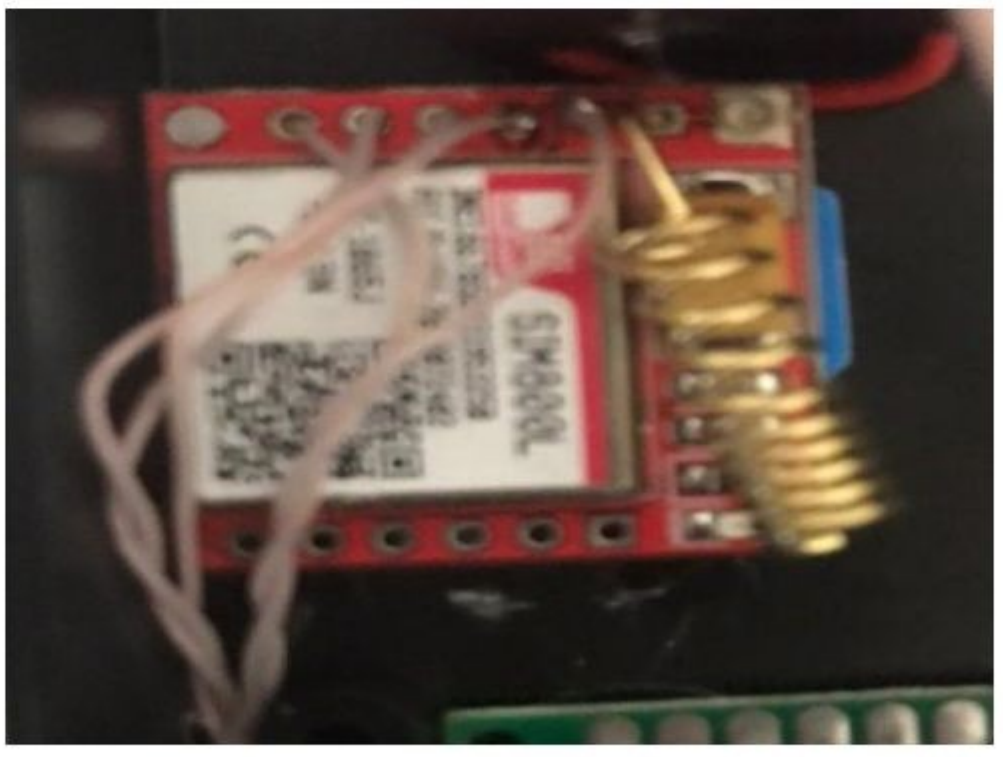


Рисунок 3.6 – Вигляд GSM-модулю з сім-карткою

Успішним результатом стало відпрацювання усіх датчиків у різних умовах. Датчик ультразвуку спрацьовував коли був на відстані від 5 – 30 см. Магнітогерконовий датчик спрацьовував коли від'єднували або ж приєднували магніт. Датчик руху дуже чутливий, але також вдалося його протестувати і на кожен рух він спрацьовував. Датчик тиску був протестований на найвищому рівні, так як це основний датчик захисту об'єкта. Було виявлено, що вага повинна становити не менше 400 г і бути чітко встановленим на датчик тиску. При правильному розташуванні об'єктів (див. рис. 3.7) результати системи захисту будуть задовільними.

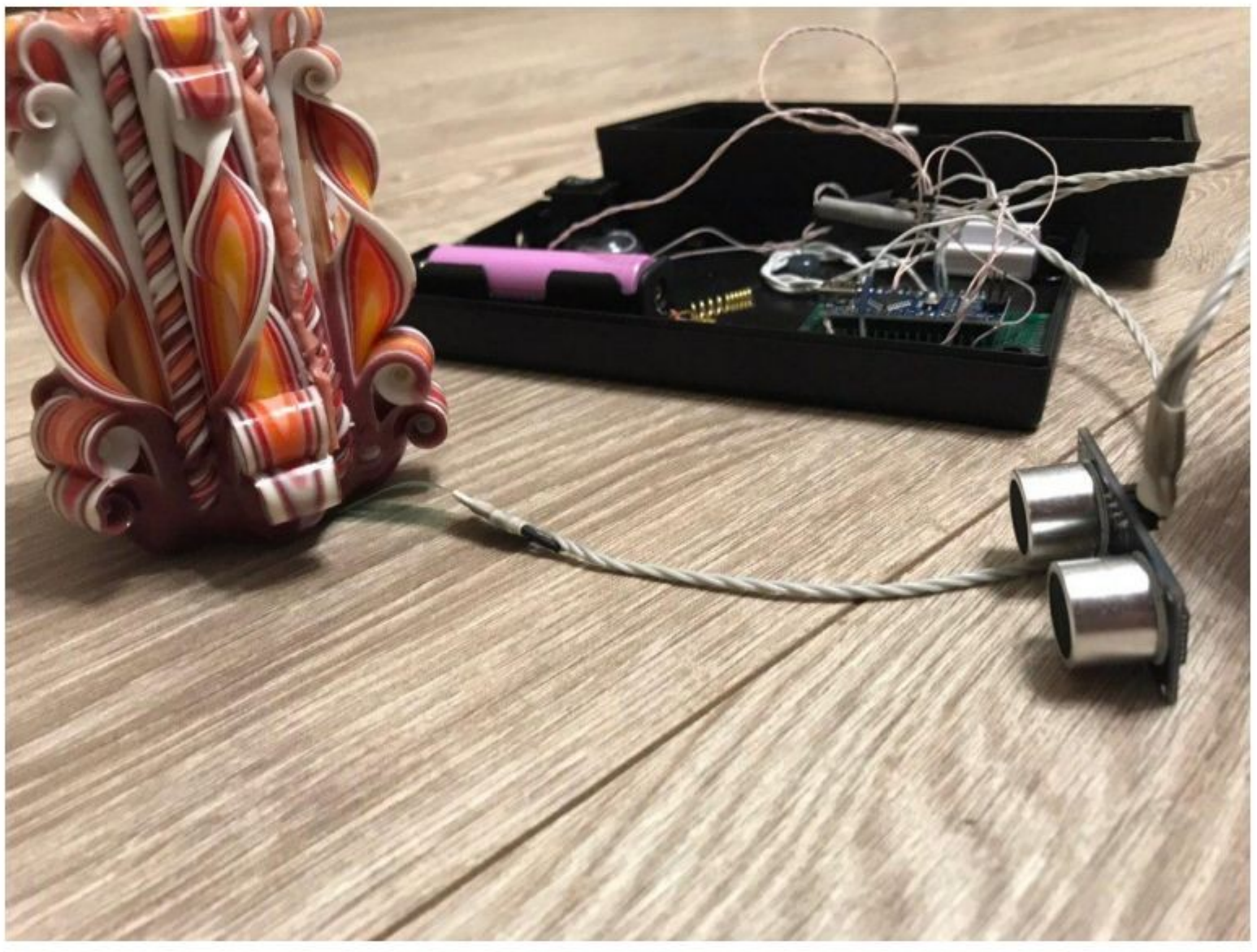


Рисунок 3.7 – Вигляд правильного розташування датчиків та об'єкта захисту

За допомогою можливості прослуховувати порт даного пристрою є можливість отримання логів від системи в такому вигляді (див. рис. 3.8), за допомогою яких можна визначити чи пристрій увімкнений, перевірити чи пристрій прийняв сигнал, відправив повідомлення сповіщення, а також перевірити чому якийсь з датчиків не спрацював.

Рисунок 3.8 – Вигляд отримання логів з системи

Отже, було проведено тестування результатом якого є те, що всі датчики працюють корректно і виявлено, що об’єкти захисту не будуть викрадені непоміченими.

4 ЕКОНОМІЧНА ЧАСТИНА

4.1 Технологічний аудит розробленої системи програмно-технічного захисту музейного комплексу

Останнім часом, як було відзначено у попередніх розділах роботи, суттєво загострилася проблема забезпечення надійної охорони життя людей, об'єктів бізнесу, житлових приміщень, виробництв, об'єктів соціально-культурного призначення тощо. Сьогодні ця задача розв’язується шляхом створення спеціальних охоронних систем, призначення яких полягає у забезпеченні надійного рівня захисту об’єктів і зменшенні необхідності втручання людей у вирішення питань цілодобового контролю за функціонуванням об'єктів, що перебувають під охороною.

Головне призначення будь-якої охоронної системи полягає в оперативному і гарантованому сповіщенні користувачів цих систем або/та правоохоронних структур достовірною інформацією про несанкціоноване втручання до об'єктів, що охороняються. Як стверджують фахівці, рішення цієї задачі можливе тільки при правильному оснащенні об'єктів охорони сучасними високонадійними технічними засобами охоронної сигналізації.

Не випадково, що сьогодні розробники програмно-технічних засобів охорони об’єктів цілеспрямовано працюють над тим, щоб удосконалювати існуючі охоронні системи захисту шляхом впровадження в них методів машинного навчання і штучного інтелекту, оскільки розроблені новостворені спеціалізовані алгоритми зможуть швидко обробляти сигнали, що надходять від датчиків, і швидко приймати рішення про активацію цих сигналів. А це має знизити навантаження на співробітників, що охороняють об’єкти, збільшить ефективність охорони і застрахує користувачів систем охорони від зловживань з боку самих охоронців.

Оскільки останнім часом під загрозою бути вкраденими або пошкодженими все частіше потрапляють саме музейні експонати (через їхню велику вартість та унікальність), то перед нашою магістерською кваліфікаційною роботою було

поставлене завдання розробити недорогу систему захисту музейних виставкових експонатів, яка б мала вигляд програмно-апаратного комплексу, забезпечувала надійний захист музейних виставкових експонатів від несанкціонованого доступу і була створена на базі мікроконтролерної платформи Arduino.

Для цього нами було: проаналізовано існуючі технології та процеси, які використовуються в системах програмно-технічного захисту; досліджено та проведено аналіз існуючих аналогів і зроблено висновки щодо їхнього рівня захисту; розроблено та обґрунтувано вибір апаратної складової; розроблено програмну частину системи захисту; виконано тестування коректності роботи програмно-технічної системи захисту.

У підсумку, нами було розроблено систему захисту музейних виставкових експонатів у вигляді програмно-апаратного комплексу на базі мікроконтролерної платформи Arduino.

Для визначення технічного рівня та комерційного потенціалу нашої розробки проведемо її технологічний аудит. Для проведення технологічного аудиту були запрошені фахівці з цього питання: к.т.н., доцент Куперштейн Л.М., к.т.н., доцентка Войтович Л.П. та ст. викладачка Каплун В.А.

Запрошені експерти здійснювали оцінювання технічного рівня та комерційного потенціалу нашої розробки за методикою та рекомендаціями Державного комітету України з питань науки, інновацій та інформатики [22], які наведено в таблиці 4.1.

Таблиця 4.1 – Критерії оцінювання технічного рівня та комерційного потенціалу будь-якої розробки

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Кри-терій	0	1	2	3	4

Продовження таблиці 4.1

Технічна здійсненність концепції:					
	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах
Ринкові переваги (недоліки):					
	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
Ринкові перспективи					
	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів

Продовження таблиці 4.1

	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність					
	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
0	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
1	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років

Продовження таблиці 4.1

2	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Експерти проводили технологічний аудит нашої розробки шляхом виставлення оцінок за бальною шкалою (від «0» до «4»; [21]) (дивися таблиці 4.1 та 4.2).

Таблиця 4.2 – Потенційні технічні рівні та комерційний потенціал розробки

Середньоарифметична сума балів $\overline{СБ}$, розрахована на основі висновків експертів	Технічний рівень та комерційний потенціал розробки
0 – 10	Низький
11 – 20	Нижче середнього
21 – 30	Середній
31 – 40	Вище середнього
41 – 48	Високий

В результаті проведеного аудиту експерти виставили розробленій нами системі програмно-технічного захисту музейних експонатів такі оцінки, які зведено в таблицю 4.3:

Таблиця 4.3 – Результати технологічного аудиту нашої розробки

Критерії	Прізвище, ініціали експерта		
	Куперштейн Л.М	Войтович Л.П.	Каплун В.А.

Продовження таблиці 4.3

	Бали, виставлені експертами:		
1	2	2	2
2	2	2	2
3	2	2	3
4	2	2	2
5	2	2	3
6	1	2	2
7	2	2	3
8	2	2	2
9	2	2	2
10	2	2	2
11	2	2	2
12	2	2	2
Сума балів	$СБ_1 = 23$	$СБ_2 = 24$	$СБ_3 = 27$
Середньоа рифметична сума балів $\overline{СБ}$	$\overline{СБ} = \frac{\sum_{1}^{3} СБ_i}{3} = \frac{23 + 24 + 27}{3} = \frac{74}{3} = 24,67.$		

Оскільки середньоарифметична сума балів, що їх виставили експерти, дорівнює 24,67-ти балам (див. табл. 4.3), то, керуючись рекомендаціями, наведеними в таблиці 4.2, можна зробити висновок, що розроблена нами система програмно-технічного захисту музейного комплексу має технічний рівень та комерційний потенціал, який вважається «середнім».

Такий досить високий рівень нашої розробки пояснюється тим, що нами запропоновано таку структурну модель системи захисту музейних виставкових експонатів, яка має розширені функціональні можливості у вигляді комбінованих систем захисту об'єктів з додатковим сповіщенням про фізичне втручання до об'єкту захисту, що дозволяє підвищити захист будь-якого музейного об’єкта від несанкціонованого втручання.

4.2 Розрахунок витрат на розробку системи програмного-технічного захисту музейного комплексу

Під час розробки системи програмно-технічного захисту музейного комплексу були використані такі статті витрат [22]:

4.2.1. Основна заробітна плата $З_о$ розробників (формула 4.1):

$$З_о = \frac{М}{Т_р} \cdot t \text{ грн}, \qquad (4.1)$$

де М – місячний посадовий оклад конкретного розробника; В 2019 р. місячні оклади коливаються в межах: М = (4173…14000) грн/міс.;

$Т_р$ – число робочих днів в місяці; приймемо $Т_р$ = 20 днів;

t – число робочих днів роботи розробників.

Розрахунки основної заробітної плати розробників зведено в таблицю 4.4:

Таблиця 4.4 – Основна заробітна плата розробників (округлено до цілих чисел)

Найменування посади виконавця	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на оплату праці, грн	Примітка
1. Науковий керівник магістерської кваліфікаційної роботи	11900	595	25 годин	2479	При 36-годинній робочій неділі
2. Студент- магістрант	1950	98	77 днів	7546	
3. Консультант з економічної частини	10140	507	2,5 години	211	При 36-годинній робочій неділі
4. Інші	6000	300	4	1200	
Всього				$З_о$ = 11436 грн	

4.2.2. Додаткова заробітна плата $З_д$ виконавців роботи розраховується як (10…12)% від величини їх основної заробітної плати, тобто:

$$З_д = \alpha \cdot З_о = (0,1 \ldots 0,12) \cdot З_о . \quad (4.2)$$

Приймемо, що $\alpha = 0,1075$. Тоді для нашого випадку отримаємо:

$$З_д = 0,1075 \times 11436 \approx 1229 \text{ грн.}$$

4.2.3. Нарахування на заробітну плату $НР_{зп}$ розробників розраховуються за формулою (4.3):

$$Н_{зп} = (З_о + З_д) \cdot \frac{\beta}{100}, \quad (4.3)$$

де β = 22% – ставка єдиного внеску на загальнообов'язкове державне соціальне страхування.

Для нашого випадку отримаємо:

$$НР_{зп} = (11436 + 1229) \times 0,22 \approx 2786 \text{ грн.}$$

4.2.4. Амортизація А основних засобів, обладнання, комп'ютерів тощо розраховується за формулою (4.4) :

$$А = \frac{Ц \cdot Н_а}{100} \cdot \frac{Т}{12} \text{ грн}, \quad (4.4)$$

де Ц – загальна балансова вартість основних засобів, обладнання, комп'ютерів

тощо, які використовувалися під час виконання роботи, грн;

$Н_а$ – річна норма амортизаційних відрахувань; $Н_а$ = (5...25)%;

Т – термін, використання кожного виду основних засобів, місяці.

Зроблені розрахунки зведемо у таблицю 4.5.

Таблиця 4.5 – Розрахунок амортизаційних відрахувань

Найменування обладнання, приміщень тощо	Балансова вартість, грн.	Норма амортизації, %	Термін використання, міс.	Величина амортизаційних відрахувань, грн.

Продовження таблиці 4.5

1. Обладнання: комп'ютери, принтери тощо	33850	20	3,2 (33% використання)	596
2. Приміщення кафедри, факультету, бібліотеки тощо	13500	3,5	3,2 (50% використання)	63
Всього				*А = 659 грн*

4.2.5. Витрати на матеріали М:

$$М = \sum_{1}^{n} Н_i \cdot Ц_i \cdot К_i - \sum_{1}^{n} В_i \cdot Ц_в \quad грн, \qquad (4.5)$$

де $Н_i$ – витрати матеріалу *i*-го найменування, кг; $Ц_i$ – вартість матеріалу *i*-го найменування, грн./кг.; $К_i$ – коефіцієнт транспортних витрат, $К_i$ = (1,1…1,15); $В_i$ – маса відходів матеріалу *i*-го найменування, кг; $Ц_в$ – ціна відходів матеріалу *i*-го найменування, грн/кг; n – кількість видів матеріалів.

4.2.6. Витрати на комплектуючі К:

$$К = \sum_{1}^{n} Н_i \cdot Ц_i \cdot К_i \quad грн., \qquad (4.6)$$

де $Н_i$ – кількість комплектуючих *i*-го виду, шт.; $Ц_i$ – ціна комплектуючих *i*-го виду, грн; $К_i$ – коефіцієнт транспортних витрат, $К_i$ = (1,1…1,15); n – кількість видів комплектуючих.

Загальна вартість основних матеріалів та комплектуючих, які були використані під час виконання роботи, складає приблизно 1420 грн.

4.2.7. Витрати на силову електроенергію $В_е$ розраховуються за формулою (4.7):

$$В_е = \frac{В \cdot П \cdot Ф \cdot К_п}{К_д}, \qquad (4.7)$$

де В – вартість 1 кВт-год. електроенергії, в 2019 р. В ≈ 2,8 грн/кВт;

П – установлена потужність обладнання, кВт; П = 1,72 кВт;

Ф – фактична кількість годин роботи обладнання, годин.

Приймемо, що Ф = 195 годин;

$К_п$ – коефіцієнт використання потужності; $К_п < 1 = 0,87$.

$К_д$ – коефіцієнт корисної дії, $К_д = 0,77$.

Тоді витрати на силову електроенергію становитимуть:

$$В_е = \frac{В \cdot П \cdot Ф \cdot К_п}{К_д} = \frac{2,8 \cdot 1,72 \cdot 195 \cdot 0,87}{0,77} \approx 1061 \text{ грн.}$$

4.2.8. Інші витрати $В_{ін}$ (опалення, освітлення, ремонт, утримання приміщень тощо) розраховуються як (100…300)% від основної заробітної плати розробників, тобто:

$$В_{ін} = (1….3) \times (З_о + З_{роб}). \quad (4.8)$$

Для нашого випадку отримаємо:

$$В_{ін} = 1,90 \times 11436 \approx 21728 \text{ грн.}$$

4.2.9. Сума всіх попередніх статей дає витрати на виконання роботи безпосередньо магістрантом – $В_{заг}$.

$$В_{заг} = 11436 + 1229 + 2786 + 659 + 1420 + 1061 + 21728 = 40319 \text{ грн.}$$

4.2.10. Загальні витрати на остаточне завершення роботи та оформлення їх результатів розраховуються за формулою (4.9):

$$ЗВ = \frac{В_{заг}}{\beta}, \quad (4.9)$$

де β – коефіцієнт, який характеризує етап виконання даної роботи на шляху до її можливого впровадження. Для нашого випадку доцільно прийняти, що $\beta \approx 0,65$.

Тоді: $ЗВ = \frac{40319}{0,65} \approx 62029,00$ грн або приблизно 63 тисяч грн.

Тобто загальні витрати на виконання нашої роботи становлять приблизно 63 тис. грн.

4.3 Розрахунок економічного ефекту від можливої комерціалізації нашої розробки

Аналіз місткості ринку даної продукції показує, що в Україні кількість постійно та тимчасово функціонуючих музеїв, виставок та ярмарок, які потрібно охороняти, є досить значною і оцінюється приблизно 500 шт. Окрім того, їх кількість буде стрімко зростати (за рахунок розвитку економіки та прогнозованого рівня зростання злочинності). Тобто, якщо наша розробка буде впроваджена з 1 січня 2021 року (оскільки потребує незначного доопрацювання), то її результати будуть виявлятися протягом 2021-го, 2022-го та 2023-го років.

Прогноз зростання попиту на нашу розробку складає по роках:

- 2021 р. – приблизно + на Δ200 шт.;
- 2022 р. – приблизно + на Δ350 шт.;
- 2023 р. – приблизно + на Δ600 шт.

Якщо існуючі подібні системи програмно-технічного захисту музейних комплексів коштують на ринку в середньому приблизно 10 тис. грн, то нашу розробку можна буде реалізовувати на ринку дещо дешевше, наприклад, за 9,75 тис. грн, чи на 0,25 тис. грн дешевше, що підвищить конкурентоспроможність розробленої нами системи програмно-технічного захисту музейних комплексів.

Можливе збільшення чистого прибутку $\Delta П_i$, що його може отримати потенційний інвестор від впровадження нашої розробки становитиме [21].

$$\Delta П_i = \sum_{1}^{n} (\Delta Ц_o \cdot N + Ц_o \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\upsilon}{100}), \qquad (4.10)$$

де $\Delta Ц_o$ – зміна основного якісного показника від впровадження результатів розробки у цьому році. Таким показником є зміна ціни нової розробки; для нашого випадку це буде: $\Delta Ц_o = (9,75 – 10,0) = -0,25$ тис. грн;

N – основний кількісний показник, який визначає обсяг діяльності у році до впровадження розробки; N = 500 шт.;

ΔN – покращення основного кількісного показника від впровадження результатів розробки. Таке покращення відповідно по роках становитиме:

Δ_{21} =+200, Δ_{22} = +350 та Δ_{23} = +600 шт.;

$Ц_o$ – основний якісний показник, який визначає обсяг діяльності у році після впровадження розробки; для нашого випадку $Ц_o$ = 9,75 тис. грн;

n – кількість років, протягом яких очікується отримання позитивних результатів від впровадження розробки; n = 3 роки;

λ – коефіцієнт, який враховує сплату податку на додану вартість; $\lambda = 0,8333$;

ρ – коефіцієнт, який враховує рентабельність продукту. Рекомендується приймати ρ = (0,2...0,5); візьмемо ρ = 0,5;

υ – ставка податку на прибуток. У 2019 році υ = 18%.

Величина чистого прибутку $\Delta П_1$ для потенційного інвестора протягом першого року від можливого впровадження нашої розробки (2021 р.) може становити:

$$\Delta П_1 = [-0,25 \cdot 500 + 9,75 \cdot 200] \cdot 0,8333 \cdot 0,5 \cdot (1 - \frac{18}{100}) \approx 624 \text{ тис. грн.}$$

Величина чистого прибутку $\Delta П_2$ для потенційного інвестора від можливого впровадження нашої розробки протягом другого (2022 р.) року може становити:

$$\Delta П_2 = [-0,25 \cdot 500 + 9,75 \cdot 350] \cdot 0,8333 \cdot 0,5 \cdot (1 - \frac{18}{100}) \approx 1123 \text{ тис. грн.}$$

Величина чистого прибутку $\Delta П_3$ для потенційного інвестора від можливого впровадження нашої розробки протягом третього (2023 р.) року може становити:

$$\Delta П_3 = [-0,25 \cdot 500 + 9,75 \cdot 600] \cdot 0,8333 \cdot 0,5 \cdot (1 - \frac{18}{100}) \approx 1956 \text{ тис. грн.}$$

Приведена вартість всіх можливих чистих прибутків ПП розраховується за формулою:

$$ПП = \sum_{1}^{\tau} \frac{\Delta П_i}{(1+\tau)^t}, \qquad (4.11)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої роботи, грн;

т – період часу, протягом якого виявляються результати впровадженої роботи, роки. Для нашого випадку т = 3 роки;

τ – ставка дисконтування; приймемо ставку дисконтування τ = 0,047 (4,7%);

t – період часу від моменту здійснення тих чи інших платежів (отримання прибутків та вкладення інвестицій) до моменту впровадження розробки.

Тоді приведена вартість всіх чистих прибутків ПП, що їх може отримати потенційний інвестор від можливого впровадження нашої розробки, складе:

$$ПП = \frac{624}{(1+0,047)^2} + \frac{1123}{(1+0,047)^3} + \frac{1956}{(1+0,047)^4} \approx 569 + 978 + 1628 = 3175 \text{ тис. грн.}$$

Далі розрахуємо початкову теперішню вартість інвестицій PV, що можуть бути вкладені потенційним інвестором у випадку реалізації нашої розробки:

$$PV = (2…5) \times ЗВ, \quad (4.12)$$

де ЗВ – витрати на розробку; ЗВ = 63 тис. грн (див. формулу 4.9).

Тоді для нашого випадку отримаємо:

$PV = (2…5) \times 63 = 5 \times 63 = 315$ тис. грн.

Тоді абсолютний ефект від можливих вкладених інвестицій $Е_{абс}$ може становити:

$$Е_{абс} = ПП – PV, \quad (4.13)$$

де ПП – приведена вартість всіх можливих чистих прибутків від можливого впровадження нашої розробки, грн;

PV – теперішня вартість інвестицій PV = 315 тис. грн.

$Е_{абс}$ = 3175 – 315 = 2860 тис. грн або кожного року приблизно по 953 тис. грн.

Внутрішня норма дохідності $Е_в$ інвестицій, вкладених у комерціалізацію нашої розробки, розраховується за формулою (4.14):

$$E_{в} = \sqrt[T_ж]{1 + \frac{E_{абс}}{PV}} - 1, \qquad (4.14)$$

де $E_{абс}$ – абсолютний ефект вкладених інвестицій; $E_{абс}$ = 2860 тис. грн;

PV – теперішня вартість початкових інвестицій PV = 315 тис. грн;

$T_ж$ – життєвий цикл розробки, роки. $T_ж$ = 4.

Для нашого випадку отримаємо:

$$E_{в} = \sqrt[4]{1 + \frac{2860}{315}} - 1 = \sqrt[4]{1 + 9,079} - 1 = \sqrt[4]{10,079} - 1 = 1,7817 - 1 \approx 0,7817 \approx 78,17\ \%.$$

Далі визначимо ту мінімальну дохідність, нижче за яку потенційний інвестор не буде займатися комерціалізацією нашої розробки.

Мінімальна дохідність або мінімальна (бар'єрна) ставка дисконтування $\tau_{мін}$ визначається за формулою (4.15):

$$\tau = d + f, \qquad (4.15)$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2019 році в Україні d = (0,10...0,19);

f – показник, що характеризує ризикованість вкладень; зазвичай, величина f = (0,05...0,60), але може бути і значно більше.

Для нашого випадку отримаємо:

$\tau_{мін} = 0,15 + 0,55 = 0,70$ або $\tau_{мін} = 70\%$.

Оскільки величина $E_в = 78,17\% > \tau_{мін} = 70\%$, то потенційний інвестор може бути зацікавлений у комерційному впровадженні нашої розробки.

Далі розраховуємо термін окупності коштів, які можуть бути вкладені у нашу розробку. Термін окупності $T_{ок}$ можна розрахувати за формулою (4.16):

$$T_{ок} = \frac{1}{E_{в}}. \qquad (4.16)$$

Термін окупності $T_{ок}$ коштів, вкладених у нашу розробку, становитиме:

$$T_{ок} = \frac{1}{0,7817} \approx 1,279 \text{ років},$$

що свідчить про потенційну доцільність комерціалізації нашої розробки.

Результати виконаної економічної частини магістерської кваліфікаційної роботи зведено у таблицю:

Показники	Задані у ТЗ	Досягнуті у магістерській кваліфікаційній роботі	Висновок
1. Витрати на розробку системи програмно-технічного захисту музейного комплексу	Не більше 70 тис. грн	63 тис. грн.	Виконано
2. Абсолютний щорічний ефект від можливого впровадження розробки, тис. грн	не менше 900 тис. грн за рік	953 тис. грн щорічно протягом 3-х років	Виконано
3. Внутрішня норма дохідності вкладених інвестицій, %	не менше 70%	78,17%	Досягнуто
4. Термін окупності, роки	до 3-х років	1,279 років	Виконано

Таким чином, основні техніко-економічні показники розробленої системи програмно-технічного захисту музейного комплексу, визначені у технічному завданні, виконані.

ВИСНОВКИ

Для забезпечення захисту музейних експонатів було проаналізовано основні види захисту в музейних установах. Було виявлено, що з основних заходів безпеки в музейних установах виділяють: контрольно-пропускний режим, охоронний режим, впровадження технічних систем захисту, центральний диспетчерський пункт, протипожежна безпека, що не забезпечують захист музейним експонатам належним чином.

Після аналізу існуючих систем захисту в музеях було вирішено розробити програмно-технічну систему захисту музейних експонатів при використанні декількох датчиків спрямованих саме на об'єкт захисту та дистанційним керуванням системою за допомогою GSM-модуля та мобільного додатку.

Було розроблено алгоритм роботи апаратної та програмної частини, які взаємодіють між собою, обґрунтовано вибір датчиків та програмних засобів для реалізації завдання. Для апаратної частини було використано модуль GSM, плату Arduino, та комплекту необхідних датчиків (датчик тиску, датчик ультразвуку, магнітногерконовий датчик, датчик руху), завдяки чому була досягнена мета магістерської кваліфікаційної роботи, та виконані поставлені задачі.

Система розроблена на основі комбінованих технологій як для апаратної так і для програмної частини показала результати в ході тестування, які підтверджують доцільність обраних технологій та мов програмування. Було протестовано усі можливі варіанти викрадення музейного експонату, і дійшли висновку того, що усі датчики спрацьовували належним чином і при кожній спробі викрадення спрацьовувала сирена та відправлялося сповіщення на мобільний додаток, окрім датчика руху, якого не можливо відкалібрувати через неправильний підбір датчика руху.

Програма для апаратної частини було розроблено за допомогою мови програмування C++. Щодо мобільного додатку, то використовувався

кроссплатформлений фреймворк React Native. Завдяки вдалому вибору технологій програмування вдалося вирішити усі поставлені задачі.

Дане проектне рішення призвело до реалізації, як апаратної частини, так і програмної частини. Перевагою системи є простота у використанні, а також це є економічно вигідним варіантом для забезпечення високого рівня захисту, завдяки правильному вибору датчиків для системи програмно-технічного захисту музейного експонату.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Василенок, В. Л. , Вус, М. А., Горшков, В. В. Введение в безопасность предпринимательства : Учебное пособие / В. Л. Василенок– Санк- Петербург : Высшая административная школа мэрии, 1999. – 99 с.
2. Дворский, М. Н., Палатченко, С. Н. Техническая безопасность объектов предпринимательства : Учебное пособие / М. Н. Дворский. – М. : А-депт, 2006. – 304 с.
3. Барсуков, В.С., Марущенко, В. В., Шигин, В. А. Интегральная безопасность: Информационно-справочное пособие / В. С. Барсуков.–М.: РАО “Газпром”, 2004. – 170 с.
4. Преимущества и недостатки использования Arduino [Електронний ресурс]. – Режим доступу: URL http://tim4dev.com/2016/07/arduino-advantages-disadvatages/ – Назва з екрану.
5. Arduino основи програмування [Електронний ресурс]. – Режим доступу: http://geekmatic.in.ua/ua/arduino_osnovyi_programmirovaniya– Назва з екрану.
6. Key Components of Smart Home Gateway [Електронний ресурс]. – Режим доступу: URL https://mysmahome.com/feature/4658/key-components-of-smart-home-gateway-2/ – Назва з екрану.
7. Smart home systems: Everything you need to know [Електронний ресурс]. – Режим доступу: URL https://www.the-ambient.com/guides/smart-home-ecosystems-152 – Назва з екрану.
8. UATAG - стеклянный идентификатор подлинности [Електронний ресурс]. – Режим доступу: URL https://marketer.ua/uatag/ – Назва з екрану.
9. Комплект беспроводной сигнализации Tecsar Alert Ward [Електронний ресурс]. – Режим доступу: URL https://worldvision.com.ua/news/manuals/obzor-komplekta-besprovodnoy-signalizatsii-tecsar-alert-ward--1687 – Назва з екрану.

10. Alfa KS-SF05R - Охранные системы [Електронний ресурс]. – Режим доступу: URL http://a-ss.com.ua/index.php?route=product/product&product_id=125 – Назва з екрану.
11. Плюсы и минусы платформ React Native и Real Native [Електронний ресурс]. – Режим доступу: URL https://dou.ua/lenta/articles/react-vs-real/ – Назва з екрану.
12. React Native – Одного Js мало [Електронний ресурс]. – Режим доступу: URL https://habr.com/ru/post/323214/ – Назва з екрану.
13. React Native – A framework for a building awesome apps [Електронний ресурс]. – Режим доступу: URL https://facebook.github.io/react-native/ - Назва з екрану.
14. Пьезоэлектрический зуммер SHD4216 [Електронний ресурс]. – Режим доступу: URL https://doubleshop.com.ua/p496744104-pezoelektricheskij-zummer-shd4216.html – Назва з екрану.
15. GSM – сигнализация для людей [Електронний ресурс]. – Режим доступу: URL http://www.atmel.com/dyn/resources/prod_documents/doc0368.pdf – Назва з екрану.
16. Датчик движения DP-102 5B [Електронний ресурс]. – Режим доступу: URL https://www.novoelectronica.ru/catalog/katalog/elektronnye-komponenty/datchiki-dvizhenija/datchik-dvizhenija-dp-102 – Назва з екрану.
17. Датчик відкриття магнітогерконовий DCS-40 [Електронний ресурс]. – Режим доступу: URL http://big-brother.net.ua/uk/goods/datchyk-vidkryttya-magnitogerkonovyy-alay-somk-1-1 – Назва з екрану.
18. Ултразвуковой датчик расстояния Ардуино HC-SR04 [Електронний ресурс]. – Режим доступу: URL https://arduinomaster.ru/datchiki-arduino/ultrazvukovoj-dalnomer-hc-sr04/ – Назва з екрану.
19. Датчик давления для Arduino от Sparkfun [Електронний ресурс]. – Режим доступу: URL https://arduino.ua/prod242-datchik-davleniya-dlya-arduino-ot-sparkfun – Назва з екрану.

20. Arduino Software (IDE) [Електронний ресурс]. – Режим доступу: URL https://www.arduino.cc/en/main/software – Назва з екрану.
21. Козловський В. О. Методичні вказівки до виконання студентами-магістрантами економічної частини магістерських кваліфікаційних робіт. – Вінниця: ВНТУ, 2012. Zhou F. Security Issues and Possible Solutions in PACS Systems through Public Networks: стаття / Feng Zhou, Jin Wang, Bin Li, Jeong-Uk Kim. - Yangzhou, Seoul 2014.
22. Методичні рекомендації з комерціалізації розробок, створених в результаті науково-технічної діяльності – К.: Наказ Державного комітету України з питань науки, інновації та інформатики (Лист № 1/106-4-97 від 13.09.2010 р.).

Додаток А

Міністерство освіти і науки України

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

ЗАТВЕРДЖУЮ
д.т.н., проф. зав. кафедри ЗІ
_____ В. А.Лужецький
_____ 2019 р.

ТЕХНІЧНЕ ЗАВДАННЯ
до магістерської кваліфікаційної роботи на тему
"Система програмно-технічного захисту музейного виставкового експонату"
08-20.МКР.010.00.000 ТЗ

Розробив студент групи 1БС-18м

_____ Мусійчук М.Т.

Керівник магістерської кваліфікаційної роботи к. т. н., доц. кафедри ЗІ

_____ Куперштейн Л.М.

_____ _____ 2019 р.

Вінниця 2019

1 Назва та область використання

Система програмно-технічного захисту музейного виставкового експонату. Область використання: музейні установи.

2 Підстави для розробки

Робота виконується згідно наказу №254 ректора ВНТУ від 02.10.2019 р.

3 Мета та призначення розробки

Покращення рівня захищеності музейного виставкового експонату від несанкціонованого доступу.

4 Джерела розробки

4.1 Василенок, В. Л. , Вус, М. А., Горшков, В. В. Введение в безопасность предпринимательства : Учебное пособие / В. Л. Василенок– Санк-Петербург : Высшая административная школа мэрии, 1999. – 99 с.
4.2 Савельев А.Я., Овчинников В.А. Конструирование ЭВМ и систем - М.: Высшая школа, - 1989.-312 с.
4.3 Блум Д. Изучаем Arduino. Инструменты и методы технического волшебства. /Д. Блум. – П. : БХВ, 2016. – 336 с.
4.4 Програмирование Arduino [Електронний ресурс]. – Режим доступу: URL : http://academician.kiev.ua/programming_in_brief.php – Назва з екрану.

5 Технічні вимоги

5.1 Контролер пристрою – Arduino Nano;
5.2 Керування системою – GSM/мобільний додаток;
5.3 Операційна система додатку керування – Android;
5.4 Режим роботи – активний;
5.5 Погодні умови – -10ºС…+30ºС;
5.6 Живлення – відбувається від аккумулятора.

6 Вимоги до програмної документації

6.1 Графічна і текстова документація повинна відповідати діючим стандартам України.

6.2 Пристрій повинен супроводжуватись:

- Системою програмно-технічного захисту.
- Структурою програмно-технічного засобу.
- Мобільним додатком керування.
- Результатами тестування системи.

7 Стадії та етапи розробки

Робота по темі виконується у такі етапи:

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	
1	Аналіз завдання. Вступ	01.09.2019 – 04.09.2019	
2	Аналіз літературних джерел за напрямком магістерської кваліфікаційної роботи	05.09.2019 – 15.09.2019	
3	Науково-технічне обґрунтування	16.09.2019 – 22.09.2019	
4	Розробка технічного завдання	23.09.2019 – 29.09.2019	
5	Розробка рішень	30.09.2019 – 12.10.2019	
6	Практична реалізація, моделювання, експериментування, результати	14.10.2019 – 10.11.2019	
7	Розробка розділу економічного обґрунтування доцільності розробки	11.11.2019 – 17.11.2019	
8	Аналіз виконання ТЗ, висновки	18.11.2019 – 24.11.2019	
9	Оформлення пояснювальної записки	25.11.2019 – 30.11.2019	
10	Попередній захист та доопрацювання МКР	28.11.2019 – 01.12.2019	
11	Перевірка магістерської роботи на наявність плагіату	02.12.2019 – 10.12.2019	
12	Представлення МКР до захисту	11.12.2019 – 14.12.2019	
13	Захист МКР	16.12.2019 – 20.12.2019	

8 Порядок контролю та прийому

8.1 До приймання кваліфікаційної роботи представляється:

- ПЗ до магістерської кваліфікаційної роботи;
- робоча реалізація програмно-технічної системи;
- результати тестування;
- ілюстративні матеріали для захисту.

8.2 Рубіжний контроль керівника _____

8.3 Попередній захист на кафедрі 28 – 29 листопада

8.4 Захист на ДЕК 17 – 18 грудня

Розробив студент групи 1БС-18м _____ Мусійчук М.Т.

Додаток Б. Лістинг програми

```
#include <SoftwareSerial.h>
#include "Adafruit_FONA.h"

#include <string.h>

#define FONA_RX 5
#define FONA_TX 6
#define FONA_RST 7

int moveSensor = 8;
int switchPin = 4; //Gercon
//int vibrationSensor = 7;
int trigPin = 2;
int echoPin = 3;
int zummerPin = 9;
//int voicePin1 = 12;
//int voicePin2 = A0;
int powerSensor = A0;

char smsbuffer[160];
char PowerOFF[] = "Sirena is off";
char sirena[] = "Sirena is on!";
char sms1[] = "Warning!!! Moving is detected";
char smsW[] = "Security is active!";
char sendsms[160];
String phoneNumber = "+380632754682";

Adafruit_FONA fona = Adafruit_FONA(FONA_RST);
SoftwareSerial fonaSS = SoftwareSerial(FONA_TX, FONA_RX);
SoftwareSerial *fonaSerial = &fonaSS;

void setup()
{
 pinMode(zummerPin, OUTPUT);
 // pinMode(vibrationSensor, OUTPUT);
 pinMode(switchPin, INPUT);
// pinMode(voicePin2, INPUT);

 Serial.begin(115200);
 pinMode(moveSensor, INPUT);
```

```
pinMode(trigPin, OUTPUT);
pinMode(echoPin, INPUT);
pinMode(powerSensor, INPUT);

fonaSerial->begin(4800);
if (!fona.begin(*fonaSerial))
{
    Serial.println(F("Couldn't find FONA"));
    while (1)
        ;
}
Serial.println(F("FONA is OK"));
Serial.print(F("Found "));
sendMessage("HELLO");

for (int i = 0; i < 100; ++i)
{
    fona.deleteSMS(i);
}
}
bool isFirstCheckDistanceSensor = true;
bool isFirstVoiceSensor = true;
bool isSrenaOn = false;
int defaultDistance = 0;
int defaultVoice = 0;
bool systemIsWork = false;

char replybuffer[255];
void loop()
{
    delay(1000);
    retriveSMS();
    if (!systemIsWork)
    {
        return;
    }
    checkMoveSensor();
    checkDistanceSensor();
    checkVoiceSensor();
    checkFSRSensor();
    startSirena();
}
void retriveSMS()
```

```
{
    // Retrieve SMS value.
    uint16_t smslen;
    if (!fona.readSMS(1, replybuffer, 250, &smslen))
    { // pass in buffer and max len!
        Serial.println("Failed!");
    }
    Serial.println(replybuffer);
    int command = atoi(replybuffer);
    if (command == 1)
    {
        sendMessage("Systema pracue");
        systemIsWork = true;
    }

    if (command == 0)
    {
        sendMessage("Systema vymknena");
        isSrenaOn = false;
        systemIsWork = false;
    }

    if (command == 2)
    {
        sendMessage("Sygnalizacia vymknena");
        isSrenaOn = false;
    }
    fona.deleteSMS(1);
}
void checkFSRSensor()
{
    int fsrReading = analogRead(powerSensor);
    if (fsrReading != 0)
    {
        isSrenaOn = true;
        sendMessage("Object vykradeno");
    }
}

void checkVoiceSensor()
{

    //int sensorValue = analogRead(voicePin2);
    if (isFirstVoiceSensor)
```

```
{
    isFirstVoiceSensor = false;
   //defaultVoice = sensorValue;
}

/* if (defaultVoice - sensorValue > 10)
{
    isSrenaOn = false;
    sendMessage("Shum na objecti");
} */
}

void checkMoveSensor()
{
    int moveSensorData = digitalRead(moveSensor);
    if (moveSensorData > 0)
    {
        isSrenaOn = true;
        sendMessage("Ruh na objecti");
    }
}

    void checkDistanceSensor()
    {
        digitalWrite(trigPin, HIGH);
        /* Подаем импульс на вход trig дальномера */
        delayMicroseconds(10);                          // равный 10 микрос
екундам
        digitalWrite(trigPin, LOW);                     // Отключаем
        int impulseTime = pulseIn(echoPin, HIGH); // Замеряем длину и
мпульса
        int distance_sm = impulseTime / 58;       // Пересчитываем в
сантиметры

        if (isFirstCheckDistanceSensor)
{
    isFirstCheckDistanceSensor = false;
    defaultDistance = distance_sm;
}

if (abs(defaultDistance - distance_sm) > 10)
{
    isSrenaOn = true;
```

```
        sendMessage("Pryblyzhenna do objecta");
    }
}
void sendMessage(String text)
{
    char number[20];
    phoneNumber.toCharArray(number, 20);
    char sms[100];
    text.toCharArray(sms, 100);

    fona.sendSMS(number, sms);
    fona.deleteSMS(1);
}

void startSirena()
{
    digitalWrite(zummerPin, isSrenaOn);
}
```

Мобільний додаток:

```
import React, { Component } from 'react';
  import {
    SafeAreaView,
    StyleSheet,
    ScrollView,
    View,
    Text,
    Button
} from 'react-native';
import SmsAndroid from 'react-native-get-sms-android';


export default class App extends Component {

  constructor(props) {
    super(props);
    this.state = {
        mailBody:[],
    };
  }

    getAllSms(){
      var filter = {
        box: 'inbox', // 'inbox' (default), 'sent', 'draft',
'outbox', 'failed', 'queued', and '' for all
```

```
            // the next 4 filters should NOT be used together, they
are OR-ed so pick one
            // read: 0, // 0 for unread SMS, 1 for SMS already read
            // _id: 1234, // specify the msg id
            address: '+380632754682', // sender's phone number
            // body: 'How are you', // content to match
            // the next 2 filters can be used for pagination
            indexFrom: 0, // start from index 0
            // maxCount: 10, // count of SMS to return each time
          };

          SmsAndroid.list(
            JSON.stringify(filter),
            (fail) => {
              console.log('Failed with this error: ' + fail);
            },
            (count, smsList) => {
              console.log('Count: ', count);
              var arr = JSON.parse(smsList);
              console.log('Count: ', arr);
              let arrayWithSms = [];
              for (let i = 0; i<arr.length; i++){
                arrayWithSms.push(arr[i].body)
              }
              console.log(arrayWithSms)
              // arrayWithSms = arrayWithSms.reverse()
              this.setState({
                mailBody: arrayWithSms
              })
            },
          );

        }

        componentDidMount(){
          setInterval(()=>this.getAllSms(), 1000);
          // this.getAllSms();
        }

        sendSms(command){
          SmsAndroid.autoSend(
            "+380632754682",
            command,
            (fail) => {
```

```
        console.log('Failed with this error: ' + fail);
      },
      (success) => {
        console.log('SMS sent successfully');
      },
    );
  }

  render() {
    return (
      <View style = {{ margin: 15 }}>

        <View style={{marginBottom: 15}}>
          <Button title="Turn on signalization" onPress={()=>
this.sendSms()} color = 'green'></Button>
        </View>
        <View>
         <Button title="Turn off signalization" onPress={()=>
this.sendSms('dasdasd')} style={{margin: 15}} color = 'red'></Button>
        </View>
       <ScrollView style={{marginTop: 50, height: '80%'}}>
       {
         this.state.mailBody.map((item, index) => {return(
           <View style={{borderWidth:1, flexDirection:'row'}}>
             <Text    style={{paddingLeft:10,    fontSize:20,
borderRightWidth:1,    paddingRight:10,    width:    50,    textAlign:
"center"}}>{index+1}</Text>
           <Text     style={{fontSize:20,     paddingLeft:20}}>
{item}</Text>
           </View>
         )})
       }
       </ScrollView>
      </View>
      );
    }
}
```

					08-20.МКР.010.00.000 ІЧ1			
Зм	Арк.	№ докум.	Підпис	Дат				
Розроб.		Мусійчук М.Т.			Система програмно-технічного захисту музейного виставкового експонату. Схема роботи апаратної частини з мобільним	Літ.	Арк. 1	Аркушів 1
Перевір.		Куперштейн Л.М.						
Реценз		Крупельницький				ВНТУ гр.1БС-18м		
Н. Контр.		Куперштейн Л.М.						
Затверд.		Лужецький В.А.						

					08-20.МКР.010.00.000 ІЧ2			
Зм	Арк.	№ докум.	Підпис	Дат				
Розроб.		Мусійчук М.Т.			Система програмно-технічного захисту музейного виставкового експонату. Загальний алгоритм роботи апаратної частини	Літ.	Арк.	Аркушів
Перевір.		Куперштейн Л.М.					1	1
Рецензен		Крупельницький ЛЕ				ВНТУ гр.1БС-18м		
Н. Контр.		Куперштейн Л.М.						
Затверд.		Лужецький В.А.						

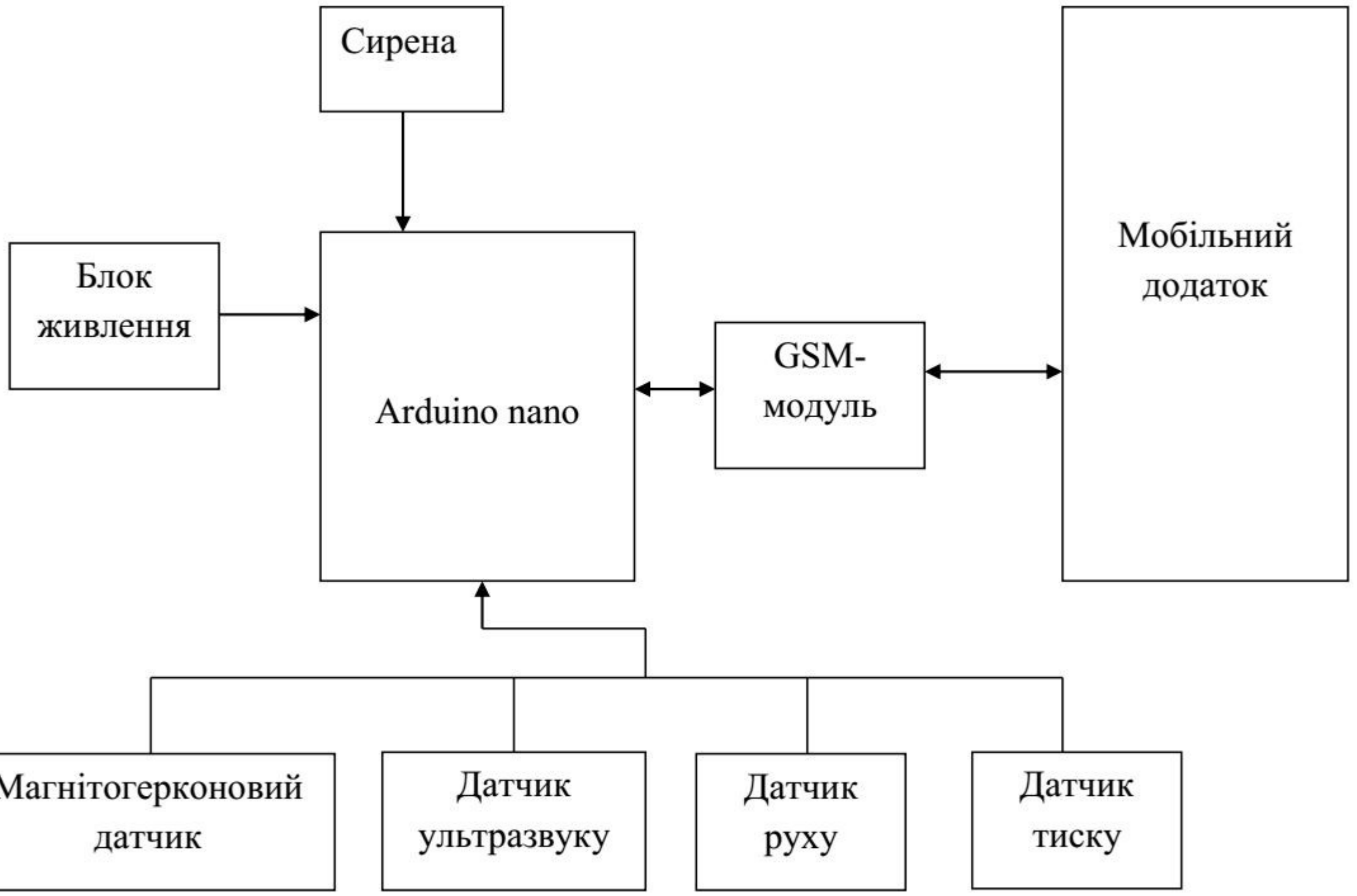
					08-20.МКР.010.00.000 ІЧЗ			
Зм	Арк.	№ докум.	Підпис	Дат				
Розроб.		Мусійчук М.Т.			Система програмно-технічного захисту музейного виставкового експонату. Схема електрична принципова	Літ.	Арк.	Аркушів
Перевір.		Куперштейн Л.М.					1	1
Реценз		Крупельницький				ВНТУ гр.1БС-18м		
Н. Контр.		Куперштейн Л.М.						
Затверд.		Лужецький В.А.						

					08-20.МКР.010.00.000 ІЧ4			
Зм	Арк.	№ докум.	Підпис	Дат				
Розроб.		Мусійчук М.Т.			Система програмно-технічного захисту музейного виставкового експонату. Вигляд головної панелі мобільного додатку	Літ.	Арк. 1	Аркушів 1
Перевір.		Куперштейн Л.М.						
Рецензен		Крупельницький				ВНТУ гр.1БС-18м		
Н. Контр.		Куперштейн Л.М.						
Затверд.		Лужецький В.А.						

					08-20.МКР.010.00.000 ІЧ5			
Зм	Арк.	№ докум.	Підпис	Дат				
Розроб.		Мусійчук М.Т.			Система програмно-технічного захисту музейного виставкового експонату. Вигляд системи програмного-технічного захисту	Літ.	Арк.	Аркушів
Перевір.		Куперштейн Л.М.					1	1
Рецензен		Крупельницький				ВНТУ гр.1БС-18м		
Н. Контр.		Куперштейн Л.М.						
Затверд.		Лужецький В.А.						

					08-20.МКР.010.00.000 ІЧ6			
Зм	Арк.	№ докум.	Підпис	Дат				
Розроб.		Мусійчук М.Т.			Система програмно-технічного захисту музейного виставкового експонату. Розміщення датчиків захисту виставкового експонату	Літ.	Арк. 1	Аркушів 1
Перевір.		Куперштейн Л.М.						
Рецензен		Крупельницький				ВНТУ гр.1БС-18м		
Н. Контр.		Куперштейн Л.М.						
Затверд.		Лужецький В.А.						

Схема роботи апаратної частини з мобільним додатком



Загальний алгоритм роботи апаратної частини

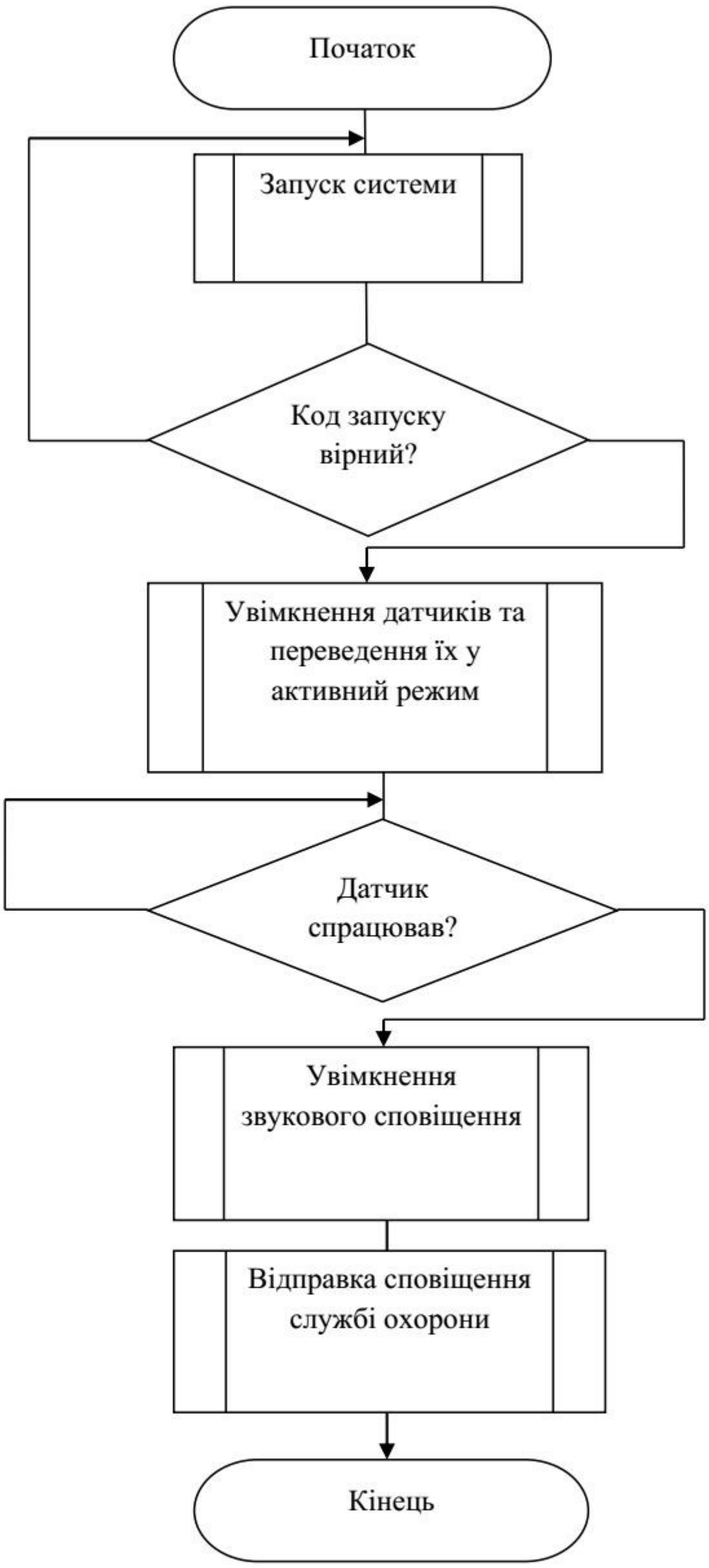
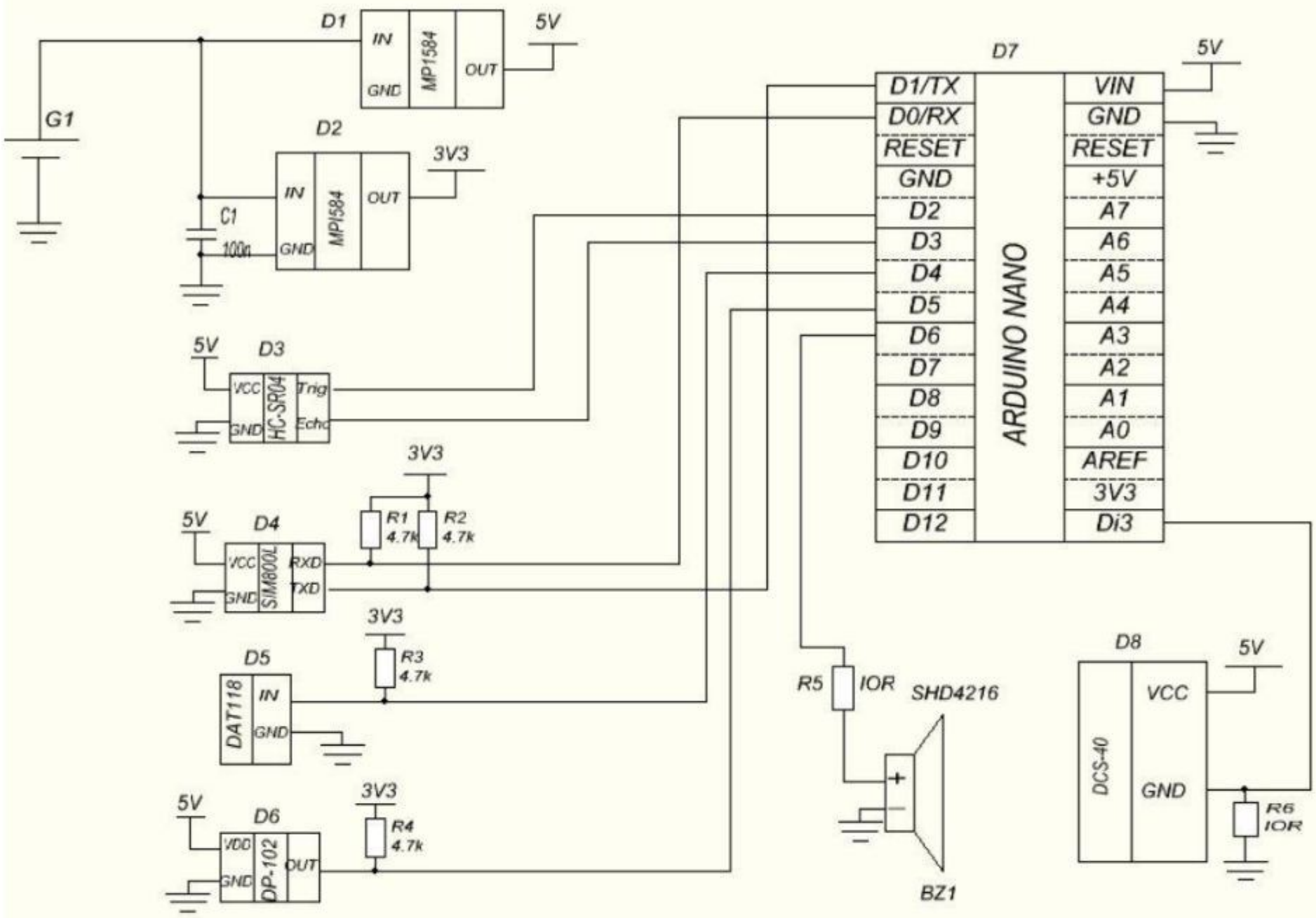
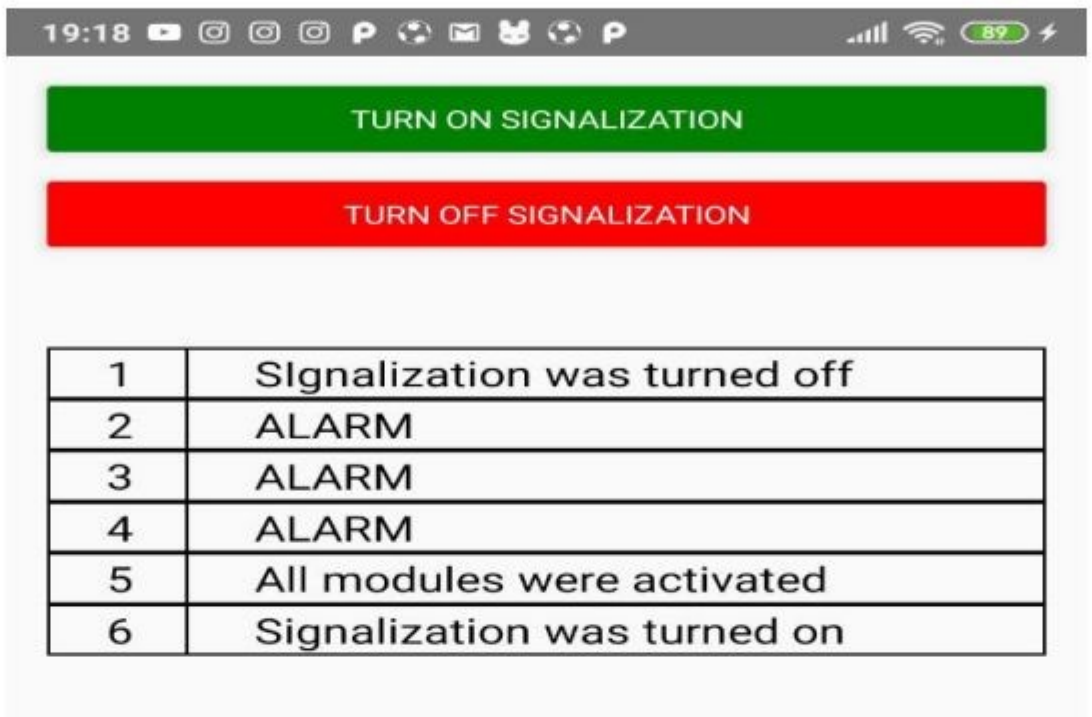


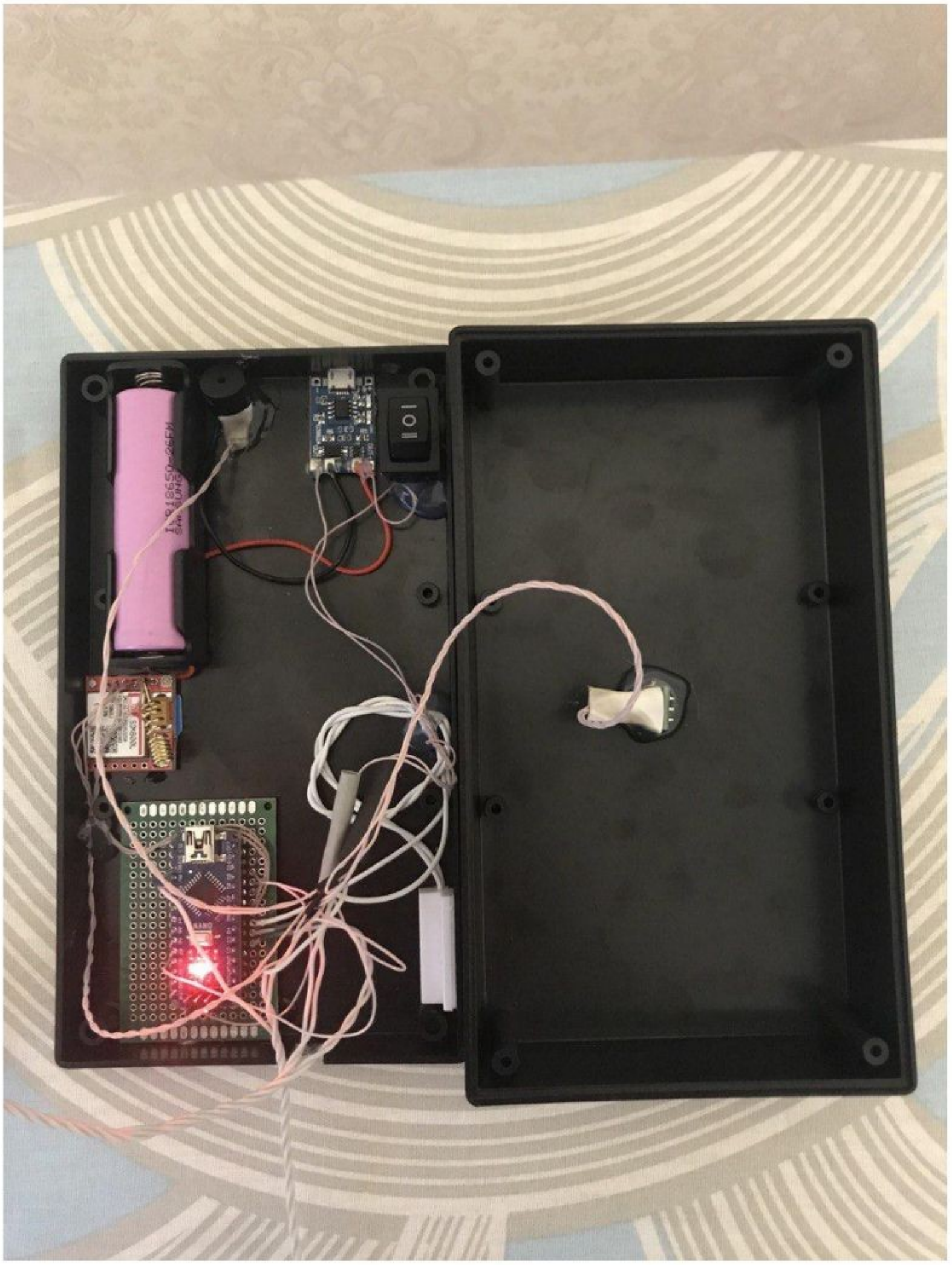
Схема електрична принципова



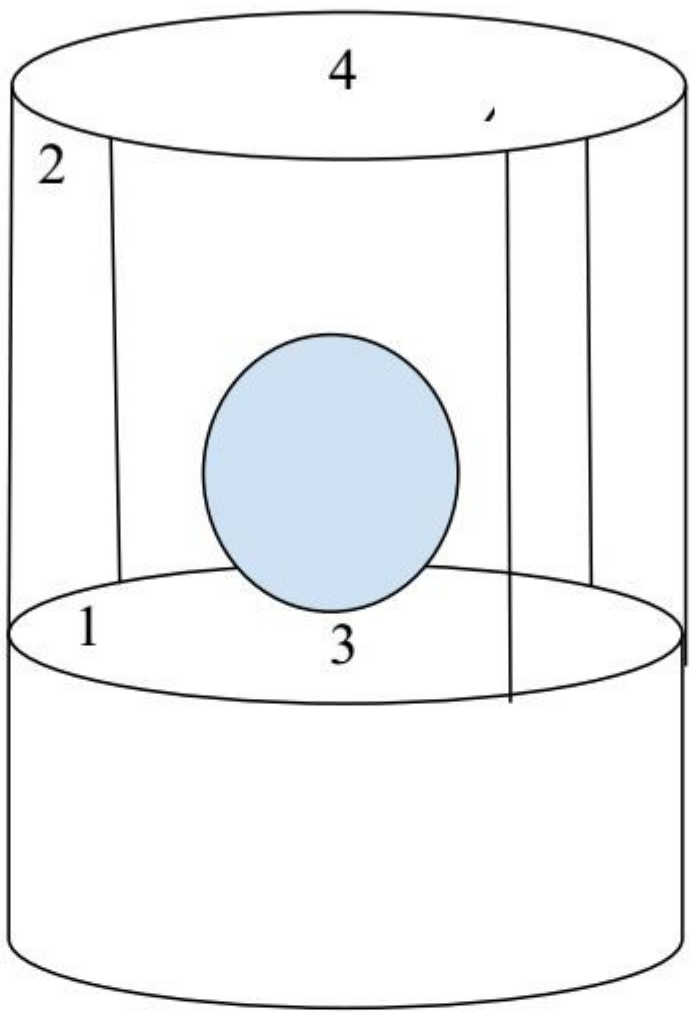
Вигляд головної панелі мобільного додатку



Вигляд системи програмного-технічного захисту



Розміщення датчиків захисту виставкового експонату



1. Датчик ультразвуку.
2. Магнітогерконовий датчик.
3. Датчик тиску.
4. Датчик руху.