МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ КОМП'ЮТЕРНОЇ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ

КАФЕДРА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач випускової кафедри

_____В.В. Козловський

«___»_____ 2022

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: «Розробка комплексної системи безпеки на об'єкті з критичною інфраструктурою»

Виконавець: В.В.Казімко

Науковий керівник: Д.П.Чирва

Нормоконтролер: М.О.Шутко

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки комп'ютерної та програмної інженерії

Кафедра: Засобів захисту інформації

Освітньо-кваліфікаційного рівня: «Бакалавр»

Напрям: 125 «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____В.В. Козловський

«___»_____2022

ЗАВДАННЯ

на виконання кваліфікаційної роботи

Казімко Віталіни Віталіївни

1. Тема роботи: «Розробка комплексної системи безпеки на об’єкті з критичною інфраструктурою» затверджена наказом ректора від 06.05.2022 №483/ст.

2. Термін виконання: 16.05.2022 – 19.06.2022

3. Вихідні дані: Розробити систему захисту об’єкту з критичною інфраструктурою, що потребує захисту з урахуванням наявності сучасних комплексних систем безпеки.

4. Зміст пояснювальної записки: Розробка та описання приміщень, створення власної комплексної системи безпеки, для підвищення ефективності.

Технічні характеристики елементів системи та економічний розрахунок.

КАЛЕНДАРНИЙ ПЛАН

виконання кваліфікаційної роботи

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1.	Зміст	16.05.2022	Виконано
2.	Вступ	17.05.2022	Виконано
3.	1. Комплексні системи безпеки	19.05.2022	Виконано
4.	2. Відеоспостереження. Захист, маскування	20.05.2022	Виконано
5.	3. Розробка комплексної системи безпеки на об’єкті з критичною інфраструктурою	30.05.2022	Виконано
6.	Висновки	02.06.2022	Виконано
7.	Оформлення пояснювальної записки	15.06.2022	Виконано

6. Дата видачі завдання:

Керівник кваліфікаційної роботи (проекту) _____ Чирва Д.П.

(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Казімко В.В.

(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота складається з: вступу, трьох розділів, висновків та переліку використаних джерел. Обсяг роботи складає 50 сторінок. Список використаних джерел містить 25 джерел.

Метою роботи є розробка комплексної системи безпеки на об’єкті критичної інфраструктури.

В кваліфікаційній роботі було розглянуто об’єкт критичної інфраструктури, наведено його будову та технічне оснащення, запропоновано план дій для унеможливлення несанкціонований доступ до інформації яка циркулює в приміщеннях. Також розглянуто інформацію про комплексні системи безпеки, системи контролю та управління доступом.

Підсумком роботи є розроблена комплексна система безпеки приміщень з обмеженим доступом, зроблено підбір оптимальних технічних засобів для створення комплексної системи безпеки.

Ключові слова: КОМПЛЕКСНА СИСТЕМА БЕЗПЕКИ, СИСТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ, ПРИМІЩЕННЯ З ОБМЕЖЕНИМ ДОСТУПОМ, ОБ’ЄКТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗАСОБИ ЗАХИСТУ, ЗАХИСТ ІНФОРМАЦІЇ.

ЗМІСТ

Скорочення

КСБ – Комплексна система безпеки

СБ – Система безпеки

ОКІ – Об’єкт критичної інфраструктури

КІ – Критична інфраструктура

СКУД – Система контролю та управління доступом

СУД – Система управління даними

ПК – Персональний комп’ютер

ІЧ – Інфрачервоний

КПП – Контрольно-пропускний пункт

НСД – Несанкціонований доступ

NIST – Національний інститут стандартів і технологій США

ВСТУП

В сучасному світі забезпечення якісного комплексного захисту будь-якого об’єкту є необхідним завданням. Така концепція безпеки включає в себе багато систем та комплексів захисту різної складності та найчастіше представлена у вигляді комплексної системи управління безпекою.

Тому розробка та встановлення КСБ на об’єктах є першочерговим завданням безпеки. Якісно організована КСБ забезпечує комплексний захист від пожеж, несанкціонованого доступу на об’єкт, протизаконних чи помилкових дій працівників. Крім того дана система дозволяє істотно економити на охороні та кількості працівників служби охорони та в цілому підвищити ефективність роботи об’єкта чи компанії, а також забезпечити охорону здоров’я та життя персоналу.

Захист об’єктів критичної інфраструктури наразі є ключовою сферою безпеки країн-членів ЄС та НАТО. Експерти Світового банку також в свою чергу наголошують на корисності приділення особливої уваги безпеці стратегічно важливих об’єктів, що має зменшити можливі наслідки катастроф. Міжнародне співтовариство не виробило єдиного загальновизнаного визначення критичної інфраструктури, проте визначення, що документовано закріплені різними державами значно перетинаються та не суперечать одне одному.

Наприклад у документі Національного інституту стандартів і технологій США (NIST) «Основа для покращення кібербезпеки критичної інфраструктури» від квітня 2018 року наведено таке визначення: «Системи та активи, фізичні чи віртуальні, що є настільки важливими для Сполучених Штатів, що недієздатність або знищення таких систем та активів матиме руйнівний вплив на безпеку, національно-економічну безпеку, здоров’я або безпеку громадян чи будь-яку комбінацію цих проблем»[2].

Згідно з Законом України «Про критичну інфраструктуру» від 16.11.2021 №1882-IX об’єктами критичної інфраструктуру визначають: «Об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони порушення функціонування яких може завдати шкоди життєво

важливим національним інтересам». Для визначення вимог до забезпечення захищеності відбувається категоріювання об’єктів критичної інфраструктури відповідно до однієї з чотирьох категорій критичності, де: I рівень – особливо важливі об’єкти державного значення; II – життєво важливі об’єкти регіонального значення; III – важливі об’єкти місцевого значення; IV – необхідні об’єкти локального значення [1]. Держспецзв’язку наразі очікує на завершення формування єдиного реєстру ОКІ України, щоб провести необхідні аудиторські роботи та покращити системи їх захисту базуючись на підходах NIST.

Зазвичай охорона об’єкту включає у себе фізичний пост охорони, що забезпечує контроль пропускного режиму робітників та клієнтів та певне електронно-технічне устаткування захисту, таке як наприклад камери відеоспостереження, магнітні замки, що дозволить відслідковувати переміщення працівників та клієнтів чи інфрачервоні датчики руху, що повідомить охорону про несанкціоноване відкриття дверей і вікон. Крім того всю інформацію з камер, КПП доцільно направляти на пульт охорони та на сервер для збереження. Для оптимізації та синхронізації роботи цих складових та зменшення витрат використовують комплексні системи управління безпеки, тобто КСБ.

Тому в даній роботі задля покращення безпеки на об’єкті критичної інфраструктури буде розроблено власну комплексну систему безпеки.

1. КОМПЛЕКСНІ СИСТЕМИ БЕЗПЕКИ

1.1 Основне про КСБ

В давнину найперші засоби захисту люди застосовували саме від стихійних лих, що дуже їх лякали. Для більшості легенд та історій основою послужили реальні події, їх руйнівні наслідки та спроби прогнозування. Найдревніші пам’ятки писемності, такі як єгипетські ієрогліфи чи наскельні зображення сповнені описів небезпек та засобів захисту від них. Археологічні розкопки дозволили виявили багато цікавих приладів та систем безпеки такі, як наприклад побудова секретних ходів-лабіринтів зі сховищами, створення зброї та інженерних пасток, різноманітні замки та засоби закриття дверей, знаряддя медичного призначення та ін. Ще в ті часи жителі розуміли, що найкращим захистом є попередження будь-якої агресії чи руйнування шляхом завчасного створення засобів захисту, завдяки знанням про різні небезпеки та можливості попередити їх виникнення.

Багато події нашої історії безпосередньо пов’язані з епідеміями, війнами, стихійними лихами чи пожежами. Під впливом таких загроз формувались племена, держави та союзи. Міста будували з розрахунком на захист від пожеж та загарбницьких посягань, використовуючи ландшафт та утворюючи складні траєкторії вулиць, враховували також розташування водойм та лісів, що є необхідними для життя.

У III ст. до н.е. в Стародавньому Китаї почали будівництво «Великого китайського муру» для захисту від кочівних племен. Сама стіна є дуже високою, у середньому 6,5 м та достатньо широка щоб на ній могли одночасно проїхати два кінні вози в різні боки. Крім того по периметру муру на певній відстані знаходяться сторожові вежі, які колись вміщали не лише гарнізони охорони, а й слугували прихистком тим хто подорожував Великим Шовковим шляхом.

А у стародавньому Єгипті в пірамідах для забезпечення збереження цінностей та спокою муміфікованих фараонів використовували вже декілька засобів захисту.

Насамперед було виставлено охорону навколо піраміди та й сам вхід розташовувався на висоті приблизно 16 метрів, крім того всередині піраміди могли бути пастки, такі як глибокі «колодязі» та пуста кімната-приманка, що мали зупинити грабіжників, а сама усипальниця чи сховище були замуровані величезними кам'яними плитами. Також зважаючи на вірування тих часів, людям казали, що не можна торкатись пірамід, якщо вони не хочуть прогнівити богів. Коли сучасні археологи в 1922 році потрапили всередину гробниці Тутанхамона, там був напис «Прокляття фараона покарає за порушення його спокою».

Світ поступово розвивався і було винайдено багато нових різних засобів захисту які були неможливими у давні часи. Тепер користувачі мають змогу не просто встановити окремі елементи захисту, такі як система контролю доступу, охоронне відеоспостереження, пожежну сигналізацію, а й об'єднати їх в єдиний комплекс безпеки для всього об'єкту.

Комплексна система безпеки (КСБ) – це багатофункціональна система охорони, що складається з охоронно-пожежної сигналізації, системи відеоспостереження та контролю доступом, які працюють централізовано з спільним єдиним пультом управління.

КСБ не тільки об'єднує елементи в єдину систему охорони, а й суттєво підвищує ефективність роботи підприємства. Проектуючи послідовне забезпечення всіх етапів захисту в КСБ можна домогтись 100% результативної безпеки на об'єкті. Так комплексна система складається з абсолютно функціонально різних підсистем безпеки, а при інтеграції в єдиний комплекс на об'єкті встановлюється спеціальне місце де збирається та відображається інформація, а також зберігається база всіх даних. Відзначимо, що усіма процесами роботи КСБ можна управляти з єдиного багатофункціонального центрального пульту. Важливим моментом є те, що завдяки такому підходу навіть для великого виробництва буде достатньо лише декілька спеціалістів служби безпеки, щоб контролювати такий об'єкт.

На сьогодні такі комплексні системи встановлюють на об’єктах охорони незалежно від їхньої площі, кількості поверхів, географічного розташування чи кількості персоналу:

- невеликих об’єктах, таких як магазини, офіси чи готелі;
- великих промислових об’єктах, таких як фабрики і заводи;
- великих адміністративних об’єктах, таких як банки, стадіони, вокзали.

Сучасні системи безпеки є абсолютно автономними та комп’ютеризованими, що значно спрощує роботу з ними для будь-якого користувача, адже для експлуатації необхідні лише мінімальні навички користування комп’ютером та мережею Internet. Більш того, якщо КСБ є інтегрованою та реалізована на IP технологіях то адміністратори системи при необхідності можуть контролювати охоронний об’єкт і управляти системою віддалено з будь-якої місця в світі при наявності виходу в інтернет.

1.2 Проектування та впровадження КСБ

Проектування і подальше впровадження комплексних СБ базується на таких основних принципах:

- Комплексність та системність – виявлення всіх можливих загроз, повний аналіз уразливостей системи безпеки об’єкта та розроблення системи щодо їх запобігання.
- Науковість та обґрунтованість – побудова СБ з використанням ефективно обґрунтованих наукових рішень. Наприклад, для вибору технічних засобів КСБ основну увагу слід приділяти створенню запасу часу достатнього для адекватного прийняття рішень та реагування на непередбачувану ситуацію.
- Рівномірність та багато рубіжність – використання декількох просторових границь чи методів захисту однакового рівня безпечності.
- Врахування людського фактуру.

Проектування будь-якої КСБ починається з ретельного обстеження та аналізу об’єкта та наявної СБ. На цьому етапі здійснюються:

- визначення можливих цілей зловмисників;
- визначення моделей загроз та порушників;
- оцінка вразливості об’єкту та наявної СБ;
- розробка рекомендацій щодо покращення безпеки об’єкта.

Найчастіше сучасні комплекси безпеки включають в себе:

- пожежну сигналізацію та систему пожежогасіння;
- систему охоронного відеоспостереження;
- охоронну та тривожну сигналізацію;
- систему контролю та управління доступом (СКУД);
- систему безперебійного живлення;
- систему оповіщення і гучного зв’язку;
- систему обліку та ідентифікації людей;
- системи передачі сповіщень;
- систему візуального відображення та аналізу інформації (зокрема ситуаційні центри та диспетчерське керування).

Така СБ не просто фіксує всі дії на об’єкті, вона передає тривожні сигнали між підсистемами приводячи їх у дію, а також інформує власників про можливу небезпеку [3][4].

1.3 СКУД

Система контролю та управління доступом – є основним, невід’ємним елементом КСБ об’єкту та взаємодіє з охоронною сигналізацією та системою відеонагляду. СКУД представляє собою сукупність програмно-апаратних та механічних засобі захисту, що призначені для моніторингу пересування по охоронній території.

СКУД – це не тільки об’єднання пропускних конструкцій, зчитувачів, контролерів, а й непростий комплекс організаційно-технічних заходів, процес контролю доступом у якому автоматизований, що допомагає одночасно надавати якісний захист матеріальних цінностей та безпеку і облік пересування людей на об’єкті. Ще одним плюсом може бути можливість встановлення ієрархічного ступеню доступу до певних приміщень та організація обліку годин перебування співробітників на підприємстві.

Сучасні системи управління можуть бути представленні безліччю різних технологій: біометричні системи, безконтактні карти, що перезаписуються, електронні замки чи циліндри, системи енергозбереження. За допомогою СКУД здійснюється автоматизований контроль доступу. Це можуть бути як невеликі однопрохідні системи для 1-2 дверей, що мають зчитувач карт чи кнопку та датчик проходу, так складні турнікетні системи для кількох десятків чи сотень тисяч людей. Незважаючи на унікальність кожної системи контролю доступом, вона завжди має чотири основних елементи: ідентифікатор користувача (зазвичай ключ-карта з інформацією про користувача), пристрій ідентифікації, керуючий мікроконтролер та виконавчий пристрій. Загальна схема СКУД показана на рис. 1.1.

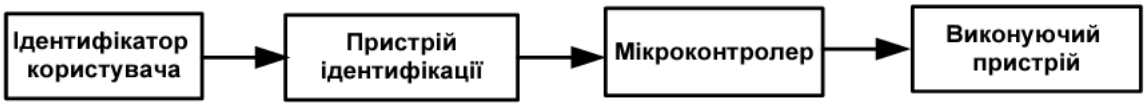

Рисунок 1.1 – Загальна схема СКУД

Роботу СКУД можна описати наступним чином. Кожна людина яка має особистий ідентифікатор з записаним на ньому персональним кодом, що був зареєстрований заздалегідь за допомогою засобів системи. Паспортні дані, фото, відомість про рівень доступу, та інші дані про власника електронного ключа заносять в персональну картку разом з паролем, що буде зберігатись в спеціально організованій комп’ютерній базі даних серверу підприємства.

Зважаючи на спосіб перевірки ідентифікатора розрізняють декілька видів СКУД:

- ручні – коли пропуск відбувається шляхом встановлення відповідності особи на основі пред'явленого пропуску з фотографією співробітнику охорони;
- механізовані – являють собою дещо удосконалені ручні з деякою автоматизацією зберігання та пред'явлення пропусків;
- автоматизовані – коли безпосередня ідентифікація та встановлення даних користувача відбувається за допомогою електронного автомату, а пропуск санкціонує оператор КПП;
- автоматичні – коли вся процедура проводиться комп'ютером [5].

Використовуючи інформацію про необхідний рівень захисту, величину і можливості підприємства та різноманіття складових СКУД розрізняють 4 класи:

- СКУД 1-го класу – малофункціональна система з невеликою ємністю, що використовує ручне чи механізоване управління виконавчими пристроями та охоронною сигналізацією, працює в автономному режимі та проводить пропуск усіх осіб, що мають ідентифікатори.
- СКУД 2-го класу – багатофункціональна система, що може працювати як в автономному так і в мережевому форматі та мати декілька рівнів безпеки, пропуск відбувається відповідно до певного приміщення чи частини території зважаючи на дату, час та допуск, що зазначений в ключі. Також система може автоматично контролювати виконавчі пристрої та вести журнал подій.
- СКУД 3-го та 4-го класів – багатофункціональні мережеві системи, що використовують складніші ідентифікатори та різні мережеві рівні [6].

1.4 Основні складові СКУД

Ідентифікатори – носії інформації, що дозволяють визначити та підтвердити особу користувача. В якості ідентифікатора можуть виступати біометричні риси та атрибутні автономні носії ознак, такі як магнітні картки, радіобрелки, смартфони, відбитки пальців, зображення сітківки ока та багато інших. Всі ідентифікатори мають певний унікально прописаний двійковий код.

Раніше в якості ідентифікаторів використовували перфоровані карти, на які дані переносились шляхом пробиття отворів при виготовлені карти, а зчитування відбувалось за допомогою оптичних та механічний пристроїв.

Згодом стали використовувати магнітні карти та карти зі штрих-кодом, в яких код записувався безпосередньо на магнітну ленту та міг бути перепрограмований чи інформація зашифровувалась за допомогою штрих-коду відповідно. Такі пристрої швидше працюють проте швидко зношуються та мають мінімальний захист від підробки.

Пізніше з’явились вінганд-карти основною перевагою яких є складність підробки за рахунок складної комбінації металевий дротів всередині карти, але вони дуже легко пошкоджуються, навіть при мінімальному згинанні можуть бути виведені з ладу.

Електронні ключі «Touch memory» в яких вся інформація знаходиться всередині мікросхемі живлення якої відбувається від батарейки в свою чергу є витривалими до механічних пошкоджень, надійні та багаторазові. Дані зчитуються при контакті ключа та зчитуючого пристрою.

На сьогодні найбільш надійними ідентифікаторами вважають Proximity-карти. Дані про користувача записані на мікрочіп, а зчитування відбувається на відстані радіочастотним способом. Вони дуже зручні у використанні, стійкі до погодних умов та мають високу пропускну спроможність.

Також для ідентифікації користувача використовують пін-код та біометричні дані: зображення сітківки ока, відбиток пальця, запис голосу і т.п. Такі ключі майже неможливо викрасти та підробити тому використовуються на об’єктах підвищеного ступеню захисту [7].

Зчитувач – пристрій, який зчитує інформацію з ідентифікатора та передає дані про користувача на контролер СКУД у вигляді цифрової послідовності. Він обирається в парі з ідентифікатором в залежності від вимог рівня безпеки та фінансових можливостей підприємства.

Пристрій центрального керування – персональний комп’ютер призначений для отримання інформації про користувачів системи та програмування СКУД. Крім того

він керує пожежною системою та системою відеонагляду. Для належного функціонування СКУД достатньо будь-якого звичайного ПК. Він здійснює управління СКУД використовуючи спеціальне програмне забезпечення, а також збирає та зберігає інформацію з контролерів, створює базу даних та формує звіти. Також завдяки запису плану території об’єкта в ПК, на якому відображені усі замки, зчитувачі, камери відеоспостереження тощо, можливо в будь-який момент в режимі реального часу дізнатись стан кожного механізму, що дозволяє оперативно оцінити ситуацію та вчасно відреагувати на проблеми.

Контролер – це основний та найважливіший елемент будь-якої системи СКУД. Завдяки ньому виконується багато функцій зокрема відбувається керування усіма зчитувачами та замками, турнікетами, шлагбаумами. Він приймає та аналізує інформацію зі зчитувачів та активує блокування чи розблокування механізмів, подає звукові та світлові сигнали. Контролери СКУД бувають автономні, мережеві та комбіновані.

Автономні контролери призначені для керування тільки однією точкою доступу з прив’язаними до неї невеликою кількістю ідентифікаторами, не більше 500. Автономні контролери працюють лише з виконавчим пристроєм без передачі інформації центральному пристрою керування та без втручання оператора. Але в подальшому їх неможливо синхронізувати з подібними елементами управління, тож це оптимальне і менш дороге рішення, якщо в майбутньому не планується розширення системи безпеки.

Мережеві контролери працюють під управлінням комп’ютера зі спеціальним програмним забезпеченням та використовуються в великих системах управління доступом. Кількість мережевих контролерів у системі може коливатись від 2 до декількох сотень, що обмінюються інформацією з центральним пунктом охорони та управлінням, адміністрацією системи чи черговим оператором. У цьому випадку розміри системи контролю доступу визначаються кількістю ідентифікаційних пристроїв, а не кількістю контрольованих дверей, оскільки один або два пристрої ідентифікації можуть бути встановлені на кожні двері [6]. Мережеві контролери надає СКУД певні додаткові можливості, крім простого контролю доступу:

- отримання звітності про відвідування персоналу;
- ведення електронної картотеки персоналу;
- відслідковування пересування співробітників;
- встановлення часових обмежень проходу через КПП;
- архів всіх операцій від часу встановлення та ін.

Також існують комбіновані контролери, що при наявності зв’язку з керуючим комп’ютером працюють як мережеві, а при відсутності – як автономні. Завдяки ним можливо побудувати відмовостійку та гнучку СКУД.

Інтерфейси для побудови СКУД. Для організацій з великою кількістю віддалених офісів і приміщень існує програмне забезпечення на основі розподілених мультисерверних платформ. Управління системою безпеки здійснюється централізовано, а локальні бази даних періодично синхронізуються через мережу.

Програмне забезпечення для СКУД визначає і дозволені зони доступу, стежить за тимчасовими інтервалами, в період яких прохід на територію є відкритим, крім того, для співробітників і гостей ці параметри можуть бути різними. Інтеграцію обладнання і додатків сторонніх розробників також забезпечує ПО. Щоб інтегрувати всі компоненти системи, включаючи контролер, в мережу, використовують такі інтерфейси:

- RS-232 служить для з'єднання контролера з комп'ютером. Стандартною швидкістю передачі даних є 9600 біт/с, а дальність – близько 15 метрів. У сучасних пристроях майже не використовується.
- RS-485 забезпечує обмін даними між кількома пристроями в напівдуплексному режимі по двопровідній лінії зв'язку. Максимальна швидкість передачі даних - 10 Мбіт/с. При цьому максимальна дальність передачі залежить від швидкості.
- Ethernet дозволяє будувати системи віддаленого доступу створювати системи безпеки на великих підприємствах з великою прохідністю, забезпечуючи швидкість передачі даних в 10 або 100 Мбіт/с.

- CAN-HS використовується в розподілених системах управління для організації високонадійних і недорогих каналів зв'язку. Швидкість передачі обирається користувачем зважаючи на відстань, число абонентів і ємність ліній передачі [8].

Виконавчі пристрої є не менш важливою складовою СКУД, адже саме вони відповідають за реалізацію активної частини контролю доступу на захищений об’єкт відповідно до команд, що надходять від пристроїв управління.

- Електрокеровані замки (або защіпки) – коли завдання СКУД полягає в обмеженні проходу через звичайні двері. Електрозащіпки рекомендують встановлювати на двері всередині офісу, там де можливість злому там мінімальна, так як вони відкриваються, як тільки з них знімається напруга. Електричні замки поділяють на електромеханічні, що поєднують електричну схему та звичайний механічний замок та електромагнітні – потужній електромагніт на який постійно подається напруга. Останні рекомендують використовувати разом з дверним доводчиком.

- Турнікети бувають двох типів виконання: поясні та повнозростові. За принципом дії вони фактично не відрізняються, після зчитування вірної інформації з ідентифікатора турнікет розблоковується та пропускає одну людину, а датчики повороту планок забезпечують облік. Поясні турнікети доволі легко перестрибнути чи проповзти під ним тож мають встановлюватись тільки в зоні візуального контролю служби безпеки. Також турнікети можуть бути обладнані ІЧ-бар’єрами чи вагочутливими датчиками, тоді при спробі обходу буде спрацьовувати сигналізація. Бувають трьохштангові турнікети, роторні турнікети, турнікети типу «метро», хвіртки та шлюзові кабіни.

- Автоматичні ворота і шлагбауми – зазвичай використовуються на в’їздах та автомобільних КПП. Для такого СКУД мають у складі спеціальні автомобільні ідентифікатори, зчитувачі для установки під полотном дороги та дистанційні зчитувачі [9].

Залежно від ступеня застосування всі виконавчі пристрої можна розділити на три основні класи:

- ВП для організації доступу до приміщень;
- ВП для організації доступу на пішохідний КПП;
- ВП для організації доступу на транспортних КПП.

2 ВІДЕОСПОСТЕРЕЖЕННЯ. ЗАХИСТ, МАСКУВАННЯ.

2.1 Способи та засоби протидії спостереженню у оптичному діапазоні хвиль.

Для захисту інформації від спостереження в оптичному діапазоні необхідно враховувати всі можливості виявлення об’єктів спостереження і фактори зниження точності вимірювання видових демаскуючих ознак. На ефективність пошуку впливають:

- яскравість;
- контрастність об’єкту по відношенню до фону;
- кут поля огляду;
- швидкість пересування об’єкта;
- час спостереження об’єкта;
- кутові розміри об’єкта.

Яскравість об’єкта, що потрапляє на вхід світлоприймача визначає потужність носія, що має перевищувати потужність перешкод для отримання якісного, чіткого зображення. Чутливість сучасних приймачів відповідає енергії кількох фотонів. Мінімальний рівень контрастності об’єкту відносно фону для його розпізнання має перевищити 0,1.

Крім того задля полегшення виявлення об’єкту є доцільним збільшення в 2 рази кутових розмірів об’єкту, що скоротить час, необхідний для виявлення в 8 разів. Чим менший кутовий розмір має об’єкт, тим довше та важче його виявити. Найлегшим є розпізнання об’єктів, що рухаються з малою швидкістю порівняно з нерухомими та тими, що пересуваються з великою швидкістю, оскільки погіршується видимий контраст. Враховуючи все вищесказане, методи протидії спостереження в оптичному діапазоні поділяються на наступні:

- Просторове приховування – використовування сліпих зон систем спостереження;
- Тимчасове приховування – маскування певних ознак об’єкта на час обстеження;

- Енергетичне приховування – приглушення яскравості та освітлюваності об’єкта, засвічення, що призведе до зменшення контрастності об’єкт/фон, засліплення чи зменшення прозорості середовища (дим, аерозолі);
- Структурне приховування – використання особливостей місцевості для маскування.

Основними ефективними засобами маскування від спостереження в оптичному діапазоні є різні екрани, маски, фарби. При чому для вибору фарб для маскування важливо враховувати не тільки кольорову гамму, а також характер можливих змін коефіцієнта відбиття в залежності від довжини хвилі. Маскувальна здатність фарби тим краще, чи меншою є різниця між коефіцієнтами відображення в інфрачервоному та видимому діапазонах хвиль.

Штучні маски для захисту від виявлення в оптичному діапазоні розрізняють в залежності від їх форм та способу розташування відносно об’єкта на такі види:

- Вертикальні маски;
- Маски-навіси;
- Маски перекриття;
- Радіопрозорі маски;
- Похилі маски.

Вертикальні маски так само як і маски перекриття призначені для захисту об’єктів розташованих на землі від спостереження. Вони включають каркас та маскувальне покриття, що повністю закриватиме об’єкт. Їх застосовують, в першу чергу, для захисту об’єктів, що перевозяться на відкритих платформах.

Маски-навіси використовують для захисту від виявлення об’єктів, розташованих на відкритих зверху майданчиках. Захист відбувається шляхом розміщення засобів на верхніх поверхах будівель, горах, на літаках та космічних апаратах.

Похилі маски в свою чергу призначені для приховування тіней об’ємних об’єктів, для унеможливлення визначення висоти об’єктів при зборі інформації з повітря (з літаків та космічних апаратів).

Радіопрозорі маски, створені з прозорих матеріалів таких як наприклад склопластик чи іншого подібного матеріалу, зазвичай представлені у формі сфер призначені для фізичного захисту та маскування антен.

Штучні оптичні маски можуть бути виготовлені з табельних засобів: маскувальної сітки, поліхлорвінілової плівки, сітчастої тканини і т.п. або з підручних матеріалів (очерету, хмизу, моху) чи у вигляді різних портативних комплектів маскування.

Для маскування військової техніки в оптичному діапазоні використовуються різні типи службових маскувальних комплектів типу МКТ: МКТ-L - для маскування на рослинному тлі або голому ґрунті, МКТ-С - для снігового фону, МКТ-Р - для гірської пустелі, МКТ-Т для маскування танків, тощо. Набір являє собою металеву розбірну рамку різних кольорів, яка розтягується, спеціальна суцільна або сітчаста тканина, двостороння та універсально кольорова, що підходить для різного фону. Камуфляжний набір має максимальний розмір покриття 12х18 м (на основі створеної для танка маски) і складається з 12 фрагментів розміром 3х6 м кожен. Деталі з’єднуються між собою шнурами, що дозволяє швидко зібрати покриття різноманітних розмірів і конфігурацій, включаючи плоскі, опуклі, вертикальні, похилі, макетні моделі, маски-навіси. Завдяки запасним зшивним шнурам, які входять у комплект камуфляжу, можна комбінувати покриття з кількох комплектів, щоб приховати великі предмети.

Штучні оптичні маски багаторазові, не є шкідливими для природи, можуть бути скомбіновані з іншими засобами захисту.

Світлонепроникні повітряні піни, однобарвні чи багатобарвні, що швидко можуть бути нанесені генераторами піни на об'єкти, надають ефективне маскування в широкому діапазоні довжин хвиль протягом декількох годин.

Деформуючими масками називаються ті, що змінюють вигляд об’єкту в оптичному діапазоні. Наприклад поміщають предмети, що перевозять залізницею під дерев’яний каркас накритий брезентом. Таким чином спостерігач зважаючи на вантажні платформи зможе лише виявити, що перевозять військовий груз але не визначити вид перевезеної техніки.

Крім деформуючих масок також можуть бути використані обманні споруди та конструкції. Вони можуть бути як об’ємними так і плоскими, штучними та функціональними. Даний вид маскування вважається найбільш дорогим способом, особливо при використанні об’ємних та функціональних, оскільки вони мають відтворюваний набір ознак об’єкта прикриття на протязі всього періоду захисту в динаміці, включаючи переконливо працюючих людей.

Енергетичне приховування об’єктів відбувається за допомогою приглушення яскравості та контрастності об’єкта відносну фону за межу сприйняття оком людини чи технічних засобів, а також шляхом їх засліплення. Найлегшим та найприроднішим проявом енергетичного приховування є виконання таємних заходів в нічний період часу. Крім цього, у об’єктів, що мають штучні джерела світла можна зменшити яскравість шляхом їх вимкнення чи екранування світлонепроникними матеріалами.

Щоб екранувати матеріали, що знаходяться всередині приміщення застосовують штори, завіси, жалюзі, тоноване скло та плівки. Найефективнішими вважаються жалюзі, які бувають вертикальні, рулонні та горизонтальні створені з пластику, металу чи дерева. Найкращими в експлуатації себе показали дерев’яні та металеві.

Для захисту від спостереження у відбитому світлі, енергетичне приховування забезпечується розглянутими раніше штучними масками, а також природними та штучними аерозолями в місці поширення.

Аерозолями називаються речовини у вигляді дисперсії краплинок рідини та твердих часинок, що розташовуються в повітрі у підвішеному стані. До природніх аерозолів відносяться тумани, дим, пил.

Натуральні аерозолі виникають зазвичай при змішуванні пилу і частинок води. В залежності від розміру частинок води метеорологічна дальність може змінитись від кількох десятків метрів, при зливах, сильному тумані чи хуртовина, до 10-20 км на серпанку. Нормальна видимість забезпечується при 20-50 км, а відмінна в тому випадку, як дальність перевищує 50 км.

Серпанок є яскравим прикладом природнього аерозольного стану атмосфери. Він виникає в результаті об’єднанні дрібнодисперсних часток повітря разом і їх взаємодії з атмосферною вологою. При підвищеній вологості повітря, в результаті

взаємодії пари води і частинок солей, що в ній знаходяться – утворюється легкий туман, димка, при якій метеорологічна дальність складає до 10 км.

Зазвичай, вплив аерозольних утворень проявляється в поглинанні та розсіянні світла часточками аерозолю. Змінення коефіцієнту поглинання у видимій області спектру відбувається в 1,5-2 рази. При збільшенні довжини хвилі втрати стають значно меншими. Наприклад при довжині хвилі $\lambda = 1{,}06$ мкм втрати енергії хвилі менші від втрат хвилі довжиною $\lambda = 0{,}55$ мкм приблизно в 10 разів. Коефіцієнт поглинання окремими частинками, їх концентрація та розмір значно впливають на аерозольне розсіювання світла. В залежності від нього визначається прозорість і метеорологічна дальність видимості.

Проте використання природніх аерозолів для захисту від спостереження є ненадійним, так як їх виникнення, що призведе до малої метеорологічної дальності мають випадковий характер. Але природні аерозолі у вигляді хмар можуть створити серйозні проблеми для спостереження наземних та надводних об’єктів використовуючи космічну розвідку. З огляду на те, що ймовірність одночасного проведення розвідки, траєкторії руху космічного апарату та хмар дорівнює добутку їх ймовірностей, то для виявлення і розпізнання об’єктів в будь-якому разі потрібні декілька прольотів над ними космічних апаратів.

Використовуючи димові шашки, аерозольні генератори, спеціальні боєприпаси та димові шашки утворюють штучні аерозольні димові завіси, що забезпечують короткочасне але ефективне приховування. При чому час приховування та площа залежать від таких факторів, як напрям і швидкість вітру, обсяг хмари диму та коливаються від 1 до 2 годин. Найефективніші завіси створюються якщо швидкість вітру 3-5 м/с.

Для утворення диму застосовують такі хімічні речовини, як епоксидні, силікатні, поліетиленові, фенольні, уретанові смоли й інші полімерні сполуки. Дим утворюється в результаті поділу частинок речовин в потоці гарячих газів або іншими способами. Аерозольна хмара може мати діаметр від 1 до 100 мкм залежно від складу компонентів з яких утворилась. Для утворення аерозольної хмари, що забезпечить

ослаблення випромінювань в інфрачервоному діапазоні в 80 разів на площі в 600 м^2 необхідно використати близько 400 г димоутворювальної речовини.

Оскільки природне спостереження відбувається за допомогою оптичних приладів, то для протидії йому застосовують активні засоби виявлення оптики. Такими є прилади нічного бачення з лазерним підсвічуванням, що мають лазерний випромінювач в ІЧ-діапазоні хвиль, промені якого сканують довкілля. При відбитті від лінзи об’єктива оптичного приладу промінь лазера відзначає його місце знаходження на зображенні точкою підвищеної яскравості [10].

2.2 Види та особливості маскування у видимому та інфрачервоному діапазонах.

Тепловим випромінюванням називається випромінювання світла нагрітими тілами, що випромінюють електромагнітні хвилі. Особливістю цього випромінювання є те, що його інтенсивність має сильну залежність від абсолютної температури. Теплове випромінювання здійснюється шляхом перетворення енергії теплового руху часток тіла в енергію випромінювання. З цієї причини випромінюванню світла обов’язково передує акт поглинання енергії випромінюючим тілом, крім того згідно з законом збереження енергії для будь-якого об’єкта енергія $\omega_{випр}$ випромінювана з одиниці поверхні тіла за одиницю часу, має дорівнювати енергії $\omega_{погл}$, що поглинається за такий самий час цією ж ділянкою поверхні.

Проте залежно від довжини електромагнітної хвилі пропускна спроможність повітря може викликати значне спотворення характеристик об’єкта при віддаленні від нього. Для виявлення об'єктів на великих відстанях у розвідці використовують так звані «вікна прозорості» – ділянки спектру найвищого пропускання. У видимій області спектру електромагнітного випромінювання такі області відповідають довжинам хвиль від 0,4 до 0,7 мкм, у ближньому ІЧ – від 0,7 до 3,0 мкм, у середньому та дальньому ІЧ – від 3 до 6 і від 8 до 14 мкм. Тому зі зменшенням контрасту місцевості зменшується ймовірність виявлення об’єкта.

Особливість виявлення об'єкта полягає у виборі частини спектра для спостереження не тільки за характеристиками пропускання атмосфери, а й за спектральним діапазоном випромінювання об'єкта. Він залежить від власної

температури об’єкта, а для фіксованої температури об’єкта існує область максимального випромінювання. При температурі мало нагрітих об'єктів (до 300 К) максимум випромінювання знаходиться в діапазоні від 8 до 14 мкм, а при підвищенні температури до 1000 К – зміщується в діапазон 3 – 5 мкм що зображено на рисунку 2.1.

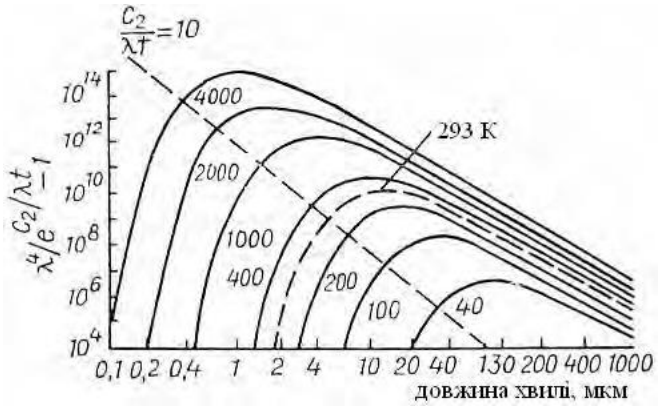

Рисунок 2.1. Ізотерми випромінювання чорних тіл за різною температурою, що розраховані за формулою Планка

Військової конструктори техніки намагаються підтримувати температуру предметів якомога ближче до температури навколишнього середовища.

Розглянемо можливість ідентифікації цілей за допомогою тепловізора. Відомо, що фіксоване спостереження у видимому діапазоні можливе за таких граничних значень контрасту: знайдена ціль $\varepsilon_{знах}$ = 0,03 ÷ 0,04; розпізнавання цілі $\varepsilon_{росп}$ = 0,05 ÷ 0,09; зникнення цілі $\varepsilon_{зник}$ = 0,016 ÷ 0,02.

Відповідно до закону Вебера-Фехнера, коли значення перевищує мінімальне значення порогу контрастної чутливості ока ε, у видимому діапазоні на задньому плані можна побачити об’єкти, що має яскравість.

Контраст яскравості К розраховується за виразом:

$$К = \frac{В_о - В_ф}{В_ф},$$

де Вф – яскравість фону, $В_о$ – яскравість об’єкта,

Найбільшу чутливість у спектрі, що відповідає зеленому світлу, має людське око. Тому ІЧ зображення зручно конвертувати у видимі зеленого кольору. Базовою умовою ідентифікації об'єктів у тепловому діапазоні є роздільна здатність приладу,

яка в сучасних тепловізорах на коротких дистанціях становить близько 0,1 К. Переведемо дану величину в одиниці енергії випромінювання.

Розрахуємо випромінювальну здатність тепловізору. Розподіл енергії випромінювання абсолютно чорного тіла залежно до довжини хвилі λ визначається за формулою Планка:

$$\varepsilon(\lambda, \mathrm{T}) = \frac{2\pi c^2 h}{\lambda^5} \frac{1}{\exp\left(\frac{hc}{kT\lambda}\right) - 1},$$

де c – швидкість світла, h – стала Планка, k – стала Больцмана.

Найінтенсивнішим джерелом випромінювання є чорне тіло. Щільність поверхневого випромінюваного (поверхнева густина) потоку об'єктів у межах об'єму, виміряного тепловізором, розраховується так:

$$\varepsilon(T) = \int_{\lambda_1}^{\lambda_2} \varepsilon(\lambda, T)\, d\lambda$$

де λ_1, λ_2 – верхня та нижня межа обсягу довжини хвиль, за якими здійснюються вимірювання.

Тоді при підставленні значень даного діапазону $\lambda_1 = 8 \cdot 10^{-6}$ м, $\lambda_2 = 14 \cdot 10^{-6}$ м при температурі в 300 К, отримаємо поверхневу щільність потоку випромінення: ε(300) = 171,907 Вт/м^2. При температурі, що перевищуватиме дане значення на ΔT=0,1 К – ε(300,1) = 172,17 Вт/м2.

Щоб визначити різницю поверхневої щільності променевого потоку, що надходить у вхідне вікно тепловізору із заданою чутливістю (ΔT = 0,1 К), розглянемо геометричну роздільну здатність пристрою, яка становить 160 х 120 пікселів для тепловізору Fluke Ti-40. На відстані 1,5 м від вхідного вікна цього пристрою можна знімати об’єкти розміром приблизно 1,6 х 1,2 м^2. Тобто на такій відстані піксель відображатиме інтегральне значення температури площі S = 10^{-4} м^2.

В результаті, об’єкт буде відображатися одним або кількома пікселями на зображенні. Тож можливість розпізнавати об'єкти залежить від розміру їх відображення. Існує зв’язок між кутовою роздільною здатністю та кількістю пікселів, що представляють об’єкт. Так, якщо кутовий розмір віддаленого об’єкта менший за

кутову роздільну здатність, об’єкт може відображатися в пристрої лише одним пікселем, і навпаки.

Природний тепловий фон середовища неоднорідний, а температура поверхні об’єкта впливає на яскравість об’єкта з власним джерелом тепла і як результат на його контраст з фоном. Тому для захисту від спостереження в ІЧ-діапазоні використовують різні теплоізолюючі екрани, враховуючи підручні матеріали з поганою теплопровідністю: брезент, листя, сіно та ін. Гарними теплоізолюючими властивостями наділені повітряні піни. Об’єкти можна приховати за допомогою властивостей відбиття, що викличе «плямисте відображення». Очевидно, що в цьому випадку відбиваюча поверхня не повинна бути плоскою. Отримання випромінювання за рахунок відображення від неба (за винятком напрямку сонця) дозволяє отримати навіть від’ємну температуру. У цьому випадку може бути досягнуто зниження середньої випромінюваної температури об'єкта.

Модель автоматичного маскування була створена базуючись на цих дослідженнях. Вона не тільки усуває необхідність залучення екіпажу, але також скорочує час необхідний для маскування та забезпечує доступ до обслуговування обладнання. Використання маскувальної сітки як покриття в системі автоматичного камуфляжу зменшить можливість виявлення об’єктів у видимому, ІЧ та радіохвильовому діапазонах згідно з параметрами сітки. Крім того, буде досягнуто додаткового зниження теплового контрасту у ІЧ-діапазоні за рахунок створення потоку повітря між сіткою та каркасом [11][12].

2019 року представники компанії HyperStealth Biotechnology Corp. Представили матеріал, для камуфляжа, нового типу – Quantum Stealth. Даний матеріал, шляхом спотворення світла навколо нього, приховує за собою об’єкт-користувач та приймає вигляд оточуючого середовища. Матеріал працює без камер, акумуляторів, ламп чи дзеркал, має невелику вагу і, за словами розробників, невелику вартість.

Крім того, матеріал маскує не тільки у видимому спектрі, а й в температурному, ІЧ та ультрафіолетовому діапазонах. Розробники зазначають, що об’єкт не зникає повністю, а розмивається, що не дозволить абсолютно приховати його від спостерігача але дозволить стати дуже непомітним на відстані кількох метрів [13].

2.3 Способи і засоби протидії радіолокаційному та гідроакустичному спостереженню.

Радіолокаційне маскування використовується для запобігання радіолокаційній розвідці шляхом надання виробу необхідної геометричної форми для перенаправлення або багаторазового повторного відображення вхідного сигналу, що спричиняє подальше загасання відбитого сигналу, або шляхом встановлення індивідуального широкосмугового маскувального комплекту на виробі. Це забезпечить маскування у тепловому, видимому і радіолокаційному діапазоні довжин хвиль.

Радіоелектронне придушення включає певні радіоелектронні перешкоди, використання неправильних цілей і пасток, вплив на місце електромагнітного випромінювання, погіршення видимості військової техніки, об’єктів і особового складу, а також дезінформацію ворога по радіо каналах. Розглянемо ці види детально.

Радіоперешкоди – це електромагнітне або акустичне випромінювання, яке може погіршити роботу радіоелектронного засобу (РЕЗ), керованої зброї та військової техніки або систем обробки інформації. Перешкоди імітують або змінюють сигнали чи зображення, що спостерігаються приймальними приладами діючи на них. До того ж, вони можуть заблокувати виявлення необхідної інформації, запобігти використанню РЕЗ для радіорозмов і пошуку цілей, знижуючи дальність і точність систем автоматичного керування.

Оскільки придушити різноманітні РЕЗ перешкодами одного виду неможливо, то для придушення радіолокації, радіонавігації, радіозв'язку, лазерної, ІЧ апаратури використовуються спеціальні види перешкод.

Помилкова ціль — це пристрій, який імітує властивості відображення реального об’єкта. Залежно від типу та діапазону використовуваних хвиль помилкова ціль може бути радіолокаційною, світловою чи акустичною. За допомогою помилкової цілі на індикаторних екранах різних розвідувальних РЕЗ формуються оцінки, подібні до оцінок реальних об’єктів. Це ускладнює ситуацію дезорієнтуючи операторів і системи розподілу, збільшуючи час на визначення цілей.

Залежно від середовища застосування помилкові цілі можуть бути наземні, повітряні, космічні та морські. У якості радіолокаційних використовуються пасивні антенні стрижні, ракети, дрони та іонізовані локальні ділянки при розпиленні або спалюванні в атмосфері легкоіонізованих елементів.

Світловими помилковими цілями є теплові імітатори, світловідбивачі, надувні макети військової техніки та об’єктів використовуються для введення в оману операторів розвідувальної служби та викрадення ракет (снарядів, авіабомб) ІЧ, лазерного та телевізійного способу наведення.

Помилкові цілі, що використовуються для відволікання ракет з ІЧ наведенням з літаків, це керовані ракети, випущені з повітряних або наземних пускових установок. Такі помилкові цілі іноді створюються шляхом заповнення резервуарів з гарячим газом, що виділяється в повітря поблизу об'єкта, що охороняється, наприклад корабля.

Пастка для керованих засобів ураження – це технічний пристрій, що імітує об’єкт для РЕЗ-керування зброї, який використовується для викрадення цілей контрольованих боєприпасів або порушення автоматичного супроводу цілі радіолокаційною станцією. Сигнал, який створює пастка, за різними характеристиками повинен бути подібним до сигналу, що виробляється об'єктом, що охороняється.

Крім того, змінюючи умови поширення енергії електромагнітного випромінювання, переважно в іоносфері, функціонування РЕЗ може бути серйозно порушено.

Зменшуючи прозорість навколишнього середовища між розвідувальними засобами та об’єктами, замаскованими аерозольними завісами, військову техніку та об’єкти можна приховати від виявлення за допомогою електронних засобів. Частинки аерозольної завіси поглинають, розсіюють і заломлюють комп’ютерну енергію, що утруднює або унеможливлює спостереження за військовою технікою розвідувальними засобами, які працюють в ультрафіолетовому (0,1-0,4 мкм) діапазоні видимому (0,4-0, 76 мкм) діапазоні та ближній частині діапазону ІЧ (0,76-1,5 мкм) хвиль.

Зниження інтенсивності випромінювання електромагнітних хвиль об'єктами. Відомо, що будь-яка військова техніка, озброєння та місцеві предмети з температурою вище абсолютного нуля (-273°C) розсіюють падаючу на них енергію світлових хвиль і випромінюють світлову енергію в ІЧ, видимій та ультрафіолетовій областях. Крім того, теплова енергія випромінюється місцевими об’єктами, місцевістю та атмосферою. Інтенсивність і спектр випромінювання залежать від властивостей об'єкта і його температури. Приймаючи та перетворюючи власне або розсіяне ІЧ випромінювання від об’єктів і фону, ви можете отримати їх видиме зображення та розташування за допомогою радіометра, теплопеленгатора або теплорадара. Розвідка, що відбувається по радіотепловому випромінюванню цілей називається радіотепловою розвідкою. Ракети, артилерійські снаряди та авіабомби, оснащені тепловими або лазерними засобами автонаведення, можуть націлюватися на джерела випромінювання або об'єкти, які розсіюють енергію світлових хвиль.

Найпотужнішими джерелами теплової енергії для військової техніки є ракети, реактивні літаки, кораблі та танки. Для приховування озброєння, військової техніки та об’єктів від виявлення та захисту їх від ураженням боєприпасами, оснащених оптично-електродними засобами самонаведення, знижують рівень випромінення та розсіювання ними світлової енергії. Тому потужність теплового випромінювання військової техніки знижується за рахунок охолодження, зменшення розмірів випромінюючої поверхні, використання теплозахисних екранів, прокладок, формування екрану навколо форсунки, введення різних домішок у паливо [14].

Захист інформації про об'єкти у воді, перш за все, полягає у запобіганні гідролокаційного спостереження. Враховуючи особливості каналу витоку, цей метод захисту в основному використовує наступні пункти:

- Використання природних явищ для маскування. Акустичні екрани, що виникаючі при перепаді температури шарів, є важкоуникними для акустичних випромінень;
- Використання звукопоглинаючих покриттів стільникових конструкцій з нейлону, поліетилену, поліпропілену, різних пластмас та містять натуральний

каучук. За кордоном проводяться експерименти з покриття корпусів підводних човнів матеріалами, що поглинають до 90% звукової енергії;

- Генерування активних гідролокаційних перешкод, включаючи повторну передачу випромінюваних сигналів підвищеної потужності [15].

2.4 Способи дезінформування та зашумлення зображення на екрані радіолокатора.

Для структурного приховування об'єктів радіолокаційного спостереження за допомогою конструкцій електромагнітні хвилі від радарів, що падають на них, відбиваються в зворотному напрямку і створюють помилкові «блискучі» точки на екрані локатора. Оскільки точний напрямок радара, що захищає об’єкт, невідомий, така конструкція повинна видавати «блискучі» точки під значним кутом можливих напрямків. В якості таких ширококутних конструкцій використовуються кутові, лінзові, дипольні рефлектори та перевипромінюючі антенні решітки.

Приховування енергії досягається шляхом зменшення ефективної площі розсіювання об'єкта двома основними способами: зміною діаграми спрямованості відбиваючих об'єктів і поглинанням радіолокаційної енергії. Відбита енергія має бути зменшена шляхом виключення утворення кутового відбивача в площині де знаходиться об’єкт, для захисту від радіолокаційного спостереження.

Прикладом технічного рішення, що забезпечує ефективне структурне та енергетичне приховування, є технологія зниження електрорушільної сили «Стели». Вона полягає в наступному:

- покращити форму об'єктів, що охороняються, шляхом зменшення площі їх поверхні, усунення кута їх опромінення близьких до 90°, заміни прямих площин на криволінійні, усунення резонансних явищ на опромінюваній поверхні;
- використання неметалевих композиційних матеріалів, які слабо розсіюють енергію електромагнітного поля радіолокаційної станції;
- використовували високоефективні (з високим коефіцієнтом поглинання та малою вагою) матеріали, які поглинають та розсіюють електромагнітні хвилі.

Інший метод приховування енергії, який широко використовується для захисту об'єктів від радіолокаційного спостереження, — це створення перешкод.

Найпростішою перешкодою є гармонійне коливання радіолокаційної частоти, яке створює генератор в місці знаходження об'єкта, що охороняється. Оскільки діаграма спрямованості випромінювання антени радара зазвичай має бічні пелюстки, такі перешкоди можуть викликати шумове засвічення екрана локатора.

Більш структурно складною є модуляція перешкоди за допомогою одного або кількох змінних параметрів. Модульовані перешкоди можуть бути безперервними та імпульсними, а їх спектр близький до радіолокаційного випромінювання. За ефектом впливу перешкоди поділяються на ті, що маскують зображення об’єкта зашумленням екрану радара, та ті, що імітують помилкові світлові плями. Змінюючи структуру та час затримки змодельованої перешкоди, можна змінити форму, розташування та характер руху помилкового засвічення на екрані локатора [16].

Радіопоглинаючі покриття.

Більшість сучасних методів розвідки та управління зброєю функціонують шляхом отримання та обробки інформації, отриманої у вигляді відбитого від об’єктів у видимому, інфрачервоному та радіолокаційному діапазонах електромагнітного випромінювання. Одним з найефективніших способів протидії таким засобам є розміщення їх між захищеними об'єктами фізичного середовища, здатними взаємодіяти з електромагнітним випромінюванням, послаблюючи сигнал або спотворюючи інформацію, що передається противнику за допомогою випромінювання. З цією метою, крім маскування аерозолями, використовуються матеріали, що поглинають радіовипромінювання.

Поглинання, локалізація та інтерференція електричних хвиль спостерігаються при взаємодії електромагнітних полів з матеріалом, що покриває поверхню об’єкта. Поглинання послаблює поле падаючої хвилі завдяки перетворення електромагнітної енергії в теплову внаслідок діелектричних і магнітних втрат.

Розсіювання відбувається завдяки перетворенню потоку електромагнітної енергії певного напрямку в потоки різних напрямків, включаючи ті, що не досягнуть прийомних антен засобів розвідки.

Інтерференція радіохвиль характеризує здатність радіопоглинаючого матеріалу відбивати хвилі в напрямку найбільшого вторинного випромінювання від нього.

Радіопоглинаючі матеріали поділяються на поглинаючі лакофарбові покриття, гнучкі поглинаючі матеріали та конструкційні поглинаючі матеріали.

Радіопоглинальні лакофарбові матеріали на основі рецептури РПР-02ЛК створені на основі спеціального рецепту, що наноситься на поверхню об'єктів для зниження радіолокаційної видимості об'єктів військової техніки.

Комплекти спеціального призначення, що базуються на гручких радіопоглинальних матеріалах використовуються на об'єктах військової техніки з метою зменшення радіолокаційної помітності.

Щоб ефективно енергетично приховати об’єкти від радіолокаційного спостереження, їх поверхні покривають матеріалами, що забезпечують градієнтне та інтерфераційне поглинання випромінюваної електромагнітної енергії.

Градієнтне поглинання забезпечується кількома шарами матеріалів, кожен з яких складається з основи-діелектрика (каучуку, пінопласту та ін.) та наповнювача (карбонільного заліза, графітного порошку, вугільного пилу тощо), який поглинає електромагнітну енергію. Зовнішній шар поглинача має діелектричну проникність, близьку до 1, та має гофровану структуру або шипи для збільшення площі. Діелектрична проникність зростає у кожному наступному шарі. Коли електромагнітна хвиля проникає через поглинаючий матеріал, її енергія зменшується, а напрямок змінюється. Через спотворення напрямку поширення хвилі її шлях у поглинаючому матеріалі стає довшим, тому поглинання збільшується. Наприклад, покриття з пористих скляних волокон товщиною 12,7 мм може поглинатиме до 99% енергії електромагнітного поля в сантиметровому діапазоні довжин хвиль.

Іншим типом радіопоглинаючого матеріалу є інтерференційний, що створює накладання прямих (падаючих) та відбитих від об'єктів електромагнітних хвиль. Найпростіший поглинаючий матеріал цього типу складається з діелектричного шару і електропровідної плівки. Тип і товщина діелектрика, магнітна проникність і хвильовий опір плівки обираються таким чином, щоб зсув фаз між падаючою і відбитою хвилями був близький до 180°. Внаслідок суперпозиції прямої хвилі та відбитої хвилі в діелектрику утворюються стоячі хвилі, а падаюча хвиля пригнічується відбитою хвилею. В результаті електронний парамагнітний резонанс

об'єкта різко падає. Проте цей ефект спостерігався у дуже вузькому діапазоні довжин хвиль. Для розширення діапазону використовується багатошарові матеріали, кожен із шар яких розрахований на свій діапазон довжин хвиль випромінюваних електромагнітних хвиль. Але багатошарові матеріали, які забезпечують ефективне поглинання в досить широкому діапазоні частот, товсті і важкі.

Сучасні поглинаючі матеріали використовують обидва способи зниження енергії відбитих електромагнітних хвиль. Наприклад, керамічний феритовий радіопоглинаючий матеріал з товщиною феритного шару 0,83 см має коефіцієнт відбиття 10% в діапазоні довжин хвиль 30-300 МГц. Виготовлений з досить легкого радіопоглинаючого матеріалу у вигляді багатошарової тканини [16].

Камуфляжне радіопоглинаюче покриття, що містить основу у вигляді сітки з діелектричного матеріалу, на якій закріплені діелектричні елементи, пов'язані з видовженими провідними елементами, що мають різну орієнтацію в просторі, що характеризується тим, що кожен діелектрик виконаний в формі смужки або стрічки з N прямокутних струмопровідних елементів, положення яких засновані на орієнтації більших осей. Даний винахід відноситься до галузі озброєння, особливо до камуфляжа, який використовують для військової техніки та бункерів.

Відомо камуфльоване радіопоглинаюче покриття (n EN № 43575 A, F41H3/02), яке містить гнучку підкладку, у вигляді сітки з діелектричного матеріалу, що являє собою нерухомий гнучкий поглинач електромагнітного випромінювання у формі смужок тканини з суцільного полотна з розрізами по довгих краях у вигляді бахроми, частина з яких згорнуті по спіралі. Тканина покрита водовідштовхувальним діелектричним матеріалом і виготовлена з ниток, що містять полімерний діелектричний матеріал, нитки виготовлені з волокон, половина з яких поглинають, а половина розсіюють вхідні радіохвилі. Частина смужок бахроми виконується під кутом від 90 до 150 градусів до поздовжньої осі.

Узгоджується з істотними характеристиками заявленого радіопоглинаючого камуфляжного покриття, на основі у вигляді сітки з діелектричного матеріалу, на якій закріплені діелектричні елементи, пов'язані з довгастими майже паралельними на

довжині від 3 до 12 мм і на відстані один від одного від 2 до 8 мм за послідовністю випадкових значення довжин і відстаней у цих діапазонах [19].

Пінополіуретан давно використовується для маскування важливих об’єктів, коли умови їх експлуатації пред’являють підвищені вимоги до пінним покриття – обмеження за вагою, розмірами (товщиною покриття), необхідність розширення діапазону поглинаючої дії (до дециметрів включно).

Незважаючи на більш високу вартість оригінальних компонентів, пінополіуретанові покриття мають багато переваг перед водо-органічними та водо-полімерними пінними покриттями, до яких належать:

- зберігають маскуючі властивості на невизначений термін;
- вища продуктивність і міцність;
- можливість використання при низьких температурах;
- більший час зберігання компонентів;
-здатність створювати покриття зі специфічними властивостями радіопоглинання в широкому діапазоні довжин хвиль.

Пінні покриття мають хороше зчеплення з будь-якою поверхнею і є стійкими до більшості органічних розчинників.

Покриття дуже гарно маскуються в радіолокаційному діапазоні, знижують яскравість об'єктів в ІЧ діапазоні до фонового рівня та ефективність лазерної та спектральної розвідки, дозволяють фарбувати в кольори типового фону місцевості та зменшують вплив на техніку та об'єкти.

Самі маскуючі засоби хімічно нейтральні і не мають обмежувального впливу на бойові дії екіпажу та функціонування об'єктів, що охороняються [16].

Покриття, що використовують ефект повного проходження хвилі в інше середовище

Цей тип покриття заснований на властивості певних матеріалів не відбивати хвилі, що падають під кутом, який називається кутом Брюстера.

Коефіцієнт відбиття R залежить від поляризації падаючої хвилі. Для компонентів вектора Е, перпендикулярних ($E_\perp$) і паралельних ($E_\parallel$) площині падіння, значення коефіцієнта відбиття визначається за формулами:

$$R_{\parallel} = \frac{tg^2(\Theta - \Theta')}{tg^2(\Theta + \Theta')}$$

$$R_{\perp} = \frac{sin^2(\Theta - \Theta')}{sin^2(\Theta + \Theta')},$$

де Θ –кут падіння електромагнітної хвилі, а Θ' – кут заломлення електромагнітної хвилі.

Коли площина поляризації збігається з площиною падіння, площина, визначена вектором Пойтинга і нормаллю до границі розподілу, відбиття не відбувається. Оскільки $R_{\parallel} = 0$ при $tg(\Theta + \Theta') = \infty$, то $(\Theta + \Theta')$ має дорівнювати $\pi/2$.

Ця вимога означає, що промені відбиття і заломлення перпендикулярні один одному, а хвиля повністю переноситься в інше середовище (покриття). Фізично це можна пояснити тим, що поле падаючої хвилі змушує електрони коливатися в матеріалі покриття. Електрони коливаються в напрямку електричного вектора, який поширюється в покритті хвилі. Напрямок диполів перпендикулярний напрямку поширення та викликають вторинну хвилю (відбиту хвилю). Оскільки збуджений диполь (коливальний електрон) не випромінює вздовж своєї осі, то в дзеркальному відображенні виникає негативний потік енергії. На рисунку 2.2 це відповідає напрямкам стрілок, які умовно зображають положення диполів.

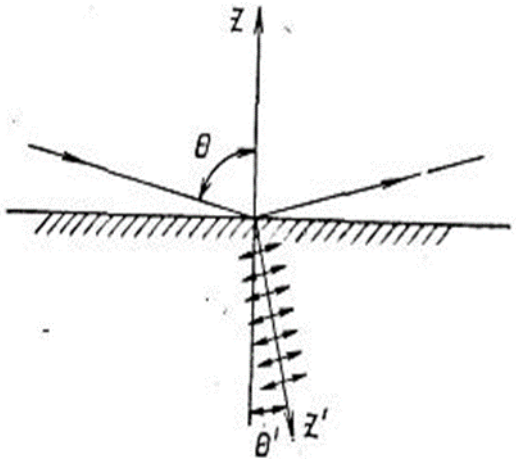

Рисунок 2.2 Принцип дії покриття, що використовує ефект повного проходження електромагнітної хвилі в інше середовище

На відміну від першого випадку, кут Брюстера при перпендикулярній поляризації існує не у всіх середовищах. Наприклад, він відсутній у діелектриків.

Плоскі хвилі з круговою та еліптичною поляризацією з двома ортогональними компонентами $E_{\perp}$ і $E_{\parallel}$, відбиваються.

Однак під час відбиття співвідношення між компонентами $E_{\perp}$ і $E_{\parallel}$ істотно змінюється. Якщо циркулярно поляризована хвиля падає на покриття під кутом Брюстера, то відбита хвиля стає лінійно поляризованою.

Ефективним буде застосування покриття, що використовує ефект повного проходження електромагнітної хвилі, якщо відповідним чином підібрати кут його встановлення, попередньо визначивши кут падіння хвилі та кут Брюстера покриття.

Виходячи з того, що діапазон кутів падіння електромагнітної хвилі на границю розподілу, при якому відсутня відбита хвиля, має різну величину, необхідно підібрати значення імпедансу, що дозволить розширити цей діапазон досягнувши його максимуму [20].

2.5 Способи активного подавлення сигналів радіолокаторів

В активній радіолокації з пасивною відповіддю прийнятий радіосигнал формується вторинним випромінюванням (відбиттям) цілями радіохвиль, що випромінюються радіолокатором. Активна робота радарів тепер вимагає використання радіолокаційного випромінювання. Радіопередаючий пристрій генерує потужні високочастотні коливання, що передаються в напрямку цілі через антену передавача $A_{п}$. Передані коливання (зондовий сигнали), що досягли цілі, відбиваються від неї. Частина енергії відбитого сигналу приймається антеною приймача $A_{пр}$ і надходить в радіоприймач для аналізу та отримання інформації про ціль.

Активна радіолокація з активною відповіддю – вид активної радіолокації, коли сигнал відповіді формується спеціальним, попередньо встановленим на об'єкті реагування, відповідачем наприклад, система реагування літака «свій-чужий». Крім ідентифікації цілі, така система також надає додаткову інформацію про висоту «свого» літака, бортовий запас палива тощо, що є надзвичайно важливими для забезпечення безпеки польотів.

Радіолокаційне виявлення об'єктів активною радіолокаційною системою засноване на відображенні сигналу радіолокаційного зондування від станції. Коли на

предмет падає електромагнітна енергія, на його поверхні утворюється електричний струм, якщо він містить провідник, або електричний заряд, якщо він містить діелектрик. В результаті об'єкт стає джерелом вторинного випромінювання електромагнітних хвиль. Тому об’єкт виявлення формує вторинне поле випромінювання, яке змінює характеристики сигналу виявлення, що є джерелом інформації про об’єкт.

Будь-який наземний об'єкт є складним радіолокаційним об'єктом, оскільки його зовнішня поверхня складається з багатьох площин, орієнтованих по-різному відносно напрямку радара. Кожна площина є елементарним відбивачем, а загальне поле вторинного випромінювання від об’єкта формується інтерференцією радіохвиль, розсіяних цими відбивачами. Отже, електронний парамагнітний резонанс об’єкта залежить від таких факторів:

• положення об'єкта відносно радара;

• габаритні розміри об'єкта;

• форма, розміри та взаємне розташування основних відбивачів, що утворюють зовнішню поверхню;

• матеріал і чистота обробки зовнішньої поверхні;

• довжина хвилі зондуючого сигналу [17].

Відповідно до джерела [18] основними напрямками захисту від активних і пасивних радіолокаційних систем є:

• оптимізування архітектури зовнішньої поверхні;

• монтаж і нанесення радіопоглинаючих покриттів і матеріалів;

• використання радіопоглинаючих, розсіювальних, теплозахисних щитів та сіток.

Перспективним підходом до зниження демаскуючих факторів об’єктів у широкому діапазоні довжин хвиль є використання широкосмугових маскувальних сіток, які не тільки допомагають змінити зовнішній вигляд об’єкта, що охороняється, але й зменшують його відбивні властивості та зменшують контраст об’єкту відповідно до фону.

Використання відволікаючих пристроїв може захистити радіолокаційні системи шляхом зміщення фазового центру некогерентних або когерентних систем передавачів.

При використанні відволікаючих пристроїв для захисту радіолокаційної системи спостереження необхідно враховувати:

• радіолокаційна система веде циклічний пошук по колу області, тому отримана картина відображення буде постійно змінюватися, а область буде опромінена бічними пелюстками різного рівня потужності та значення фази сигналу;

• керування фазами активних передавачів дуже складний, і, крім того, точність визначення координат протирадіолокаційних ракет радіолокаційними системами не дозволяє розрахувати співвідношення фаз, необхідні для такого контролю;

• оглядові радіолокаційні системи майже ніколи не використовуються в одному місці як частина групи подібних радіолокаційних систем.

Таким чином, неможливо збільшити похибку наведення протирадіолокаційних ракет, використовуючи відомі методи радіаційного контролю або регулювання фази випромінювача для групи однотипних радіолокаційних систем. Застосування методів активного захисту на основі пристроїв відволікання дозволяє значно підвищити термін служби радіолокаційних систем (на порядок зменшити ймовірність пошкодження) [17].

3 РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ БЕЗПЕКИ НА ОБ'ЄКТІ З КРИТИЧНОЮ ІНФРАСТРУКТУРОЮ

3.1 Опис об'єкту

Об'єктом охорони являється відділення банку, що розташований на першому поверсі житлового будинку, загальною площею 295м^2. Всього в офісі знаходиться 16 приміщень: приміщення охорони та ІТ, сховище, архів, каси, дві переговорні кімнати, серверна, управління бізнесом, зона кредитного відділу та обслуговування юридичних осіб, приймальне приміщення, гардеробна, санвузол, зона відпочинку та кабінет директора.

Вікна які наявні лише в кабінеті директора, одній переговорній та кредитному відділі заклеєні непрозорою плівкою з інформацією про банк, що пропускає тільки світло. На вхідних дверях встановлені захисні ролети. Усі внутрішні двері, де використовується пропуск за Wiegand картою та відбитком пальця, є броньованими. Висота стелі всіх приміщень становить 3 м. Коридори, що ведуть до службових приміщень, а також сховища, кас та додаткового виходу, переговорні обладнанні зчитувачем Wiegand карт. Крім того вхід до сховища, архіву, кабінета директора і серверної здійснюється за відбитком пальця та паролем.

Відділення працює з 9-00 до 18-00 у будні дні без перерв. На час роботи для відвідувачів відкриті двері. В неробочий час знаходження відвідувачів всередині приміщення банку не допускається.

По закінченню робочого дня, охороною вмикається сигналізація та опускаються захисні ролети на вхідні двері.

На рис. 3.1 зображено загальний план приміщення, де вказані основні позначення.

датчик пожежної сигналізації камера відеоспостереження

датчик розбиття скла панорамні камери відеоспостереження

магнітний замок біометричний замок скляні поверхні

Рисунок 3.1 – Загальний план приміщення з охоронною системою

3.2 Підбір обладнання

В даному розділі було здійснено підбір обладнання, які будуть використано в проектованій системі зважаючи на їх характеристики.

Для початку розглянемо за якими характеристиками були обрані відеокамери. Перш за все це співвідношення якості та ціни. Далі йдуть місце встановлення камери, кількість мегапікселів та кут огляду.

В СКУД зазвичай використовуються IP-камери, тому далі представлені рис 3.2 зображено камери, які були використанні для порівняння.

Рисунок 3.2 – IP-камери

В табл 3.1 порівнюються основні технічні характеристик вище зображених IP-камер.

Таблиця 3.1. Основні технічні характеристики

Характеристики	ATIS ANVD-5MIRP-20W/2.8A Prime	Uniview IPC3614LR3-PF28-D	Dahua DH-HAC-EW2501P	GV-075-IP-ME-DIA20-20 (360) POE
Ціна, грн	2264 грн	2400	4320	1966
Розширення	2560x1944	2592x1520	2592 x 1944	3096x2202
ІЧ-підсвітка	+	+	+	+
Дальність дії ІЧ	20 м	30 м	28 м	20 м
Кут огляду	98°	104.4°	180°	170°

Зважаючи на потреби даної розробки, після аналізу характеристик відеокамер було обрано, Uniview IPC3614LR3-PF28-D для всіх приміщень та Dahua DH-HAC-EW2501P для центрального приймального залу.

Тим же чином проводимо вибір інших компонентів для створення комплексної системи захисту.

Рисунок 3.3 - Контролери обрані для порівняння

В таблиці 3.2 наведено найважливіші характеристики порівнювальних контролерів.

Таблиця 3.2. Характеристики контролерів для порівняння

Характеристики	Dahua DHI-ASI1201E	Dahua DHI-ASA1222G	Dahua DHI-ASI1212A-D(V2)	Dahua DH-ASC1204B
Число подій що зберігаються в пам’яті	150 000	100 000	150 000	300
Зчитувач відбитка пальця	-	+	+	-
Кількість зчитувачів що підключаються	30 000	1000	30 000	100
Ціна, грн	2700	4860	4732	2717

Після аналізу характеристик контролерів визначено найкращий варіант для системи – це контролер Dahua DHI-ASI1201E, тому що найважливішим критерієм є

якомога більша кількість збережених подій в пам’яті, кількість можливих підключених зчитувачів та відповідність ціни до можливостей.

На рис. 3.4 зображено зчитувачі, які порівнювались.

Рисунок 3.4 – Зчитувачі, які обрані для порівняння

В таблиці 3.3 наведено найважливіші технічні характеристики для зчитувачів.

Таблиця 3.3 – Характеристики зчитувачів, що використовувались для порівняння

Характеристики	U-PROX SL MAXI	ATIS FPR-3	ATIS FPR-4	ATIS PR-08 EM-W
Ціна, грн	2256	1560	2074	340
Матеріал корпусу	Пластик	Пластик	Пластик	Пластик
Частота	125кГц	125кГц	125кГц	125кГц
Індикація	Світлова	Світлова	Світлова	Світлова та звукова

За результатами аналізу зчитувачів було обрано зчитувач для карт було ATIS PR-08 EM-W.

Рисунок 3.5 - Модель пожежного сповіщувача Dahua FAD122A-W

Таблиця 3.4 – Характеристики пожежного сповіщувача

Тип сигналу тривоги	Аудіо та оптична сигналізація
Робоча частота	433 МГц
Світлова Індикація	Стандартний стан: Червоний світлодіод блимає кожні 90 секунд. Стан тривоги: Червоний світлодіод блимає, і зумер безперервно подає звуковий сигнал Низька напруга: Червоний світлодіод блимає один раз кожні 90 секунд, а звуковий сигнал – кожні 90 секунд.
Принцип роботи	фотоелектричний
Ціна	540 грн
Температура експлуатації	-10°C - +55°C
Термін служби	+- 3 роки

Рисунок 3.6 - Електромагнітний замок ZKTECO LM-3505 C LED ідентифікацією та датчиком контролю дверей

Таблиця 3.5 – Характеристики електромагнітного замка

Принцип роботи	Магнітна взаємодія
Сила утримання	350 кг
Матеріал корпусу	Анодований алюміній
Живлення	12 В
За відсутності струму	Відкритий
Розміри	186 х 45 х 30 мм
Додатково	Вбудовані датчики LED ідентифікації та контролю стану дверей
Ціна	1218 грн

Рисунок 3.7 - Доводчик дверей RYOBI D-1504 STD

Таблиця 3.6 – Характеристики доводчика дверей

Тип дверного доводчика	Класичний дверний доводчик з ліктьовою тягою
Вага двері	До 80 кг
Ширина двері	До 1100 мм
Тип важелю	Колінчастий важіль
Кут відкриття двері	180º
Ціна	1140 грн

Рисунок 3.8 – Датчик розбиття скла Satel INDIGO

Таблиця 3.6 – Характеристики датчика розбиття скла

Тип датчика	Провідний, акустичний
Робоча напруга	12 В
Діапазон робочих температур	-30…+55 °С
Захист від взлому	+
Ціна	455 грн

Для захисту приміщень підвищеної секретності, таких як сховище, архів, серверна та кабінет директора було обрано автономний Host Dahua DHI-ASI1212A-D(V2), що забезпечу доступ по відбитку пальця та паролю, який зображений на рис. 3.9.

Зчитувачі має сенсорну клавіатуру з підсвіткою, голосові підказки, швидкість реагування на ідентифікатор складає менше ніж 0,5 секунди, крім того здатний зберігати до 3000 відбитків пальців. Математична статистика FAR менша за 0,00004%, а FRR менша за 0,15%, що є гарантією більшої надійності та безпечності.

Рисунок 3.8 – Зчитувач Dahua DHI-ASI1212A-D(V2)

Крім того, у всіх приміщення були встановлені інфрачервоні датчики руху SWAN QUAD, дальність роботи яких складає 18 метрів. Він зображений на рис 3.10.

Рис. 3.10 ІЧ-датчик CROW SWAN QUAD

3.3 Опис проектованої комплексної системи захисту

В даній роботі основному було використано технології захисту таких компаній:

- Uniview;
- ATIS;
- Dahua.

Uniview - першопрохідник і лідер в галузі IP-відеоспостереження. Спочатку компанія представила рішення IP-відеоспостереження в Китаї, зараз Uniview третя за величиною компанія на ринку Китаю. У 2018 році Uniview посіла 4 місце на глобальному ринку у своїй галузі.

Uniview пропонує комплексні продукти для IP-відеоспостереження, у тому числі IP-камери, IP-відеореєстратори, енкодери, декодери, клієнтське ПЗ та додатки для зберігання даних, що охоплюють різні сфери, включаючи роздрібну торгівлю, спостереження в будинках, промисловість, освіта, комерційний сектор , міську безпеку тощо [21].

Інформація про Dahua. Dahua Technology – виробляють одні з найкращих пристроїв та системи безпеки, є постачальниками послуг відеоспостереження та контролю доступу.

За даними релізу IHS на 2016 рік, Dahua володіє другою за величиною часткою ринку відеоспостереження. За даними журналу A&S Security, компанія займає четверте місце у світі за обсягом доходу від продажу обладнання для відеоспостереження.

Крім цього, Dahua є одним з провідних постачальників OEM та ODM послуг для компаній, що займаються системами безпеки. Dahua є творцем стандарту відеоспостереження HDCVI – передачі аудіо- та відеоданих по коаксіальному кабелю [22].

Установка КСБ на дослідному об’єкті містить розробку схеми розташування пристроїв, що входять в систему такі як:

- зчитувачі;
- контролери;
- пожежні датчики;

- ІЧ-датчики та датчики розбиття скла;
- ідентифікатори;
- відеокамери.

3.4 Економічний розрахунок

Перелік засобів захисту, що були використані в розробці:

- 20 IP-камер Uniview IPC3614LR3-PF28-D по 2 400грн/шт та 2 Dahua DH-HAC-EW2501P 4 320 грн/шт;
- 1 контролер Dahua DHI-ASI1201E, який коштує 2700 грн;
- 7 зчитувачів, для Wiegand карт, ATIS PR-08 EM-W, по 340 грн;
- 4 зчитувачі, для ідентифікації відбитку пальця, Dahua DHI-ASI1212A-D(V2), вартість якого 4 732 грн;
- 34 пожежних датчики Dahua FAD122A-W, що коштують по 540 грн;
- 12 електромагнітних замки ZKTECO LM-3505 C LED по 1218 грн;
- 17 доводчиків дверей RYOBI D-1504 STD по 1140 грн;
- 7 датчиків розбиття скла Satel INDIGO за 455грн/шт;
- 20 ІЧ-датчиків CROW SWAN QUAD по 327 грн;
- Програмне забезпечення GG-SS-2002-Enterprise, ціна якого 7420 грн;
- Приблизна ціна за установку всіх пристроїв 30050 грн.

В загальній сумі затрати становлять:

20*2400 + 2*4320 + 2700 + 7*340 + 4*4732 + 34*540 + 12*1218 + 17*1140 + 7*455 + 20*327 + 7420 + 30050 = 180 199 (грн)

Окупність даної системи складе близько 1-1,5 років.

ВИСНОВКИ

В даній кваліфікаційній роботі було розроблено комплексну систему безпеки для об’єкта з критичною інфраструктурою.

В першому розділі було розглянуто основні відомості про КСБ. Описано основні складові системи, її переваги та необхідність встановлення комплексних систем.

Розказано про основні компоненти КСБ, перш за все про СКУД та її складові. Були наведені загальні відомості про контролери, ідентифікатори, зчитувачі – пристрої для обробки інформації, що надходить з ідентифікаторів, виконавчі пристрої.

Описані основні принципи на яких базується проектування та впровадження КСБ. А саме комплексність та системність – виявлення всіх можливих загроз, повний аналіз уразливостей системи безпеки об’єкта та розроблення системи щодо їх запобігання та науковість та обґрунтованість – побудова СБ з використанням ефективно обґрунтованих наукових рішень. Наприклад, для вибору технічних засобів КСБ основну увагу слід приділяти створенню запасу часу достатнього для адекватного прийняття рішень та реагування на непередбачувану ситуацію. Ще одним принципом є рівномірність та багато рубіжність – використання декількох просторових границь чи методів захисту однакового рівня безпечності. Також враховується людський фактор.

В другому розділі було представлено інформацію про відеоспостереження. Розказано про способи та засоби протидії спостереженню у оптичному діапазоні хвиль. Наведені види та особливості маскування у видимому та інфрачервоному діапазонах та способи і засоби протидії радіолокаційному та гідроакустичному спостереженню.

Також було розглянуто способи дезінформування та зашумлення зображення на екрані радіолокатора та способи активного подавлення сигналів радіолокаторів. Приведено приклади устаткування, що використовують на сьогоднішній день у військовій сфері.

В третьому і в останньому розділі було спроектовано, розроблено та приведено загальний план об’єкту, здійснено вибір обладнання для комплексної системи безпеки даного об’єкту. Основні пристрої КСБ були використані із таких компаній для захисту, як Uniview, ATIS та Dahua. Були використані зчитувачі Wiegand карток, зчитувач по відбитку пальця, IP-камери, пожежні датчики, датчики розбиття скла та ІЧ-датчики руху. Також був виконаний аналіз технічних характеристик кожного з пристроїв застосованих в даному проекті.

На завершення було проведено економічний розрахунок для даного проекту. Загалом було розроблено покращення за допомогою КСБ.

Література

1. https://zakon.rada.gov.ua/laws/show/1882-20#Text
2. https://www.nist.gov/cyberframework/framework
3. https://xn--80adgeboqrpy5j.com.ua/
4. https://leatcom.ua/solutions/security-solutions/
5. Оленин Ю.А. К вопросу о категорировании объектов с позиции охранной безопасности / Ю.А. Оленин, С.Ф. Алаухов // Системы безопасности, связи и телекоммуникаций. – 1999. – № 30. – С. 26
6. Системы контроля и управления доступом. Ворона В.А., Тихонов В.А. Серия «Обеспечение безопасности объектов»; Выпуск 2. 2016 г. 272 стр.
7. https://lgx.kz/identifikatory-skud
8. https://jak.koshachek.com/articles/kontroler-skud.html
9. http://um.co.ua/6/6-6/6-63235.html
10. http://ni.biz.ua/7/7_13/7_139957_metodi-i-sredstva-protivodeystviya-nablyudeniyu.html
11. Сучасний засіб маскування військових об’єктів у оптичному, тепловому та радіолокаційному діапазонах»// О.В. Стаховський, К.В. Коритченко, Ю.І. Кістерний, О.Г. Сінько, Д.Ю. Завізіон// Системи озброєння і військова техніка – 2012 – № 1(29).
12. Умение быть невидимым. Конструкция “Контраст КМС” – квинтэссенция маскировочного искусства // DefenseExpress. – 2004. – № 12(37). – С. 189-193.
13. https://www.facebook.com/FutureOfUkraine/posts/786649122168424
14. https://osvita.ua/vnz/reports/dpju/24318
15. https://uadoc.zavantag.com/text/34684.html
16. http://ni.biz.ua/18/18_7/18_70428_radiolokatsionnomu-i-gidroakusticheskomu-nablyudeniyu.html
17. https://journals.indexcopernicus.com/api/file/viewByFileId/603800.pdf
18. Під українським маскувальним покриттям – танка не видно… / М. В. Ткаліч [та ін.] // Винахідник і раціоналізатор. 2002. № 2–3. С. 5–6.

19. http://uapatents.com/3-59168-maskuvalne-radiopoglinayuche-pokrittya.html
20. «Можливості застосування існуючих радіопоглинаючих покриттів до бойових частин ракет»// А.А. Звонко // Академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів.
21. https://unv.net.ua/aboutus/company
22. https://www.dahua.market/#o-kompanii
23. https://smartsec.com.ua/produkty/sistemy-kontrolya-i-upravleniya-dostupom/
24. https://dahua-technology.com.ua/avtonomnyj-host-dahua-dhi-asi1212a-dv2
25. https://nadzor.ua/product/uniview-ipc3614lr3-pf28-d