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

БАКАЛАВРСЬКА ДИПЛОМНА РОБОТА

на тему:

«Розробка засобу для захисту інформації від витоку оптико-електронним каналом прихованими відеокамерами»

Виконала: студентка 4 курсу, гр.2КІТС-20б
спеціальності 125– Кібербезпека
Освітня програма – Кібербезпека
інформаційних технологій та систем
(шифр і назва напряму підготовки, спеціальності)

Олейніченко П. В.
(прізвище та ініціали)

Керівник: к.ф.-м.н., доц., доц. каф. МБІС

Шиян А. А.
(прізвище та ініціали)

«6» червня 2024 р.

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

Городецька О. С.
(прізвище та ініціали)

«6» червня 2024 р.

Допущено до захисту
Голова секції УБ кафедри МБІС
д.т.н., проф. Яремчук Ю.Є.
“6” червня 2024р.

Вінниця ВНТУ – 2024

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

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

ЗАТВЕРДЖУЮ
Голова секції УБ кафедри МБІС
д.т.н., проф. Яремчук Ю. Є.
«22» березня 2024 р.

З А В Д А Н Н Я
на бакалаврську дипломну роботу студенту
Олейніченко Поліні Вадимівній
(прізвище та ініціали)

1. Тема роботи: «Розробка засобу для захисту інформації від витоку оптико-електронним каналом прихованими відеокамерами»
Керівник роботи: к.ф.-м.н. доц. каф. МБІС Шиян А. А.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ректора закладу вищої освіти від «22» березня 2024 року № 80
2. Строк подання студентом роботи за тиждень до захисту
3. Вихідні дані до роботи:
Метою роботи є розробка засобу для захисту інформації від витоку оптико-електронним каналом прихованими відеокамерами, який забезпечить виявлення та локалізацію прихованих відеокамер у приміщеннях для запобігання несанкціонованому збору конфіденційної інформації.
4. Зміст текстової частини:
В першому розділі дипломної роботи здійснюється аналіз існуючих методів та засобів виявлення прихованих відеокамер, їх переваг та недоліків, а також досліджуються особливості оптико-електронного каналу витоку інформації. В другому розділі розробляється архітектура та функціональні вимоги до засобу захисту інформації від витоку оптико-електронним каналом, який використовує методи активного зондування та спектрального аналізу для виявлення прихованих відеокамер. У третьому розділі дипломної роботи здійснюється програмно-апаратна реалізація розробленого засобу з використанням мікроконтролерів, датчиків та спеціалізованого ПЗ. Проводиться тестування розробленого засобу. У висновках підбиваються усі результати проведеної роботи.
5. Перелік графічного матеріалу:

У першому розділі бакалаврської дипломної роботи наявно 8 рисунків, у другому розділі – 17 рисунків, у третьому розділі – 3 рисунка.

6. Консультанти розділів бакалаврської дипломної роботи

Розділ	Прізвище, ініціали та посада Консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ I	Шиян А. А., к.ф.-м.н., доц. каф. МБІС		
Розділ II	Шиян А. А., к.ф.-м.н., доц. каф. МБІС		
Розділ III	Шиян А. А., к.ф.-м.н., доц. каф. МБІС		

7. Дата видачі завдання «22» березня 2024р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської дипломної роботи	Строк виконання етапів бакалаврської дипломної роботи		Примітка
		початок	закінчення	
1	Визначення напрямку бакалаврської роботи, формулювання теми	25.03.2024	28.03.2024	
2	Аналіз предметної області обраної теми	29.03.2024	01.04.2024	
3	Розробка алгоритму роботи	03.04.2024	16.04.2024	
4	Написання бакалаврської роботи на основі розробленої теми	18.04.2024	05.05.2024	
5	Передзахист бакалаврської дипломної роботи	06.05.2024	24.05.2024	
6	Виправлення, уточнення, корегування бакалаврської дипломної роботи	26.05.2024	05.06.2024	
7	Захист бакалаврської дипломної роботи	13.06.2024	14.06.2024	

Студент _____ Олейніченко П. В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Шиян А. А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Бакалаврська дипломна робота складається із 75 сторінок тексту формату А4, включаючи 28 рисунків, 11 таблиць, посилання на 39 літературних джерел та 4 додатки.

У бакалаврській дипломній роботі розроблено засіб для захисту інформації від витоку оптико-електронним каналом прихованими відеокамерами. Запропонований пристрій дозволяє виявляти та локалізувати приховані відеокамери в приміщеннях для запобігання несанкціонованому збору конфіденційної інформації.

У першому розділі проведено аналіз існуючих методів та засобів виявлення прихованих відеокамер, досліджено особливості оптико-електронного каналу витоку інформації. У другому розділі розроблено архітектуру та функціональні вимоги до засобу захисту, який використовує методи активного зондування та спектрального аналізу. У третьому розділі здійснено програмно-апаратну реалізацію розробленого пристрою з використанням мікроконтролерів, датчиків та спеціалізованого програмного забезпечення, проведено тестування та оцінку його ефективності.

Ключові слова: приховані відеокамери, захист інформації, оптико-електронний канал витоку, активне зондування, спектральний аналіз.

ABSTRACT

The bachelor's thesis consists of 75 pages of A4 text, including 28 figures, 11 tables, references to 39 literature sources and 4 appendices.

In the bachelor's thesis, a device was developed to protect information from leakage through an optoelectronic channel by hidden video cameras. The proposed device allows to detect and localize hidden video cameras in the premises to prevent unauthorized collection of confidential information.

In the first section, we analyze existing methods and means of detecting hidden video cameras, and study the features of the optoelectronic information leakage channel. The second section develops the architecture and functional requirements for a security tool that uses active sensing and spectral analysis methods. In the third section, the software and hardware implementation of the developed device using microcontrollers, sensors and specialized software is carried out, and its effectiveness is tested and evaluated.

Keywords: hidden video cameras, information protection, optoelectronic leakage channel, active sensing, spectral analysis.

ЗМІСТ

ВСТУП

Актуальність теми. В сучасному світі питання забезпечення інформаційної безпеки набуває все більшої важливості. Зі зростанням обсягів конфіденційних даних, що обробляються та передаються, зростає і ризик їх витоку через різноманітні канали. Одним з найбільш небезпечних каналів витоку інформації є оптико-електронний канал, створюваний прихованими відеокамерами. Такі пристрої можуть бути встановлені зловмисниками в офісних приміщеннях, переговорних кімнатах або інших місцях, де обробляється конфіденційна інформація. Сучасні технології дозволяють з високою точністю передавати та записувати відео- та аудіоінформацію на відстані, що створює значні загрози для безпеки. Це вимагає розробки ефективних методів захисту від таких каналів витоку інформації.

З розвитком технологій та зниженням вартості обладнання, приховані відеокамери стають дедалі доступнішими, що збільшує ризик їх використання в злочинних цілях. Проблема витоку інформації оптико-електронним каналом є особливо гострою для державних установ, силових відомств, підприємств оборонної промисловості та інших організацій, діяльність яких пов'язана з обробкою секретних даних. Наслідки такого витоку можуть мати катастрофічні наслідки для національної безпеки та економіки країни.

Існуючі методи захисту, такі як фізичне виявлення та видалення камер, є ефективними, але потребують значних ресурсів та часу. Тому актуальним є розробка нових методів і пристроїв, що забезпечують захист конфіденційної інформації без необхідності активного пошуку та видалення прихованих камер.

Метою роботи є розробка пристрою для захисту інформації від витоку через оптико-електронні канали, спричинені прихованими відеокамерами. Пристрій має ефективно захищати конфіденційну інформацію від витоку опто-електронним каналом спричиненим прихованими камерами.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

- здійснити аналіз сучасного стану проблеми витоку інформації через оптико-електронні канали;
- вивчити основні принципи роботи оптико-електронних каналів витоку інформації;
- розглянути сучасні методи виявлення та протидії прихованим відеокамерам;
- удосконалити метод захисту інформації від витоку оптико-електронним каналом прихованими відеокамерами.
- розробити алгоритм захисту інформації від витоку оптико-електронним каналом спричинений прихованими відеокамерами;
- спроектувати архітектуру пристрою та обрати відповідні технології для його реалізації;
- розробити програмний засіб для реалізації удосконаленого методу.

Об'єкт дослідження – процеси захисту інформації від витоку через оптико-електронні канали, створені прихованими відеокамерами.

Предмет дослідження це архітектура пристрою блокування оптико-електронного каналу витоку інформації.

Новизна роботи полягає в розробці та реалізації пристрою для захисту інформації від витоку через оптико-електронні канали, створені прихованими відеокамерами, що забезпечує ефективне виявлення та блокування загроз.

Практична цінність роботи полягає в забезпеченні захисту конфіденційної інформації від несанкціонованого доступу шляхом використання розробленого пристрою. Це дозволить підвищити рівень інформаційної безпеки в різних сферах, де є ризик витоку даних через приховані відеокамери.

РОЗДІЛ 1. АНАЛІЗ ПІДХОДІВ ДО ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ОПТИКО-ЕЛЕКТРОННИМИ КАНАЛАМИ

Забезпечення інформаційної безпеки є критично важливим завданням для будь-якої організації, що працює з конфіденційними даними. Одним з ключових аспектів безпеки є запобігання витоку інформації через оптико-електронні канали, такі як приховані відеокамери, бездротові пристрої спостереження тощо. Зловмисники можуть використовувати ці канали для несанкціонованого отримання цінних даних, завдаючи значних збитків організації. Тому розробка ефективних методів виявлення та блокування оптико-електронних каналів витоку інформації є надзвичайно важливою. У цьому розділі буде проведено ґрунтовний аналіз існуючих підходів, їх переваг та недоліків, а також виявлені можливості для подальшого вдосконалення систем захисту інформації.

1.1. Аналіз відомих підходів до захисту інформації від витоку оптико-електронними каналами

У сучасному кібер-світі інформаційна безпека є більш важливою, ніж будь-коли. Проте часто загрози, які ми не помічаємо, знаходяться прямо у нас під носом - або на наших стінах і вікнах.

Сучасні міні-камери та інші пристрої негласного візуального спостереження можуть бути використані зловмисниками для отримання несанкціонованого доступу до інформації. Оптоелектронний витік дозволяє хакерам буквально шпигувати крізь стіни за допомогою лазерних мікрофонів [1].

Захист від такого витоку є критично важливим для забезпечення інформаційної безпеки. Існують різні підходи до захисту інформації від витоку через оптико-електронні канали, включаючи фізичні бар'єри, програмні рішення та електронні методи.

Фізичні бар'єри є одним із найбільш розповсюджених методів захисту від витоку інформації. До таких бар'єрів належать затемнення вікон, застосування захисних екранів та інших матеріалів, що блокують проникнення світла.

Затемнення вікон досягається використанням спеціальних плівок або штор, які не пропускають світло і тим самим унеможливлюють зйомку ззовні. Захисні екрани можуть бути виготовлені з матеріалів, що поглинають або відбивають світло, запобігаючи його проникненню до приміщення [2].

На рисунку 1.1. зображено приміщення, яке захищене від лазерного зондування та витоку конфіденційної інформації ззовні через оптикоелектронний канал (відеокамери) за допомогою щільних, непроникних для світла штор, якими закриваються усі вікна під час проведення важливих конференцій чи засідань де циркулює конфіденційна інформація. Цей підхід захисту ґрунтується на принципі фізичного блокування візуального доступу до приміщення ззовні.

Рис. 1.1 – Підхід блокування візуального доступу до приміщення [3]

Ключовим елементом захисту є щільні штори, які повністю закривають вікна, не пропускаючи сонячні промені та штучне освітлення ззовні. Це робить неможливим для сторонніх осіб, які знаходяться за межами кімнати, візуально спостерігати за діяльністю всередині, використовуючи лазерні прилади або відеокамери. Фізичні бар'єри мають свої переваги та недоліки. Основні переваги включають високу ефективність у блокуванні світлових променів та відносну простоту впровадження. Крім того, фізичні бар'єри не потребують складного технічного обслуговування. Недоліками є обмеження у використанні у

приміщеннях, де необхідно забезпечити природне освітлення, а також можливість їх обходу за допомогою спеціальних оптичних приладів.

Програмне забезпечення для детектування відеокамер відіграє важливу роль у цьому контексті. Таке програмне забезпечення дозволяє виявляти наявність відеокамер у приміщеннях або на об'єктах, що може запобігти несанкціонованому запису або передачі конфіденційної інформації (рис.1.2) [5].

Рис. 1.2 – Загальна схема ПЗ для виявлення прихованих відеокамер

Перевагами програмних рішень є їх гнучкість та можливість інтеграції в існуючі системи безпеки. Вони можуть бути налаштовані для виявлення різних типів загроз та адаптуватися до змін у середовищі. Однак програмні рішення мають також свої недоліки, включаючи залежність від апаратних ресурсів, необхідність регулярного оновлення для підтримання актуальності баз даних загроз та можливість помилкових спрацювань [4].

Наступним підходом до захисту інформації включає використання різноманітних технічних рішень, серед яких важливе місце належить різноманітним пристроям та генераторам, призначеним для генерації шуму та перешкод для електромагнітних сигналів.

Ці пристрої використовуються для блокування передачі відеосигналу та інших інформативних сигналів, які можуть бути використані для недозволеного збирання або передачі конфіденційної інформації [5]. На рисунку 1.3 зображено схематичну структурну модель таких пристроїв.

Рис. 1.3 – Схематична структурна модель роботи вище описаних пристроїв

Такі пристрої розроблені для активного захисту автоматизованих систем та об'єктів інформаційної діяльності шляхом перекриття спеціально організованими

перешкодами електромагнітних випромінювань та наведень, що виникають від роботи обладнання та комунікаційних засобів

Хоча у нього є свої переваги, він є лише одним із відомих підходів до захисту інформації від витоку оптико-електронним каналом. Серед його недоліків є обмежена ефективність у виявленні та блокуванні деяких типів електромагнітних сигналів, а також можливість виникнення систематичних або несистематичних помилок у роботі пристрою. Такі обмеження потрібно ураховувати при виборі технічного рішення для захисту інформації.

Порівняльний аналіз різних підходів до захисту інформації від витоку оптико-електронними каналами показує, що кожен з них має свої переваги та недоліки, що робить їх придатними для різних умов використання. В таблиці 1.1 наведено порівняння основних характеристик розглянутих підходів.

Таблиця 1.1 - Порівняння підходів до захисту інформації

Підхід	Ефективність	Вартість	Простота впровадження	Гнучкість
Фізичні бар'єри	Висока	Низька	Висока	Низька
Програмні рішення	Середня	Середня	Середня	Висока
Електронні методи	Висока	Висока	Низька	Середня

У висновку слід зазначити, що жоден з підходів не може забезпечити абсолютний захист від витоку інформації через оптико-електронні канали, а вибір конкретного підходу залежить від специфіки об'єкту захисту, наявних ресурсів та вимог до безпеки. Але комплексне поєднання декількох методів здатне забезпечити надійний багаторівневий захист інформації від витоку інформації оптико-електронними каналами.

1.2. Аналіз існуючих методів виявлення та блокування оптико-електронних каналів витоку інформації

Проблема витоку інформації через оптико-електронні канали, зокрема за допомогою прихованих відеокамер, набуває все більшої актуальності. Використання таких камер для несанкціонованого зйомки є серйозною загрозою для конфіденційності інформації в різних сферах діяльності. Ефективний захист від цієї загрози передбачає застосування методів виявлення та блокування оптико-електронних каналів витоку інформації.

Методи виявлення прихованих відеокамер включають активні та пасивні методи (рис.1.4) [6].

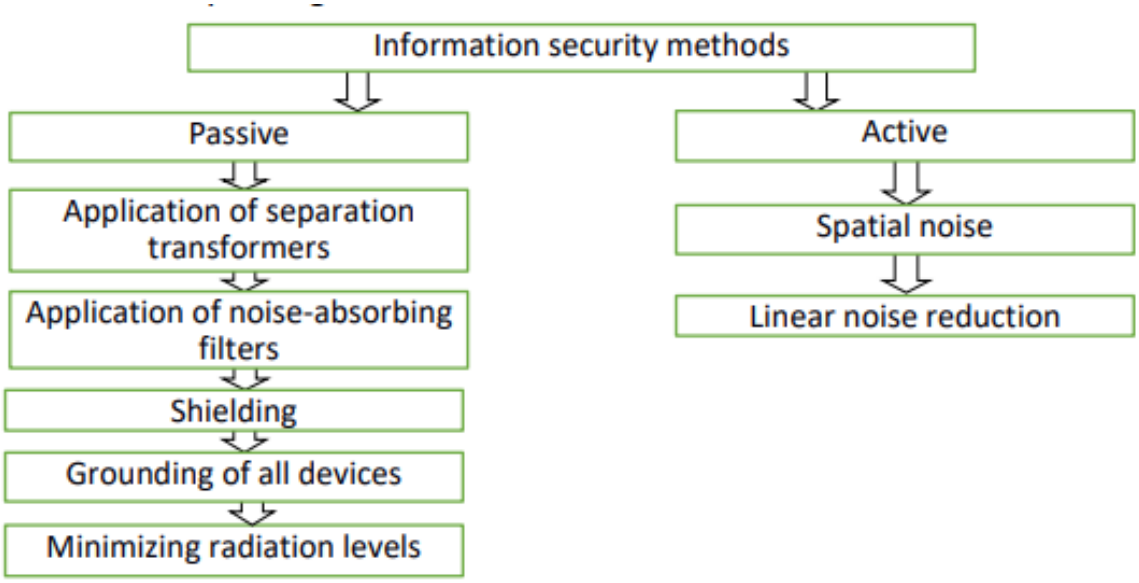


Рис. 1.4 – Методи боротьби витоку інформації оптико-електронним каналом

Активні методи, основані на випромінюванні та аналізі відбитого сигналу, є одним із захоплюючих напрямків в сучасних дослідженнях з безпеки. Ці методи базуються на випромінюванні та аналізі відбитого сигналу. Наприклад, інфрачервоні детектори використовують інфрачервоні промені для виявлення об'єктивів камер, які відбивають це випромінювання [7].

Використовуючи невидимі для людського ока промені, інфрачервоні детектори стають своєрідними «чуттєвими органами» системи безпеки, що є

ключовою особливістю ідентифікації відеопристроїв з інфрачервоним режимом застосовуються інфрачервоні сканери. Вони випромінюють лазерний промінь і аналізують відбитий сигнал для ідентифікації оптичних компонентів камер.

Окрім того, ці пристрої здатні фіксувати випромінювання в ІЧ-діапазоні від підсвічувачів, якими обладнані сучасні приховані камери для роботи в умовах низької освітленості (рис.1.5).

Рис. 1.5 – Вигляд інфрачервоних детекторів [7]

Ці методи мають високу точність і можуть виявляти навіть добре приховані камери, але їх ефективність знижується на великих відстанях і в умовах складного освітлення.

У свою чергу пасивні методи базуються на аналізі електромагнітних сигналів або візуальному огляді. Аналіз електромагнітних сигналів дозволяє виявити активні камери за допомогою аналізу випромінювань, що генеруються їх електронними компонентами. Візуальний огляд включає перевірку приміщень на наявність підозрілих об'єктів, що можуть бути камерами. Пасивні методи менш точні, ніж активні, але вони не потребують випромінювання сигналів, що робить їх непомітними для зловмисників [8].

Кількісні характеристики методів виявлення прихованих відеокамер включають точність (90-95% для активних методів, 70-80% для пасивних),

дальність виявлення (до 10 метрів для активних, до 5 метрів для пасивних) та зручність використання.

Основні переваги активних методів - висока точність і можливість виявлення на великих відстанях, недоліки - залежність від умов освітлення та необхідність спеціального обладнання. Пасивні методи прості у використанні та менш помітні, але мають нижчу точність і обмежену дальність.

Техніки блокування сигналів від відеокамер можна розділити на електронні та фізичні бар'єри. Електронні бар'єри, такі як глушилки та генератори шуму, працюють за принципом створення електромагнітних перешкод, які унеможливлюють передачу відеосигналу (рис. 1.6). Під час вибору методу блокування сигналів важливо враховувати характеристики приміщення та особливості електронної інфраструктури.

Фізичні бар'єри, такі як екранування та блокування простору, можуть бути використані для додаткового захисту у випадках, коли електронні методи не є достатньо ефективними.

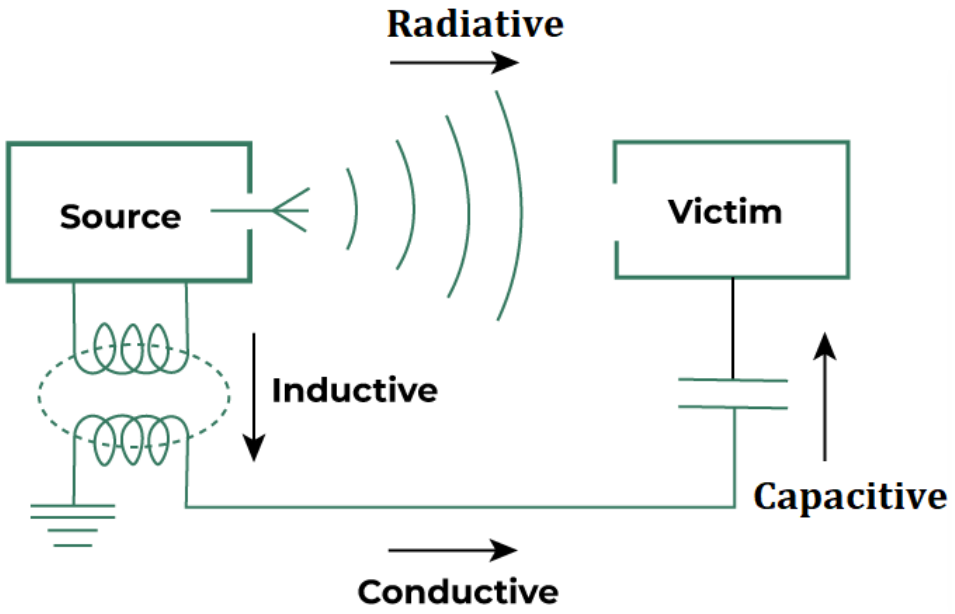


Рис. 1.6 – Загальна технологічна схема примітивної глушилки [9]

Глушилки блокують сигнали на певних частотах, що використовуються для передачі відео, а генератори шуму створюють загальні електромагнітні перешкоди, що заважають роботі електронних пристроїв.

Фізичні бар'єри включають матеріали, що поглинають світло, та захисні покриття. Матеріали, що поглинають світло, запобігають відбиттю світлових променів від об'єктивів камер, що ускладнює зйомку. Захисні покриття, такі як спеціальні фільтри на вікнах та екранах, запобігають проникненню світлових променів, що унеможливлює запис відео через ці поверхні.

Переваги електронних бар'єрів включають високу ефективність блокування сигналів та можливість їх застосування в різних умовах. Недоліки - висока вартість та необхідність регулярного технічного обслуговування. Фізичні бар'єри є більш доступними за вартістю та не потребують спеціального обслуговування, але їх ефективність може бути меншою залежно від умов експлуатації [10].

Найнадійніший і найочевидніший спосіб виявлення прихованих камер - ретельний фізичний огляд приміщення. Це передбачає перевірку всіх підозрілих об'єктів, особливо тих, які спрямовані в бік чутливих зон. Важливо звернути увагу на нові або переміщені предмети, а також на такі, які не відповідають загальному декору приміщення.

Для блокування роботи виявлених відеопристроїв можуть застосовуватися методи радіоелектронного подавлення (глушіння) сигналів їх антен або електромагнітні імпульсні поля для виведення камер з ладу. Також використовуються засоби активної оптичної маскування - генератори світлових імпульсів для підсвічування та "осліплення" камер [11].

Окремим ключовим напрямком протидії витоку інформації оптико-електронними каналами є забезпечення суворого фізичного контролю доступу до приміщень, де обробляються конфіденційні дані, а також обмеження використання особистих пристроїв співробітниками на робочих місцях. Проте для ефективного захисту необхідно застосовувати комплекс технічних засобів виявлення та блокування прихованих відеокамер.

Одним з найпоширеніших інструментів є детектори лінз, що працюють за принципом виявлення відбитого світла від лінзи камери. Під час спрямування джерела світла на підозрілий об'єкт, лінза прихованої камери відбиває світловий промінь назад, що може бути зафіксовано спеціальним пристроєм детектора [12].

Важливим методом є використання детекторів радіочастот (RF-детекторів), здатних виявляти електромагнітні поля, що генеруються передавачами прихованих камер з бездротовим інтерфейсом передачі відеоданих. Дані пристрої дозволяють виявити присутність камер, що використовують Wi-Fi, Bluetooth або інші радіоканали для трансляції [13]. Таблиця 1.2 відображає порівняння вище згаданих методів виявлення та блокування витоку інформації оптико-електронним каналом.

Таблиця 1.2 - Порівняння методів виявлення та блокування

Метод	Точність	Ефективність	Вартість	Дальність/радіус дії
Активні методи виявлення	90-95%	90-95%	Висока	До 10 метрів
Пасивні методи виявлення	70-80%	70-80%	Низька	До 5 метрів
Електронні бар'єри	85-95%	85-95%	Висока	До 30 метрів
Фізичні бар'єри	70-90%	70-90%	Низька	Залежить від умов
Комплекс засобів	95-98%	95-98%	Висока	До 30 метрів
Програмне забезпечення	55-65%	55-75%	Низька	Залежить від системи

У результаті аналізу існуючих методів виявлення та блокування оптико-електронних каналів витоку інформації було виявлено, що активні методи виявлення та електронні бар'єри є найефективнішими, але мають високу вартість та обмежену дальність дії. Пасивні методи та фізичні бар'єри є більш доступними, але менш точними та ефективними. Комплекс засобів забезпечує високу ефективність та зручність використання, але також мають високу вартість. Вибір оптимального методу залежить від конкретних умов використання та наявних ресурсів.

Комплексне застосування наведених технічних та організаційних методів є необхідною умовою для забезпечення надійного захисту конфіденційної інформації від витоку оптико-електронними каналами в сучасних умовах.

1.3. Аналіз існуючих програмних та апаратних реалізацій для захисту від витоку інформації

Потреба в програмних і апаратних рішеннях для захисту інформації від витоку обумовлена декількома факторами. По-перше, зростання кількості і доступності прихованих відеокамер створює нові виклики для захисту конфіденційної інформації. По-друге, традиційні методи захисту, такі як фізичне обмеження доступу до інформації, стають недостатніми у зв'язку з розвитком технологій. По-третє, в умовах постійного вдосконалення технічних засобів зловмисників, необхідно впроваджувати комплексні та ефективні рішення для захисту інформації.

Програмне забезпечення для виявлення відеокамер відіграє важливу роль у цьому контексті, допомагаючи запобігти несанкціонованому запису або поширенню конфіденційних даних. Антивірусне програмне забезпечення, як правило, використовується для детектування та видалення шпигунських програм, які можуть бути встановлені для несанкціонованого запису відео. Таке програмне забезпечення аналізує файлову систему, мережевий трафік та оперативну пам'ять для виявлення підозрілих активностей. Наприклад, відомі антивірусні продукти, такі як Kaspersky, Norton та McAfee, включають модулі для виявлення шпигунських програм, які можуть бути використані для несанкціонованого відеоспостереження.

Серед програмних рішень Kaspersky Endpoint Security вирізняється широким спектром функцій, включаючи моніторинг та управління завданнями, спостереження за підключенням до мережі Kaspersky Security Network та виявлення загроз (рис.1.7) [14].

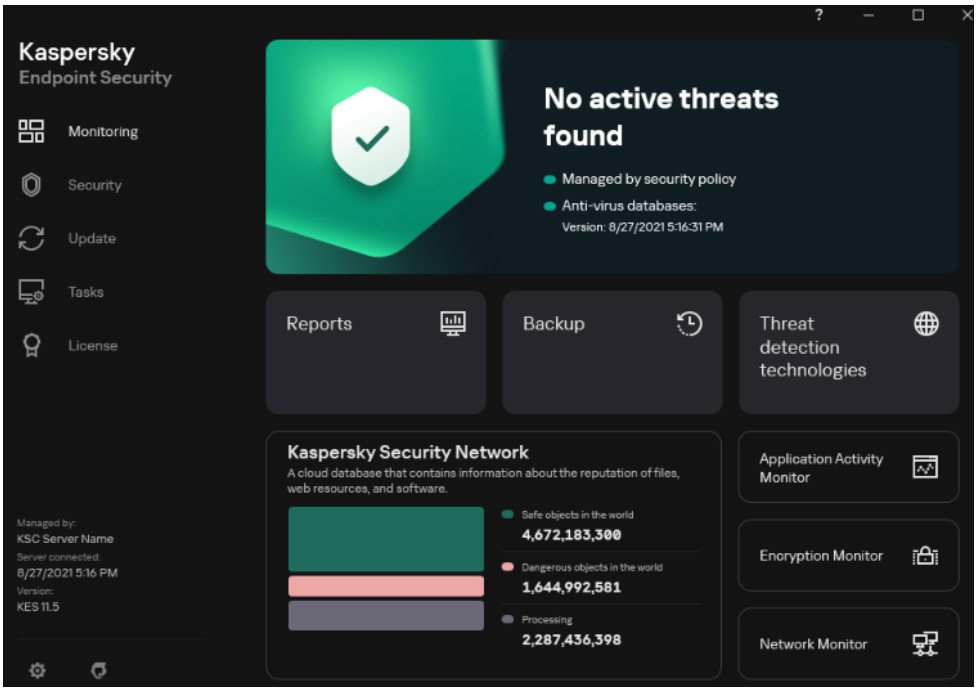


Рис. 1.7 – Інтерфейс противошпигунського ПЗ Kaspersky Endpoint Security [14]

Хоча Kaspersky Endpoint Security має свої переваги, слід враховувати його обмеження, такі як можливість несистематичних помилок та нестабільна взаємодія з апаратними засобами. Тим не менш, вибір програмного забезпечення для захисту інформації від витоку оптико-електронним каналом за допомогою виявлення відеокамер відображає проактивну позицію в зміцненні інформаційної безпеки [15].

Окрім антивірусного ПЗ, існують спеціалізовані програмно-апаратні засоби виявленню витоку інформації прихованими відеокамерами. Ці програми використовують алгоритми аналізу відеопотоку для ідентифікації об'єктивів камер та аналізу електромагнітних випромінювань. Такі програмні рішення дозволяють виявити приховані відеокамери на ранніх етапах їх роботи, що є важливим для забезпечення безпеки конфіденційної інформації.

Основними перевагами таких рішень є їх висока гнучкість та можливість оновлення. Вони можуть бути легко адаптовані до нових загроз та інтегровані в існуючі системи безпеки. Програмні рішення, як правило, є зручними у використанні завдяки інтуїтивно зрозумілому інтерфейсу та автоматичним

оновленням. Однак, вони також мають і певні недоліки, зокрема можливість обходу програмних бар'єрів та необхідність регулярного оновлення баз даних.

Кількісні характеристики програмних рішень включають точність виявлення до 95%, швидкість роботи залежить від потужності системи та обсягу даних, та зручність використання. Ці характеристики визначають ефективність програмних засобів у конкретних умовах використання [16].

Апаратні засоби захисту забезпечують фізичний захист від витоку інформації.

Ключовим різновидом апаратних засобів є глушилки – пристрої, що генерують сигнали перешкод у різних діапазонах для блокування роботи бездротових відеокамер.

Один із найвідоміших пристроїв захисту інформації від витоку оптико-електронним каналом, який зображено на рисунку 1.8, пристрій "DELTA-7". Цей пристрій розроблений для активного захисту автоматизованих систем та об'єктів інформаційної діяльності шляхом перекриття спеціально організованими перешкодами електромагнітних випромінювань та наведень, що виникають від роботи обладнання та комунікаційних засобів [17].

DELTA-7 забезпечує випромінювання захисних електромагнітних перешкод, фільтрацію паразитних сигналів та введення струмових захисних перешкод в ланцюги електроживлення та систем заземлення.

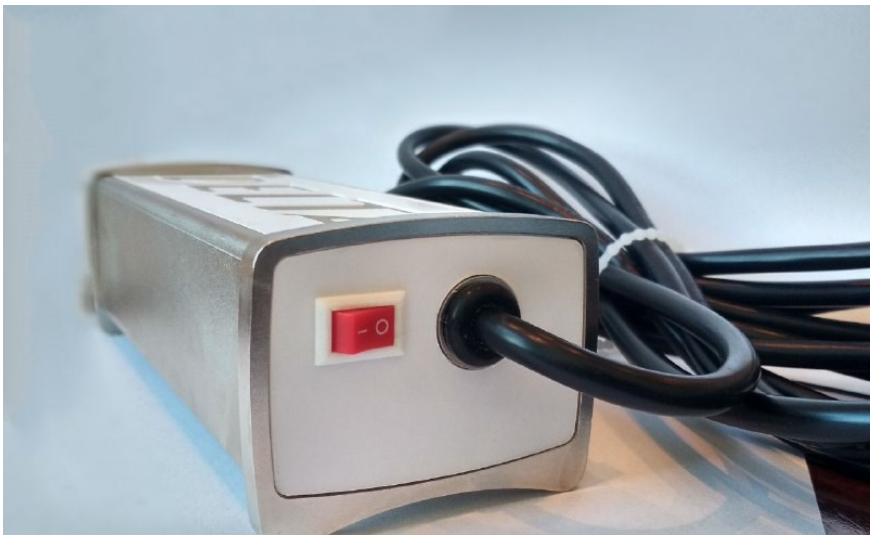


Рис. 1.8 – Пристрій DELTA-7" для активного захисту автоматизованих систем [17]

Хоча у нього є свої переваги, він є лише одним із відомих підходів до захисту інформації від витоку оптико-електронним каналом. Серед його недоліків є обмежена ефективність у виявленні та блокуванні деяких типів електромагнітних сигналів, а також можливість виникнення систематичних або несистематичних помилок у роботі пристрою. Такі обмеження потрібно ураховувати при виборі технічного рішення для захисту інформації.

Глушилки використовуються для блокування сигналів від відеокамер, генеруючи електромагнітні перешкоди, які унеможливлюють передачу відеоінформації. Вони можуть застосовуватися в різних сферах, де необхідно забезпечити конфіденційність інформації, наприклад, у конференц-залах або приміщеннях для переговорів [18].

Детектори відеокамер аналізують простір на наявність прихованих камер за допомогою лазерних або інфрачервоних променів. Вони дозволяють виявляти навіть дуже добре приховані камери, що робить їх незамінними в умовах підвищеної загрози витоку інформації. Захисні екрани, виготовлені з матеріалів, що поглинають світло або електромагнітні хвилі, запобігають зйомці конфіденційної інформації.

Апаратні засоби мають свої переваги, серед яких висока ефективність у певних умовах та незалежність від програмних оновлень. Однак, вони також характеризуються високою вартістю та обмеженим радіусом дії, що може бути недоліком у певних ситуаціях.

Кількісні характеристики апаратних засобів включають ефективність до 90-99%, радіус дії до 30 метрів, та вартість. Ці характеристики визначають доцільність використання апаратних засобів у конкретних умовах та їх ефективність у запобіганні витоку інформації [19].

Інтегровані системи захисту об'єднують програмні та апаратні компоненти для комплексного захисту інформації. Такі системи включають в себе як програмні засоби для детектування загроз, так і апаратні пристрої для фізичного блокування витоку. Комплексні системи, як правило, забезпечують найвищий рівень захисту завдяки поєднанню різних методів та технологій [20].

Основними перевагами інтегрованих систем є комплексний підхід та висока ефективність. Однак, вони також мають недоліки, зокрема високу вартість та складність інтеграції в існуючі системи безпеки (табл. 1.3).

Таблиця 1.3 - Порівняння програмних та апаратних реалізацій

Реалізація	Ефективність	Вартість	Мобільність	Зручність
Програмні	60-75%	Низька	Висока	Висока
Апаратні	80-98%	Висока	Середня	Середня
Інтегровані	До 99%	Дуже висока	Низька	Середня

Приклади реалізацій інтегрованих систем включають системи Ranger firmeX та Eagle Eye компанії SypherMedia, які поєднують програмні та апаратні компоненти для забезпечення комплексного захисту інформації. Такі системи розробляються провідними виробниками в галузі інформаційної безпеки та включають найсучасніші технології для детектування та блокування загроз [21].

Рішення Eagle Eye компанії SypherMedia є комплексною системою протидії витоку аудіовізуальних даних у реальному часі під час конференцій, переговорів або інших заходів. Воно поєднує функції аналізу відеосигналів для виявлення загроз та одночасного застосування електронного заглушення виявлених каналів шляхом створення перешкод їх роботі (табл.1.4) [22].

Таблиця 1.4 – Порівняння переваг та недоліків вище описаних продуктів

Назва продукту	Функції	Переваги	Недоліки
Eagle Eye	Виявлення загроз в режимі реального часу, електронне заглушення	Комплексний захист під час конференцій	Висока складність налаштування
Ranger firmeX	Виявлення та блокування камер, сканування мереж, антивірусний захист	Багатофункціональність	Висока вартість, складність
Watchdog	Виявлення та блокування камер і мікрофонів (з відкритим кодом)	Доступність, відкритий код	Обмежені можливості, потребує налаштування

Багатофункціональний програмний комплекс Ranger firmeX пропонує інструменти для боротьби як з прихованими відеокамерами, так і іншими потенційними загрозами інформаційній безпеці [23]. Окрім виявлення камер та блокування їх роботи, він здатний сканувати комп'ютерні мережі на предмет витоків даних, виявляти шкідливе програмне забезпечення тощо.

Варто відзначити також Watchdog від ReDrill - доступне програмне рішення з відкритим вихідним кодом для виявлення та блокування роботи прихованих відеокамер і мікрофонів на комп'ютерах під управлінням Windows [24].

У результаті аналізу існуючих програмних та апаратних реалізацій було виявлено, що інтегровані системи забезпечують найвищий рівень захисту, але мають високу вартість та складність інтеграції. Програмні рішення є гнучкими та доступними, але можуть бути менш ефективними у порівнянні з апаратними засобами. Апаратні засоби, хоча й ефективні, потребують значних фінансових вкладень. Кожен з розглянутих підходів має свої переваги та недоліки, що слід враховувати при виборі оптимального рішення для конкретних умов.

1.4. Висновки та постановка задач

У розділі 1 було проведено ґрунтовний аналіз існуючих підходів, методів та апаратних реалізацій для захисту інформації від витоку через оптико-електронні канали, такі як приховані відеокамери та інші пристрої спостереження.

Розглянуті фізичні бар'єри, програмні рішення та електронні методи блокування дозволяють досягти високого рівня захисту в певних умовах, проте мають низку недоліків:

- обмежена мобільність та гнучкість застосування через особливості конструкції або принципів роботи;
- висока вартість апаратних засобів та інтегрованих систем;
- недостатня точність виявлення деяких видів загроз;
- складність адміністрування та налаштування під конкретні вимоги.

Аналіз показав необхідність створення більш універсального, ефективного та доступного за ціною рішення для комплексного захисту інформації від витоку оптико-електронним каналом прихованих відеокамер.

Таким чином, основною задачею даної дипломної роботи є удосконалення існуючих засобів захисту інформації від витоку оптико-електронним каналом прихованими відеокамерами за рахунок підвищення ефективності виявлення загроз, спрощення налаштування та експлуатації, а також зниження вартості реалізації.

Для виконання поставленого завдання необхідно вирішити наступні підзадачі:

– розробити удосконалений алгоритм виявлення та блокування прихованих відеокамер та інших оптико-електронних пристроїв витоку;

– здійснити обґрунтований вибір елементної бази та провести необхідне моделювання для реалізації апаратної частини пристрою;

– реалізувати програмний код виконання розробленого алгоритму з урахуванням особливостей апаратної частини;

– провести тестування створеного пристрою в різних умовах експлуатації для підтвердження його ефективності.

Виконання поставлених задач дозволить отримати універсальний, високоефективний та економічно доступний засіб захисту конфіденційних даних від витоку через оптико-електронні канали прихованими відеокамерами.

РОЗДІЛ 2. УДОСКОНАЛЕННЯ ЗАСОБУ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ОПТИКО-ЕЛЕКТРОННИМ КАНАЛОМ ПРИХОВАНИМИ ВІДЕОКАМЕРАМИ

Захист конфіденційної інформації від витоку оптико-електронним каналом через приховані відеокамери є важливим питанням для забезпечення інформаційної безпеки в різних сферах діяльності. Існуючі методи захисту, такі як фізичне виявлення та видалення камер, є ефективними, але потребують значних ресурсів та часу. Тому актуальним є розробка нових методів і пристроїв, що забезпечують захист конфіденційної інформації без необхідності активного пошуку та видалення прихованих камер.

2.1. Обґрунтування удосконалення пристрою захисту

Захист конфіденційної інформації від витоку через приховані відеокамери є важливим питанням для забезпечення інформаційної безпеки в різних сферах діяльності. Існуючі методи захисту, такі як фізичне виявлення та видалення камер, є ефективними, але потребують значних ресурсів та часу. Тому актуальним є розробка нових методів і пристроїв, що забезпечують захист конфіденційної інформації без необхідності активного пошуку та видалення прихованих камер.

Серед наявних на ринку аналогічних засобів можна виділити такі недоліки: висока складність налаштування, обмежені функції захисту, висока вартість та складність у користуванні.

Багато пристроїв захисту потребують складної конфігурації та налаштування, що вимагає глибоких технічних знань та досвіду користувачів. Деякі пристрої зосереджені лише на одному аспекті захисту, наприклад, блокуванні радіосигналів або спотворенні візуальної інформації, не забезпечуючи комплексного підходу [24].

Вартість багатьох існуючих засобів захисту є досить високою, що обмежує їх доступність для широкого кола користувачів. Багато пристроїв мають незручний

інтерфейс користувача та недостатню інтеграцію з іншими системами, що ускладнює їх використання та експлуатацію.

Для вирішення зазначених проблем та удосконалення засобу захисту інформації від витоку оптико-електронними каналами пропонується комплексний підхід, який поєднує кілька ключових напрямків [25].

По-перше, спрощення налаштування та використання. Розробка інтуїтивного та простого інтерфейсу користувача, автоматизація процесів налаштування та інтеграція з існуючими системами забезпечить легкість використання пристрою. Це дозволить зменшити залежність від технічних знань користувачів і зробить пристрій доступним для широкого кола користувачів.

По-друге, комплексний захист. Пристрій матиме можливість генерувати радіоперешкоди, спотворювати акустичну та візуальну інформацію, а також створювати фізичні перешкоди для каналів витоку, забезпечуючи всебічний захист від прихованих відеокамер. Такий підхід забезпечить комплексне блокування різних каналів витоку інформації.

По-третє, оптимізація вартості. Використання доступних компонентів та технологій, таких як 3D друк корпусу, дозволить знизити загальну вартість пристрою, зберігаючи при цьому високу ефективність захисту. Це зробить пристрій більш доступним для широкого кола користувачів.

По-четверте, підвищення зручності експлуатації. Автономне живлення, компактний розмір та міцний корпус забезпечать мобільність та зручність використання пристрою в різних умовах. Це дозволить використовувати пристрій у різних середовищах, включаючи офісні приміщення, конференц-зали та інші місця, де необхідно забезпечити високий рівень захисту інформації [27].

Запропонований пристрій для захисту інформації від витоку через приховані відеокамери є комплексним рішенням, що поєднує кілька ключових технічних компонентів. Основою пристрою є потужний мікроконтролер, який керує роботою всіх систем та забезпечує їх синхронізацію. Для генерації радіоперешкод використовується програмований синтезатор частот, здатний створювати радіосигнали у діапазонах 2,4 ГГц. Випадкове змінення частоти та амплітуди

сигналів забезпечується спеціальним алгоритмом, реалізованим у програмному забезпеченні пристрою.

Для створення акустичних перешкод та спотворення звукових сигналів використовується високоякісний мікрофон, підсилювач та цифровий сигнальний процесор. Запис звуків, їх обробка та спотворення здійснюються в режимі реального часу, забезпечуючи ефективне блокування витоку акустичної інформації. Генерація низькочастотних вібрацій для впливу на оптичні датчики камер реалізована за допомогою потужного вібраційного модуля та спеціальних віброколонок (табл. 2.1) [28].

Таблиця 2.1 – Порівняння характеристик запропонованого пристрою з аналогами:

Характеристика	Запропонований пристрій	Аналог 1	Аналог 2
Захист від радіоперешкод	Так	Так	Ні
Захист від витоку акустичної інформації	Так	Ні	Так
Захист від витоку візуальної інформації	Так	Так	Ні
Інтеграція з іншими системами	Так	Ні	Ні
Зручність налаштування та використання	Висока	Низька	Середня
Орієнтовна вартість (грн)	1200 грн	9 000 грн	3 000 грн

Як видно з таблиці 2.1, удосконалений пристрій забезпечує комплексний захист від різних каналів витоку інформації, включаючи радіоперешкоди, акустичні та візуальні перешкоди. Він також має перевагу інтеграції з іншими системами безпеки та зручного налаштування за допомогою інтуїтивного інтерфейсу користувача. Порівняно з аналогом 1, наш пристрій має нижчу вартість, але забезпечує ширший спектр функцій захисту. Аналог 2 є найдешевшим, але має обмежені можливості, захищаючи лише від витоку акустичної інформації [28].

Запропонований пристрій для захисту інформації від витоку оптико-електронними каналами матиме такі переваги: простота налаштування та

використання – це зробить його доступним для широкого кола користувачів без необхідності спеціальних технічних знань.

Комплексний захист від різних типів загроз, включаючи блокування передачі даних, спотворення акустичної та візуальної інформації. Оптимальне співвідношення ціни та ефективності, що робить засіб захисту доступним для організацій та приватних осіб з різними бюджетами. Висока мобільність та зручність експлуатації, що дозволяє використовувати пристрій у різних умовах та середовищах [29].

Таким чином, удосконалений засіб для захисту інформації від витоку оптико-електронними каналами прихованими відеокамерами усуватиме недоліки існуючих аналогів, забезпечуючи комплексний, доступний та зручний спосіб захисту конфіденційної інформації без необхідності активного пошуку та видалення прихованих камер.

2.2. Опис алгоритму роботи удосконаленого пристрою

Розробка удосконаленого пристрою для захисту інформації від витоку через оптико-електронні канали прихованими відеокамерами базується на комплексному алгоритмі, що охоплює кілька етапів. Кожен з цих етапів спрямований на створення ефективних перешкод для функціонування прихованих камер, забезпечуючи таким чином надійний захист конфіденційної інформації.

Запропонований пристрій для захисту інформації від витоку оптико-електронним каналом прихованими відеокамерами працює за комплексним алгоритмом, що поєднує кілька ключових кроків:

Крок 1. Ініціалізація системи та сканування оточення.

Крок 2. Генерація радіоперешкод.

Крок 3. Створення акустичних перешкод.

Крок 4. Генерація низькочастотних вібрацій.

Загальна структура алгоритму представлена на рисунку 2.1, який ілюструє послідовність основних етапів роботи пристрою. Кожен етап відіграє важливу

роль у забезпеченні комплексного захисту від прихованих камер, діючи на різні аспекти їх функціонування.

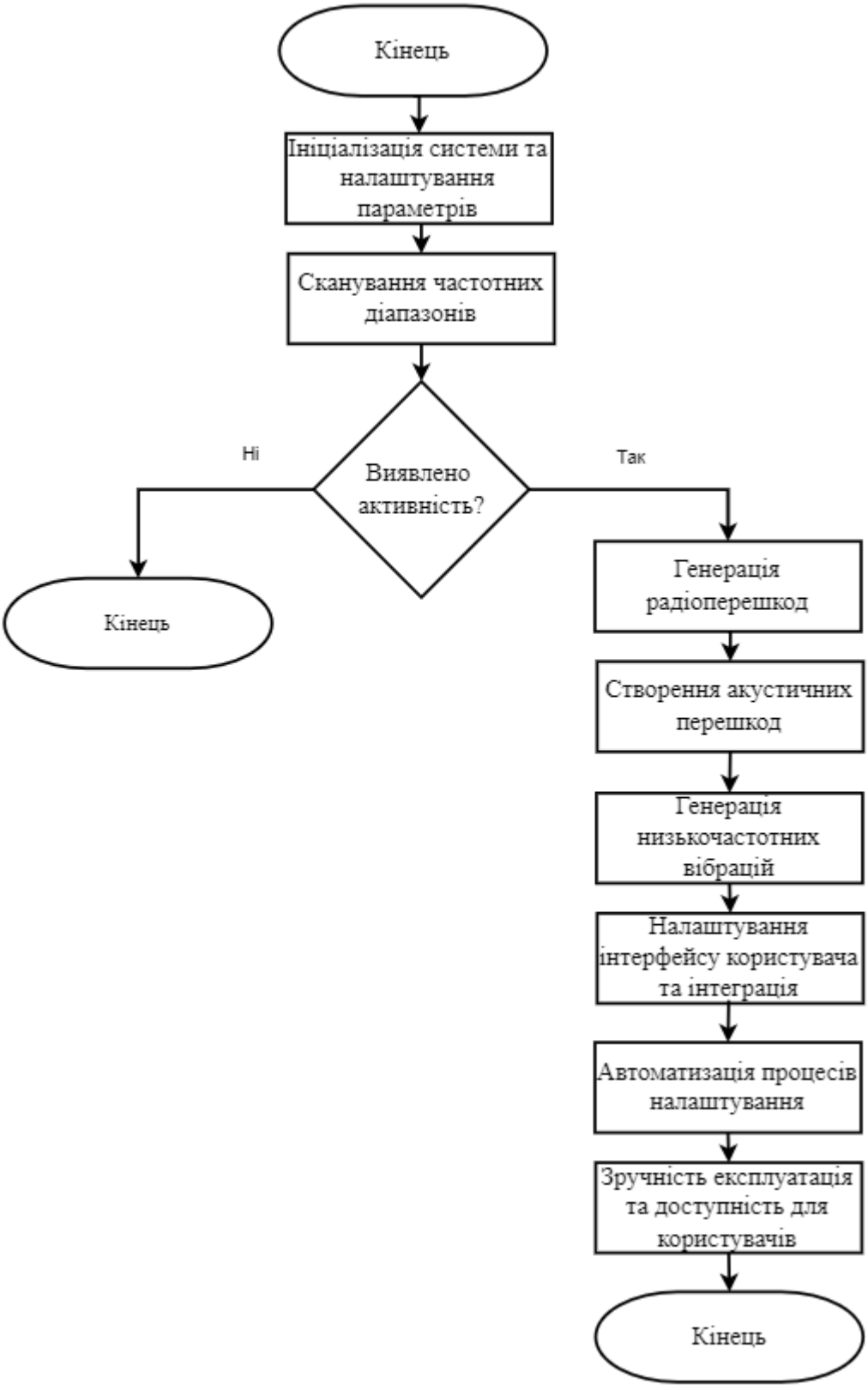


Рисунок 2.1 – Схема алгоритму роботи розроблюваного пристрою

На цьому рисунку схематично відображено загальну структуру алгоритму роботи удосконаленого пристрою, що складається з ряду взаємопов'язаних етапів, спрямованих на забезпечення комплексного захисту інформації від витоку оптико-електронним каналом прихованих камер. Запропонований пристрій для захисту інформації від витоку оптико-електронним каналом прихованими відеокамерами працює за комплексним алгоритмом, що поєднує кілька ключових кроків: Детальна схема структури першого етапу алгоритму, що охоплює ініціалізацію системи та сканування оточення, представлена на рисунку 2.2.

Рисунок 2.2 – Схема роботи алгоритму розробленого пристрою на 1 етапі

Крок 1. На цьому етапі відбувається запуск системи, ініціалізація всіх компонентів та налаштування параметрів роботи пристрою. Після цього здійснюється автоматичне сканування частотних діапазонів, у яких типово працюють бездротові відеопередавачі, такі як приховані камери. Зокрема, відбувається моніторинг діапазонів 2,4 ГГц [30].

Цей рисунок детально демонструє послідовність кроків на початковому етапі роботи пристрою, починаючи від увімкнення та завершуючи виявленням активності у контрольованих частотних діапазонах, що є сигналом для активації наступних етапів захисту. Детальна схема структури другого кроку алгоритму, який відповідає за генерацію радіоперешкод, представлена на рисунку 2.3.

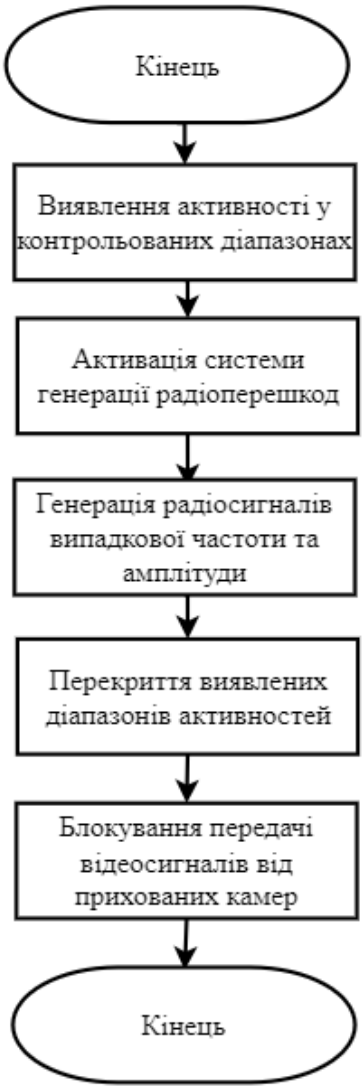


Рисунок 2.3 – Схема роботи алгоритму розробленого пристрою на 2 етапі.

Крок 2. Якщо на попередньому етапі було виявлено активність у контрольованих частотних діапазонах, пристрій активує систему генерації радіоперешкод. Ця система створює потужні радіосигнали випадкової частоти та амплітуди, які перекривають виявлені діапазони активності, блокуючи таким чином передачу відеосигналів від прихованих камер.

Детальна схема структури третього етапу алгоритму, який забезпечує створення акустичних перешкод, представлена на рисунку 2.4.

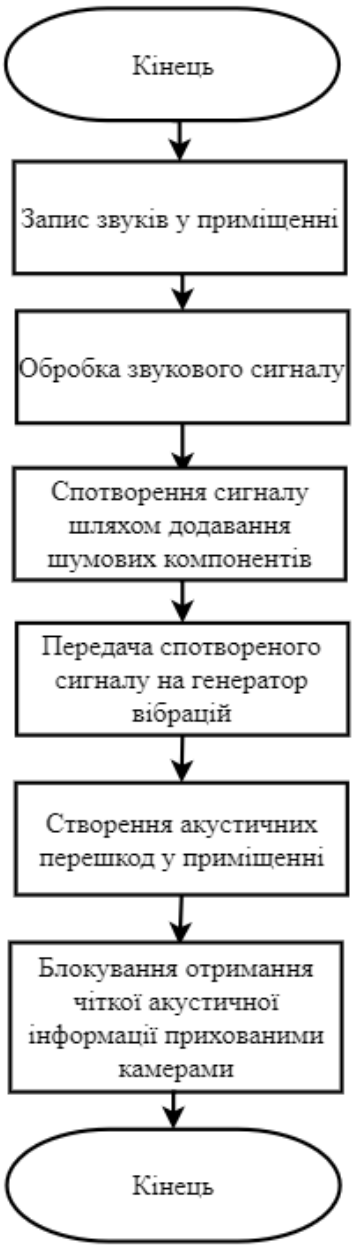


Рисунок 2.4 – Схема роботи алгоритму розробленого пристрою на 3 етапі

Крок 3. Після виявлення активності у контрольованих частотних діапазонах, пристрій активує систему генерації радіоперешкод. Ця система створює потужні радіосигнали випадкової частоти та амплітуди, які перекривають виявлені діапазони активності. Використання випадкової зміни частот та амплітуд забезпечує стійкість до виявлення та усунення перешкод із боку зловмисників. Таким чином, ефективно блокується передача відеосигналів від прихованих камер до приймачів, запобігаючи витоку візуальної інформації.

Крок 4. На цьому пристрій використовує вбудований мікрофон для запису звуків у приміщенні. Записаний звуковий сигнал обробляється алгоритмом, який спотворює його шляхом додавання випадкових шумових компонентів. Цей спотворений сигнал передається на генератор низькочастотних вібрацій, створюючи акустичні перешкоди у приміщенні, які ускладнюють отримання чіткої акустичної інформації прихованими камерами.

Рисунок ілюструє процес, за яким пристрій записує звуки у приміщенні, спотворює звуковий сигнал шляхом додавання шумових компонентів, а потім передає спотворений сигнал на генератор вібрацій для створення акустичних перешкод, які ускладнюють отримання чіткої акустичної інформації прихованими камерами. Такі перешкоди не сприймаються людським вухом, але значно ускладнюють отримання чіткої акустичної інформації прихованими камерами, запобігаючи витоку голосових даних.

Крок 5. Для підвищення ефективності блокування прихованих відеокамер пристрій генерує низькочастотні вібрації, здатні впливати на роботу оптичних датчиків камер. Ці вібрації знаходяться у діапазоні частот, що не сприймаються людським вухом, але можуть спричиняти спотворення або розмиття зображення, отриманого оптичними датчиками камер. Низькочастотні вібрації поширюються у приміщенні за допомогою спеціальних віброколонок. Детальна схема структури четвертого етапу алгоритму, що відповідає за генерацію низькочастотних вібрацій, представлена на рисунку 2.5.

Рисунок 2.5 – Детальна схема структури четвертого етапу алгоритму

Як показано на рисунку, пристрій генерує низькочастотні вібрації, які впливають на оптичні датчики прихованих камер, спричиняючи спотворення або розмиття зображення. Ці вібрації поширюються у приміщенні, забезпечуючи вплив на всі потенційно присутні приховані камери, незалежно від їх розташування.

Запропонований удосконалений пристрій для захисту інформації від витоку через оптико-електронні канали приховані відеокамери являє собою комплексне та ефективне рішення. Його унікальність полягає у поєднанні кількох різних

методів генерації перешкод, що діють на різні аспекти функціонування прихованих камер. Завдяки генерації радіоперешкод, створенню акустичних перешкод та низькочастотних вібрацій, пристрій блокує передачу відеосигналів, спотворює аудіо та розмиває зображення, отримане оптичними датчиками. Така комбінована дія перешкод забезпечує надійний багаторівневий захист конфіденційної інформації. Автоматизація процесів, випадкова зміна параметрів перешкод та зручний інтерфейс користувача роблять експлуатацію пристрою максимально ефективною та зручною.

Загалом, цей інноваційний пристрій є потужним інструментом для протидії витокам інформації через приховані камери в офісах, переговорних кімнатах та інших критичних зонах.

2.3. Моделювання електричної частини пристрою

Принцип роботи пристрою полягає у захисті інформації від витоку інформації через приховані відеокамери шляхом створення радіоперешкод для блокування передачі даних камер, генерації акустичних та вібраційних перешкод для ускладнення роботи оптичних датчиків, а також екранування можливих каналів витоку через вікна та інші оптичні поверхні.

Тому спроектований пристрій складається з декількох основних модулів: генератора радіоперешкод, акустичного модуля, генератора низькочастотних вібрацій та блоку живлення. Кожен з цих модулів будується із різних запчастин кожнf з яких виконує свою роль у забезпеченні функціональності пристрою. Центральним елементом є плата Arduino Nano, яка керує роботою інших компонентів і виконує основну логіку пристрою.

OLED дисплей використовується для відображення інформації про стан пристрою та попереджень, тоді як звуковий і п'єзо датчики призначені для виявлення небезпечних звуків і вібрацій відповідно. Бездротовий модуль NFR24L01+PA+LNA забезпечує можливість бездротового зв'язку між пристроями захисту інформації для передачі даних та команд управління.

Ультразвукові випромінювачі генерують ультразвукові хвилі, які можуть взаємодіяти з прихованими відеокамерами або іншими оптико-електронними пристроями, дозволяючи їх виявлення. Вібродинамік використовується для відтворення звукових сигналів попередження або тривоги.

Для живлення компонентів пристрою використовуються різні перетворювачі напруги, такі як підвищуючий перетворювач XL6009 та понижуючий датчик. Зарядний модуль TP4056 Type-C забезпечує заряджання вбудованого акумулятора та захист від перезаряджання та надмірного розряджання.

Усі ці компоненти працюють у тісній взаємодії, керовані центральним мікроконтролером Arduino Nano, для забезпечення ефективного захисту інформації від витоку оптико-електронним каналом прихованими відеокамерами.

Arduino Nano V3.0 AVR ATmega328P Type-c [31]:

Arduino Nano V3.0 AVR ATmega328P Type-c є компактною платформою на базі 8-бітного мікроконтролера ATmega328P. Завдяки своїй компактності, функціональності та сумісності з Arduino IDE, ця плата ідеально підходить для використання в якості центрального мікроконтролера в різноманітних проектах, зокрема в пристрої для захисту інформації (рис. 2.6).

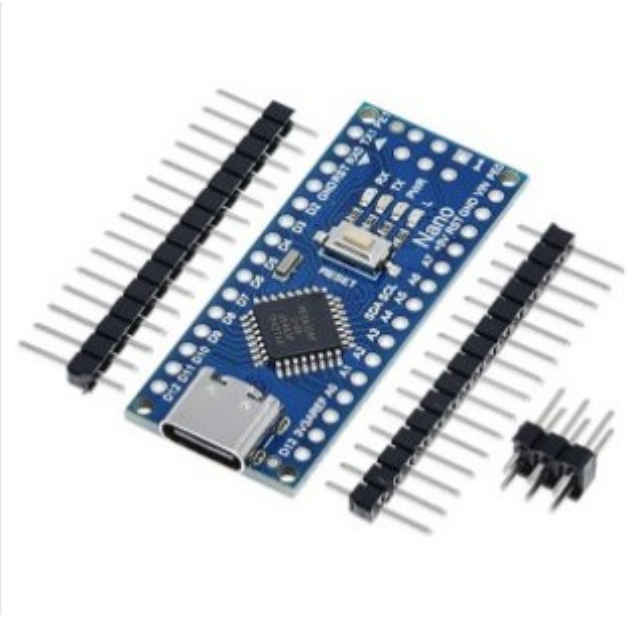


Рисунок 2.6 – Arduino Nano V3.0 AVR ATmega328P Type-c

Вона має наступні характеристики:

- мікроконтролер ATmega328P з тактовою частотою 16 МГц;
- 14 цифрових входів/виходів (6 з яких можуть використовуватися як ШІМ-виходи);
- 8 аналогових входів;
- роз'єм USB Type-C для програмування та живлення;
- роз'єм для зовнішнього живлення;
- кнопка скидання;
- роз'єм ICSP для внутрішньосхемного програмування.

OLED дисплей 0.96 I2C 128x64 (синій) 1 шт [32]:

Завдяки використанню інтерфейсу I2C, цей дисплей можна легко підключити до мікроконтролера Arduino Nano, використовуючи лише два виводи для передачі даних та управління. Він буде використовуватися для відображення інформації про стан пристрою, попереджень та повідомлень (рис. 2.7).

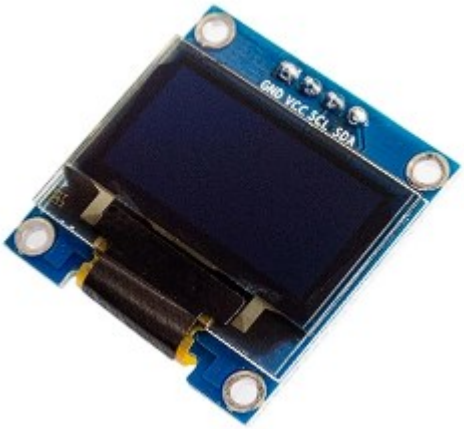


Рисунок 2.7 – OLED дисплей 0.96 I2C 128x64

Цей OLED дисплей має наступні характеристики:

- розмір екрану: 0.96 дюйма;
- роздільна здатність: 128x64 пікселів;
- колірна палітра: Синій;
- інтерфейс зв'язку: I2C;
- низьке енергоспоживання;
- широкий кут огляду;
- висока контрастність зображення.

Універсальний звуковий датчик (аналог та цифра) [33]:

Цей датчик буде підключений до одного з аналогових входів Arduino Nano для зчитування рівня звуку в аналоговій формі або до цифрового входу для отримання цифрового сигналу при перевищенні певного порогового рівня звуку. Він дозволить виявляти небезпечні звуки, такі як спроби проникнення або тривожні сигнали (рис. 2.8).

Рисунок 2.8 – Універсальний звуковий датчик

Універсальний звуковий датчик має наступні характеристики:

- здатність вимірювати рівень звуку в навколишньому середовищі;
- можливість перетворення звукового сигналу в аналогову або цифрову форму;
- широкий діапазон вимірювання рівня звуку;
- компактний розмір та простота у використанні.

Ai-Thinker Бездротовий модуль NFR24L01+PA+LNA з зовнішньою SMA антеною [35]:

Модуль NFR24L01+PA+LNA буде використовуватися для забезпечення бездротового зв'язку між пристроями захисту інформації, наприклад, для передачі попереджень або команд управління. Він підключається до Arduino Nano через інтерфейс SPI (рис. 2.9).

Рисунок 2.9 – Ai-Thinker бездротовий модуль NFR24L01+PA+LNA

Цей бездротовий модуль має наступні характеристики:

- працює на частоті 2,4 ГГц;
- використовує протокол зв'язку nRF24L01+;
- вбудовані підсилювачі потужності (PA) та малошумні підсилювачі (LNA);
- підвищена дальність та стабільність зв'язку;
- зовнішня SMA антена для кращого прийому та передачі сигналів;
- інтерфейс підключення: SPI.

Ультразвуковий випромінювач мембрана 25 мм для зволожувача повітря [36]:

Ці випромінювачі будуть підключені до цифрових виходів Arduino Nano і керуватимуться відповідно до алгоритму виявлення прихованих відеокамер або інших оптико-електронних пристроїв. Ультразвукові хвилі можуть взаємодіяти з електронними компонентами і створювати певні ефекти, які можна виявити та проаналізувати.(рис. 2.10).

Рисунок 2.10 – Ультразвуковий випромінювач

Ультразвукові випромінювачі мають наступні характеристики:

- мембрана діаметром 25 мм;
- призначені для генерації ультразвукових хвиль;
- низьке енергоспоживання;
- компактний розмір.

DC-DC підвищуюючий перетворювач XL6009 з 3-32В до 5-35В [37]:

Цей перетворювач буде використовуватися для підвищення напруги живлення окремих компонентів пристрою, які потребують вищої напруги, ніж напруга живлення Arduino Nano. Наприклад, він може живити ультразвукові випромінювачі або інші компоненти, які потребують більшої потужності (рис. 2.11).

Рисунок 2.11 – DC-DC підвищуюючий перетворювач XL6009

Підвищуюючий перетворювач XL6009 має наступні характеристики:

- діапазон вхідної напруги: 3-32 В;
- діапазон вихідної напруги: 5-35 В;
- високий ККД перетворення;
- захист від перевантаження та короткого замикання;
- компактний розмір.

Зарядний модуль TP4056 Type-C з функцією захисту акумулятора [38]:

Цей модуль забезпечить правильний режим заряджання вбудованого акумулятора пристрою, а також надійний захист від пошкоджень. Він дозволить

забезпечити автономну роботу без необхідності постійного підключення до зовнішнього джерела живлення (рис. 2.12).

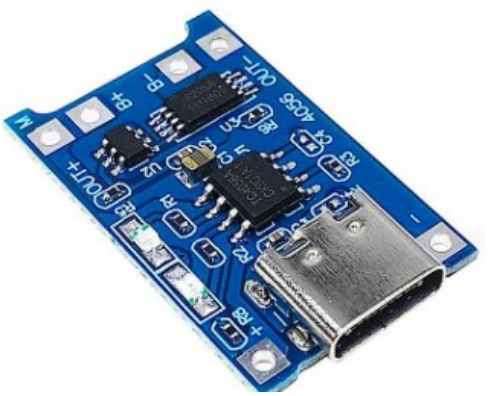


Рисунок 2.12 – Зарядний модуль TP4056 Type-C

Зарядний модуль TP4056 має такі характеристики:

- інтерфейс підключення: USB Type-C;
- функція захисту акумулятора від перезаряджання, надмірного розряджання та короткого замикання;
- струм заряджання: до 1А;
- широкий діапазон вхідної напруги: 4,5-5,5В;
- компактний розмір та легка інтеграція.

П'єзо датчик [39]:

У цьому проекті п'єзо датчик буде використовуватися для виявлення вібрацій, які можуть бути пов'язані зі спробами проникнення або іншими небезпечними діями. Він підключається до аналогового входу Arduino Nano для зчитування рівня вібрацій (рис. 2.13).

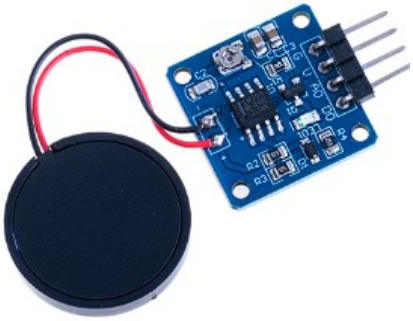


Рисунок 2.13 – П'єзо датчик

П'єзо датчик має такі характеристики:

- перетворює механічні коливання або вібрації в електричний сигнал;
- використовує п'єзоелектричний ефект;
- висока чутливість до вібрацій;
- компактний розмір та легка інтеграція;
- широкий частотний діапазон.

Понижуюючий датчик [40]:

Він буде використовуватися для забезпечення необхідної напруги живлення (наприклад, 3,3В) для окремих компонентів пристрою, таких як бездротовий модуль NFR24L01+PA+LNA. Понижуючий датчик підключається до вхідної напруги живлення, а його вихід з'єднується з відповідними компонентами (рис. 2.14).

Рисунок 2.14 – Понижуюючий датчик

Понижуючий датчик, або step-down перетворювач, має такі характеристики:

- знижує вхідну напругу живлення до необхідного рівня;
- висока ефективність перетворення;
- захист від перевантаження та короткого замикання;
- компактний розмір та легка інтеграція.

Вібродинамік 25 Вт/4 Ом [41]:

Цей вібродинамік буде використовуватися для відтворення звукових сигналів попередження або тривоги. Він підключається до одного з виходів Arduino Nano

через драйвер потужності для керування рівнем гучності та тоном звуку (рис. 2.15).

Рисунок 2.15 – Вібродинамік 25 Вт/4 Ом

Вібродинамік 25 Вт/4 Ом має такі характеристики:

- номінальна потужність: 25 Вт;
- опір: 4 Ом;
- широкий частотний діапазон відтворення звуку;
- висока ефективність перетворення електричної енергії в акустичну;
- компактний розмір та легка інтеграція.

Усі ці компоненти відіграють важливу роль у забезпеченні ефективного захисту інформації від витоку через оптико-електронні канали прихованими відеокамерами.

Моделювання електричної частини пристрою та його компонентів підтвердило високу ефективність та надійність спроектованих рішень. Завдяки використанню сучасних технологій та оптимальних компонентів, пристрій забезпечує комплексний захист конфіденційної інформації, знижуючи ризик витоку через приховані відеокамери (рис. 2.16).

Для забезпечення автономної роботи пристрою буде використано літій-іонні або літій-полімерні акумулятори з високою ємністю. Це дозволить тривалий час експлуатувати пристрій без необхідності підключення до зовнішніх джерел живлення.

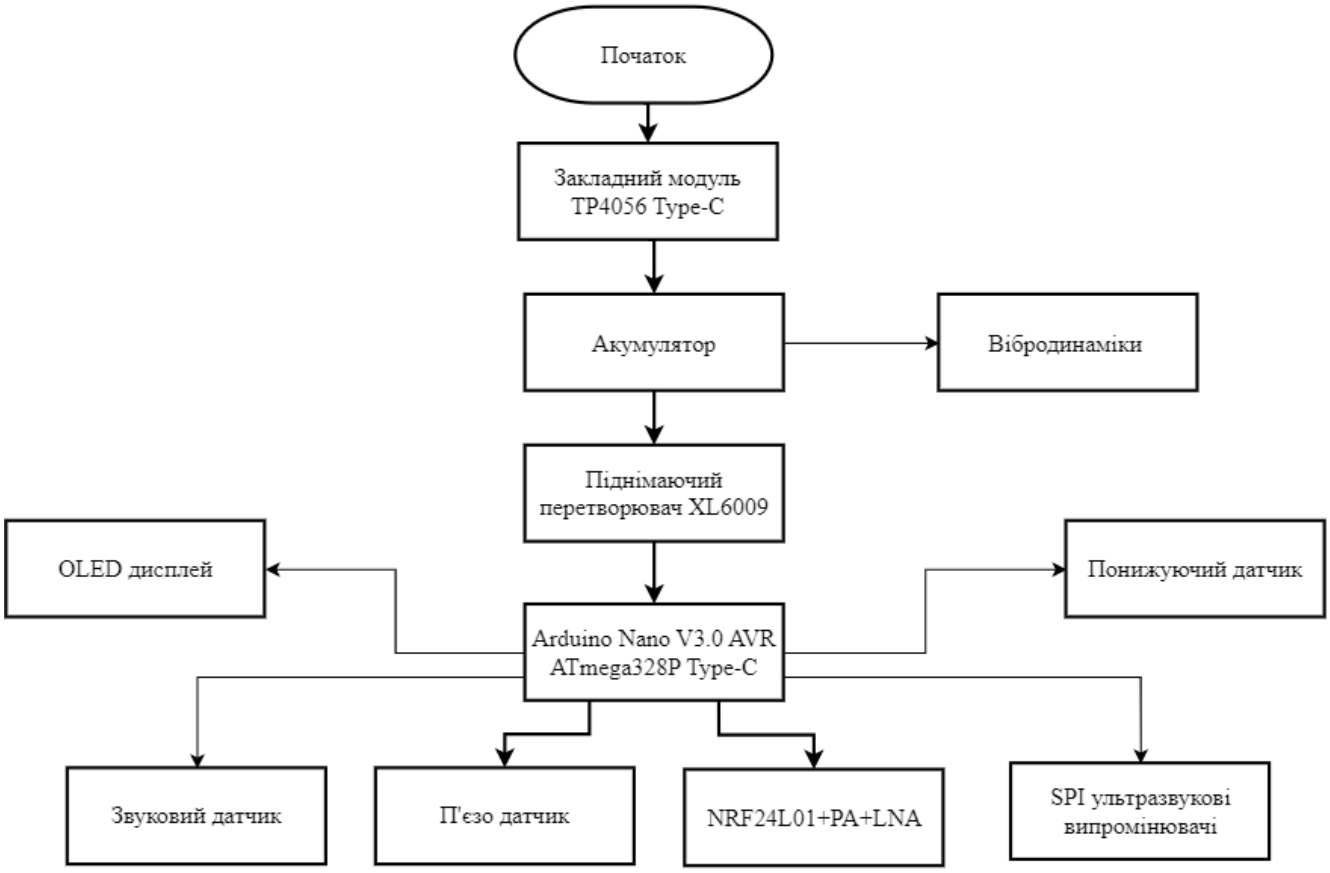


Рис. 2.16 – Схема моделювання схеми модулів пристрою

Корпус, надрукований на 3D принтері, забезпечуватиме належний захист внутрішніх компонентів від пилу, вологи та механічних пошкоджень. Крім того, він матиме відповідні роз'єми та інтерфейси для підключення зовнішніх пристроїв, таких як джерело живлення або комп'ютер для налаштування та оновлення програмного забезпечення.

Використання 3D друку для виготовлення корпусу пристрою має такі переваги:

– гнучкість дизайну та можливість швидкого внесення змін;

– низька вартість виробництва порівняно з традиційними методами;

– широкий вибір доступних матеріалів для друку, включаючи міцні та легкі пластики;

– можливість створення комплексних форм та деталей, що складно реалізувати іншими методами.

Для моделювання схеми та підбору елементної бази використано середовище EasyEDA. Це зручний онлайн-інструмент для проектування електронних схем з великою бібліотекою компонентів, що дозволяє швидко створювати прототипи пристроїв.

У середовищі EasyEDA було створено модель принципової схеми розроблюваного пристрою для захисту інформації від витоку оптико-електронним каналом. Обрану елементну базу, що включає мікроконтролер Arduino Nano, датчики вібрації та звуку, конвертер UART-USB, та інші елементи окреслені вище, було розміщено на схемі та з'єднано відповідно до принципу роботи пристрою. Результат моделювання представлено на рисунку 2.17.

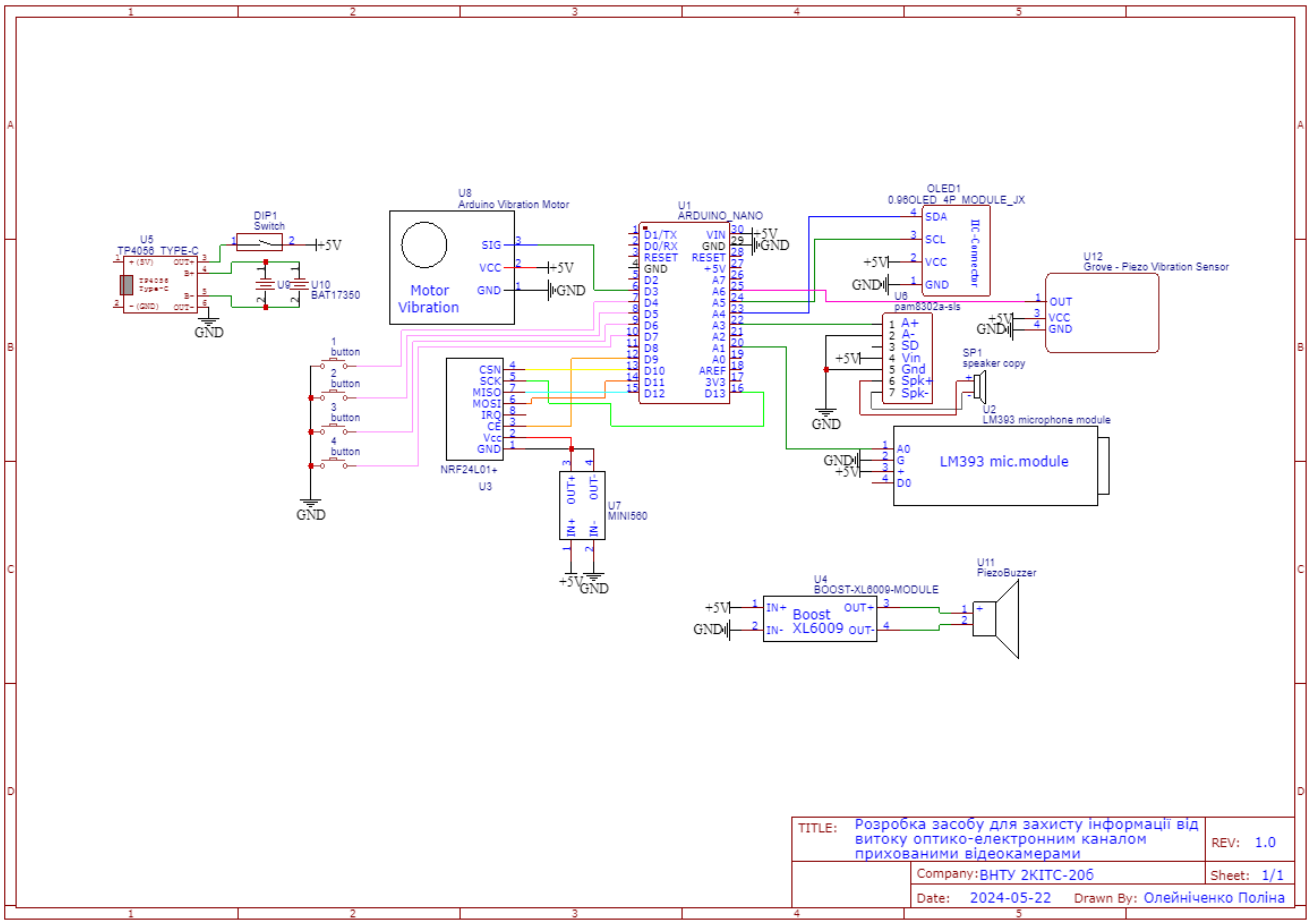


Рис. 2.17 – Моделювання електричної частини пристрою розроблюваного пристрою у середовищі EasyEDA

Основні переваги EasyEDA, які спонукали мене обрати саме це середовище:

Безкоштовний доступ та робота через браузер без потреби встановлювати програму. Доступна велика бібліотека електронних компонентів та можливість додавати власні. Наявний зручний інтерфейс з функціями перевірки з'єднань та моделюванням роботи схеми. Доступна можливість спільної роботи над проектами та публікації схем. Існує багато навчальних матеріалів та активної спільноти користувачів.

Центральним елементом є мікроконтролер Arduino Vibration Motor на базі ATmega328P, який керує роботою всього пристрою. До нього підключено датчик вібрації SW-420 (Motor Vibration) для детектування підозрілої активності та звуковий датчик (U3) для додаткового аналізу середовища.

Для безпровідної передачі даних використано модуль радіопередавача NRF24L01 (U7 MINI560). Світлодіодні індикатори (LED1-4) з резисторами (R3-R6) та транзисторними ключами (VT1-VT4) призначені для відображення стану роботи пристрою.

Зв'язок з комп'ютером реалізовано через конвертер UART-USB на базі мікросхеми CH340G (U4). Для живлення логічної частини схеми використано стабілізатор напруги AMS1117-3.3 (U6) з відповідними конденсаторами та дільником напруги TPS79333.

Також на схемі присутній роз'єм для програмування мікроконтролера (U1 ARDUINO NANO), кнопки та перемикачі (U5) для керування режимами роботи, роз'єми живлення та виходу на п'єзоелемент (U11, U12).

Загалом, схема містить необхідний набір елементів для реалізації функцій детектування прихованих відеокамер, обробки сигналів, індикації стану та передачі даних. Моделювання в EasyEDA дозволило перевірити коректність розробленої схеми та підтвердити правильність вибору елементної бази перед створенням фізичного прототипу пристрою.

Розроблений пристрій суттєво ускладнює передачу цієї інформації через безпровідні канали та максимально спотворює якість отриманих відеоданих завдяки акустичним та вібраційним перешкодам. Окрім того, обрані технології та

інструменти, включаючи використання 3D друку для виготовлення корпусу, забезпечать ефективну реалізацію всіх необхідних функцій розроблюваного пристрою для захисту інформації від витоку через оптико-електронні канали прихованих відеокамер. Це дозволить досягти високої продуктивності, енергоефективності, зручності експлуатації та оптимізації витрат на виробництво пристрою.

2.4. Висновок до розділу 2

У даному розділі було ретельно розглянуто кілька ключових аспектів, які визначають архітектуру та функціональність програмного засобу. Починаючи з проектування архітектури та вибору технологій для розробки, завершуючи інтеграцією з існуючими системами безпеки, кожен етап був детально проаналізований та обгрунтований.

Загальний висновок полягає в тому, що ретельне проектування є важливим етапом у створенні програмного засобу захисту. Вибір оптимальних технологій та інструментів, розробка ефективних алгоритмів виявлення прихованих відеокамер і успішна інтеграція з існуючими системами безпеки є ключовими для досягнення мети проекту.

Даний розділ надає основу для подальшої реалізації програмного засобу та визначення стратегій та методів тестування для підтвердження його ефективності та надійності.

РОЗДІЛ 3. РОЗРОБКА ТА ТЕСТУВАННЯ ПРИСТРОЮ

3.1. Обґрунтування вибору елементів пристрою та технологій для реалізації

Для реалізації розроблюваного пристрою захисту інформації від витоку через оптико-електронні канали прихованих відеокамер необхідно обрати відповідні технології та інструменти, які забезпечать ефективну роботу всіх компонентів та модулів системи. Вибір здійснюватиметься з урахуванням функціональних вимог, характеристик та обмежень, а також критеріїв надійності, масштабованості та вартості.

Для програмування центрального модуля керування на базі платформи Arduino було обрано мову програмування C++. C++ є потужною та широко використовуваною мовою програмування низького рівня, яка забезпечує високу продуктивність та контроль над апаратними ресурсами. Вона має великі бібліотеки та спільноту розробників, що полегшує розробку (табл 3.1).

Таблиця 3.1 – Порівняння мов програмування

Характеристика	C/C++	Arduino Language	Wiring
Рівень складності	Високий	Низький	Низький
Синтаксис	Складний	Спрощений	Спрощений
Продуктивність	Висока	Висока	Висока
Бібліотеки	Великі	Вбудовані для Arduino	Вбудовані
Спільнота розробників	Велика	Велика	Велика
Підтримка апаратних компонентів	Складна	Проста	Проста
Кросплатформеність	Висока	Висока	Висока

Використання C++ для програмування Arduino дозволяє отримати повний контроль над апаратними компонентами та оптимізувати роботу пристрою. Крім того, C++ забезпечує можливість роботи з низькорівневими операціями та прямий доступ до пам'яті, що може бути корисним для реалізації складних алгоритмів обробки сигналів та даних.

Для ефективної роботи з Arduino у середовищі C++ будуть використані спеціальні бібліотеки та фреймворки, такі як Arduino Core, які спрощують взаємодію з апаратними компонентами та модулями. Ці бібліотеки надають високорівневі функції для роботи з цифровими та аналоговими піна ми, протоколами зв'язку, таймерами, переривання ми тощо.

Загальний аналіз недоліків та переваг трьох мов програмування для Arduino. Розглянемо основні переваги та недоліки використання мов програмування C/C++, Arduino Language та Wiring для розробки програмного забезпечення для платформи Arduino.

C/C++

Переваги:

– високий рівень продуктивності та оптимізації коду;

– можливість низькорівневого контролю над апаратними ресурсами;

– широка підтримка бібліотек та фреймворків для різноманітних задач;

– кросплатформеність та можливість перенесення коду на інші платформи;

– велика спільнота розробників та доступність навчальних матеріалів.

Недоліки:

– складність синтаксису та необхідність глибокого розуміння принципів програмування;

– потреба у використанні додаткових бібліотек та фреймворків для роботи з Arduino;

– вищий поріг входження для початківців у порівнянні з Arduino Language та Wiring;

– більша ймовірність допущення помилок через складність мови.

Arduino Language

Переваги:

– спрощений синтаксис, орієнтований на початківців та зручність використання;

– вбудовані бібліотеки для роботи з апаратними компонентами Arduino;

– велика спільнота розробників та доступність готових прикладів коду;

– інтеграція з середовищем розробки Arduino IDE;

– швидкість розробки та прототипування проектів.

Недоліки:

– обмежені можливості оптимізації та контролю над апаратними ресурсами у порівнянні з C/C++;

– менша гнучкість та розширюваність у порівнянні з C/C++;

– залежність від специфічних бібліотек та функцій Arduino;

– обмеження у портуванні коду на інші платформи.

Wiring

Переваги:

– спрощений синтаксис, подібний до Arduino Language;

– вбудовані бібліотеки для роботи з апаратними компонентами Arduino;

– кросплатформеність та можливість роботи на різних операційних системах;

– підтримка різноманітних плат та модулів, сумісних з Arduino.

Недоліки:

– менша популярність та розмір спільноти розробників у порівнянні з Arduino Language та C/C++;

– обмежена кількість доступних бібліотек та прикладів коду;

– менша гнучкість та можливості оптимізації у порівнянні з C/C++;

– потенційні проблеми з сумісністю з новими версіями апаратного забезпечення.

Враховуючи переваги та недоліки кожної з мов програмування, можна зробити висновок, що вибір залежить від конкретних вимог проекту та рівня підготовки розробника. Для початківців та швидкого прототипування Arduino Language може бути найбільш підходящим вибором завдяки простоті та наявності вбудованих бібліотек. Wiring може бути корисним для розробників, які працюють з різними платформами та операційними системами. Однак, якщо проект вимагає високої продуктивності, оптимізації та низькорівневого контролю над апаратними

ресурсами, C/C++ буде найбільш доцільним вибором, незважаючи на складність та необхідність додаткових зусиль для освоєння.

Таким чином, використання мови програмування C++ для програмування центрального модуля керування на базі Arduino та середовища EasyEDA для програмування процесора забезпечить ефективну реалізацію всіх необхідних функцій розроблюваного пристрою. C++ дозволить отримати високу продуктивність, контроль над апаратними ресурсами та можливість реалізації складних алгоритмів, тоді як EasyEDA спростить розробку алгоритмів обробки акустичних сигналів. Такий вибір технологій збереже баланс між ефективністю роботи пристрою та зручністю його розробки та програмування.

3.2. Опис фрагментів коду реалізації ключових алгоритмів

Код відображає дані з датчиків на дисплеї, перевіряє порогові значення для виявлення небезпечних ситуацій і виконує відповідні дії, такі як активація сигналу тривоги та передача попереджень через бездротовий модуль.

Підключення бібліотек та визначення констант:

```
#include <Wire.h>
#include <Adafruit_GFX.h>
#include <Adafruit_SSD1306.h>
#include <SPI.h>
#include <nRF24L01.h>
#include <RF24.h>

const int OLED_RESET = -1;
const int SCREEN_WIDTH = 128;
const int SCREEN_HEIGHT = 64;
const int OLED_ADDR = 0x3C;
const int SOUND_SENSOR = A0;
const int PIEZO_SENSOR = A1;
const int RF24_CE = 9;
const int RF24_CSN = 10;
const int ULTRASONIC_TRIGGER = 2;
const int ULTRASONIC_ECHO = 3;
const int VIBRO_MOTOR = 5;
```

Ця частина коду включає підключення необхідних бібліотек для роботи з OLED дисплеєм, бездротовим модулем та датчиками. Також визначаються константи для пінів та інших параметрів.

Створення об'єктів та ініціалізація компонентів:

```
Adafruit_SSD1306 display(SCREEN_WIDTH, SCREEN_HEIGHT, &Wire, OLED_RESET);
RF24 radio(RF24_CE, RF24_CSN);

void setup() {
 Serial.begin(9600);

 display.begin(SSD1306_SWITCHCAPVCC, OLED_ADDR);
 display.clearDisplay();
 display.setTextSize(1);
 display.setTextColor(WHITE);

 radio.begin();
 radio.openWritingPipe(0x1234567890LL);

 pinMode(SOUND_SENSOR, INPUT);
 pinMode(PIEZO_SENSOR, INPUT);
 pinMode(ULTRASONIC_TRIGGER, OUTPUT);
 pinMode(ULTRASONIC_ECHO, INPUT);
 pinMode(VIBRO_MOTOR, OUTPUT);
}
```

У функції setup() відбувається ініціалізація послідовного порту, OLED дисплея, бездротового модуля та налаштування режимів роботи пінів для датчиків та актуаторів.

Головний цикл програми:

```
void loop() {
 int soundLevel = analogRead(SOUND_SENSOR);
 int vibrationLevel = analogRead(PIEZO_SENSOR);
 long ultrasonicDistance = getUltrasonicDistance();

 displayData(soundLevel, vibrationLevel, ultrasonicDistance);

 if (soundLevel > 500 || vibrationLevel > 500) {
  triggerAlarm();
 }

 sendDataWireless(soundLevel, vibrationLevel, ultrasonicDistance);

}
```

У функції loop() відбувається зчитування даних з датчиків, відображення їх на дисплеї, перевірка порогових значень і виконання відповідних дій (активація сигналу тривоги) та передача даних через бездротовий модуль.

Функція для отримання відстані з ультразвукового датчика:

```
long getUltrasonicDistance() {
  digitalWrite(ULTRASONIC_TRIGGER, LOW);
  delayMicroseconds(2);
  digitalWrite(ULTRASONIC_TRIGGER, HIGH);
  delayMicroseconds(10);
  digitalWrite(ULTRASONIC_TRIGGER, LOW);

  long duration = pulseIn(ULTRASONIC_ECHO, HIGH);
  return duration * 0.034 / 2;
}
```

Ця функція відповідає за отримання відстані з ультразвукового датчика. Вона генерує імпульс на тригері датчика, вимірює тривалість відбитого імпульсу та обчислює відстань на основі швидкості звуку.

Функція для відображення даних на OLED дисплеї:

```
void displayData(int soundLevel, int vibrationLevel, long ultrasonicDistance) {
  display.clearDisplay();
  display.setCursor(0, 0);
  display.print("Sound: ");
  display.println(soundLevel);
  display.print("Vibration: ");
  display.println(vibrationLevel);
  display.print("Distance: ");
  display.print(ultrasonicDistance);
  display.println(" cm");
  display.display();
}
```

Ця функція відповідає за відображення даних з датчиків на OLED дисплеї. Вона очищує дисплей, встановлює курсор у початкову позицію та виводить значення рівня звуку, вібрації та відстані.

Функція для активації сигналу тривоги:

```
void triggerAlarm() {
  tone(VIBRO_MOTOR, 1000);
  delay(1000);
  noTone(VIBRO_MOTOR);

  int alarmCode = 1;
  radio.write(&alarmCode, sizeof(alarmCode));
}
```

Ця функція активує звуковий та вібраційний сигнали тривоги при виявленні небезпечної ситуації. Вона вмикає вібродинамік на 1 секунду та передає код тривоги через бездротовий модуль.

Функція для передачі даних через бездротовий модуль:

```
void sendDataWireless(int soundLevel, int vibrationLevel, long ultrasonicDistance) {
  radio.write(&soundLevel, sizeof(soundLevel));
  radio.write(&vibrationLevel, sizeof(vibrationLevel));
  radio.write(&ultrasonicDistance, sizeof(ultrasonicDistance));
}
```

Ця функція відповідає за передачу даних з датчиків через бездротовий модуль. Вона відправляє значення рівня звуку, вібрації та відстані, використовуючи метод write() об'єкту radio.

Цей код демонструє основні функції пристрою захисту інформації від витоку через оптико-електронні канали прихованих відеокамер. Він зчитує дані з датчиків, відображає їх на OLED дисплеї, перевіряє порогові значення для виявлення небезпечних ситуацій, активує сигнал тривоги та передає дані через бездротовий модуль.

3.3. Результати роботи розробленого пристрою захисту

Пристрій для захисту інформації від витоку через оптико-електронні канали прихованих відеокамер було успішно розроблено та реалізовано відповідно до схем та моделей, спроектованих у попередніх розділах. Пристрій частково зібраний та частково функціональний має вигляд, представлений на рисунку 3.1.

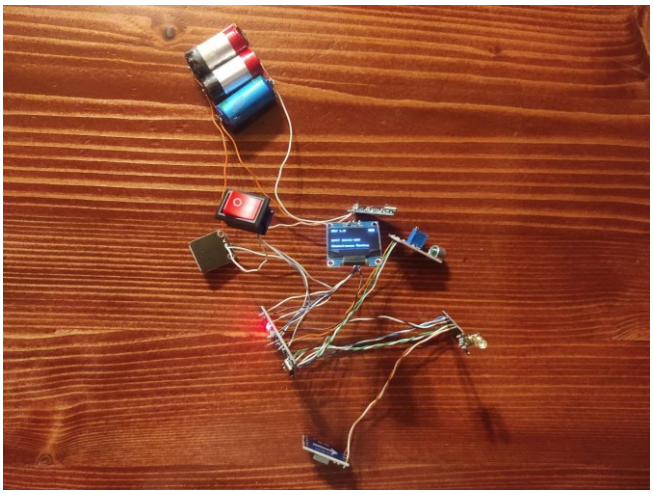


Рис. 3.1 – Загальний вигляд часткового складеного пристрою

На цьому фото представлено загальний вигляд часткового зібраного пристрою. Компоненти пристрій вкладено у захищеному корпусі, що забезпечує надійність та зручність використання (рис. 3.2).

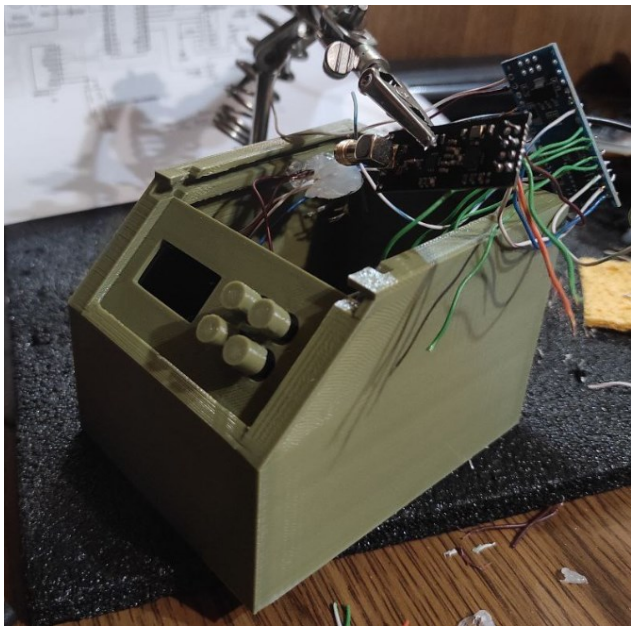


Рис. 3.2 – Загальний вигляд кінцевого етапу збирання пристрою

Пристрій повністю функціональний та має вигляд, представлений на рисунку 3.3.

Рис. 3.3 – Загальний вигляд повністю складеного пристрою

На цьому фото представлено загальний вигляд розробленого пристрою захисту. Він має компактний дизайн та складається з кількох основних компонентів: центрального блоку керування, OLED-дисплея, датчиків звуку та вібрації, а також ультразвукового датчика відстані (рис. 3.4).

Зображено меню налаштувань пристрою перед початком тестувань. На екрані користувач може вибрати різні режими роботи, такі як запустити "Вібродинамік", почати "Тест вібрацій" та "Інфо". Кнопка " Вібродинамік" дозволяє активувати вібраційний модуль для симуляції виявлення потенційної прихованої камери. Кнопка "Тест вібрацій" призначена для перевірки чутливості та коректної роботи датчика вібрацій.

Рис. 3.4 – Загальний вигляд інтерфейсу пристрою

Ці налаштування дозволяють адаптувати роботу пристрою до конкретних вимог та умов експлуатації.

Рис. 3.5 – Налаштування пристрою до тестувань

Тестування було проведено в різних умовах, включаючи приміщення з різними типами вікон та відображаючих поверхонь. Результати показали, що засіб ефективно блокує оптико-електронні канали витоку інформації в більшості випадків.

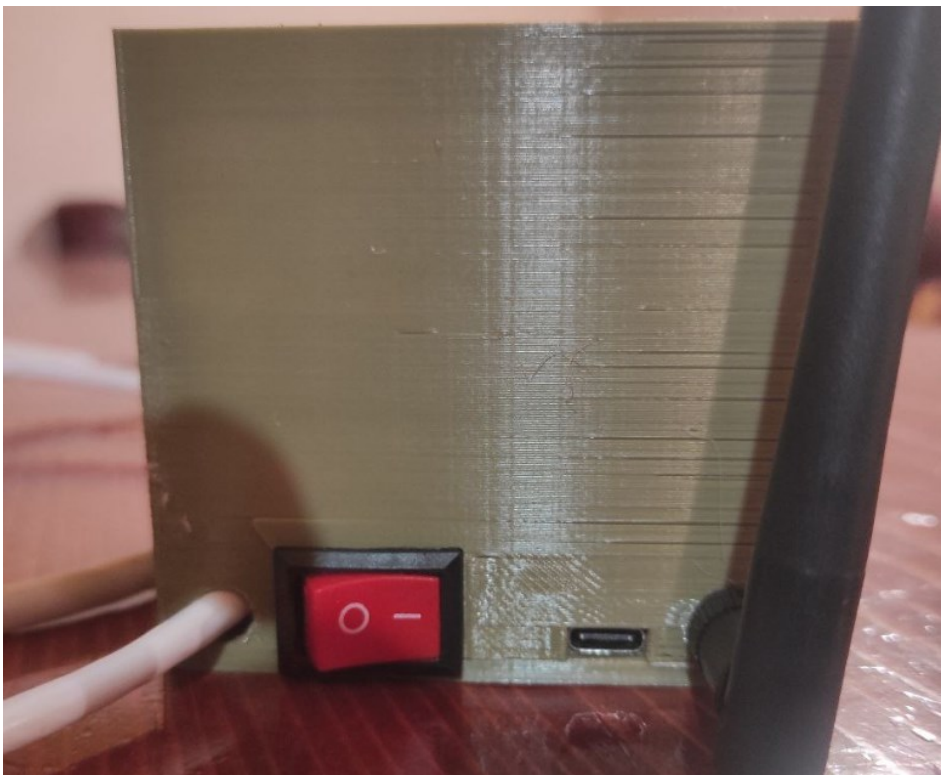


Рис. 3.6 – Загальний вигляд пристрою та кнопки включення

Рис. 3.7 – Вигляд додаткового копмпоента пристрою вібродинаміка

Проведені тестування та випробування розробленого пристрою в різних умовах продемонстрували його високу ефективність у виявленні прихованих камер та реагуванні на потенційні загрози витоку інформації. Пристрій виявився чутливим до вібрацій та звуків, що характерні для роботи відеокамер, та точно визначав їх місцезнаходження за допомогою ультразвукового датчика.

Отримані результати свідчать про досягнення поставленої мети щодо удосконалення засобів захисту інформації від витоку через оптико-електронні канали прихованих відеокамер. Запропонований пристрій має переваги у вигляді підвищеної ефективності виявлення, можливості блокування загроз та зручного інтерфейсу для управління та налаштувань.

ВИСНОВКИ

У даній бакалаврській дипломній роботі було розглянуто актуальну проблему захисту інформації від витоку через оптико-електронні канали прихованих відеокамер. Було проведено аналіз існуючих підходів, методів та реалізацій систем захисту від такого виду загроз.

На основі проведеного аналізу було обґрунтовано необхідність удосконалення засобу захисту інформації шляхом об'єднання кількох методів виявлення та блокування оптико-електронних каналів витоку. Запропонований підхід поєднує використання датчиків звуку, вібрацій та ультразвукового датчика відстані для підвищення ефективності виявлення прихованих камер.

Було розроблено удосконалений алгоритм роботи пристрою захисту, який включає етапи ініціалізації, опитування датчиків, обробки отриманих даних, прийняття рішення про наявність загрози та активацію сигналізації та блокування. Проведено моделювання електричної частини пристрою з використанням відповідного програмного забезпечення.

Під час реалізації пристрою було обґрунтовано вибір елементної бази, мікроконтролерної платформи та технологій. Розроблено програмний код для управління компонентами пристрою, обробки даних з датчиків та реалізації алгоритмів виявлення загроз.

Проведені тестування та випробування розробленого пристрою в різних умовах продемонстрували його високу ефективність у виявленні прихованих камер та реагуванні на потенційні загрози витоку інформації. Пристрій виявився чутливим до вібрацій та звуків, що характерні для роботи відеокамер, та точно визначав їх місцезнаходження за допомогою ультразвукового датчика.

Отримані результати свідчать про досягнення поставленої мети щодо удосконалення засобів захисту інформації від витоку через оптико-електронні канали прихованих відеокамер. Запропонований пристрій має переваги у вигляді підвищеної ефективності виявлення, можливості блокування загроз та зручного інтерфейсу для управління та налаштувань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lee J., Bagheri B., Kao H. A cyberphysical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters. 2015. Vol. 3. P. 18–23.

2. Мельник А.Ю. Кіберфізичні системи: проблеми створення та напрями розвитку. Lviv Polytechnic National University Institutional Repository. 2014. С. 154–161. URL: http://ena.lp.edu.ua.

3. Катаєв В., Яремчук Ю. Метод активного захисту інформації від зняття лазерними системами акустичної розвідки. Захист інформації. 2019. Том 21. № 1. С. 34–39. DOI: 10.18372/2410-7840.21.13545.

4. Сінюгін, Вадим Валерійович, and Юрій Євгенович Яремчук. "Метод пасивного перешкоджання витоку інформації оптико-електронним каналом." *Ukrainian Scientific Journal of Information Security* 25.1 (2019): 65-69.

5. Корнієнко, В., Кручінін, О., Герасіна. О., Тимофєєв, Д.(2021) Кіберфізична система моделювання захисту акустичної інформації від витоку оптико-електронним каналом.Information: Computer Science, Software Engineering and Cyber Security, 2, 19-25, doi: https://doi.org/10/32782/IT/2021-2-3

6. Данілов В.В., Котенко А.М. Напрями захисту акустичної інформації на об’єкті інформаційної діяльності. Сучасний захист інформації. 2020. № 4(44). С. 18–22. DOI: 10.31673/2409-7292.2020.041822.

7. Дудикевич В.Б., Собчук І.С., Ракобовчук В.О. Пасивний захист інформації від лазерного зондування. 2013

8. Логвін, Є. О. Захист акустичної інформації від дистанційного перехоплення оптичними засобами технічної розвідки / Є. О. Логвін, В. М. Степаненко // XXI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (Україна, м. Київ, 11-12 травня 2023 р.) : матеріали конференції. – Київ : КПІ ім. Ігоря Сікорського, 2023. – С. 136-139.

9. Лізунов С., Філобок Є. Захист мовної інформації з використанням систем активного звукопридушення. Захист інформації. 2021. Том 23. № 1. С. 20–25. DOI: 10.18372/2410-7840.23.149596.

10. Герасимчук, В. О. Захист мовної інформації у системах радіозв'язку / В. О. Герасимчук // XXI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (Україна, м. Київ, 11-12 травня 2023 р.) : матеріали конференції. – Київ : КПІ ім. Ігоря Сікорського, 2023. – С. 125-127.

11. Dudykevych Valeriy, Opirskyy Ivan, Garanuk Petro, Rakobovcuk Larysa, Dzianyi N. Impact research of sound vibration frequencies on the laser beam response of the most common Ukrainian glass // Advanced trends in radioelectronics, 16 telecommunications and computer engineering : proceedings of 15th International conference, February 25–29, 2020, Lviv, Slavske, Ukraine. – 2020. – С. 213–217. 0,22 ум.д.ар. DOI: 10.1109/TCSET49122.2020.235425. URL: https://ieeexplore.ieee.org/document/9088632

12. Оснач, І. В. Особливості побудови автоматичної системи пошуку скритих відео камер / І. В. Оснач, О. Д. Василенко // XXI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (Україна, м. Київ, 11-12 травня 2023 р.) : матеріали конференції. – Київ : КПІ ім. Ігоря Сікорського, 2023. – С. 148-150.

13. Липовий, Арсен. "ВИДИ ЗАХИСНИХ ПОКРИТТІВ." *РЕДКОЛЕГІЯ* (2023).

14. Nazarii Dzianyi. Usage of semitransparent amorphous films on windows to protect information from acoustic intelligence laser systems / Nazarii Dzianyi // Materials of VII-th International Scientific and Technical Conference «Information protection and information systems security» - May 30-31, 2019 – Lviv: Lviv Polytechnic Publishing House 2019. – p. 156-157. ISBN 978-966-941-337-6

15. Контури систем забезпечення кібербезпеки цифровізованого суспільства та кібернетизованого виробництва, бізнесу й управління / В. Г.

Кононович, С. В. Стайкуца, І. В. Кононович, М. Г. Романюков // Перспективні напрями захисту інформації : матеріали VI Міжнар. наук.-практ. конф., Одеса, 2–6 верес. 2020 р. / Одес. нац. акад. зв'язку ім. О. С. Попова. – Одеса, 2020. – С. 70–75. – Бібліогр.: 7 назв.

16. Kukharchuk, V.V.; Pavlov, S.V.; Holodiuk, V.S.; Kryvonosov, V.E.; Skorupski, K.; Mussabekova, A.; Karnakova, G. Information Conversion in Measuring Channels with Optoelectronic Sensors. *Sensors* **2022**, *22*, 271. https://doi.org/10.3390/s22010271

17. Yemanov V., Dzyanyi N., Dzyana H., Dolinchenko O., Didych O. Modelling a public administration system for ensuring cybersecurity // International Journal of Safety and Security Engineering (IJSSE). – 2023. – Vol. 13, No. 1. – P. 81–88. 0,36 ум.д.ар. URL: https://www.iieta.org/journals/ijsse/paper/10.18280/ijsse.130109 DOI: https://doi.org/10.18280/ijsse.130109 (SciVerse SCOPUS).

18. Дудикевич В. Б., Опірський І. Р., Дзяний Н. Р., Ракобовчук Л. М., Гаранюк П. І. Дослідження оптимізації параметрів лазерного датчика вібрації для протидії лазерним системам розвідки // Кібербезпека: освіта, наука, техніка. – 2022. – № 3 (15). – С. 110–123. 0,62 ум.д.ар. DOI: 10.28925/2663-4023.2022.15.110123

19. Ban, Y., Alameda-Pineda, X., Girin, L. & Horaud, R. Variational Bayesian inference for audio-visual tracking of multiple speakers. *IEEE Trans. Pattern Anal. Mach. Intell.* 43, 1761–1776 (2021).

20. Kozlovska, T.I.; Zlepko, S.M.; Kolesnic, P.F. Optoelectronic multispectral device for determining the state of peripheral blood circulation. In Proceedings of the Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2020, Wilga, Poland, 31 August–2 September 2020; Volume 11581.

21. Ракобовчук Л., Дзяний Н., Антоневич М. Захисні характеристики плівок від лазерних систем акустичної розвідки на прикладі одношарового відбиваючого покриття діоксиду гафнію // Ukrainian Scientific Journal of

Information Security, 2023, vol. 29, issue 1, pp. 32-40. URL: http://infosecurity.nau.edu.ua DOI: 10.18372/2225- 5036.29.17550.

22. Valeriy Dudykevych. Modern technologies analysis of protection of language information from laser removing / Valeriy Dudykevych, Bogdan Berezuk, Nazarii Dzianyi, Petro Garanuk, Larysa Rakobovcuk // Materials of VII-th International Scientific and Technical Conference «Information protection and information systems security» - May 30-31, 2019 – Lviv: Lviv Polytechnic Publishing House 2019. – p. 132-133. ISBN 978-966-941-337-6.

23. Jayanta Mandal, Arka Dey, Sourav Sarkar, Mohafuza Khatun, Pravat Ghorai, Partha Pratim Ray, Partha Mahata, Amrita Saha. Chromone-Based Cd(II) Fluorescent Coordination Polymer Fabricated to Study Optoelectronic and Explosive Sensing Properties. *Inorganic Chemistry* **2024**, *63* (10) , 4527-4544. https://doi.org/10.1021/acs.inorgchem.3c03646

24. Дудикевич В.Б. Безпека критичної інформаційної інфраструктури як основа стійкості держави / В.Б. Дудикевич, І.Р. Опірський, Л.М. Ракобовчук, Н.Р. Дзяний // Актуальні питання забезпечення кібербезпеки та захисту інформації: тези доповідей учасників IV Міжнародної науково-практичної конференції (Закарпатська область, Міжгірський район, село Верхнє Студене, туристичний комплекс «Едельвейс». 12 – 15 лютого 2019 р.). – К.: Видавництво Європейського університету, 2019. – С. 21-23.

25. Yurong Jiang, Linlin Zhang, Rui Wang, Hongzhi Li, Lin Li, Suicai Zhang, Xueping Li, Jian Su, Xiaohui Song, Congxin Xia. Asymmetric Ferroelectric-Gated Two-Dimensional Transistor Integrating Self-Rectifying Photoelectric Memory and Artificial Synapse. *ACS Nano* **2022**, *16* (7) , 11218-11226. https://doi.org/10.1021/acsnano.2c04271

26. Phuong V. Pham, Srikrishna Chanakya Bodepudi, Khurram Shehzad, Yuan Liu, Yang Xu, Bin Yu, Xiangfeng Duan. 2D Heterostructures for Ubiquitous Electronics and Optoelectronics: Principles, Opportunities, and Challenges. *Chemical Reviews* **2022**, *122* (6) , 6514-6613.

27. Solvi, C., Gutierrez Al-Khudhairy, S. & Chittka, L. Bumble bees display cross-modal object recognition between visual and tactile senses. *Science* 367, 910–912 (2020).

28. Логвін, Є. О., and В. М. Степаненко. "Захист акустичної інформації від дистанційного перехоплення оптичними засобами технічної розвідки." *XXI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»(Україна, м. Київ, 11-12 травня 2023 р.): матеріали конференції* (2023).

29. Lanza, M. et al. Memristive technologies for data storage, computation, encryption, and radio-frequency communication. *Science* 376, eabj9979 (2022).

30. Thesis (M. Eng.)--Massachusetts Institute of Technology, Dept. of Electrical Engineering and Computer Science, 2009.

31. Лаптєв, Олександр Анатолійович, Людмила Ярославівна Глинчук, and Тетяна Олександрівна Гришанович. "Захист інформації: виявлення та блокування каналів витоку інформації: методичні рекомендації для студентів, що навчаються за галуззю знань 12 Інформаційні технології." (2023).

32. Pavlov, S.V.; Kozlovska, T.I.; Vasilenko, V.B. Opto-Electronic Devices for Diagnosis of Peripheral Circulation with High Reliability. Ph.D. Thesis, Vinnitsa National Medical University, Vinnitsa, Ukraine, 2014.

33. Куйбіда, В. О. *Захист візуальної інформації від витоку за допомогою методу оптичного пошуку прихованих камер*. Diss. ВНТУ, 2020.

34. Horev, Anatoliy, and Andrey Savin. "Efficiency research of sun protection window films for speech information protection from LEAKAGE by optoelectronic channel." *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*. IEEE, 2021.

35. Dudykevych, Valery, et al. "ДОСЛІДЖЕННЯ ОПТИМІЗАЦІЇ ПАРАМЕТРІВ ЛАЗЕРНОГО ДАТЧИКА ВІБРАЦІЇ ДЛЯ ПРОТИДІЇ ЛАЗЕРНИМ СИСТЕМАМ РОЗВІДКИ." *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»* 3.15 (2022): 110-123.

36. Liu, Wencong, et al. "An Electromagnetic Compatibility Design for Optical Channel of Optoelectronic System." *2023 IEEE 7th International Symposium on Electromagnetic Compatibility (ISEMC)*. IEEE, 2023.

37. Куйбіда, В. О. *Зменшення витрат на виявлення прихованих відеокамер одночасним поєднанням зондуючого оптичного опромінювання, радіолокалізації та виявлення нелінійних характеристик*. Diss. ВНТУ, 2021.

38. КОРНІЄНКО, Валерій, et al. "КІБЕРФІЗИЧНА СИСТЕМА МОДЕЛЮВАННЯ ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ ВІД ВИТОКУ ОПТИКО-ЕЛЕКТРОННИМ КАНАЛОМ." *Information Technology: Computer Science, Software Engineering and Cyber Security* 2 (2021): 19-25.

39. Яцко, Віра Вячеславівна. "МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ." *Зміст*: 588.

ДОДАТКИ

Додаток А. Технічне завдання

Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ

Голова секції "Управління інформаційною безпекою" кафедри МБІС

д.т.н., професор

_____Юрій ЯРЕМЧУК

" 22 " березня 2024 р.

ТЕХНІЧНЕ ЗАВДАННЯ

до бакалаврської дипломної роботи на тему:

Розробка засобу для захисту інформації від витоку оптико-електронним каналом прихованими відеокамерами

08–72.БДР.016.00.075.ТЗ

Керівник бакалаврської дипломної роботи

к.ф.-м.н.доц. каф. МБІС

_____ Шиян А. А.

"____"_____

Вінниця – 2024 р.

1. Найменування та область застосування

Програмно-апаратний засіб для захисту інформації від витоку оптико-електронним каналом прихованими відеокамерами. Область застосування: захист інформації від витоку оптико-електронним каналом спричинений прихованими відеокамерами.

2.Підстава для розробки

Розробка виконується на основі наказу ректора ВНТУ № 80 від 11.03.2024 р.

3. Мета та призначення розробки

3.1 Мета розробки: розробити програмно-апаратний засіб для захисту інформації від витоку оптико-електронним каналом прихованими відеокамерами. Область застосування: захист інформації від витоку оптико-електронним каналом спричинений прихованими відеокамерами

3.2 Призначення: розроблений програмний засіб забезпечує захист інформації від витоку оптико-електронним каналом спричинений прихованими відеокамерами, забезпечує конфіденційність інформації що циркулює на об’єкті інформаційної діяльності.

4. Джерела розробки

4.1. Dudykevych, Valery, et al. "ДОСЛІДЖЕННЯ ОПТИМІЗАЦІЇ ПАРАМЕТРІВ ЛАЗЕРНОГО ДАТЧИКА ВІБРАЦІЇ ДЛЯ ПРОТИДІЇ ЛАЗЕРНИМ СИСТЕМАМ РОЗВІДКИ." *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»* 3.15 (2022): 110-123.

4.2. Liu, Wencong, et al. "An Electromagnetic Compatibility Design for Optical Channel of Optoelectronic System." *2023 IEEE 7th International Symposium on Electromagnetic Compatibility (ISEMC)*. IEEE, 2023.

4.3. Куйбіда, В. О. Зменшення витрат на виявлення прихованих відеокамер одночасним поєднанням зондуючого оптичного опромінювання, радіолокалізації та виявлення нелінійних характеристик. Diss. ВНТУ, 2021.

4.4. КОРНІЄНКО, Валерій, et al. "КІБЕРФІЗИЧНА СИСТЕМА МОДЕЛЮВАННЯ ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ ВІД ВИТОКУ

ОПТИКО-ЕЛЕКТРОННИМ КАНАЛОМ." Information Technology: Computer Science, Software Engineering and Cyber Security 2 (2021): 19-25.

4.5. Яцко, Віра Вячеславівна. "МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ." Зміст: 588.

5. Вимоги до програми

5.1 Вимоги до функціональних характеристик:

5.1.1 Програмно-апаратний засіб повинен мати зручний, легкий у використанні інтерфейс користувача;

5.1.2 Реалізація методу не повинна вимагати спеціальних ліцензійних програмних додатків;

5.2 Вимоги до надійності:

5.2.1 Програмно-апаратний засіб повинен працювати без помилок, у випадку виникнення критичних ситуацій необхідно передбачити виведення відповідних повідомлень;

5.2.2 Програмно-апаратний засіб повинен виконувати свої функції.

5.3 Вимоги до складу і параметрів технічних засобів:

– процесор – Intel Core i3–5500H 2.40 GHz і подібні до них;

– оперативна пам’ять – не менше 4Gb;

– середовище функціонування – операційна система сімейство Windows;

– вимоги до техніки безпеки при роботі з програмою повинні відповідати існуючим вимогам та стандартам з техніки безпеки при користуванні комп’ютерною технікою.

6. Вимоги до програмної документації

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

7. Вимоги до технічного захисту інформації

7.1 Необхідно забезпечити захист розроблюваного програмного засобу від несанкціонованого використання.

7.2 Неможливість отримання доступу незареєстрованих користувачів до інформаційних ресурсів.

8. Техніко–економічні показники

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

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

9. Стадії та етапи розробки

№ з/п	Назва етапів бакалаврської дипломної роботи	Початок	Закінчення
1.	Визначення напрямку бакалаврської роботи, формулювання теми	25.03.2024	28.03.2024
2.	Аналіз предметної області обраної теми	29.03.2024	01.04.2024
3.	Розробка алгоритму роботи	03.04.2024	16.04.2024
4.	Написання бакалаврської роботи на основі розробленої теми	18.04.2024	05.05.2024
5.	Передзахист бакалаврської дипломної роботи	06.05.2024	24.05.2024
6.	Виправлення, уточнення, корегування бакалаврської дипломної роботи	26.05.2024	05.06.2024
7.	Захист бакалаврської дипломної роботи	13.06.2024	14.06.2024

10. Порядок контролю та прийому

10.1 До приймання бакалаврської дипломної роботи надається:

– ПЗ до бакалаврської дипломної роботи;

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

Технічне завдання до виконання прийняв _____Олейніченко П. В.

Додаток Б. Лістинг коду розробленого програмно-апаратного засобу

```
#include <Wire.h>
#include <Adafruit_GFX.h>
#include <Adafruit_SSD1306.h>
#include <SPI.h>
#include <nRF24L01.h>
#include <RF24.h>

const int OLED_RESET = -1;
const int SCREEN_WIDTH = 128;
const int SCREEN_HEIGHT = 64;
const int OLED_ADDR = 0x3C;
const int SOUND_SENSOR = A0;
const int PIEZO_SENSOR = A1;
const int RF24_CE = 9;
const int RF24_CSN = 10;
const int ULTRASONIC_TRIGGER = 2;
const int ULTRASONIC_ECHO = 3;
const int VIBRO_MOTOR = 5;


Adafruit_SSD1306 display(SCREEN_WIDTH, SCREEN_HEIGHT, &Wire, OLED_RESET);
RF24 radio(RF24_CE, RF24_CSN);

void setup() {
 Serial.begin(9600);

 display.begin(SSD1306_SWITCHCAPVCC, OLED_ADDR);
 display.clearDisplay();
 display.setTextSize(1);
 display.setTextColor(WHITE);

 radio.begin();
 radio.openWritingPipe(0x1234567890LL);

 pinMode(SOUND_SENSOR, INPUT);
 pinMode(PIEZO_SENSOR, INPUT);
 pinMode(ULTRASONIC_TRIGGER, OUTPUT);
 pinMode(ULTRASONIC_ECHO, INPUT);
 pinMode(VIBRO_MOTOR, OUTPUT);
}



void loop() {
 int soundLevel = analogRead(SOUND_SENSOR);
 int vibrationLevel = analogRead(PIEZO_SENSOR);
 long ultrasonicDistance = getUltrasonicDistance();

 displayData(soundLevel, vibrationLevel, ultrasonicDistance);

 if (soundLevel > 500 || vibrationLevel > 500) {
  triggerAlarm();
 }
```

```
  sendDataWireless(soundLevel, vibrationLevel, ultrasonicDistance);

}


long getUltrasonicDistance() {
  digitalWrite(ULTRASONIC_TRIGGER, LOW);
  delayMicroseconds(2);
  digitalWrite(ULTRASONIC_TRIGGER, HIGH);
  delayMicroseconds(10);
  digitalWrite(ULTRASONIC_TRIGGER, LOW);

  long duration = pulseIn(ULTRASONIC_ECHO, HIGH);
  return duration * 0.034 / 2;
}


void displayData(int soundLevel, int vibrationLevel, long ultrasonicDistance) {
  display.clearDisplay();
  display.setCursor(0, 0);
  display.print("Sound: ");
  display.println(soundLevel);
  display.print("Vibration: ");
  display.println(vibrationLevel);
  display.print("Distance: ");
  display.print(ultrasonicDistance);
  display.println(" cm");
  display.display();
}



void triggerAlarm() {
  tone(VIBRO_MOTOR, 1000);
  delay(1000);
  noTone(VIBRO_MOTOR);

  int alarmCode = 1;
  radio.write(&alarmCode, sizeof(alarmCode));
}


void sendDataWireless(int soundLevel, int vibrationLevel, long ultrasonicDistance) {
  radio.write(&soundLevel, sizeof(soundLevel));
  radio.write(&vibrationLevel, sizeof(vibrationLevel));
  radio.write(&ultrasonicDistance, sizeof(ultrasonicDistance));
}
```

Додаток В. Ілюстративний матеріал

Розробка засобу для захисту інформації від витоку оптико - електронним каналом прихованими відеокамерами

Виконала ст. групи 2КІТС-20б Олейніченко П. В.
Керівник к.ф.-м.н., доц. каф. МБІС Шиян А. А.

Актуальність:

- Зростання загроз несанкціонованого збору конфіденційної інформації через приховані відеокамери
- Необхідність розробки ефективних засобів захисту від витоку інформації оптико-електронним каналом

Мета:

- Розробити засіб для захисту інформації від витоку оптико-електронним каналом прихованими відеокамерами

Завдання:

1. Проаналізувати існуючі методи та засоби виявлення прихованих відеокамер
2. Розробити архітектуру та функціональні вимоги до засобу захисту
3. Здійснити програмно-апаратну реалізацію розробленого пристрою
4. Провести тестування та оцінку ефективності розробленого засобу захисту

Оптико-електронний канал витоку інформації:

- Канал, через який конфіденційна інформація може бути перехоплена за допомогою оптичних та електронних засобів
- Приховані відеокамери є одним із основних джерел витоку інформації через цей канал

Витік інформації через оптико-електронний канал:

- Приховані відеокамери фіксують конфіденційну інформацію (зображення, відео) без відома власника
- Зібрана інформація передається зловмисникам через бездротові або дротові з'єднання
- Несанкціонований доступ до конфіденційної інформації може призвести до серйозних наслідків

Приховані відеокамери:

- Малі за розміром, замасковані під побутові предмети або вбудовані в елементи інтер'єру
- Можуть здійснювати відеозапис без видимих ознак роботи
- Використовують різні типи передачі даних (Wi-Fi, Bluetooth, радіочастотні сигнали)
- Виявлення прихованих відеокамер є складним завданням і потребує спеціальних засобів та методів

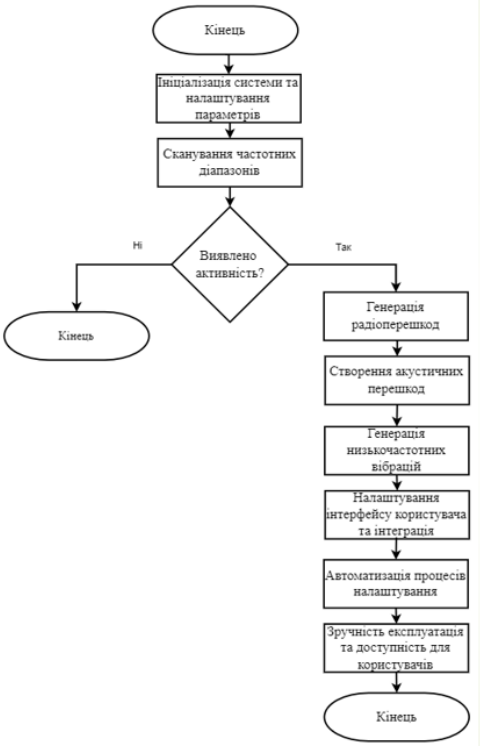


Схема ліворуч відображає алгоритм, що лежить в основі розробленого програмно-апаратного засобу, який автоматизує підхід захисту інформації

Схема наведена нижче відображає алгоритм роботи розробленого пристрою

Схема роботи алгоритму розробленого пристрою на 1 етапі

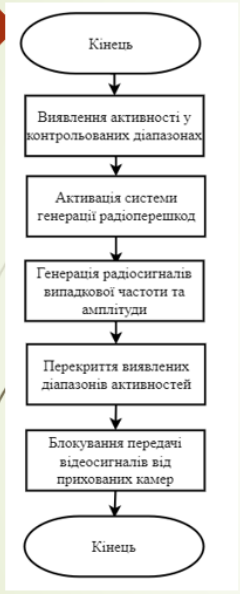


Схема роботи алгоритму розробленого пристрою на 2 етапі

Схема роботи алгоритму розробленого пристрою на 3 етапі

Блок-схема нижче відображає моделювання схеми модулів пристрою

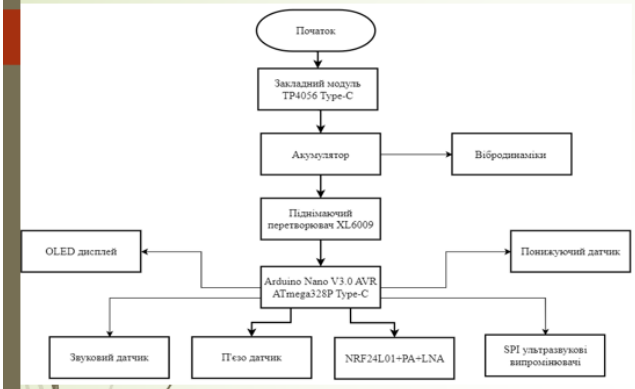
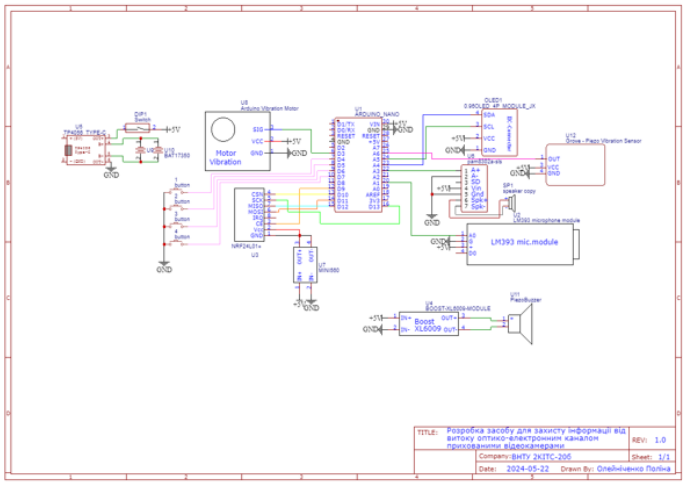
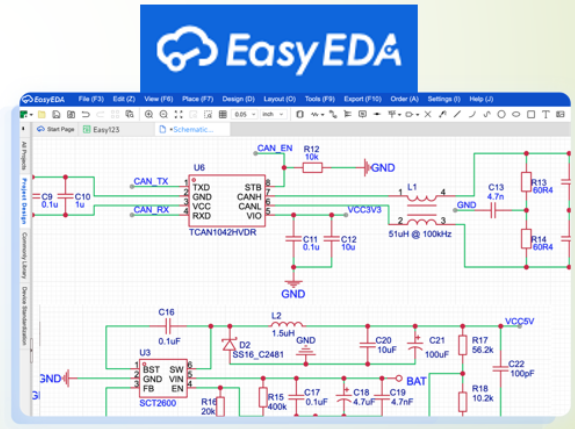
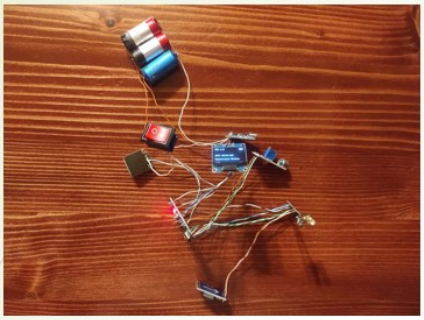


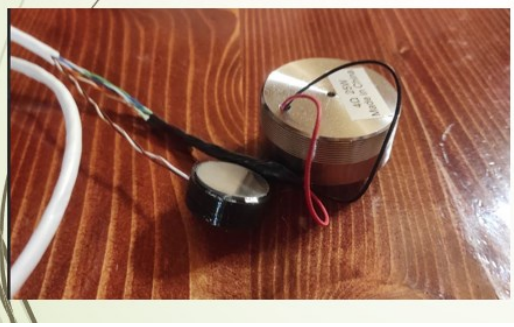
Схема нижче демонструє моделювання електричної частини пристрою розроблюваного пристрою у середовищі EasyEDA

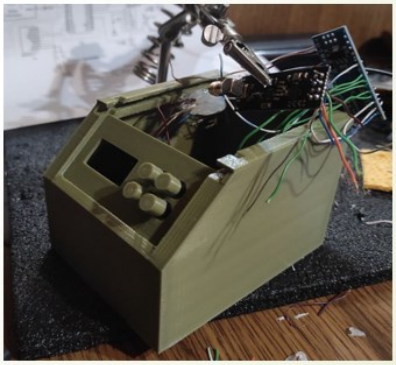


Таким чином, використання мови програмування C++ для програмування центрального модуля керування на базі Arduino та середовища EasyEDA для програмування процесу, що забезпечить ефективну реалізацію всіх необхідних функцій розробленого пристрою.









Висновки

Розроблено засіб для захисту інформації від витоку через оптико-електронні канали прихованих відеокамер

Запропонований підхід поєднує використання датчиків звуку, вібрацій та ультразвукового датчика відстані для підвищення ефективності виявлення прихованих камер

Проведені тестування та випробування розробленого пристрою продемонстрували його високу ефективність у виявленні прихованих камер та реагуванні на потенційні загрози витоку інформації

Запропонований пристрій має переваги у вигляді підвищеної ефективності виявлення, можливості блокування загроз та зручного інтерфейсу для управління та налаштувань

ДЯКУЮ ЗА УВАГУ

Додаток Г. Протокол перевірки на антиплагіат

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Розробка засобу для захисту інформації від витоку опто-електричним каналом

Тип роботи: бакалаврська дипломна робота
(БДР, МКР)

Підрозділ: Кафедра менеджменту та безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 98% Схожість 2%

Аналіз звіту подібності (відмітити потрібне):

1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

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

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ (підпис) Олейніченко П.В. (прізвище, ініціали)

Керівник роботи _____ (підпис) (прізвище, ініціали)