Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Клименко Світлани Володимирівни*

академічної групи *125м-22з-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка та дослідження системи охорони периметру*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
Кваліфікаційної роботи	д.т.н.,проф. Корнієнко В.І.			
розділів:				
спеціальний	д.т.н.,проф. Корнієнко В.І.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

ДНІПРО
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____2023року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту ***Клименко Світлани Володимирівни*** **академічної групи** ***125м-22з-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності ***125 Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка та дослідження системи охорони периметру***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз принципів побудови сучасних систем охорони приватних об'єктів	03.09.2023 – 10.10.2023
Розділ 2	Розробка та дослідження системи охорони периметру	11.10.2023 – 24.11.2023
Розділ 3	Розрахунок собівартості приймально-контрольного пристрою, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень	25.11.2023 – 04.12.2023

Завдання видано _____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Клименко С.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 100 с., 50 рис., 11 табл., 4 додатки, 22 джерела.

Об`єкт дослідження: процес побудови модернізованої системи охорони периметру приватного об'єкту.

Предмет дослідження: є процес побудови модернізованої системи охорони периметру приватного об'єкту з урахуванняv методики оцінки ризиків кібербезпеки та визначення оптимальної кількості й місць розташування камер відеоспостереження приватної території.

Метою дослідження підвищення ефективності системи охорони периметру приватного об'єкту шляхом осучаснення елементних складових та дослідження автоматизованого проєктування IP Video System Design Tool.

Методи розробки: аналіз існуючих систем та пристроїв охорони периметру, на базі обраних пристроїв проведення модернізації електричної принципової схеми, аналіз захищеності технології Інтернету речей та дослідження системи охорони периметру.

У першому розділі проведено аналіз існуючих пристроїв та систем охорони периметру приватного об'єкту, визначено актуальність та постановка задачі.

У спеціальній частині наведено опис приватного об'єкту, який потребує захисту охорони периметру, розроблено структурну, функціональну та модернізовану електричну принципову схеми приймально-контрольного пристрою системи захисту периметру.

В економічному розділі визначено економічну доцільність розробки та впровадження системи охорони периметру, а також проведено розрахунок витрат та економічний ефект.

Результати дослідження можуть бути застосовані при розробці пристроїв для захисту периметру будь-якої складності.

ПРИЙМАЛЬНО-КОНТРОЛЬНИЙ ПРИСТРІЙ, СИСТЕМА ОХОРОНИ ПЕРИМЕТРУ, ІНФРАЧЕРВОНЕ ВИПРОМІНЮВАННЯ, GSM ОПОВІЩЕННЯ, ВІДЕОСПОСТЕРЕЖЕННЯ.

ABSTRACT

Explanatory note: p. 100, fig. 50, tab. 11, 4 additions, 22 sources.

The object of research: the process of building a modernized system of protection of the perimeter of a private object.

The subject of the study: is the process of building a modernized system of protection of the perimeter of a private object, taking into account the methodology of cyber security risk assessment and determining the optimal number and locations of video surveillance cameras of a private territory.

The purpose of the study increasing the efficiency of the perimeter protection system of a private object by modernizing the elementary components and researching the automated design of the IP Video System Design Tool.

Development methods: analysis of existing perimeter protection systems and devices, modernization of the electrical circuit diagram based on the selected devices, security analysis of the Internet of Things technology and research of the perimeter protection system.

In the first section, an analysis of existing devices and systems for protecting the perimeter of a private facility was carried out, the relevance and formulation of the problem were determined.

In a special part, a description of a private object that needs perimeter protection is provided, a structural, functional and modernized electrical circuit diagram of the receiving and control device of the perimeter protection system is developed.

In the economic section, the economic feasibility of the development and implementation of the perimeter security system is determined, as well as the calculation of costs and economic effect is carried out.

The research results can be applied in the development of devices for perimeter protection of any complexity.

RECEIVING AND CONTROL DEVICE, PERIMETER PROTECTION SYSTEM, INFRARED RADIATION, GSM ALARM, VIDEO SURVEILLANCE

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АЦП – Аналого-цифровий перетворювач, АЦП (англ. Analog-to-digital converter, ADC) – пристрій, що перетворює вхідний аналоговий сигнал в дискретний код (цифровий сигнал), який кількісно характеризує амплітуду вхідного сигналу. Зворотне перетворення здійснюється за допомогою цифро-аналогового перетворювача (ЦАП).

АКБ – Інтелектуальний датчик акумуляторної батареї оцінює поточний стан акумуляторної батареї. Він встановлений на мінусову клему і вимірює струми заряду і розряду, напругу, внутрішній опір і температуру акумулятора.

Веб-інтерфейс – це сукупність засобів, за допомогою яких користувач взаємодіє з веб-сайтом або веб-застосунком через браузер.

ГШР – Група швидкого реагування – це спеціальний підрозділ охорони з певною специфікою роботи.

ДСТУ – Державні стандарти України, які розроблені відповідно до чинного законодавства України, що встановлюють для загального і багаторазового застосування правила, загальні принципи або характеристики, які стосуються діяльності чи її результатів, з метою досягнення оптимального ступеня впорядкованості.

ІЧ-сенсор – Сенсор з чутливим елементом, що реагує на інфрачервоне випромінювання.

ПКП – Приймально-контрольних пристрій

ШС – Шлейф сигналізації.

ПЦС – Пункт централізованого спостереження(ПЦС).

AAC – Advanced Audio Coding

AVI – Audio Video Interleave

DVR – Digital Video Recorder

GSM – Global System for Mobile Communications – це телекомунікаційний стандарт, розроблений у Європі для мобільних мереж другого покоління (2G). З середини 2010-х років це глобальний стандарт, що охоплює 90% ринку та обслуговує більшість мобільних телефонів у світі.

SMS – це послуга обміну (передачі і прийому) короткими текстовими повідомленнями в телекомунікаційних мережах, доступна для більшості мобільних телефонів та інших комунікаційних пристроїв, таких як пейджер, модем, КПК, або навіть настільний комп'ютер (за допомогою функцій програмного забезпечення).

IP-відео реєстратор – це камера відеоспостереження, яка має вбудований веб-сервер, мережевий інтерфейс (Ethernet або Wi-Fi) і яка має можливість підключення до мереж інтернет LAN, WAN, Wi-Fi.

GPRS прилад – це універсальний модуль моніторингу з вбудованим GSM-телефоном, що підтримує технологію 3G. Його можна використовувати як автономний пристрій або для розширення системи охоронної сигналізації або автоматики.

HDMI – High Definition Multimedia Interface

H.264 – Advanced Video Coding

MJPEG – Motion JPEG – покадровий метод відеостиснення.

MPEG-4 – Moving Picture Experts Group.

PCM – Pulse Code Modulation.

Pelco-D – Протокол управління камерою, що використовується в галузі відеоспостереження.

Pelco-P – Протокол управління камерою, що використовується в галузі відеоспостереження

PTZ-камера – Pan / Tilt / Zoom камера

RS-485 – Recommended Standard 485

RS-232 – Recommended Standard 232

TCP/IP – Transmission Control Protocol/Internet Protocol

VGA – Video Graphics Array

Wi-Fi – Wireless Fidelity

ЗМІСТ

ВСТУП

У наш час забезпечення власної безпеки, а також охорони рухомої та нерухомої власності стало не примхою, а необхідністю. Рішення даної задачі можливе тільки за умови грамотного оснащення систем безпеки сучасними високонадійними технічними засобами охорони. Клієнтами охоронних компаній стають все більше людей, це і власники квартир, приватних маєтків, підприємств, організацій, транспортних засобів та навіть стратегічні об'єкти у держаній власності. Попит на новітні та високонадійні системи безпеки зростає, тому компанії виробники таких систем постійно знаходяться в атмосфері жорсткої конкуренції, яка спонукає їх до стрімкого технічного розвитку.

Захист периметру – особливо важливий елемент комплексу заходів безпеки, як для об'єктів ядерно-озброєного комплексу, включаючи атомні електростанції, так і для більш простих господарських об'єктів. Системи охорони периметрів дозволяють отримати найбільш ранню інформацію про проникнення порушника на територію, що захищається, на підставі якої приймаються попереджувальні та оперативні заходи щодо своєчасної нейтралізації можливих протиправних дій на охоронюваному об'єкті. Тому периметрові засоби – головна складова частина всіх комплексів технічних засобів охорони, що є основою будь-якої інтегрованої системи захисту об'єкта.

Система охорони периметру повинна максимально оперативно й точно виявляти місце проникнення порушника. Це важливо для ефективного реагування підрозділів охорони. Система охорони периметру – головний і визначальний фактор припинення можливої взаємодії порушника з головними життєвими центрами особливо важливого об'єкту вже на початковій стадії атаки.

Різноманітність умов застосування периметрових засобів виявлення робить практично неможливим використання будь-якого одного або декількох типів апаратури. Вибір оптимального комплексу засобів виявлення для охорони периметру визначається також конфігурацією і конструкцією периметрової огорожі, наявністю і розмірами так званої «зони відчуження», поведінковими

моделями потенційного порушника: його можливостями подолання рубежів охорони, характером зовнішніх факторів, техногенними умовами роботи системи охорони, вимогами до маскування сигналізаційних систем, ну і, звісно, фінансовими можливостями замовника. Ці умови і визначають необхідність створення широкої номенклатури периметрових засобів виявлення.

В даний час на ринку систем безпеки пропонуються сотні охоронних пристроїв, які можуть виконувати будь-які задачі, як вітчизняного, так і зарубіжного виробництва [1].

Виходячи з вищеописаного можна стверджувати, що актуальність роботи полягає у тому, що на сьогоднішній день забезпечення безпеки є необхідністю. Тому попит на новітні та високонадійні системи безпеки зараз тільки зростає. Саме тому розробка вдосконаленої моделі системи охорони периметру приватного об'єкту, дослідження системи охорони периметру є актуальною темою кваліфікаційної роботи магістра.

Об`єкт дослідження: процес побудови модернізованої системи охорони периметру приватного об'єкту.

Предмет дослідження: є процес побудови модернізованої системи охорони периметру приватного об'єкту з урахуванням методики оцінки ризиків кібербезпеки та визначення оптимальної кількості й місць розташування камер відеоспостереження приватної території.

Метою дослідження підвищення ефективності системи охорони периметру приватного об'єкту шляхом осучаснення елементних складових та дослідження автоматизованого проєктування IP Video System Design Tool.

Для досягнення мети необхідно провести розгляд основних елементів базової охоронної системи та визначити можливість їх використання при створенні охоронної системи приватного об'єкту. Провести дослідження напрямків забезпечення захищеності об'єкту, визначення на їх основі основних частин для проєктування системи охорони за допомогою інженерних та програмних рішень, що використовують для проєктування системи охорони периметру.

Методи розробки: аналіз існуючих систем та пристроїв охорони периметру, на базі обраних пристроїв проведення модернізації електричної принципової схеми, аналіз захищеності технології Інтернету речей та дослідження системи охорони периметру.

Наукова новизна результатів полягає у розробці модифікованого приймально-контрольного пристрою системи захисту периметру приватного будинку, а також представленої методики оцінки ризиків кібербезпеки та застосування сучасних додатків для проєктування та монтажу відеосистем охорони приватної прибудинкової території.

Практична цінність роботи полягає у тому, що було запропоновано використання системи автоматизованого проєктування IP Video System Design Tool, яке дозволило швидко знайти оптимальну кількість і розташування камер відеоспостереження приватної території, виконати розрахунок системи відеоспостереження, оцінити довжину кабелів і відобразити на плані місцевості зони ідентифікації, розпізнавання, детектування, змоделювати перешкоди в 2D і 3D для виявлення мертвих зон.

У першому розділі проведено аналіз існуючих пристроїв та систем охорони периметру приватного об'єкту, проведено аналіз захищеності систем охорони периметру та висвітлені проблеми ризиків, що виникають в таких системах, визначено актуальність та постановка задачі.

У спеціальній частині наведено опис приватного об'єкту, який потребує захисту охорони периметру, розроблено структурну та функціональну схеми, проведено вибір та обґрунтування електричної принципової схеми приймально-контрольного пристрою системи захисту периметру. Представлена методика оцінки ризиків кібербезпеки та досліджена система охорони периметру.

В економічному розділі визначено економічну доцільність розробки та впровадження системи охорони периметру, а також проведено розрахунок витрат та економічний ефект.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Сучасна концепція захисту об'єктів

В основі систем захисту об'єктів і організації їх функціонування лежить принцип створення послідовних рубежів, в яких загрози повинні бути своєчасно виявлені. Визначення послідовних рубежів (або захисних зон) з одночасним виявленням загроз за кожною конкретною зоною дозволяє вибрати технічні засоби забезпечення безпеки для найбільш ефективного вирішення завдань охорони об'єкта. Такі рубежі (або зони безпеки) повинні розташовуватися послідовно – в загальному випадку, від огорожі навколо території об'єкта до критичних елементів об'єкта, таких як сейфи, сховища цінностей та інформації, вибухонебезпечні матеріали, зброя тощо (Рис. 1.1). Чим складніше і надійніше захист кожної зони безпеки, тим більше часу буде потрібно порушнику на її подолання і тим більше ймовірність того, що розташовані в зонах засоби виявлення загроз (ЗВЗ) подадуть сигнал тривоги. Отже, у служби охорони буде більше часу для визначення причин тривоги і організації ефективної протидії загрозам [3]. Початковою зоною забезпечення безпеки є прилегла територія. Вона не є частиною об'єкта і може використовуватися порушниками для підготовчих робіт з організації несанкціонованих дій, наприклад, для спостереження і вивчення режиму охорони об'єкта і його охоронних структур. Тому прилегла територія також може розглядатися як зона забезпечення безпеки і контролюватися, в першу чергу, засобами відеоспостереження. Першою зоною є зовнішній периметр території об'єкта охорони. Загрози: подолання периметральних засобів інженерно-технічної захищеності (в тому числі їх руйнування) для проникнення на територію з метою вторгнення на об'єкт. У першій зоні можуть використовуватися засоби інженерно-технічної захищеності (загородження, паркани), відеоспостереження, засоби периметрального захисту в

складі системи охоронної сигналізації, а також фізична охорона, тобто працівники власної служби безпеки або співробітники позавідомчої охорони.

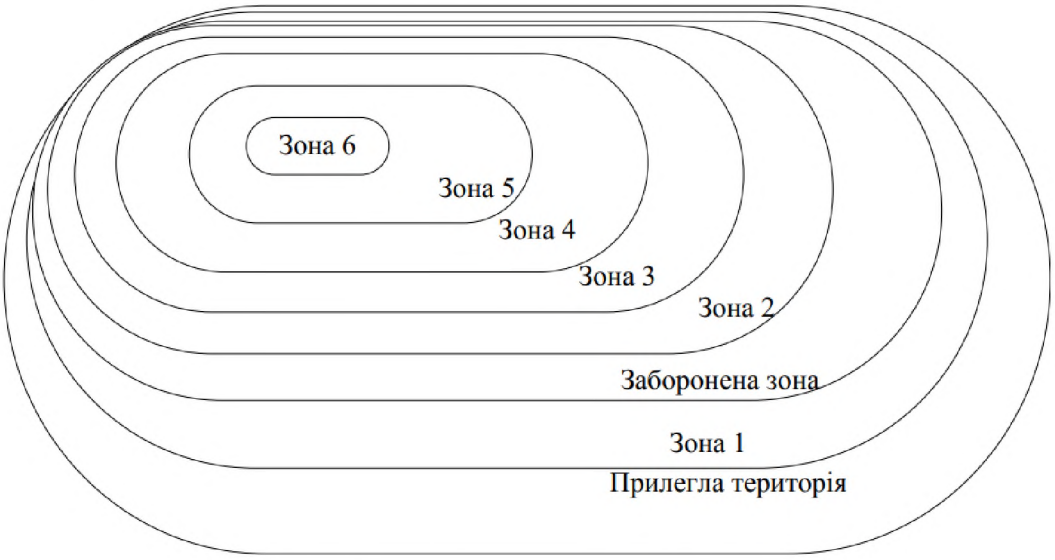

Рис. 1.1 – Розташування зон забезпечення безпеки

Заборонена зона (або зона відторгнення) за необхідності організовується уздовж основної огорожі периметра з внутрішньої сторони території об'єкта і призначена для розміщення на ній технічних засобів охорони (ТЗО) і виконання службових завдань особовим складом підрозділів охорони. Заборонена зона повинна бути ретельно спланована і розчищена. В ній не повинно бути ніяких будівель, предметів і рослинності, які ускладнюють застосування ТЗО і дії сил охорони. Заборонена зона може бути використана для організації охорони об'єкта за допомогою сторожових собак. Для забезпечення нормальної роботи ТЗО на відкритих майданчиках та периметрів об'єктів ширина забороненої зони повинна перевищувати ширину їх зони виявлення. Друга зона охорони включає в себе територію, на якій знаходиться об'єкт, що охороняється. Загрози: несанкціоноване проникнення на територію з метою подальшого вторгнення на об'єкт. При захисті даної зони використовується комплекс заходів, що складається з технічних засобів відеоспостереження і охоронно-пожежної сигналізації (ОПС). Третю зону охорони становлять елементи периметра об'єкту, що охороняється, будівлі або приміщення: будівельні конструкції ПО периметру

будівлі або приміщень об'єкта, тобто всі віконні і дверні прорізи; місця введення комунікацій, вентиляційні канали; виходи до пожежних драбин; несучі та не несучі стіни; вентиляційні короба, димоходи. Загрози: несанкціоноване проникнення в будівлю через слабко укріплені, незаблоковані засобами сигналізації ділянки, а також підготовчі роботи для подолання технічних засобів забезпечення безпеки. Ця зона контролюється засобами відеоспостереження, ОПС і фізичної охорони. Четверта зона – внутрішній простір приміщень об'єкта. За допомогою технічних засобів системи контролю та управління доступом в четвертій зоні повинні бути організовані пропускний режими. Для цього виконується поділ об'єкта на три основні зони доступу [11]:

– перша зона (зона вільного доступу) – будівлі, території, приміщення, доступ до яких персоналу, відвідувачам і особам, які проживають на об'єкті, не обмежений;

– друга зона (зона обмеженого за часом або рівнем пріоритету доступу) – приміщення, доступ до яких дозволений в обмежений час (наприклад, покупцям магазину в робочі години, персоналу – відповідно до режиму роботи) або обмеженому складу персоналу, а також відвідувачам об'єкта за разовими перепустками або в супроводі персоналу об'єкта;

– третя зона – спеціальні приміщення об'єкта, доступ до яких мають строго певні співробітники і керівники (наприклад, приміщення керівництва об'єкта і охорони), а також приміщення безпосереднього зосередження і зберігання матеріальних та інших цінностей.

Пропуск користувачів на об'єкт через пункти контролю доступу повинен здійснюватися: в першій зоні доступу за однією ознакою ідентифікації; у другій зоні доступу за двома ознаками ідентифікації (наприклад, електронна картка і ключ від механічного замка); в третій зоні доступу не менше, ніж за двома ознаками ідентифікації. Загрози: несанкціоноване проникнення в приміщення з матеріальними і фінансовими ресурсами; виведення з ладу засобів відеоспостереження і ОПС; установка підслуховуючих та інших пристроїв знімання інформації; нейтралізація працівників охорони або служб безпеки для подальшого нападу на касирів з метою заволодіння грошовими коштами або

іншими матеріальними або фінансовими ресурсами; захоплення заручників; проникнення в комп'ютерну мережу підприємства зі злочинними цілями; фізичне знищення керівників об'єкта з метою розвалу підприємства як конкурента; напад на співробітників охорони для вчинення терористичних або інших актів; розкрадання, крадіжка з місць безпосереднього зберігання цінностей. Ці зони контролюються технічними засобами ОПС, системами контролю та управління доступом, відеоспостереження спільно із засобами захисту інформації (ЗЗІ), фізичної охороною. П'ята зона – окремі предмети, наприклад, сейфи, картини, скульптури і підходи до них. Загрози: розкрадання, акти вандалізму. Для захисту використовується відповідні технічні засоби охоронної сигналізації та відеоспостереження. Шоста зона – власне система безпеки. Включає в себе захист технічних і програмних засобів забезпечення безпеки. Загрози: несанкціонований доступ до елементів системи безпеки з метою або повного виведення її з ладу, або блокування окремих елементів, що робить неможливим виконання ними основних функцій при зовнішньому збереженні працездатності. Для запобігання загрозам використовуються сенсори розтину корпусів і зняття зі стіни, самодіагностика елементів системи, пристрої виявлення блокування сенсорів та ін. Кожна з зон може включати в себе кілька рубежів охорони в залежності від значимості об'єкта або його критичних елементів, контрольованих даної зоною. При цьому критична зона (наприклад, область безпосереднього зберігання матеріальних цінностей) повинна знаходитися в центрі, і для підходу до неї необхідно подолання всіх зон і рубежів охорони [1, 9].

Практика створення та експлуатації комплексів технічних засобів охоронних сигналізацій показала, що в більшості випадків для побудови ефективної охорони потрібна наявність комбінованих технічних засобів охоронних систем, що враховують можливість дублювання функцій виявлення на основі використання різних фізичних принципів дії засобів виявлення.

Під загрозою розуміють потенційно можливі дії, процес або явище, які можуть призвести до нанесення матеріального, інформаційного, морального або фізичного збитку.

Загрози безпеці об’єкту захисту можна класифікувати наступним чином:

1. За природою виникнення:

- загроза випадкового характеру;
- навмисні дії порушника.

2. Відносно об’єкта захисту:

- зовнішні;
- внутрішні.

До загроз випадкового характеру належать: стихійні лиха, катастрофи природного та техногенного характеру, аварії, порушення в роботі систем життєзабезпечення об’єкта, а також помилкові дії персоналу.

Навмисні дії порушника проявляються у вигляді крадіжок матеріальних цінностей, вандалізму, саботажу, диверсій і терору.

До зовнішніх загроз відносяться кримінальні дії, несправедлива конкуренція, промисловий шпіонаж.

Внутрішні загрози – навмисні дії персоналу. Як правило, це самі співробітники або зовнішні структури шляхом підкупу чи шантажу проникають на територію, що охороняється.

В основі ефективної протидії загрозі проникнення порушника в приміщення, що охороняється, лежить проведення апріорних оцінок:

- пріоритетів у системі захисту;
- шляху можливого проникнення порушників;
- інформації, яку може знати порушник про організацію системи захисту об’єкта;
- технічних можливостей порушника і тощо, тобто оцінок сукупності кількісних і якісних характеристик ймовірного порушника.

Така сукупність отриманих оцінок називається “моделлю” порушника. Ця модель, поряд з категорією об’єкта, служить основою для вибору методів організації охорони об’єкта, визначає складність і скритність застосовуваних

технічних засобів охоронної сигналізації та відеоспостереження, варіанти інженерно-технічного захисту, кадровий склад служби охорони тощо [2].

На рис.1.2 представлена узагальнена структурна схема системи забезпечення комплексної безпеки об’єкта.

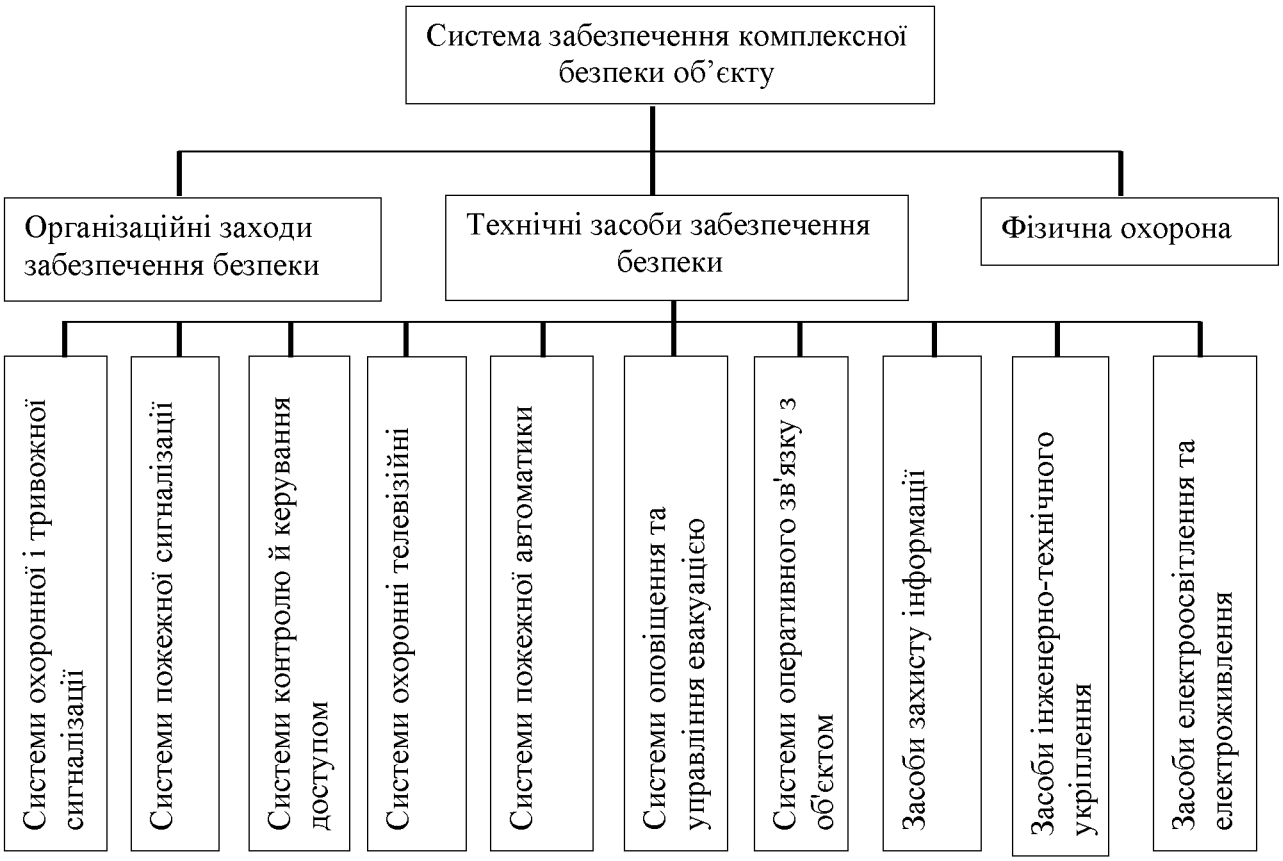

Рис. 1.2 – Структура системи забезпечення комплексної безпеки об’єкта в межах напрямку інженерно-технічної безпеки

1.2. Актуальність та обґрунтування побудови сучасних систем охорони приватних об’єктів.

Системи відеоспостереження вчасно і з високою точністю сповіщають про проникнення на об’єкт, що знаходиться під охороною та записують усі необхідні дані для розслідування правоохоронними органами будь-якого випадку. Відеоспостереження вже давно є невід’ємною частиною нашого життя. Воно активно використовується для забезпечення безпеки комерційних об’єктів, громадських місць і приватних домоволодінь. З розвитком Інтернету речей та

інформаційних технологій інтелектуальність систем відеоспостереження істотно зросла, і вони зараз стають розумним в буквальному сенсі цього слова. Система розумного відеоспостереження являє собою сукупність відеокамер і сенсорів, об'єднаних на базі технології Інтернету речей (IoT). Один з варіантів побудови системи представлено на рис. 1.2.

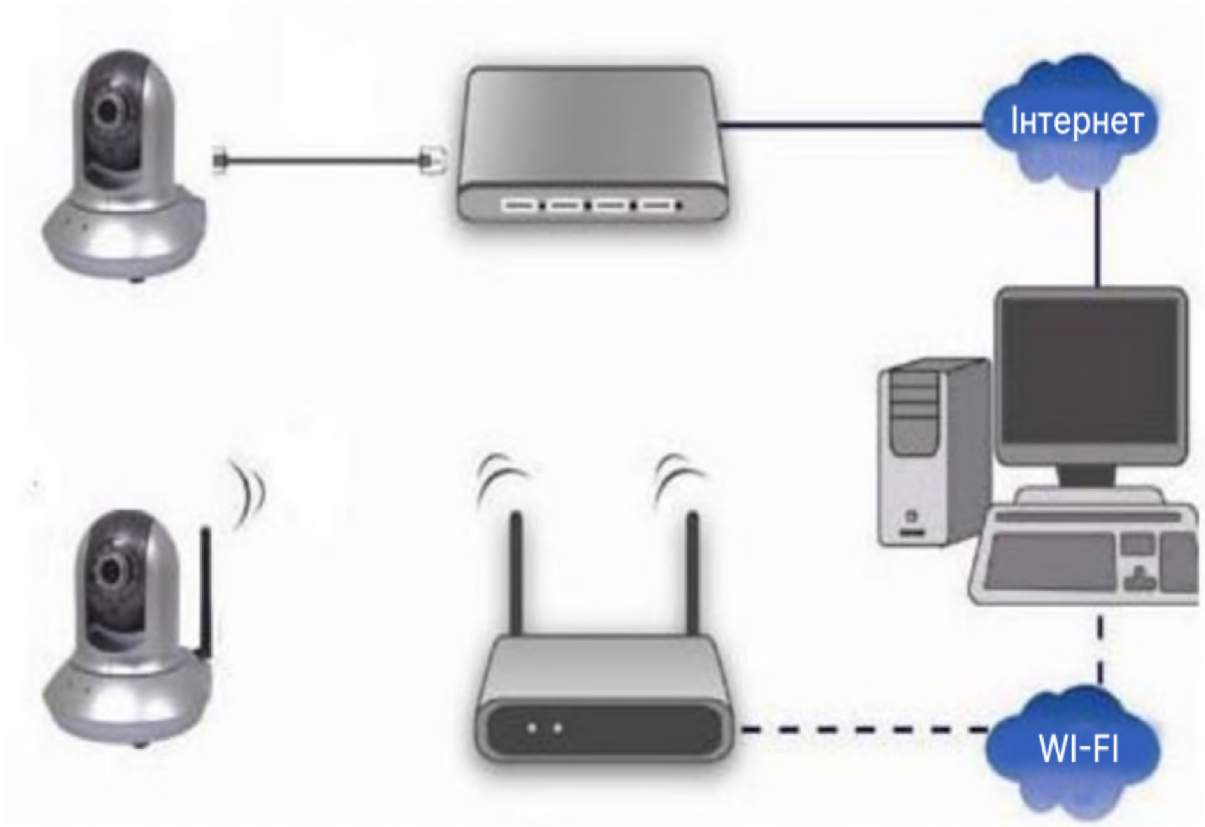

Рис. 1.2 – Типова архітектура системи домашнього відеоспостереження

Структура домашньої охоронної системи: устаткування централізованого управління охоронною системою централь зі встановленим на ньому ПЗ для управління та контролю за сигналізацією; пристрої збору і обробки інформації з датчиків охоронної сигналізації: прилади приймально-контрольні охоронні (панелі); сенсорні пристрої датчики охоронної сигналізації. Схематичних рішень для побудови систем охорони периметру багато, відповідно, багато і типів систем охорони периметру. Вибір однієї системи із багатьох є питанням доцільності та рентабельності. У таблиці 1 наведені найбільш використовувані типи периметральних охоронних систем [3].

Таблиця 1.1 – Основні типи периметральних охоронних систем

Тип системи	Тип огорожі	Можливість захисту неогородженого простору	Переваги	Недоліки
Радіопроменеві	Будь-яка	Так (на стійках)	Незалежність від погодних умов	Мертві зони перед передавачем і приймачем, необхідне забезпечення прямої видимості
Радіохвильові	Будь-яка	Так (підземно)	Незалежність від рельєфу або лінії огорожі	Велика залежність від радіо магнітної обстановки
Інфрачервоні	Будь-яка	Ні	Простота в обслуговуванні та установці	Велика кількість помилкових спрацювань
Оптоволоконні	Будь-яка	Так (підземно)	Несприйнятливість до електромагнітних перешкод	Складність при монтажі та ремонті
Ємнісні	Будь-яка	Ні	Незалежність від рельєфу або лінії огорожі	Складний та дорогий монтаж
Вібраційні	Будь-яка	Так (підземно)	Незалежність від рельєфу або лінії огорожі	Помилкові спрацювання при великому вітрі
Вібраційно-сейсмічні	Бетонна	Так (підземно)	Можливість виявлення як підкопу так і рухомої людини	Розташування оддалік автомагістральних доріг і ліній електропередач, не працює в болотистих і скельних ґрунтах
Системи активної охорони	Сітка, металева огорожа	Ні	Не шкодить людині	Смертельно для дрібних тварин і птахів.

Розглянемо детальніше кожний тип периметральних охоронних систем:

Радіопроменеві системи. Передавач радіопроменевої системи охорони периметра створює об'ємне електромагнітне поле, зазвичай еліптичної форми. У

разі знаходження стороннього об'єкта в зоні контролю відбувається зміна поля. Реєстрація зміни здійснюється приймачем, перехідним в збуджений стан при відхиленні характеристик електромагнітного поля від заданих. Існують системи, в яких передавач випромінює високочастотні поля. При попаданні рухомого об'єкту в зону, контрольовану таким приладом, відбувається зміна частоти відбитих коливань (ефект Доплера), реєстрована приймачем.

Переваги: відносно невелика коштовність, відносно велика відстань контролю (приблизно 200-600 м).

Недоліки: необхідна зона прямої видимості між передавачем і приймачем (в зоні виявлення мають бути відсутні нерівності ґрунту (висота допустимих нерівностей для кожного засобу різна і лежить в діапазоні від 80 до 400 мм), чагарник, гілки дерев та інші сторонні предмети), поблизу зони виявлення не повинен проїжджати автотранспорт, є мертві зони біля стойок приймача і передавача [3]. На рис. 1.3. представлено приклад роботи променевої системи захисту периметру.

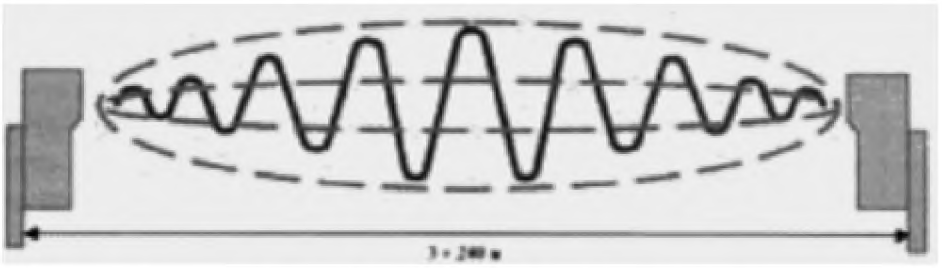

Рис. 1.3 – Приклад дії радіопроменевої системи захисту периметру

Радіохвильові системи. Найпростіша радіохвильова система складається з двох фідерів, розташованих паралельно один одному на певній відстані. При пропущенні через них струму навколо утворюється стабільне електромагнітне поле. При попаданні об'єкта всередину контрольованої фідерами зони електромагнітне поле збурюється, що і реєструється приймачем - аналізатором. Радіохвильові системи можна дуже легко встановлювати приховано (фідери закопуються в землю, декоративно монтуються на стіни будівель, закладаються в паркан і т.п.). Радіохвильову систему охорони периметру застосовують лише на прямих ділянках периметру. Системи розраховані на виявлення порушника, який

долає рубіж охорони у повний зріст або зігнувшись. Принцип роботи радіохвильової системи захисту периметру представлено на рис. 1.4.

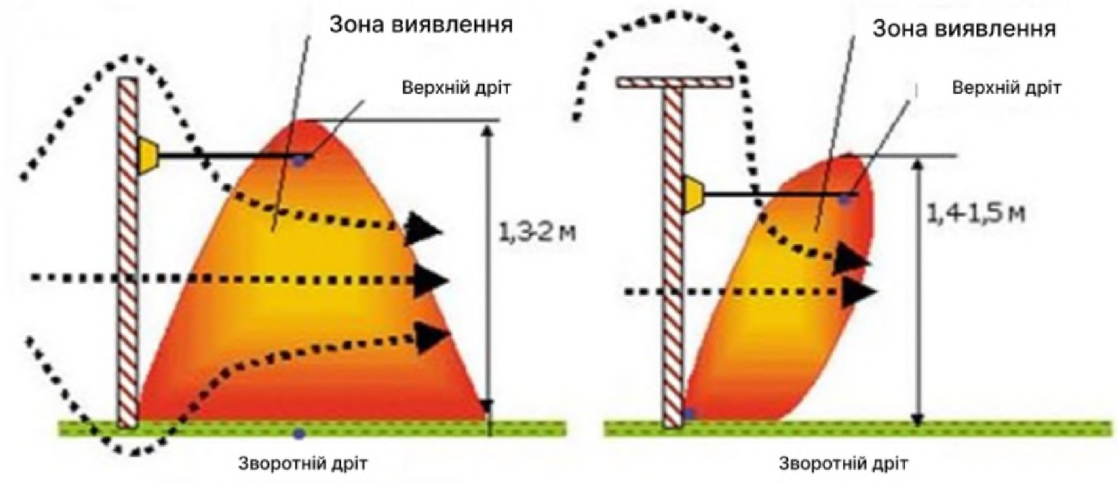

Рис. 1.4 – Принцип роботи радіохвильової системи захисту периметру

Переваги: можливість забезпечити потайне розміщення засобів виявлення, створити візуально замасковану локальну зону, зберігається чутливість незалежно від рельєфу місцевості, виду рослинності, висока завадостійкість при русі автотранспорту і людей на близькій відстані від рубежу.

Недоліки: наявність мертвих зон біля приймача та передавача (для запобігання цього недоліку приймач і передавач встановлюють з перекриттям в декілька метрів), невелика чутливість біля землі (30-40 сантиметрів). При різких змінах метеорологічних факторів, при затяжних сильних дощах, активному таненні снігу може різко змінитися чутливість по довжині ділянки, а отже, і знизитися ймовірність виявлення порушника, зважаючи на малу глибину закладення випромінюючих кабелів, в зоні їх розміщення забороняється проводити будь-які роботи з ґрунтом (посадку рослин, прокладку підземних комунікацій, влаштування фундаментів і т.п.) [3].

Інфрачервоні системи. ІЧ- системи діляться на два класи: активні і пасивні. Перші з них складаються з двох частин: передавача, випромінюючого імпульсні ІЧ- промені (від одного і більше невидимих людським оком променів) і приймача, який подає сигнал тривоги у разі переривання одного або декількох променів. Дія другого класу ІЧ-систем заснована на реєстрації зміни рівня

теплового випромінювання фону при русі людей або тварин в зоні виявлення. Конфігурація зон буває різною: «штора» (перетин поверхні), «промінь » (лінійний рух), «об'єм» (переміщення в просторі). Принцип роботи ІЧ системи захисту периметру представлено на рис.1.5.

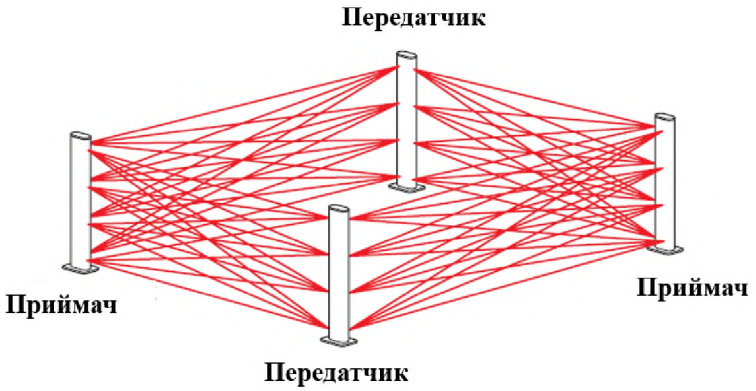

Рис. 1.5 – Принцип роботи ІЧ системи захисту периметру

Переваги: можливість створення вузької зони виявлення (це особливо важливо для об'єктів, де обладнання смуги відчуження з внутрішньої сторони огорожі неможливо), відносно велика відстань контролю (приблизно 600 м).

Недоліки: в екстремальних погодних умовах (при рясному мокрому снігопаді, сильному поривчастому дощі, густому тумані або при різких засвіченнях фарами) дають помилкові спрацьовування, в умовах підвищеної запиленості та загазованості необхідно періодично протирати оптичні елементи сповіщувачів [3].

Оптоволоконні системи. Відрізняються малою сприйнятливістю до будь-яких електромагнітних перешкод, що дозволяє використовувати їх у несприятливій електрофізичній обстановці. До одного кінця кабелю підключається мініатюрний напівпровідниковий лазер, а протилежний кінець кабелю зістикований з фотодіодом, що перетворює оптичний сигнал в електричний. При зовнішніх діях на кабель передається сигнал тривоги. Досвід застосування таких систем невеликий, але викликає серйозний інтерес, особливо

через несприйнятливість до електромагнітних перешкод [4]. Принцип роботи оптоволоконної системи захисту периметру представлено на рис.1.6.

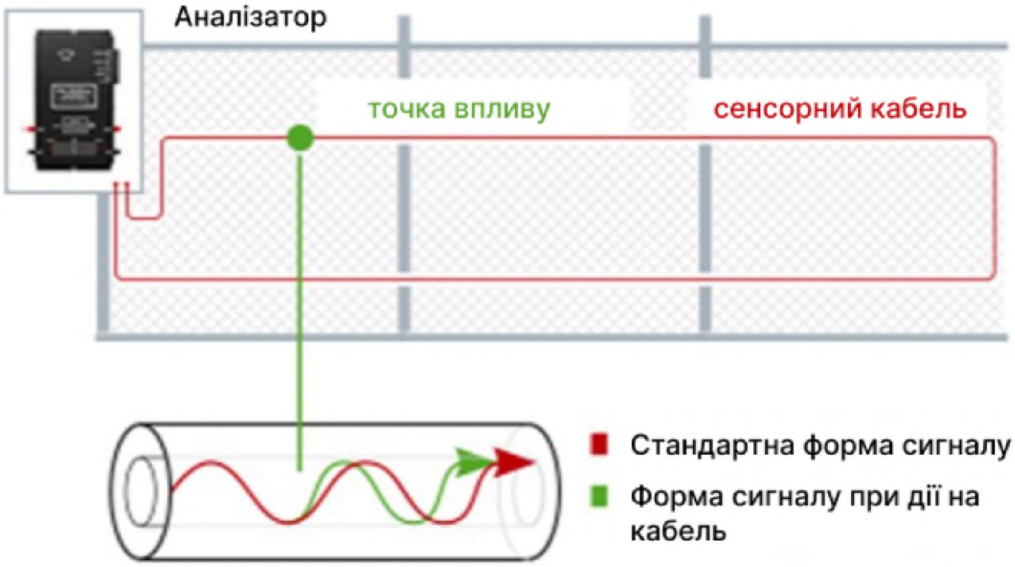

Рис. 1.6 – Принцип роботи оптоволоконної системи захисту периметру

Ємнісні системи. Ємнісні засоби охорони периметру слугують для охорони протяжних ділянок місцевості і периметрів об'єктів шляхом блокування верхньої частини огорож, виконаних з бетону, цегли, дерева, металевих решіток і т.п. Ємнісний засіб виявлення являє собою антенну систему - ланцюг провідних елементів (чутливий елемент), що зміцнюються на ізоляторах по периметру об'єкта і з'єднаних в загальний електричний контур. Система підключена до електронного блоку, що видає сигнал тривоги при зміні ємності антенного пристрою щодо землі.

Ємнісні системи охорони периметра використовують ефект зміни характеристик електричного поля при наближенні або дотику порушника до огорожі об'єкта. Тобто коли людина наближається до електродів або торкається їх, ємність антенної системи змінюється, що реєструється електронним блоком, що видає сигнал тривоги. Принцип роботи ємнісної системи охорони периметру представлено на рис.1.7.

Системи ємностей у периметрі універсальні і привабливі своєю нечутливістю до нерівностей профілю ґрунту або лінії огорожі. Вітчизняні

охоронні ємнісні системи в цілому відрізняються достатньо високою надійністю і широко використовуються на різних об'єктах протягом останніх 20-30 років [5].

Рис. 1.7 – Принцип роботи ємнісної системи охорони периметру

Вібраційна система. Для проникнення всередину приміщення найпривабливішим місцем для порушника є двері та віконні отвори, тому вони в першу чергу потребують надійного захисту. Правильна організація системи сигналізації цього рубежу дозволить не тільки максимально швидко оповістити про спробу злому, але і запобігти проникненню.

Вібраційні системи охорони будуються на основі інтелектуальних мікропроцесорних сповіщувачів, здатних до навчання. В процесі настройки користувачем задається кількість і сила ударних впливів на охоронювану поверхню – порогове значення чутливості, при перевищенні якого датчик видає сигнал тривоги. У разі потужного удару датчик ігнорує лічильник імпульсів і моментально генерує тривожний сигнал – функція явного вторгнення.

Завдяки механізмам самонавчання і широкому динамічному діапазону вібродатчики забезпечують найвищий рівень захисту при спробах вирізання або злому дверей, при їх свердлінні або пробою, продовжуючи ефективно працювати в приміщеннях з сильними акустичними перешкодами (наприклад, якщо поруч ведуться будівельні роботи) [5].

Приклад захисту вібраційною системою охорони представлено на рис.1.8.

Рис.1.8 – Приклад захисту вібраційною системою охорони

Система «активної» охорони. До таких систем відносять електрошокову. Електрошокова система охорони периметра являє собою активну систему захисту периметра, засновану на електропровідності інженерного загородження, і виконується із сталевого оцинкованого дроту або троса діаметром 2,5мм, який монтується на склопластикових стійках по верху паркана (огорожі) у вигляді козирка або повнозростового паркану. Система реагує на спробу вторгнення порушника відображає його проникнення методом нелетальної дії на тіло людини струмом високої напруги [1-5].

Але якщо ми хочемо надійно захистити об'єкт, то ефективним рішенням буде поєднання периметральних систем охорони з такими системами, як телевізійне відеоспостереження та GSM-системою.

Відеоспостереження є невід'ємною частиною нашого сьогодення в комплексі з охоронною сигналізацією в багатьох фірмах та організаціях. Система відеоспостереження набагато підвищує ефективність відбиття і ліквідації загрози. Сучасний перелік обладнання, представлений на ринку, дозволяє реалізувати системи відеоспостереження будь-якої складності, від однієї - двох камер зображення, з яких виводиться на монітор охоронця, до десятків відеокамер, об'єднаних в мережу з віддаленим переглядом через Internet [6-10].

1.3. Аналіз загроз та ризиків в системах охорони периметру.

Безпека у будь-якій системі залежить від об'єктів і підсистем, що до неї безпосередньо входять. У випадках, коли до вже сформованої системи додають деякі інші об'єкти, компоненти, а також пристрої, рівень безпеки такої системи зазвичай змінюється, але у гірший бік.

Таке відбувається у комунікаційних і інформаційних системах, що отримали у своє розпорядження нові пристрої для Інтернету речей. Поряд із новими можливостями і послугами, вони беруть на себе також і роль потенційно вразливої системи [10].

Загрози, які створює Інтернет речей, стають більш поширеними. Таким чином, за останнє десятиліття спостерігалося збільшення випадків порушень кібербезпеки та кіберзлочинів, скоєних з використанням пристроїв IoT.

Використовуючи дані про подібні інциденти, можна швидко зробити висновки, що кількість атак зростає і прямо пропорційна збільшенню кількості тих же пристроїв IoT. У 2022 році компанія Check Point підготувала звіт Global Threat Index, в якому сформовано рейтинг десяти найбільш часто використовуваних уразливостей в кібератаках. Перші три місця посіли вразливості в Інтернеті речей. Дві з них є критичними, оскільки дозволили віддалено запускати шкідливий код на маршрутизаторі, а одна вразливість успішно обійшла механізми автентифікації маршрутизатора. Ці вразливості IoT дозволили зловмиснику запустити шкідливий програмний код, отримати контроль над пристроями та отримати доступ до певної інформації. Таким чином, певна система була повністю скомпрометована [10]. Також слід зазначити про подібний звіт від компанії CISCO, у якому приділено увагу особливо декільком питань, одне з котрих пов'язано з прогалинами в системі безпеки у зв'язку з розширенням Інтернету речей та застосуванням хмарних сервісів [11].

1.4. Аналіз апаратури, що застосовується для побудови інтегрованої системи захисту периметру.

Відеоспостереження є невід'ємною частиною нашого сьогодення в комплексі з охоронною сигналізацією в багатьох фірмах та організаціях. Система відеоспостереження набагато підвищує ефективність відбиття і ліквідації загрози.

Системи зовнішнього відеоспостереження (вуличне відеоспостереження) встановлюється:

- на автомобільних стоянках і заправних станціях,
- по периметру котеджних селищ,
- на фасаді офісних будівель, банківських і державних установ, музеїв, шкіл і тощо,
- у громадських місцях для контролю правопорядку (вокзали, спортивні стадіони, криміногенні райони і т.д.),
- на території логістичних і промислових комплексів,
- на будівельних майданчиках для контролю за ходом робіт.

Основні компоненти апаратури відеоспостереження:

- відеокамери (аналогові та цифрові),
- пристрої для управління поворотними відеокамерами (пульти, джойстики),
- обладнання обробки відеосигналів (квадратори, мультиплексори, плати відео захоплення, програмне забезпечення),
- обладнання запису відеозображення (аналогові відеомагнітофони та цифрові відеореєстратори),
- обладнання виведення (монітори, стільникові телефони, блоки прийому-передачі по витій парі),
- джерела забезпечення резервного безперебійного живлення UPS,
- обладнання захисту від перешкод і громо-захисту.

Технічні засоби відеоспостереження можуть бути пов'язані між собою:

- за допомогою дротів – система дротяного відеоспостереження

- чи за допомогою радіозв'язку – система безпровідного відеоспостереження [4-5].

На рисунку 1.9. зображено приклад охорони периметру за допомогою системи відеоспостереження.

Рис. 1.9 – Охорона периметру за допомогою відеокамер

GSM сигналізація, GSM контролер, GSM пейджер, GSM дозвонщик – все це один пристрій, призначений для контролю та охорони майна квартири, будинку, магазину, дачі, офісу, складу, автомобіля, гаража та інших віддалених об'єктів, передачі сигналу тривоги – автодозвону або SMS-повідомлення з віддаленого об'єкта за допомогою мереж стільникового зв'язку на телефон власника об'єкта, довірених осіб або служби охорони, і дистанційного керування електроприладами на об'єкті, що охороняється. GSM охоронна система може включати в себе один або кілька GSM контролерів, а також засоби контролю і управління цими GSM контролерами – мобільні телефони та (або) комп'ютери [6-9].

До кожного GSM контролеру можна підключити:

- різні дискретні і резистивні датчики. Наприклад, контактні датчики, геркони, терморезистори для контролю температури, датчики охоронної та пожежної сигналізації і т. п .;
- відеокамери;

- мікрофон і звуковий динамік;
- виконавчі пристрої ;
- кнопки для установки датчиків на охорону безпосередньо на об’єкті;
- кнопки та (або) зчитувач коду різних ідентифікаторів (карт, брелоків) для зняття датчиків з охорони;
- GSM охоронні системи дозволяють;
- отримувати за допомогою стільникового телефону і (або) комп’ютера тривожні повідомлення про спрацювання датчиків, інформаційні повідомлення про стан обладнання, повідомлення про постановку і зняття датчиків з охорони, а також інші важливі повідомлення;
- дистанційно ставити і знімати датчики з охорони за допомогою стільникового телефону і (або) комп’ютера;
- ставити датчики на охорону на об’єктах з допомогою кнопок, підключених до контролерів;
- знімати датчики з охорони на об’єктах з допомогою кнопок, підключених до контролера, і (або) різних ідентифікаторів (карт, брелоків);
- дистанційно вмикати і вимикати виконавчі пристрої (за допомогою стільникового телефону або комп’ютера) ;
- отримувати відеокадри від відеокамер, підключених до контролера, на екрані свого стільникового телефону і (або) комп’ютера;
- отримувати відеокадри, записані в пам’ять контролера за час його автономної роботи, на екрані свого смартфона або комп’ютера;
- вести дистанційне прослуховування звукового фону на віддалених об’єктах за допомогою свого стільникового телефону і мікрофонів, підключених до контролерів;
- використовувати контролери в якості переговорних пристроїв, тобто здійснювати діалог з людьми, що знаходяться на віддаленому об’єкті, за допомогою свого стільникового телефону, а також мікрофонів і динаміків, підключених до контролерів;

• дистанційно задавати налаштування і режими автоматичної роботи устаткування GSM охоронної системи на віддаленому об'єкті за допомогою стільникового телефону і (або) комп'ютера.

Крім охорони і контролю віддалених об'єктів, GSM контролери можуть бути також використані для організації контролю доступу (входу) на об'єкт за допомогою ідентифікаторів (карт, брелоків). У цьому випадку, наприклад, увійти в охоронюваний будинок або приміщення можна тільки після пред'явлення свого ідентифікатора зчитувача, встановленого поряд з дверима і підключеного до контролера. Після зчитування коду ідентифікатора GSM контролер може розблокувати прохід через двері і одночасно з цим зняти з охорони датчики, встановлені по периметру або в приміщенні. У пам'яті контролера може зберігатися до 16 кодів ідентифікаторів[4-9].

Рис. 1.10 – Приклад використання GSM сигналізації

1.5. Засоби збору, обробки, відображення інформації та управління

Як було зазначено раніше, апаратно-технічні засоби збору та обробки інформації та управління формують центральну і периферійні СЗОІУ (система збору та обробки інформації та управління периферійна), що входять до складу комплексних інтегрованих системи безпеки. Пристрої (контролери, розширювачі, пульти управління) безпосередньо на апаратному рівні взаємодіють зі своїми сенсорами, виконавчими пристроями, а на інформаційному рівні зв'язують їх по локальному інтерфейсу (RS-485, RS-232) з робочими станціями або з сервером. Вони призначені для виконання безперервного збору інформації від сенсорів, формування і передачі повідомлень про стан об'єкта [4-6] та контролю їх справності. У зв'язку з цим засоби збору і обробки інформації повинні мати такі функціональні характеристики:

– інформаційна ємність;

– достатня кількість контрольованих приладом зон безпеки;

– інформативність;

– кількість переданих (прийнятих) повідомлень на системи передачі сповіщень;

– час прийому повідомлення від сесорів (максимально допустимий час контролю всіх сенсорів, підключених до приладу);

– рівень захисту від несанкціонованого доступу до приладу при виконанні функцій взяття під охорону і зняття з охорони об'єкта;

– параметри завадостійкості лінії (каналу) зв'язку приладу з сенсорами;

– параметри і характеристики інтерфейсу каналу зв'язку приладу з засобами передавання тривожних сповіщень.

Приймально-контрольні пристрої (ПКП) в системах охорони є проміжною ланкою між об'єктовими первинними засобами виявлення проникнення або пожежі (сенсорами) і СПП (система передачі повідомлень). ПКП охоронний (охоронно-пожежний) – це технічний засіб охоронної або охоронно-пожежної

сигналізації для прийому сповіщень від сенсорів (шлейфів сигналізації) або інших приймально-контрольних приладів, перетворення сигналів, видачі повідомлень для безпосереднього сприйняття людиною, подальшої передачі повідомлень та включення сенсорів, а в деяких випадках і для електроживлення охоронних сенсорів .

Прийнята така класифікація ПКП охоронних систем [2, 4] .

1. ПЗ (мережеве, системне і прикладне програмне забезпечення сервера і робочих станцій, а також вбудоване програмне забезпечення системних контролерів, контрольних панелей і модулів) організації тривожної сигналізації на об'єкті розглядають ПКП:

- автономні – призначені для забезпечення автономної сигналізації, при якій повідомлення про стан контрольованого об'єкта видаються тільки на звукові та світлові сенсори, встановлені на об'єкті, що охороняється, або в безпосередній близькості до нього;

- локальні – призначені для забезпечення локальної сигналізації на об'єкті, при якій повідомлення про стан, а також управління контрольованим шлейфом (зонами) здійснюється за допомогою засобів відображення інформації та управління (індикаторні панелі, пульти), що входять до складу ППК;

- централізовані – призначені для централізованої сигналізації і роботи спільно або в складі СПП (система передачі повідомлень), при якій сповіщення з ПКП передаються на пульт центральної сигналізації системи передачі повідомлень (СПП) за допомогою використання різних каналів зв'язку (телефонні лінії, радіоканали, виділені лінії і ін.).

2. За способом контролю сенсорів ПКП поділяються на:

- безадресні (без реєстрації адреси сенсора) – прилади, мають тільки безадресні шлейфи сигналізації;

- адресні – прилади, що мають адресні шлейфи сигналізації;

- комбіновані – прилади, що мають безадресні і адресні шлейфи сигналізації.

3. За структурою шлейфу сигналізації розглядають ПКП:

- зі шлейфами сигналізації радіальної структури;

- зі шлейфами сигналізації кільцевої структури (магістральні);

- зі шлейфами сигналізації деревовидної структури;

- зі шлейфами сигналізації комбінованої структури.

4. За каналом зв'язку з сенсорами розглядають ПКП:

- з дротяними каналами зв'язку;

- з бездротовим (радіоканал або ін.) каналом зв'язку;

- з іншими каналами зв'язку (силова електромережа і т.д.).

5. За інформаційною ємністю розглядають ПКП:

- малої інформаційної ємності – до восьми шлейфів сигналізації (адрес);

- середньої інформаційної ємності – від дев'яти до 64 шлейфів сигналізації (адрес);

- великої інформаційної ємності – понад 64 шлейфів сигналізації (адрес).

6. За інформативністю розглядають ПКП:

- малої інформативності – до восьми видів сповіщень;

- середньої інформативності – від дев'яти до 16 видів сповіщень;

- великої інформативності – понад 16 видів повідомлень.

ПКП для локальної сигналізації повинні додатково до основних функцій забезпечувати: а) відображення за допомогою індикаторів, розташованих на приладі, виносному табло або пульті управління, стану ПКП або кожного шлейфа сигналізації або адреси; б) звукову сигналізацію про тривогу за допомогою вбудованого або зовнішнього звукового оповіщувача. ПКП пожежний – технічний засіб, призначений для прийому сигналів від пожежних сенсорів, здійснення контролю цілісності шлейфа пожежної сигналізації, світлової індикації та звукової сигналізації подій, формування стартового імпульсу запуску приладу управління пожежного.

1.6. Висновок. Постановка задачі

Питання забезпечення ефективного захисту об'єктів, розглянуті вище, сприяють формуванню базової теоретичної і практичної підготовки в області інтегрованих комплексних систем охорони периметру об'єктів. Вивчення основних термінів, визначень і принципів організації інтегрованих комплексних систем безпеки дозволяє вирішувати наступні завдання проєктування і аналізу функціонування систем безпеки: вибір варіанту охорони об'єкту з використанням комплексу технічних засобів забезпечення безпеки відповідно до вимог технічної охорони об'єкта; виконання основних етапів проєктування системи безпеки з використанням основних принципів розробленої концепції безпеки; розробка структурної схеми інтегрованої системи безпеки на основі даних про вхідні в неї підсистеми контролю доступу, систем відеоспостереження; синтез окремих компонентів комплексних систем безпеки на базі готових уніфікованих функціональних вузлів, розрахунок їх основних параметрів і характеристик; виконання оптимізації структури системи охорони периметру з використанням методів оцінки ефективності її функціонування. Виконання зазначених завдань розвиває здатності збирати, обробляти, аналізувати і систематизувати науково-технічну інформацію за темою дослідження систем охорони периметру, вибирати перспективні методи вирішення професійних завдань на основі сучасного розвитку оптико-електронних і телевізійних систем безпеки.

Для розробки приймально-контрольного пристрою з оповіщенням по GSM каналу інтегрованої системи захисту периметру необхідно провести аналіз апаратури для системи захисту периметру. Розробити структурну та функціональну схеми ПКП. Провести аналіз та обґрунтування електричної принципової схеми ПКП системи захисту периметру приватного об'єкту. Представити розрахунок надійності модифікованого управляючого пристрою системи охорони приватного об'єкту. Надати методику оцінки ризиків кібербезпеки в системах Інтернет-речей. Провести дослідження та аналіз безпеки системи охорони периметру за допомогою сучасного ПЗ. Провести розрахунок собівартості ПКП та економічного ефекту щодо впровадження охоронної системи приватного об'єкту.

2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз приватного об’єкту.

Об’єкт охорони представляє собою ділянку землі не прямокутної форми, площею 1326 квадратних метра з двоповерховою будівлею з цегли та гаражу, загальною площею 564 квадратних метрів, з двома виходами з території на дорогу та одним виходом з будівлі (рис. 2.1 та рис. 2.2.).

Рис. 2.1. – Об’єкт охорони, оснащений активною інфрачервоною системою охорони периметру та комплектом відеокамер з інфрачервоними датчиками руху

Рис. 2.2. – Об’єкт охорони, оснащений пасивною (вхід до воріт) та активною (на огорожі) інфрачервоною системою охорони периметру.

2.2. Вибір і обґрунтування структурної схеми інтегрованої системи захисту периметру.

Розглянемо принципи побудови системи безпеки об'єкта, на основі яких встановлюються вимоги до створення та організації функціонування таких систем в цілому і складових її технічних засобів. При побудові захисту спеціального об'єкта необхідно керуватися такими принципами:

1. Адекватність прийнятим моделям загроз (розроблені організаційні та адміністративні заходи, технічні засоби захисту об'єктів і їх елементів повинні відповідати прийнятим загрозам і моделям порушників).

2. Зональна побудова або зональним принципом (системи безпеки повинна передбачати організацію та створення зон обмеженого доступу, що забезпечують "багаторівневий" захист об'єктів під охороною і їх критичних елементів).

3. Повинен бути забезпечений необхідний рівень ефективності для всіх типів порушників і способів вчинення злочинних дій.

4. Адаптивність (системи безпеки не повинна створювати перешкод функціонуванню об'єкта і повинна адаптуватися до технологічних особливостей його роботи, в тому числі в надзвичайних ситуаціях з урахуванням прийнятих на об'єкті заходів технологічної та пожежної безпеки).

5. Дотримання принципів побудови системи безпеки дозволяє забезпечити ефективність захисту об'єктів, яка визначається здатністю технічних підсистем комплексних і інтегрованих систем безпеки протистояти нештатним ситуаціям на об'єкті з урахуванням виявлених загроз і моделей порушників.

Розглянемо більш докладно зональний принцип побудови системи безпеки, який дозволяє раціонально зробити вибір і розподіл технічних засобів підсистем для охорони об'єкта і його критичних зон. Під критичними зонами (елементами) об'єкта розуміють приміщення, їх конструктивні елементи, ділянки, реалізація загрози в відношенні яких може привести до найбільш суттєвих втрат. Для своєчасного виявлення і нейтралізації потенційних загроз

необхідно визначити послідовні зони (або рубежі) забезпечення безпеки з одночасним виявленням загроз ПЗ кожній конкретній зоні. У загальному випадку зона під охороною може бути визначена як частина об'єкту, що охороняється та включає в себе: один шлейф охоронної сигналізації (для комплексів охоронної сигналізації), один шлейф пожежної сигналізації (для установок пожежної сигналізації), один шлейф охоронно-пожежної сигналізації або сукупність шлейфів охоронної та пожежної сигналізації (для комплексів охоронно-пожежної сигналізації) та до якої може бути обмежений доступ.

Шлейф сигналізації – це коло (електричне, радіоканальне, оптоволоконне або інше), що з'єднує вихідні вузли сенсорів, що включає в себе допоміжні (виносні) елементи і з'єднувальні лінії і призначена для передачі на прилад приймально-контрольний або на пристрій об'єкту системи передачі повідомлень інформації від сенсорів про контрольовані ними параметрах, а в деяких випадках – для подачі електроживлення на сенсори.

Рубіж охоронної сигналізації – це шлейф або сукупність шлейфів, контролюючих охоронювані зони території, будівлі або приміщення (периметр, обсяг або площа, самі цінності або підходи до них) на шляху можливого руху порушника до матеріальних цінностям, при подоланні яких видається відповідне повідомлення про проникнення. Під кордоном охорони розуміється сукупність охоронюваних зон, контрольованих кордоном сигналізації [12,13].

При організації зонування об'єкта повинно забезпечуватися посилення захисту від периферії до центру, тобто до критичних елементів, які визначають категорію об'єкта. Якщо при оцінці ефективності системи безпеки з'ясовується, що існуючих охоронюваних зон недостатньо для нейтралізації потенційних загроз, то можуть організовуватися додаткові трубежі захисту всередині існуючих зон. Основу планування і технічного оснащення зон безпеки складає принцип рівнозахищенності їх кордонів. Наприклад, якщо при обладнанні зони периметра будівлі на одному з вікон першого поверху не буде металевої решітки або її конструкція ненадійна, то міцність і надійність інших решіток вікон цього поверху не мають ніякого значення, так як зона буде досить легко і швидко

подолана порушником через незахищене (або слабо захищене) вікно. Отже, кордони зон безпеки не повинні мати незахищених ділянок. Властивість адаптивності системи безпеки дозволяє своєчасно і гнучко враховувати динаміку потенційних і реальних загроз і небезпек об'єкту.

Таким чином, технічна система охорони периметру приватного об’єкту повинна володіти адекватністю відносно спектру загроз і небезпек об'єкту з урахуванням контрольних зон в своїй підконтрольній області та адаптивністю до змін умов функціонування об'єкту.

Виходячи з аналізу об’єкту захисту та можливих загроз, державних нормативних документів, що регулюють процес проєктування і обладнання будівель системами охоронних сигналізацій, можемо спроєктувати структурну схему системи захисту периметру приватного об’єкту.

Відповідно до розмірів об’єкта охорони, особливості прилеглого до нього периметру – рівній місцевості без загороджувальних пристосувань, можна зробити висновок щодо приналежності об’єкта охорони до категорії «В» за ДСТУ 78.11.001-98 – дозволено обладнання об’єктів категорії «В» двома рубіжами охоронної сигналізації. Тому прийнято рішення про побудову інтегрованої системи захисту периметра приватного об’єкту, яка складається з інфрачервоної, GSM та системи відеоспостереження систем захисту об’єктів, які розраховані на підключення 13 сповіщувачів (12 активних і 1 пасивний), GSM-контролеру та комплекту відеоапаратури DS-J142I/7104HGHI-SH. Структурна схема представлена на рис. 2.3.

Якщо більш детально розглянути вищенаведену схему, то можна побачити, що вона складається з інфрачервоної (активної та пасивної) системи охорони периметру, GSM системи оповіщення та системи відеоспостереження.

Розглянемо структурні схеми цих систем окремо та наведемо їх на рис.2.4., рис. 2.5., рис.2.6.

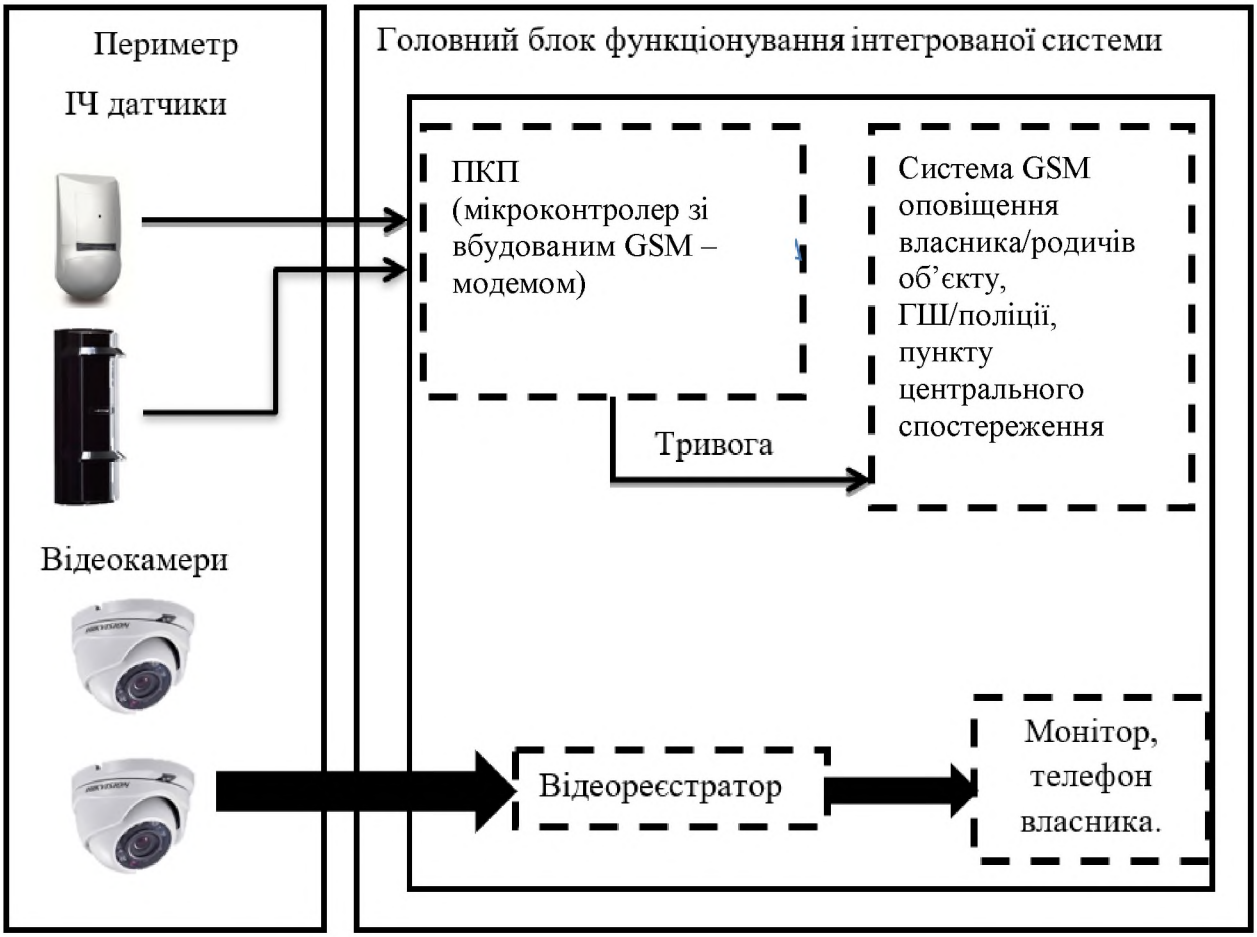

Рис. 2.3. – Структурна схема інтегрованої системи захисту приватного об'єкту

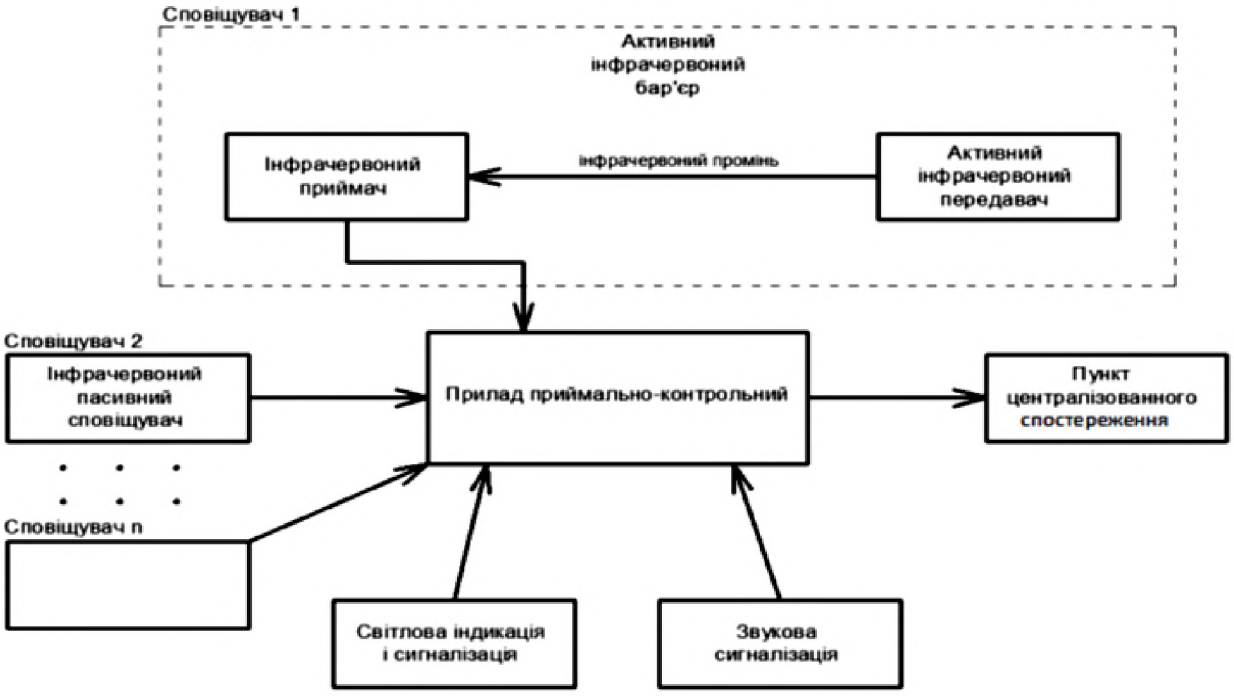

Рис.2.4 – Структурна схема інфрачервоної системи захисту периметра

Рис.2.5. – Структурна схема системи відеоспостереження

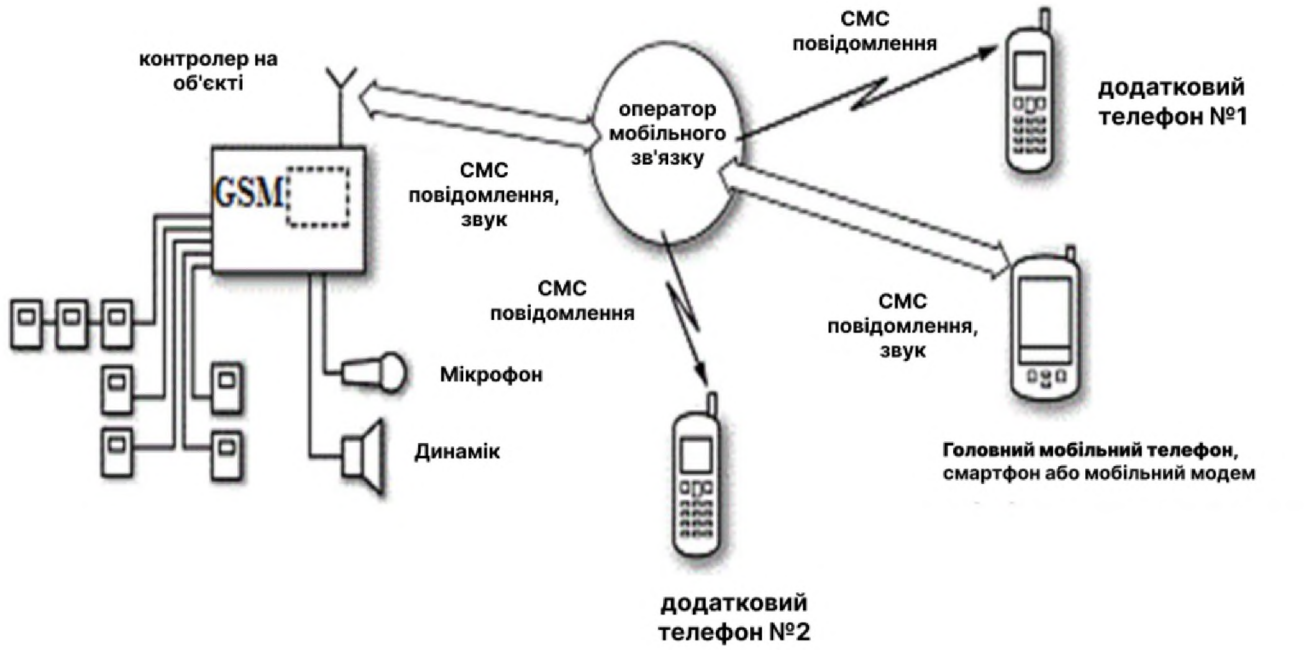

Рис.2.6. – Структурна схема GSM системи оповіщення

На рис.2.7. представлена структурна схема ПКП, яка складається з наступних блоків: блок обробки та управління, блок індикації, блок підключення зовнішніх пристроїв управління та оповіщення, блок живлення.

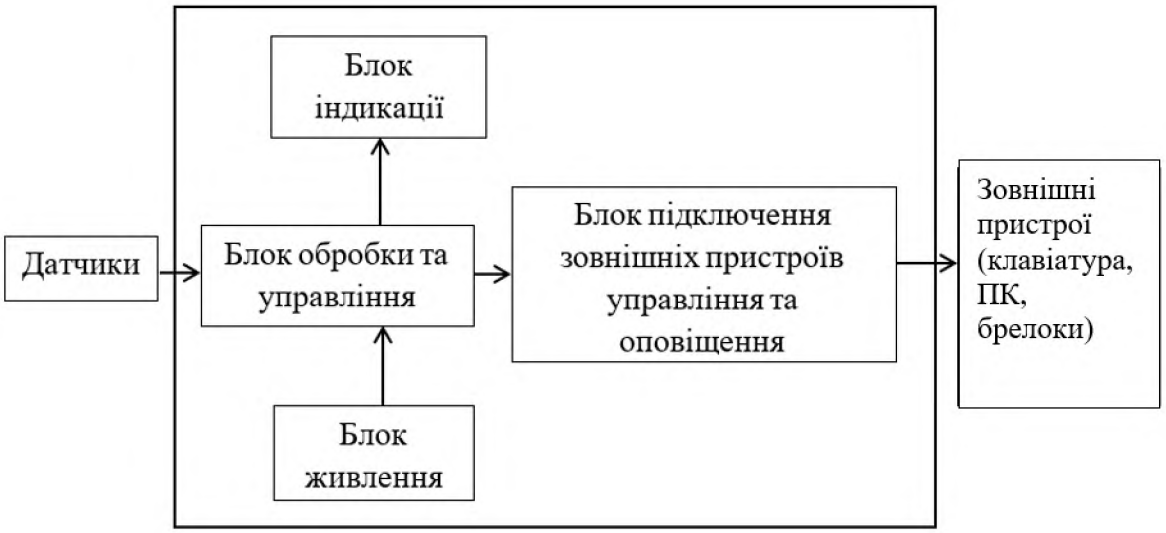

Рис. 2.7. – Структурна схема ПКП

Розглянемо функції, які виконує кожен блок структурної схеми:

1) Блок індикації. Блок індикації повинен забезпечувати чітке, зручне і своєчасне оповіщення про можливу загрозу. Для виконання цих функцій може використовуватись система виносних світло діодів.

2) Блок обробки та управління. Даний блок забезпечує управління всім приладом в цілому. Він приймає інформацію, яка надходить з шлейфів сигналізації, обробляє її і видає на блок індикації результат. Для забезпечення всіх функцій керування до блоку включено мікроконтролер, на який і покладена головна робота пристрою. Також до складу даного блоку входить енергонезалежна пам'ять для запису та зберігання напівпостійних даних системи, користувацьких або заводських налаштувань. З'єднання пам'яті з мікроконтролером здійснюється за допомогою дводротової шини I^2C.

3) До блоку підключення зовнішніх пристроїв управління та сповіщення входять:

- схема підключення виносної клавіатури – КЛО – здійснює введення інформації при програмуванні та управлінні приладом, відображаючи інформацію за допомогою світлодіодів;
- схема підключення до GSM – для моніторингу, сповіщення або дистанційного програмування через GSM телефонну мережу;
- схема підключення до ПК для програмування приладу;
- радіо-брелоки – для керування системою .

4) Блок живлення**.** Забезпечує автоматичне перемикання на живлення від акумулятора (10,8В – 13,2В), коли зникає напруга в мережі 220В/50Гц, та зворотне перемикання при відновленні мережі. Включає схему заряду акумулятора. Залежно від положення джампера JMP1 прилад знаходиться в одному з трьох режимів: режим запису заводських установок, режим програмування конфігурації приладу, режим охорони. Запис заводських установок здійснюється автоматично, програмування конфігурації приладу здійснюється за допомогою клавіатури. У режимі охорони прилад вимірює опір шлейфів, та залежно від результату вимірювання видає команди на виходи пульта централізованого спостереження (ПЦС), світлові і звукові оповісники, або залишається у черговому режимі. Підключення та зняття приладу з охорони проводиться за допомогою коду, що вводиться з клавіатури.

Проаналізувавши структурну схему ПКП, представимо узагальнену функціональну схему (рис. 2.8). Базовим елементом будь-якої системи сигналізації є шлейф сигналізації (ШС), який є електричним ланцюгом, що сполучає вихідні ланцюги оповісників, містить допоміжні (виносні) елементи (діоди, конденсатори, резистори), сполучні дроти і призначений для передачі на ПКП сигналів про проникнення, спробу проникнення.

Коли спрацьовує будь-який оповісник в шлейфі, відповідний сигнал приходить на вузол контролю стану ШС, який аналізує тривалість сигналу, що поступив. Пройшовши через вузол контролю стану ШС, сигнал надходить до вузлу пам’яті (де запам’ятовується) та вузлу обробки сигналу. Останній переводить ПКП до режиму «тривога», при якому сигнальне реле включається,

світловий сигналізатор переходить в переривистий режим роботи, а звуковий – включається на певний час.

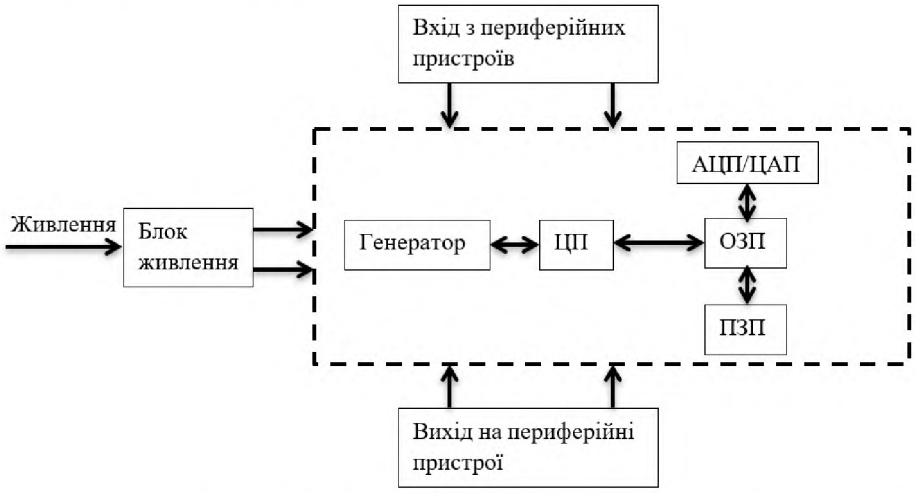

Рис. 2.8. – Узагальнена функціональна схема ПКП:

ЦП – центральний процесор; ОЗП – оперативно запам'ятовуючий пристрій; ПЗП – постійно запам'ятовуючий пристрій; АЦП/ЦАП – аналогово-цифровий перетворювач / цифро-аналоговий перетворювач.

У системах централізованої охорони сигнальні реле підключаються до крайових пристроїв систем передачі сповіщень, за допомогою яких інформація передається на ПЦС.

Після закінчення часу охорони відбувається зняття об'єкту з охорони. При цьому ПКП відключається від стеження за станом відповідного шлейфу. Узяття на охорону і зняття з охорони здійснюється або за допомогою клавіатури, або за допомогою ключів – доступу.

ПКП стежить за станом підключених датчиків (норма/тривога). Якщо система знаходиться під охороною та один з підключених датчиків переходить в режим «тривога», контрольна панель активує підключені сигнальні пристрої по заданому алгоритму.

2.3. Приймально-контрольний пристрій системи захисту периметру.

Як зазначалось вище, ПКП призначений для організації охоронної сигналізації. Він є центральним елементом в охоронній системі, підключається до сповіщувачів, які виявляють факт проникнення порушника на об'єкт, що охороняється.

У приймально-контрольний пристрій надходять сигнали сповіщувачів, які активують систему тривоги при несанкціонованому відвідуванні об'єкта, що охороняється. Приймально-контрольний пристрій є апаратною системою, яка може включати в себе керуючий модуль, блоки, які приймають і реєструють сигнали; блок живлення, виконавчі модулі (блоки реле), а також клеми, які підключають шлейфи сигналізації. Все перераховане встановлено в корпусі, обладнаному екраном і панеллю керування. Також до ПКП можуть підключатись клавіатури для програмування, різні (світлові, звукові, інші.) оповіщувачі.

ПКП систем охорони периметру можна класифікувати за:

- інформаційною ємністю – визначається кількістю шлейфів сигналізації, контрольованих приладом;
- інформативністю – визначається кількістю сповіщень, сформованих ПКП (наприклад, "норма", "несправність", "тривога" і т.д.).

ПКП виконують наступні основні функції:

- приймання та обробка сигналів від сповіщувачів,
- живлення сповіщувачів (по ШС або окремій лінії),
- контроль стану ШС,
- передачу сигналів на пункт централізованого спостереження (ПЦС),
- управління звуковими та світловими сповіщувачами,
- забезпечення процедур взяття під охорону і зняття об'єкта з охорони,
- контроль своєчасного прибуття групи затримання.

2.4. Вибір та обґрунтування електричної принципової схеми приймально-контрольного пристрою системи захисту периметру приватного об'єкту.

В кваліфікаційній роботі магістра використовувалась схема, яка представлена на рис. 2.9 та має наступні можливості:

- Спостереження за станом чотирьох шлейфів сигналізації (ШС) у всіх режимах роботи, крім режиму «Програмування», і відображення стану шлейфів за допомогою світлодіодних індикаторів, розташованих на передній панелі приладу (свічення індикатора – «шлейф в нормальному стані», в іншому випадку – присутній обрив або замикання шлейфу сигналізації).
- Підтримка приладом наступних типів зон (шлейфів) сигналізації:
- «Нормальна» (сигнал «Тривога» формується відразу при надходженні сигналу порушення цілісності шлейфу сигналізації, шлейф після спрацювання не відновлюється);
- «Із затримкою» (користувачеві надається час на вихід і на вхід, щоб можна було встигнути включити прилад і покинути об'єкт або розкрити об'єкт і відключити прилад);
- «Коридор» (при спрацьовуванні зони та подальшого її повернення в нормальний стандартний тип зона знову береться під охорону);
- «Цілодобова, пожежна» (шлейф сигналізації постійно під охороною, зняття та взяття проводиться за допомогою спеціальної SMS-команди);
- «Цілодобова, тривожна кнопка» (шлейф сигналізації постійно під охороною, зняття та взяття проводиться за допомогою спеціальної SMS-команди, при спрацьовуванні шлейфу проводиться тільки дозвін, відправлення SMS-повідомлення про саботаж, сирена при цьому не вмикається);
- «Відключена» (система не реагує ні на які зміни на вході ШС).

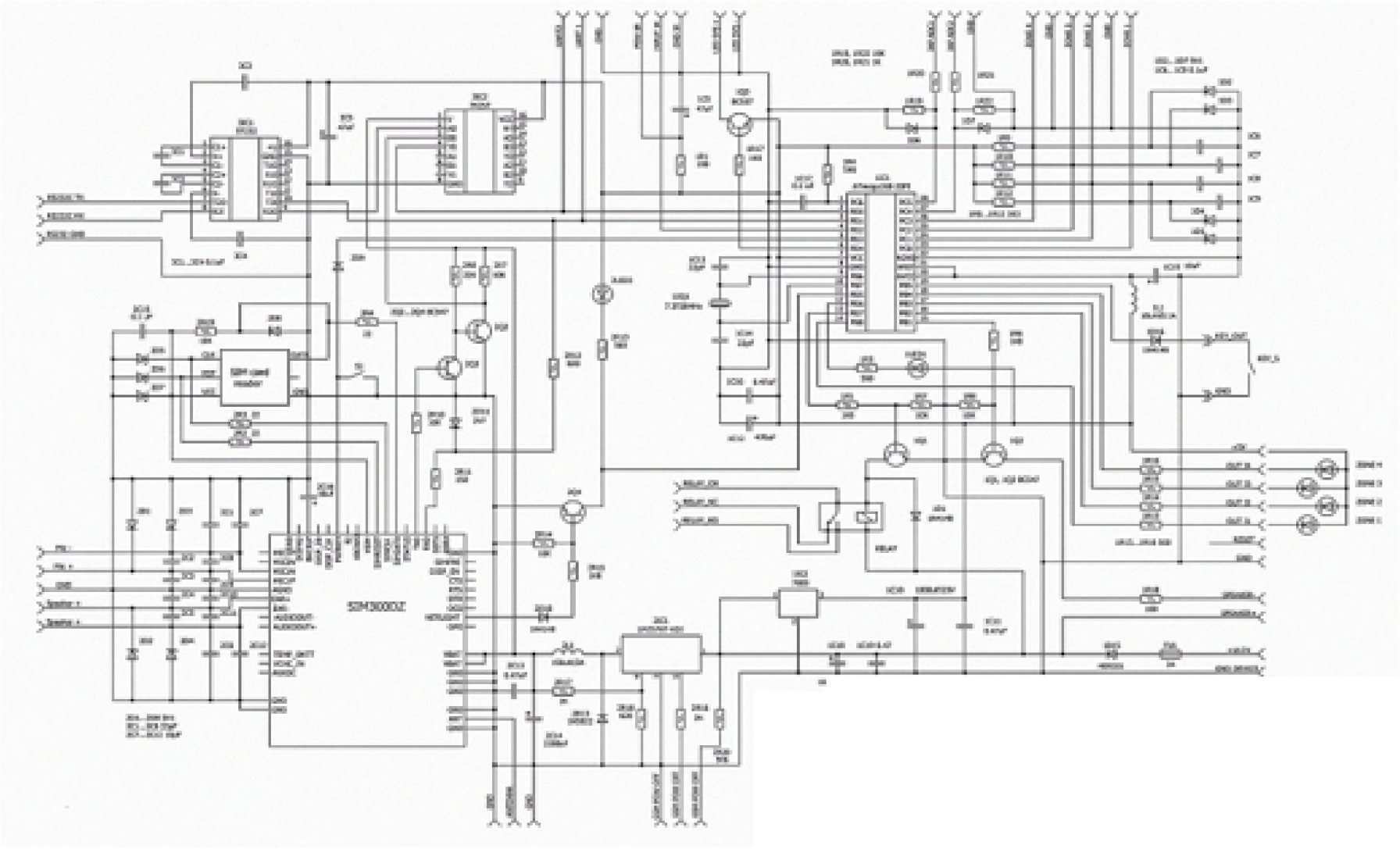

Рис. 2.9 – Не модернізована електрична
принципова схема ПКП

- Включення режиму «Охорона» за допомогою «прихованої», або «секретної» кнопки, «секретного» перемикача (замість якого може бути використана клавіатура з замикаючими контактами, типу «Satel»), пульта дистанційного керування, ключа TouchMemory (Dallas) або додаткової клавіатури , залежно від прошивки контролера.
- Підтримується два режими роботи приладу:

✓ сигналізація GSM (GSM-термінал підключений і з ним здійснюється обмін даними);

✓ автономна сигналізація (GSM-термінал не бере участі в роботі системи, пристрій працює як автономна сигналізація).

- Зняття з охорони і постановка під охорону за допомогою дзвінка з певного телефону (може бути вимкнено) з передачею відповідного SMS про стан системи. Передача SMS-повідомлення, що підтверджує взяття об'єкта під охорону (може бути вимкнено).
- Відправка SMS-повідомлень і автодозвін на три мобільних або стаціонарних (якщо підтримується підтримка SMS-функцій оператором зв'язку) номери телефонів.
- Переключення приладу в режим «Знятий з охорони» за допомогою тільки пульта дистанційного керування, клавіатури, шляхом прийому SMS-повідомлення з мобільного номера 1 і (або) дозвіну з цього номера (може бути вимкнено), а також «секретного» перемикача, залежно від прошивки контролера.
- Можливість дистанційного керування пристроєм шляхом передачі SMS-повідомлень певного змісту (може бути відключена).
- Можливість прослуховування охоронюваного об'єкта шляхом дзвінка на номер SIM-карти системи (за наявності внутрішнього мікрофона в GSM-терміналі, також може бути відключена).
- Програмування основних функцій і параметрів приладу (номери телефонів, час затримки, час роботи сирени і т.д.) за допомогою комп'ютерної програми Lite Programmer в режимі «Програмування» приладу. При цьому вихід

USB-порту комп'ютера (виходи RxD і TxD) підключаються до відповідного роз'єму приладу сигналізації за допомогою спеціального кабелю.

- Подача приладом певного сигналу користувачеві про нестачу коштів на рахунку мобільного карти.
- Подача приладом певного сигналу користувачеві про відсутність сигналу зв'язку з мобільною станцією.
- Передача сигналу SMS при пропажі напруги живлення мережі (220В) в режимі "Охорона" (може бути вимкнено). Також при зниженні напруги живлення резервного джерела (акумулятора) нижче заданого рівня (8-9В) надсилається повідомлення, після чого прилад переходить в «сплячий» режим, вихід з якого можливий тільки при відновленні живлення (мережевого або акумуляторного).
- Застосування вбудованого модему GSM дозволяє обійтися без зайвих блоків і підключень, а також підвищити сумісність і стабільність зв'язку GSM-каналу.
- Прилад дозволяє здійснити комутацію зовнішніх звукових або світлових оповіщувачів (дзвінок, сирена, лампа) з робочою напругою до 250В і споживаною потужністю до 200Вт.

Після модернізації схеми на рис.2.9, вона отримала новий вигляд, який представлений на рис. 2.10.

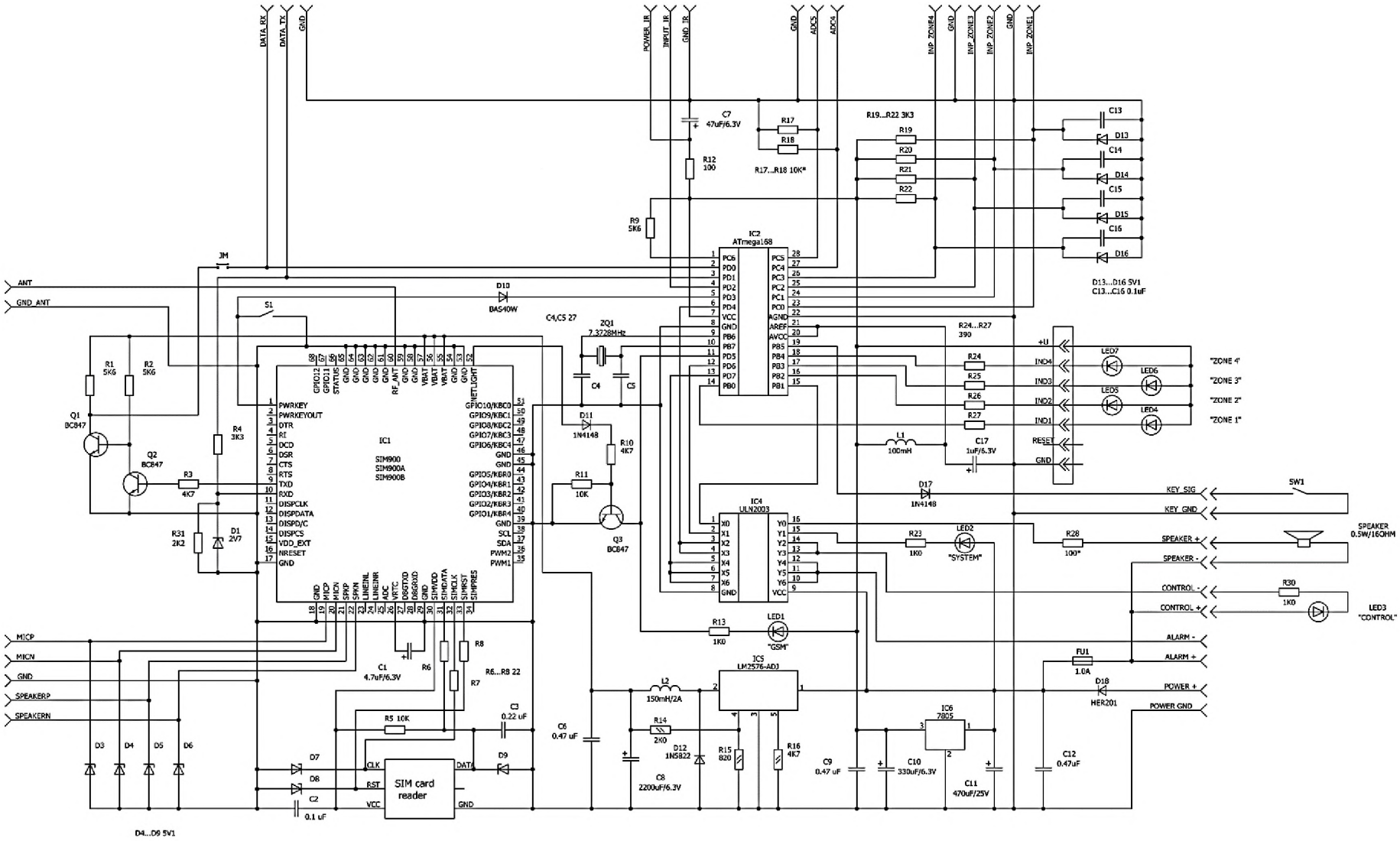

Рис. 2.10– Модернізована електрична принципова схема ПКП

Основні функціональні можливості ПКП залишилися після модернізації схеми та працюють с більшою надійністю.

Розглянемо більш детально принцип роботи пристрою.

На одній платі, для зручності та мінімізації загальних розмірів прибору, об'єднані три пристрої: блок мікроконтролера, модуль GSM, перетворювач USB-UART для обміну даними з комп'ютером в режимі програмування. Схема пристрою відрізняється порівняльною простотою і відносною стандартизацією елементної бази. Всі установки і функції приладів програмуються за допомогою спеціального програмного забезпечення, що виключає можливість перепрограмування на об'єкті, в тому числі і з кримінальною метою.

Ядром системи сигналізації є мікроконтролер ATmega168 виробництва відомої фірми Atmel Corp. Це досить відомі мікроконтролери, тому не будемо загострювати увагу на принципі їх роботи або архітектурі.

Мікроконтролер контролює стан шлейфів сигналізації, підключених до входів АЦП, і, залежно від режиму роботи, здійснює подальші дії, як то: дозвін і відсилання SMS-повідомлень, включення реле сирени, і т.д. Входи АЦП PC0-PC3 призначені для контролю стану шлейфів сигналізації, МК проводить вимірювання напруги на цих виводах, і, в залежності від напруги, формує сигнал «обрив», «норма» або «замикання». На PC5, PC6 подаються напруги з виходу блоку живлення для контролю значень.

В якості GSM-модуля обраний широко відомий модуль SIM900 виробництва китайської фірми SimCom. Для живлення модуля застосований імпульсний стабілізатор напруги на мікросхемі LM2576T-ADJ. У схемі використовуються контрольні світлодіоди: LED2 - контроль роботи системи (в робочих режимах блимає з частотою 3-5 разів на секунду, в режимі програмування горить постійним світлом), LED1 - контроль роботи модуля GSM (при наявності зв'язку і роботи модуля моргає з частотою 1 спалах протягом 2-3 секунд, в інших випадках є проблеми зі зв'язком або з самим модулем). Крім цього, до виводах IND1 ... IND4 підключаються світлодіоди

контролю стану шлейфів сигналізації (LED4...LED7 - катоди, + U - загальний анод).

KEY_S - власне, сама «секретна» кнопка або перемикач. SPEAKER - роз'єм для підключення динаміка, він може бути на будь-який опір, потужність не менше 0,25 Вт.

Застосовувані елементи і комплектуючі як вітчизняного, так і імпортного виробництва. Була обрана друкована плата зі застосуванням SMD елементів, тому перелік обмежений. Діоди - КД521, КД522, стабілітрони на 5В - КС147, КС156. Мікроконтролер - ATmega168, в будь-якому корпусі. Замість логічної мікросхеми 74257 можливе застосування 74HC257, 74HCT257, 74HC157, і навіть К555КП11. 3IC1 - ST232, MAX232.

Технічні характеристики:

- Кількість шлейфів сигналізації - 4.
- Опір виносного елемента (кінцевого), кОм - 2,7.
- Максимальний опір шлейфа охорони без урахування опору виносного елемента, Ом - 750.
- Напруга живлення мережі змінного струму, В - 220 (110 ... 260 при використанні імпульсного джерела живлення)
- Напруга живлення постійного струму, В - 12 (8 ... 17, без використання акумулятора резервного джерела живлення; 8 ... 25 якщо не використовуються АКБ і активні датчики сигналізації).
- Споживана потужність від мережі змінного струму, в наступних режимах роботи (без підключених активних датчиків сигналізації), не більше:
  - «Черговий», без використання GSM-модуля - 6 Вт;
  - «Черговий», при використанні GSM-модуля - 11 Вт;
  - «Охорона», при використанні GSM-модуля - 12 Вт;
  - «Тривога», при використанні GSM-модуля і вимкненою сирени - 16 Вт;
  - Пікове споживання - 43 Вт

- Споживаний струм від джерела постійного струму (без підключених активних датчиків сигналізації), при напрузі 12,6 В, в наступних режимах роботи, не більше:
- «Черговий», без використання GSM-модуля - 0,16 А;
- «Черговий», при використанні GSM-модуля - 0,23 А;
- «Охорона», при використанні GSM-модуля - 0,28 А;
- «Тривога», при використанні GSM-модуля і вимкненою сирени - 0,34 А;
- Пікове (імпульсний) споживання - 1,8 А.
- Підтримувані стандарти GSM: 900/1800/1900 MHz.
- Максимальний розмір текстового повідомлення SMS, символів - 85 (при використанні латиниці в повідомленнях).
- Межі установок часу:
- Час затримки на вхід - 0 ... 150 секунд;
- Час затримки на вихід - 0 ... 250 секунд;
- Час роботи сирени - 30 ... 250 секунд[19].

Основні зміни та нововведення:

1) Заміна старого GSM модуля SIM300DZ на новий SIM900. Модуль є чотиридіапазонний GSM / GPRS прилад, що працює на частотах 850/900/950/1900 МГц, призначений для передачі голосу, даних, SMS повідомлень, тощо.

Рис. 2.11 – Зовнішній вигляд модуля SIM900

Основні технічні характеристики модуля - Діапазон частот: GSM850, EGSM900, DCS1800, PCS1900; - сумісність з GSM phase 2/2 +; Випромінювана потужність: class 4 (2W / 900 MHz), class 1 (1W / 1800 MHz); Управління: AT commands (GSM 07.10); Напруга живлення модуля: 3,4 - 4,5 В; Струм споживання: в сплячому режимі - 1,5 мА; в режимі передачі - до 500 мА; максимальний - 1,8 А; Робоча температура: -30 ... +80 С; Розміри: 24x24x3 мм; Маса: 3,4 г.

Як можна побачити, даний модуль за габаритами відрізняється від свого попередника, модуля SIM300, приблизно в півтора рази. Та за параметрами і функціональністю теж перевершує на порядок.

2) Інтерфейс MAX232 (перетворювач RS232-UART(Рис2.12)), змінено на більш сучасний USB-UART(Рис.2.13). Адже при програмуванні функцій пристрою в більшості випадків персональний, стаціонарний, комп'ютер буде недоступний, все це, в основному, робиться на місці за допомогою ноутбука. А в більшості ноутбуків порт RS232 вже давно відсутній, там USB. До того ж, перетворювач використовується практично один раз, в інших випадках він просто споживає струм, що для автономних пристроїв, особливо тих, які більшу частину робочого часу працюють від акумуляторів, абсолютно неприпустимо.

Рис. 2.12 – RS232-UART

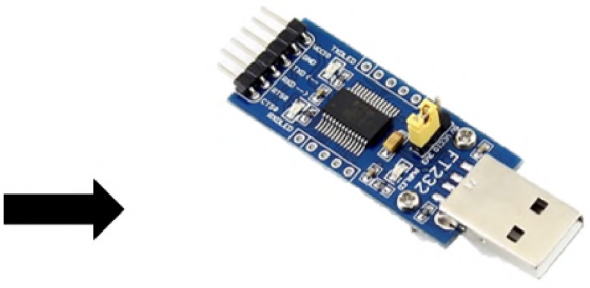

Рис. 2.13– USB-UART

3) Заміна діоду D10. Дана проблема виявлялася вже кілька разів. Основні показники: модуль не вмикається мікроконтролером, а примусово вмикається. Як з'ясувалося, проблема полягає в тому, що діод D10 (1N4148) не підтягував повністю до маси, і напруга на контакті включення модуля була набагато більше допустимої і автоматичне включення не відбувалося. Рішення проблеми виявилося в заміні діода 1N4148 на будь-який Шоттки, ті ж BAS40, BAT85, тощо.

2.5. Методика оцінки ризиків кібербезпеки в системах Інтернет-речей.

Дійсно, очевидно, що неможливо побудувати ідеальну систему оцінки ризиків для пристроїв охоронної системи, якщо вектори ризику або атрибути ризику не визначені. На додаток до вихідних векторів ризику від традиційних систем, спеціальні вектори таких пристроїв також повинні бути прийняті до уваги для системи оцінки ризиків охоронної системи в цілому.

Було визначено чотири типи класів векторів ризику охоронної системи, яка схожа до класів векторів ризику IoT: орієнтовані на хмару, орієнтовані на реальний час, автономні та орієнтовані на відновлення.

Розглянемо список векторів ризику для кожного з цих класів, які використовуються для оцінки ризику кожної системи IoT та наведемо у таблиці 2.1.

Шкала та ранжування оцінки ризику. Першим кроком в оцінці ризику є визначення загроз для активу IoT, що розглядається, з наступним визначенням внутрішнього ризику та його впливу. Вплив ризику має такі оцінки, як високий – тобто вплив може бути суттєвим, середній – вплив буде шкідливим, але його можна відновити та/або є незручним і низький – вплив буде мінімальним або взагалі відсутнім.

Наступним кроком є визначення ймовірності даного експлойту з урахуванням середовища контролю, яке має приватний об’єкт. Приклади рейтингів вірогідності:

1. Високий – джерело загрози має високу мотивацію та достатньо спроможність, а засоби контролю для запобігання використанню вразливості неефективні.

Таблиця 2.1. – Список векторів ризику

№	Пов'язані з хмарою	Реальний час	Автономний	Відновлення
1	Платформи хмарних обчислень	Оперативні моделі в реальному часі	Автоматизовані середовища	Економічний ефект
2	Навички хмарних технологій	Індивідуальні продукти	Робототехніка та автономні системи	Оцінка впливу
3	Хмарні центри обробки даних	Платформа для отримання інформації в реальному часі	Робототехніка та штучний інтелект	SWOT-аналіз (сила, слабкість, можливості, загроза).
4	Хмарне Пов'язані з хмарою	Цифрові записи реального часу та сумісні записи	Робототехніка в IoT	Фінансово-податковий державний контроль
5	Хмарний моніторинг	Кіберфізичні системи	Штучний інтелект і системи управління	N/A
6	Інтеграція в хмарні обчислення	N/A	N/A	N/A
7	Хмарні мережі безпеки	N/A	N/A	N/A

2. Середній – джерело загрози вмотивоване та спроможне, але існують засоби контролю, які можуть перешкодити успішному використанню вразливості.

3. Низький – джерело загрози не має мотивації чи можливостей, або існують засоби контролю, щоб запобігти або, принаймні, значно перешкодити використанню вразливості.

Рейтинг ризику можна розрахувати як рейтинг ризику (rr) = вплив (якщо використовується) × ймовірність (експлойту).

Деякі приклади рейтингу ризику:

1. Серйозний – існує значна та термінова загроза для організації, і усунення ризику повинно бути негайним.

2. Підвищений – існує життєздатна загроза для організації, і усунення ризику має бути завершено в розумний період часу.

3. Низький – загрози є нормальними і загалом прийнятними, але все ж можуть мати певний вплив на організацію.

Впровадження додаткових удосконалень безпеки може забезпечити додатковий захист від потенційних або непередбачених наразі загроз.

Розрахунок рангу ризику виконується на основі кількісного зважування (це стосується впливу ризику) та оцінки ризику (це стосується ймовірності ризику), як пояснено вище.

Таблиця 2.2 показує, як можна зробити ранжирування для кожного ризику. Якщо ранг ризику дуже високий, то ризик має серйозний вплив. Існує п’ять рівнів ризиків IoT на основі розрахунку рангу. Існують ризики з рангом $\leq$ 10, і ці ризики належать до дуже низького рівня, оскільки вони не варті розгляду. Необхідно враховувати низькі та помірні ризики. Високі та дуже високі ризики потребують кращого запобігання, оскільки їхній вплив є сильним.

Таблиця 2.2 показує рейтинг ризику для деяких векторів IoT. Згідно з документом NIST-IoT, ці одиничні вектори належать до категорії «захист пристрою». Як згадувалося, інші дві категорії – це захист даних і особиста конфіденційність. Захист пристрою включає чотири сфери зниження ризиків, включаючи управління активами, керування вразливістю, керування доступом і виявлення інцидентів.

Управління активами: для підтримки точної інвентаризації всіх пристроїв IoT та їхніх відповідних характеристик, що допомагає використовувати цю інформацію для цілей управління ризиками кібербезпеки та конфіденційності. Управління вразливістю: для виявлення та усунення відомих уразливостей у програмному забезпеченні та мікропрограмі пристроїв Інтернету речей, щоб зменшити ймовірність і полегшити використання та компрометацію.

Таблиця 2.2. – Ранжування для кожного ризику

Якісний рівень	Кількісна вага (Вт)	Оцінка ризику (S)	Ранг r=W*S (приклад)	Діапазон рангів ризику	Опис
Дуже високо	96-100	1,0	97×1,0=97	81-100	Ризик викликає дуже велике занепокоєння; сильний вплив
Високий	80-95	0,8	90×0,8=72	51-80	Ризик викликає велике занепокоєння
Середній	31-79	0,5	50×0,5=25	21-50	Ризик викликає помірне занепокоєння
Низький	11-30	0,2	25×0,2=5	5-20	Ризик не викликає занепокоєння
Дуже низько	0-10	0,1	10×0,1=1	0-4	Ризик не викликає занепокоєння

Управління вразливістю: для виявлення та усунення відомих вразливостей у програмному забезпеченні та мікропрограмі пристроїв

Інтернету речей, щоб зменшити ймовірність і полегшити використання та компрометацію.

Керування доступом: для запобігання несанкціонованому та неправильному фізичному та логічному доступу людей, процесів та інших комп'ютерних пристроїв до пристроїв IoT.

Виявлення інцидентів безпеки пристрою: для моніторингу й аналізу активності пристроїв Інтернету речей на ознаки інцидентів безпеки пристрою. Виявлення вразливості активів є одним із найважливіших кроків у процесі оцінки ризиків. Пристрої IoT є основними активами, які тут розглядаються. Приклади векторів Інтернету речей і їх обчислення показників ризику наведено в таблиці 2.3 для кожної з вищезазначених областей зменшення ризику в категорії «Захист пристрою». Ідеальним наступним кроком є визначення загроз, а також впливу та ймовірності ризиків. Мета полягає в тому, щоб захистити пристрій IoT від атак, таких як атаки розподіленої відмови в обслуговуванні (DDoS), прослуховування мережевого трафіку або компрометації інших пристроїв у тому ж сегменті мережі. Як і в цьому прикладі, рейтинг можна розрахувати для ризиків у кожній категорії, включаючи безпеку даних і конфіденційність.

Таблиця 2.3 показує деталі рангу кожного одиничного вектора та наслідки рангу ризику. Наприклад, якщо пристрій IoT не підтримує використання надійних облікових даних, цьому вектору IoT надається вага 95 разом із оцінкою ризику 0,9, що обчислює рейтинг ризику як 85. Цей ранг має високий пріоритет через більшу ймовірність несанкціонованого доступу та підробки через неправильне використання облікових даних

Таблиця 2.3 – Приклади векторів Інтернету речей і їх обчислення показників ризику

Вектор ризику	Кількісна вага (Вт)	Оцінка ризику (S)	Ранг r=W*S	Опис /Наслідки
Пристрій IoT не має унікального вбудованого	75	0,8	60 (серед-ній)	Це впливає на віддалений доступ і керування

ідентифікатора				вразливими місцями
Виробник не розкриває зовнішні залежності пристрою IoT	60	0,7	42 (середній)	Управління ризиком зовнішнього програмного забезпечення та послуг неможливе
Пристрій IoT не може мати виправлення чи оновлення програмного забезпечення	60	0,6	36 (середній)	Неможливо автоматично визначити відомі вразливості
Пристрій IoT не підтримує приховування відображених символів пароля	80	0,7	56 (середній)	Збільшує ймовірність крадіжки облікових даних
Пристрій IoT не може реєструвати свої робочі події та події безпеки	70	0,6	42 (середній)	Імовірність виявлення зловмисних дій значно менша

Таким чином у кваліфікаційній роботі магістра наведено короткий виклад оцінки ризиків IoT разом із системою оцінки ризиків, щоб підкреслити кількісний підхід. Це дослідження було зосереджено на ширшому домені IoT, досліджено приклади векторів Інтернету речей і проведено обчислення їх показників ризику.

2.6. Розробка та дослідження системи охорони периметру.

Дослідження та аналіз системи охорони периметру полягає у проєктуванні, тобто оптимальному розташуванні системи відеоспостереження, розрахунках потрібного місця на жорсткому диску, яке залежить від роздільної здатності камери, стиснення потоку відео, кількості кадрів в секунду, кількості камер та способу запису відео – по руху або постійна.

Проєктування та розрахунки проводились за допомого професійного програмного забезпечення IP Video System Design Tool. Основні можливості ПЗ: дозволяє швидко знайти оптимальну кількість і розташування камер відеоспостереження, виконати розрахунок системи відеоспостереження, визначити зони огляду, розташувати камери на існуючому або створеному з нуля плані приміщення, розміщувати тестові об’єкти і перешкоди: стіни, автомобілі, людей в тривимірному просторі для виявлення мертвих зон.

Основні етапи роботи з програмою.

1) Запускаємо програму, на першій вкладці програми «Креслення установки камери» (рис. 2.14) розташовані вид збоку і вид зверху для камер, які використовуємо. В нашому випадку це камери DS-2CE56C0T-IRM фірми Hikvision.

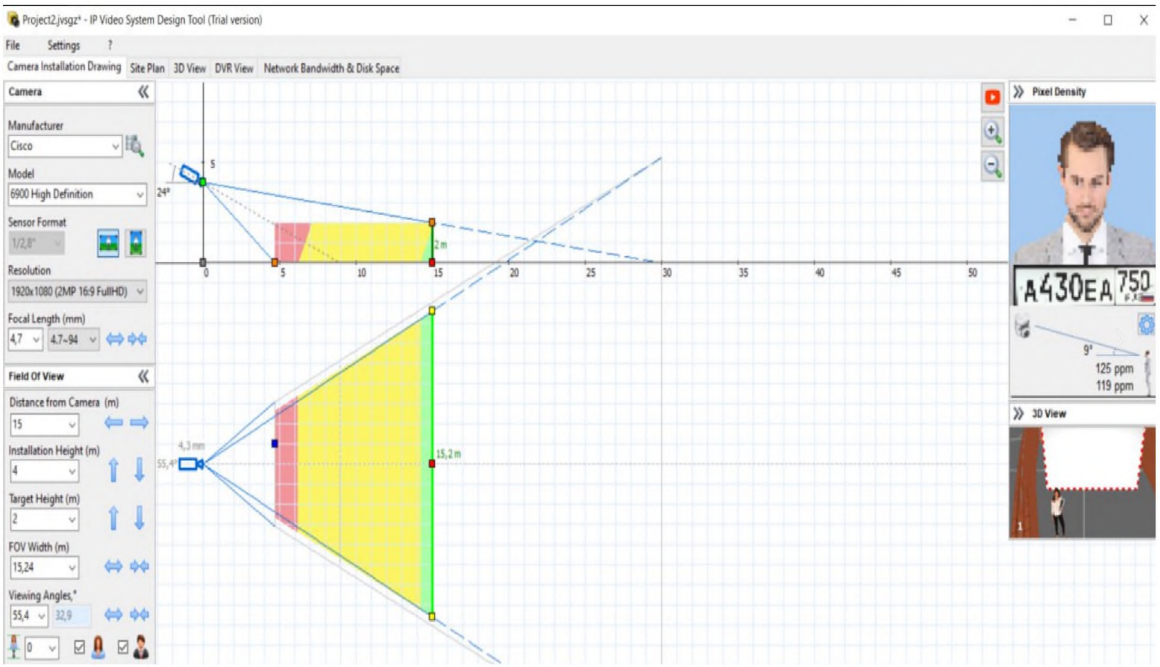

Рис. 2.14 – Налаштування камери (DS-2CE56C0T-IRM фірми Hikvision)

2) Далі переходимо до вкладки «План місцевості». Завантажуємо креслення нашого об’єкту (рис. 2.15). Потім створюємо 3D моделі потрібних нам ділянок (рис 2.16) та видаляємо креслення (рис 2.17).

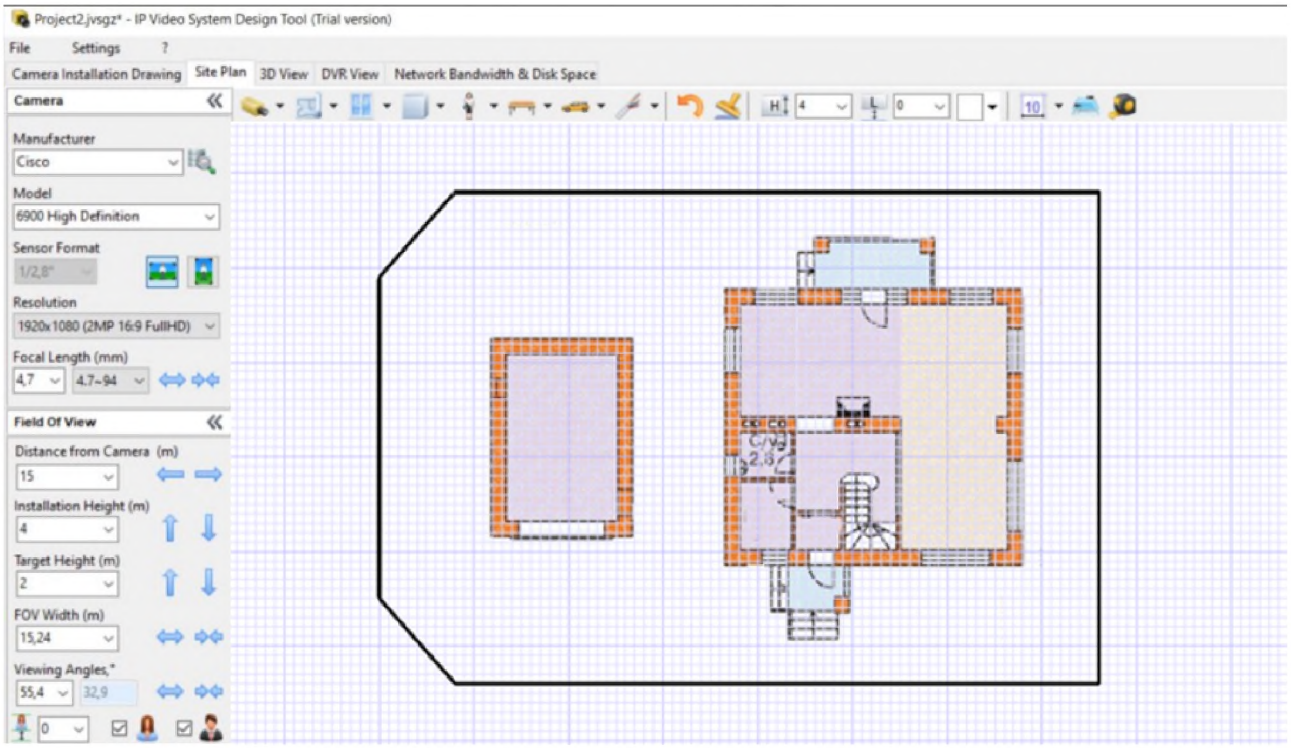

Рис. 2.15 – Завантаження креслення об’єкту

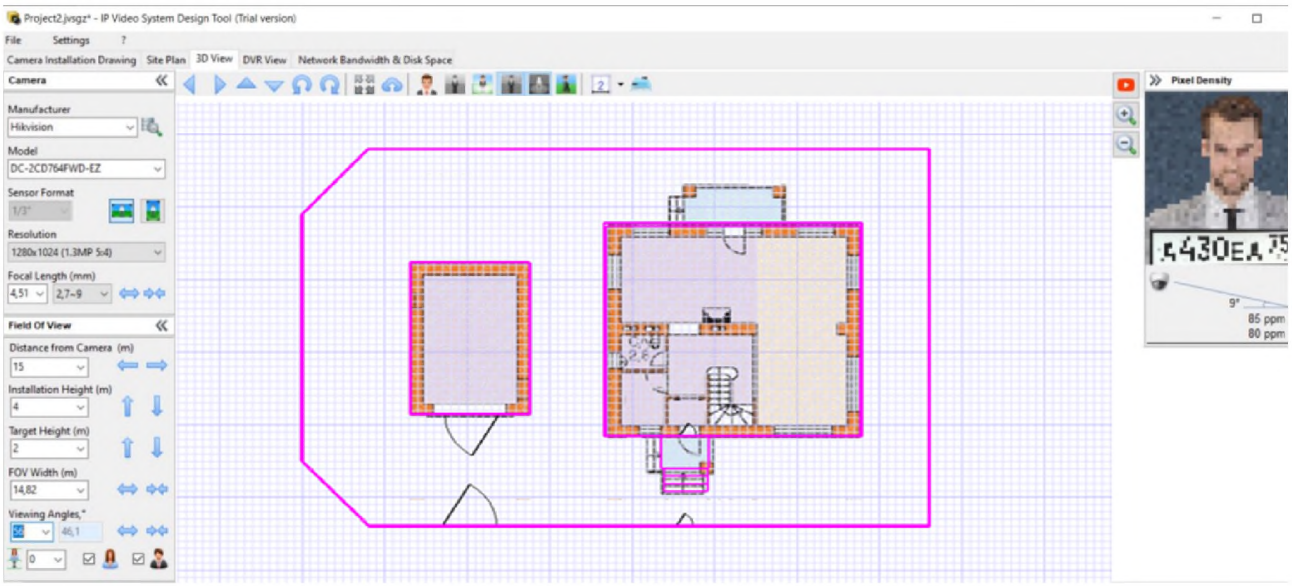

Рис. 2.16 – Створення 3D моделей

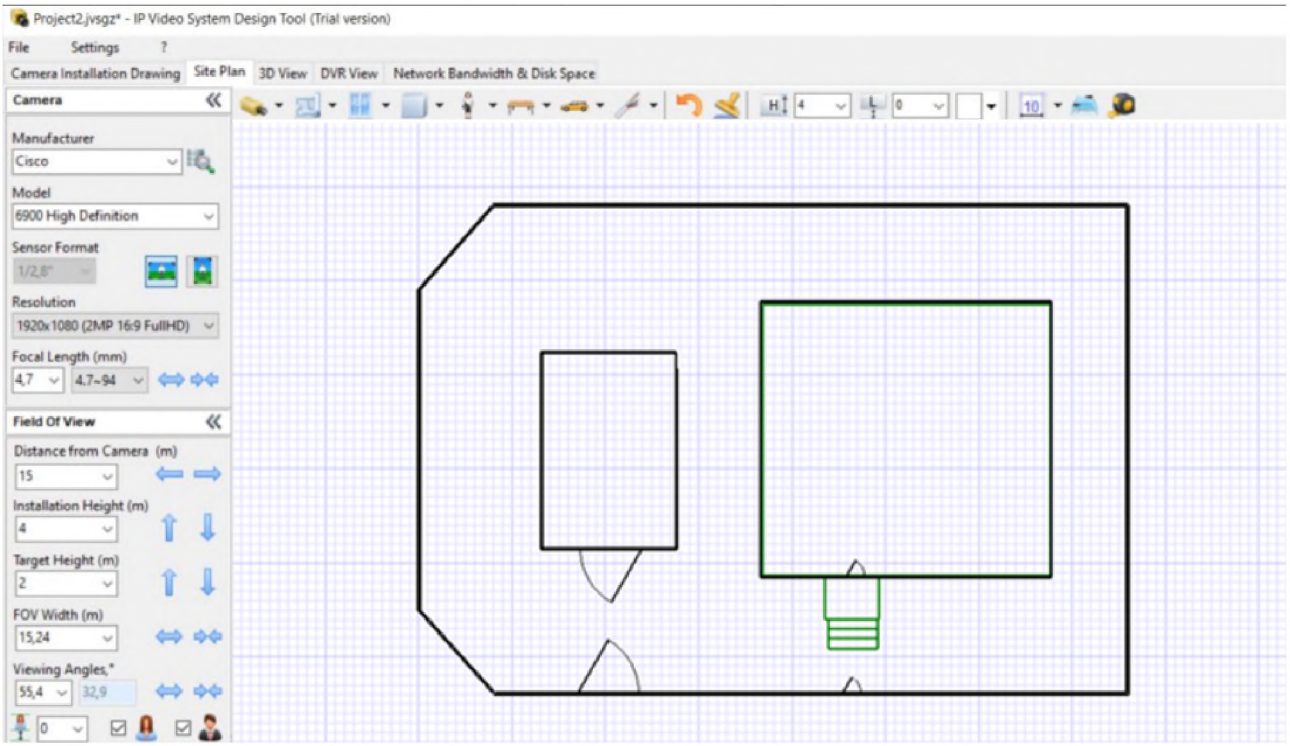

Рис. 2.17 – Видалення креслення

3) Далі на цій же вкладці розставляємо камери у потрібних нам місцях (рис. 2.18).

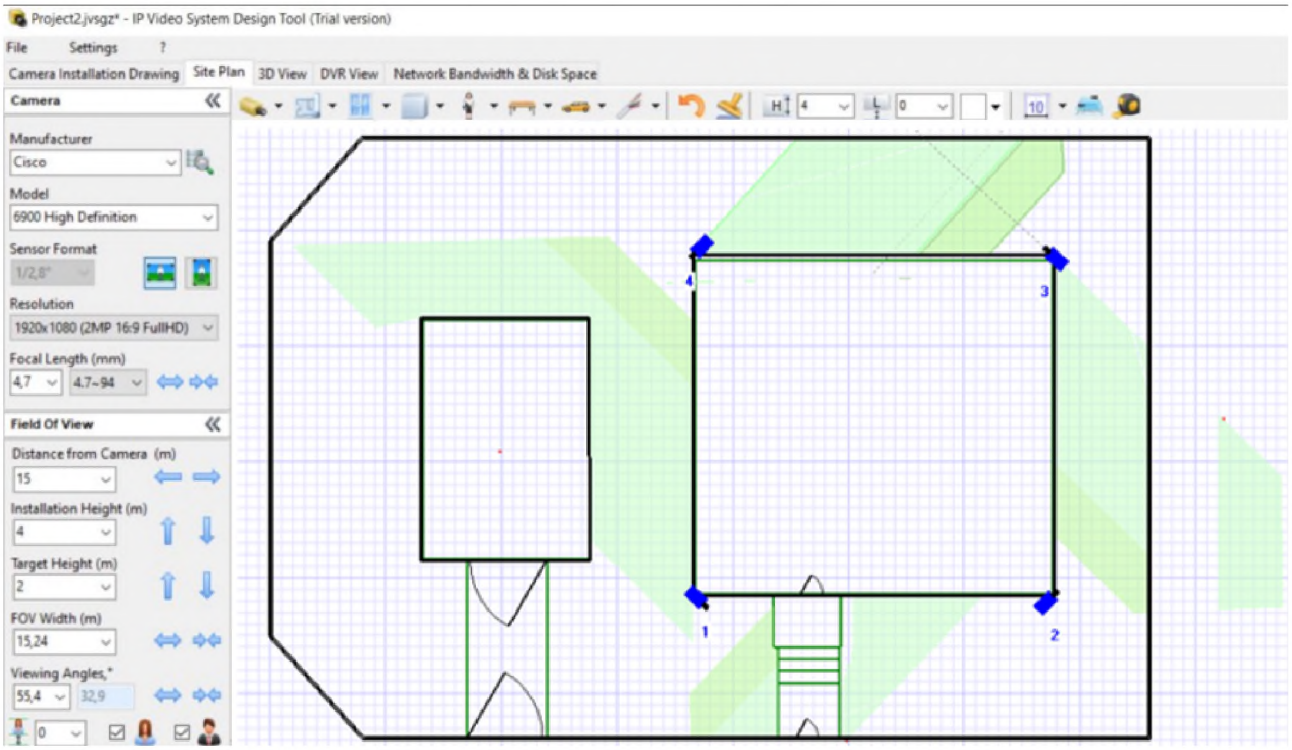

Рис. 2.18 – Розташування камер

4) На вкладці «3D вид» можемо проглянути реальне зображення з наших камер (рис. 2.19, 2.20, 2.21, 2.22).

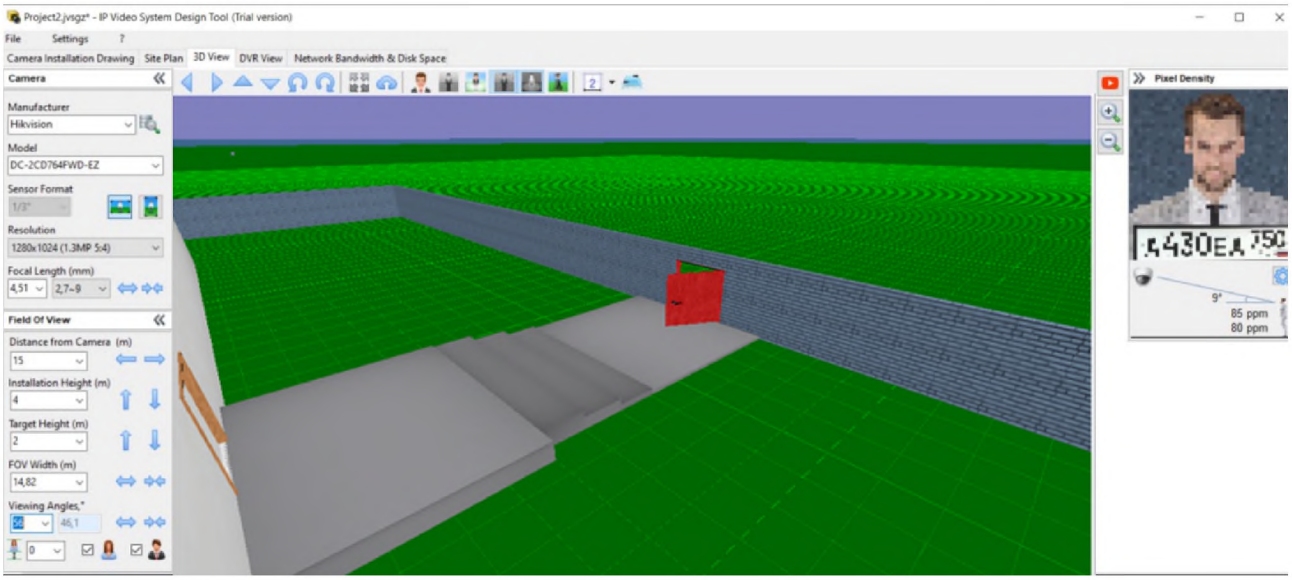

Рис.2.19. – Вид з камери 1

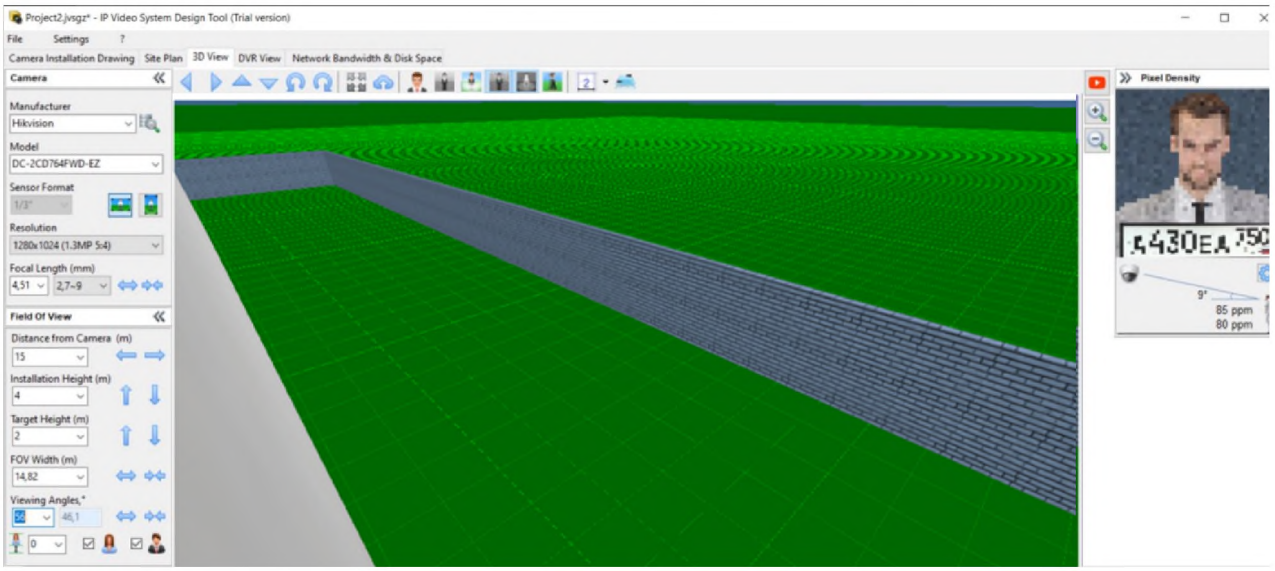

Рис.2.20. – Вид з камери 2

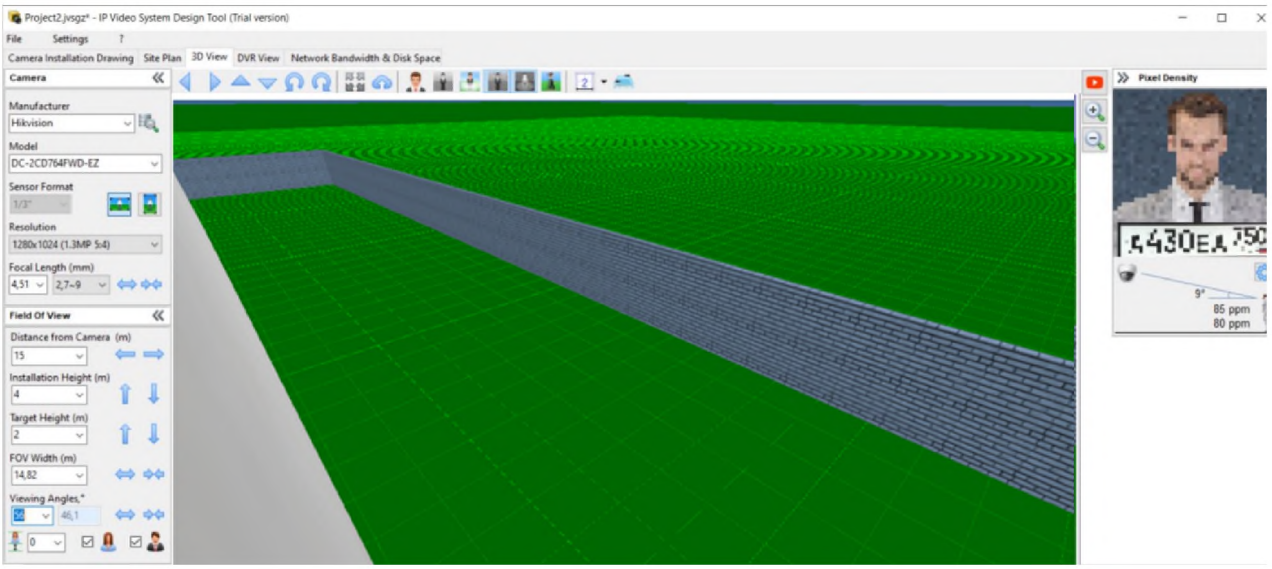

Рис.2.21. – Вид з камери 3

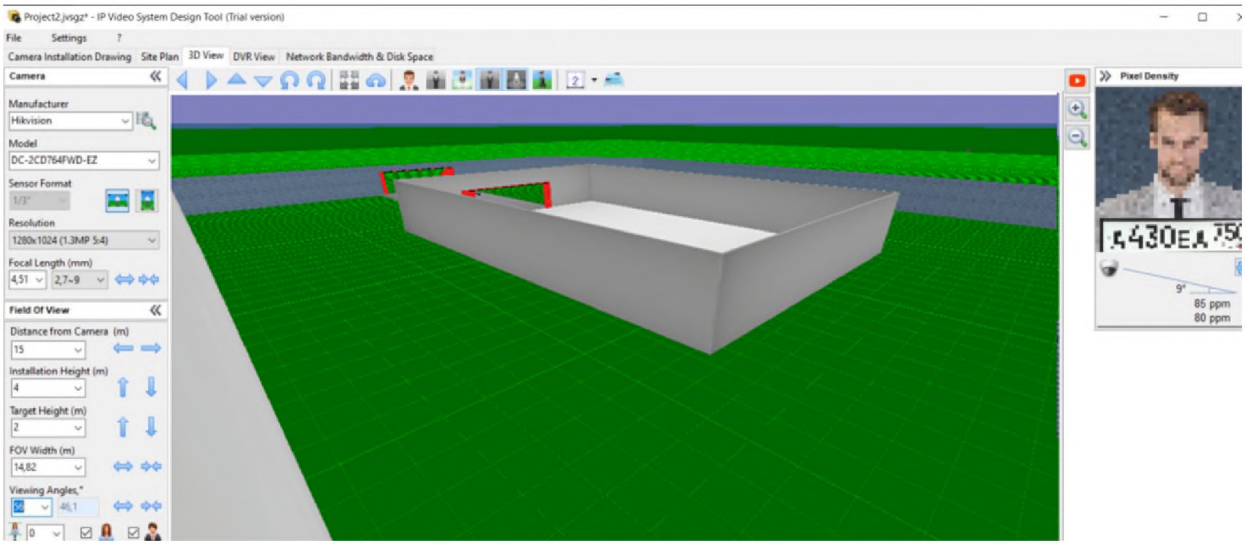

Рис.2.22. – Вид з камери 4

Таким чином, завдяки такому розташуванню, отримаємо ефективний захист периметру з мінімальною кількістю «мертвих зон». Отже, камери обрані та розставленні, тепер розрахуємо необхідну кількість місця на диску для зберігання відеоархіву і необхідний обсяг трафіку для реєстратора.

5) Переходимо на вкладку «Трафік і Обсяг диску». Заповнюємо потрібні нам поля та отримуємо результат (рис. 2.23).

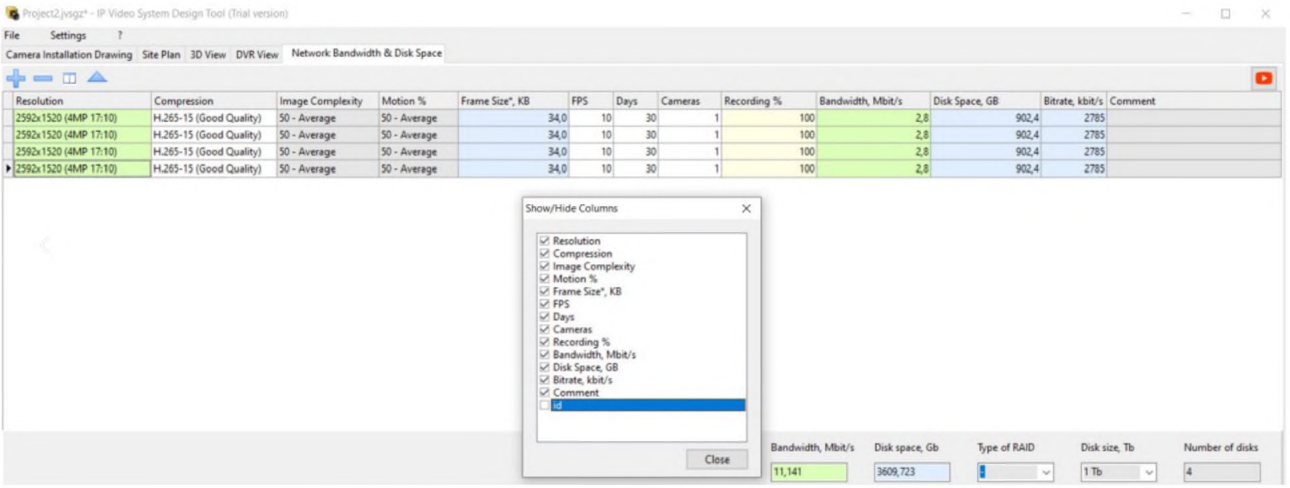

Рис.2.23 – Розрахунок об'єму жорсткого диску

Вибрані наступні показники відеокамери: кодек відео стиснення реєстратора – H.264-10 (Висока якість); кількість кадрів в секунду – 16 (оптимальна кількість кадрів); режим запису – постійний; кількість днів запису – 30.

В результаті отримали наступні дані: потрібний об'єм диску 917,2 ГБ (на 4 камери, по 229,3 ГБ кожна), обсяг мережевого трафіку для реєстратора 6,28 МБ/с (на 4 камери, по 1573 Кб/с кожна).

Для порівняння розрахуємо об'єм диску ручним способом.

Розрахунок розміру нестислого кадру.

Нестиснутий кадр в будь-якому вигляді, незалежно від того, що знімає камера, завжди має однаковий обсяг. Розрахунок розміру нестислого зображення здійснюється за формулою: ширина кадру × на висоту × на глибину кольору.

Глибина кольору вказується кількістю біт, що визначаються за кількістю кольорів: Ч-Б зйомка - 1 біт; 16 кольорів - 4 біт (достатній для передачі чіткого зображення); 256 кол. - 8 біт.; 16 млн. кол. - 24 біт.

Таким чином, розрахунок обсягу кадру з роздільною здатністю 1280 на 720 пікселів і глибиною 16 кольорів матиме такий вигляд: 1280 × 720 × 4 = 3686400 біт. Переведемо в кілобайти: 3686400 ÷ 8 ÷ 1024 = 450 Кбайт.

Також потрібно розрахувати архів.

Для розрахунку архіву записів системи відеоспостереження візьмемо орієнтовне значення обсягу нестислого зображення в роздільній здатності 1280×720, і розділивши на ступінь стиснення, в нашому випадку кодека H.264 (~74,9) отримаємо розмір стисненого кадру 6 Кбайт. 450 ÷ 74,9 = 6 Кбайт – розмір стисненого 1 кадру. Швидкість запису камери – 16 кадрів на секунду, к/с. Кількість запису кадрів за одну годину - 16 × 60 × 60 = 57600 к/год. Об'єм запису 1 камери за 1 годину – 57600 × 6 ÷ 1024 = 337 МБ. Об'єм запису за добу – 337 × 24 ÷ 1024 = 7,9 ГБ. Об'єм запису за місяць – 7,9 × 30 = 237 ГБ.

Так як камер у системі охорони периметру чотири, то в результаті отримаємо – 237 × 4 = 948 ГБ, що практично збігається з програмним розрахунком.

Результати програмної перевірки при використанні IP Video System Design Tool переконливо вказують на те, що дослідження системи охорони периметру виконує свої функції із захисту в повному обсязі.

2.7. Висновок

Проведений аналіз технічних засобів, що утворюють систему охорони периметру, наведено у розділі спеціальної частини. Всі вони відрізняються у схемо-технічних рішеннях, а саме відрізняються функціональними особистостями. Проведений вибір основних систем відеоспостереження на основі чого визначені структура та технічні особливості модернізованої системи охорони периметру. Все це враховано при проєктуванні системи охорони периметри приватного будинку.

Розроблені структурна, функціональна та електрична принципіальна схема. На основі спеціалізованого програмного забезпечення IP Video System Design Tool визначено основні етапи створення проєкту інтегрованої системи охорони приміщення приватного призначення і наведено рекомендації щодо налаштування та з'єднання елементів цієї інтегрованої системи охорони периметру на основі новітніх програмних і інженерних рішень.

З'ясовано, що інструменти в розглянутих програмах дозволяють провести визначення місць розташування мережних відеокамер, які дозволять усунути у процесі створення реального проєкту «сліпі» зони в тих місцях периметру охорони території, де найвищий рівень захисту повинен бути забезпечений згідно з вимогами замовника на 100 відсотків.

Також у розділі представлено оцінка ризиків IoT, яка надає можливість підкреслити кількісний підхід. Досліджено приклади векторів Інтернету речей і проведено обчислення їх показників ризику.

3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою даного розділу є обґрунтування економічної доцільності розробляти новий модифікований приймально-контрольний пристрій. Досягнення цієї мети потребує виконання таких розрахунків, як:

– опис базового об’єкту для розрахунків;

– порівняльна характеристика базового та нового об’єкту;

– розрахунок собівартості приймально-контрольного пристрою;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проєктування;

– річний економічний ефект від впровадження запропонованих заходів;

– показники економічної ефективності впровадження приймально-контрольного пристрою для захисту периметру.

3.1 Опис базового об’єкту

У якості базового об’єкту обираємо друковану плату приймально-контрольного пристрою DMA39-4Z (рис.3.1) розроблену компанією "digital Мікроавтоматика", яка знаходиться за адресою: Україна, м. Дніпро, вул. Запорізьке шосе, 56 [20].

Рис. 3.1 – ПКП DMA39-4z

Основні характеристики плати:

- 4 охоронні зони;
- 4 керовані виходи;
- 1 мікрофонний вхід;
- вхід "постановки-зняття" з охорони (можливість підключити клавіатуру);
- вхід для підключення провідного (настільного) телефону;
- десять номерів додзвону;
- голосове інтерактивне меню;
- здійснення дзвінків з підключеного настільного телефону;
- програмування з комп'ютера через COM порт, з настільного телефону або з віддаленого комп'ютера через Інтернет використовуючи HyperTerminal вашого комп'ютера;
- SMS звіт, за запитом, про настройки системи і стан рахунку;
- типи зон - кожна зона може бути:
    1. вхідна;
    2. миттєвого типу;
    3. прохідна;
    4. 24-х годинна;
    5. зона бездіяльності.

3.2 Порівняльна характеристика базового та нового об’єкту

Конструкція ПКП, розроблена в даному дипломному проекті має наступні відмінні характеристики:

- простота схеми (завдяки використанню сучасного мікроконтролера кількість деталей зведена до мінімуму, що спрощує збірку й виключає необхідність налагодження пристрою);
- індикація стану шлейфів сигналізації
- два режими роботи приладу:

- сигналізація GSM (GSM - термінал підключений і з ним здійснюється обмін даними);
- автономна сигналізація (GSM-термінал не бере участі в роботі системи, пристрій працює як автономна сигналізація).
- захист внутрішніх ланцюгів пристрою від невірного підключення полюсів зовнішнього джерела живлення;
- менший розмір самої друкованої плати

Очікується, що новий пристрій завдяки своїм перевагам буде користуватися більшою популярністю та знайде свого споживача.

3.3 Розрахунок собівартості ПКП

Розрахуємо собівартість розробленого ПКП за допомогою калькулювання, тобто визначимо собівартість одиниці продукції за встановленою номенклатурою витрат з урахуванням місця їх виникнення.

Статті калькуляції:

1. Основні та допоміжні матеріали, $С_м$;
2. Зворотні відходи, $С_{зв}$;
3. Покупні вироби і напівфабрикати, $С_{пв}$;
4. Паливо та енергія на технологічні цілі, $С_е$;
5. Основна заробітна плата робітників, $С_{оз}$;
6. Додаткова заробітна плата робітників, $С_{дз}$;
7. Соціальне відрахування $С_{сф}$;
8. Витрати на підготовку та освоєння виробництва, $С_{осв}$;
9. Амортизаційні відрахування, $С_{ав}$;
10. Витрати на утримання та експлуатацію обладнання, $С_р$;
11. Інші витрати, $С_{інш}$;
12. Загальновиробничі витрати, $С_{знв}$;
13. Виробнича собівартість, $С_{вс}$.

Основні та допоміжні матеріали

Витрати на основні й допоміжні матеріали визначаємо на основі норм витрат з урахуванням транспортно-заготівельних витрат, які становлять 12% від вартості основних та допоміжних матеріалів відповідно

$$C_м=(1+K_{тз})\cdot\sum_{i=1}^{n} H_м \cdot Ц_м, \quad (3.1)$$

де $H_м$ – норма витрат матеріалу; $Ц_м$ – оптова ціна матеріалів; $K_{тз}$ - коефіцієнт, який враховує транспортно-заготівельні витрати $K_{тз}$=12% від $C_м$; n – номенклатура матеріалів, які використовуються. Розрахунок наведено в табл. 3.1. та 3.2.

Таблиця 3.1 – Основні та допоміжні матеріали для виготовлення приладу за новим технологічним процесом

№	Найменування матеріалу	Одиниця витрат	Норма витрат	Ціна за одиницю, грн.	Вартість, грн.
1	Стеклотекстоліт фольгований двосторонній FR4	кг	0,25	115,00	28,75
2	Фоторезист	кг	0,2	150,00	30,00
3	Проявник	кг	0,25	31,44	7,86
4	Барвник метиленовий фіолетовий	кг	0,03	7,75	0,23
6	Хлорне залізо	кг	0,4	39,00	15,60
7	Ацетон	л	0,03	27,50	0,83
8	Віденське вапно BOSCH	кг	0.1	390,00	39,00
9	Флюс	кг	0,04	15,00	0,60
10	Припой	кг	0,02	57,70	1,20
11	Фарба ПФ-115П	кг	0,04	90,00	3,60

12	Лак електроізоляційний UC	кг	0,01	90,00	0,90
13	Спирт етиловий	л	0,04	70,00	2,80
	Разом				131,37

Таблиця 3.2 – Основні та допоміжні матеріали для виготовлення приладу за базовим технологічним процесом

№	Найменування матеріалу	Одиниця витрат	Норма витрат	Ціна за одиницю, грн	Вартість, грн
1	Стеклотекстоліт фольгований двосторонній FR4	кг	0,2	90,7	18,14
2	Вода дистильована	л	1,0	9,42	9,42
3	Змочувач	л	0,04	5,3	0,20
4	Поливініловий спирт	кг	0,14	110	15,4
5	Амоній двухромокислий	кг	0,25	18	4,5
6	Азотнокисле срібро	кг	0,2	150	30
7	Вуглекисла мідь	кг	0,15	234	35,1
8	Флюс	кг	0,044	15	0,66
9	Припой	кг	0,02	57,7	1,2
10	Гліцерин	кг	0,2	24	4,8
11	Мідний купорос	кг	0,3	124	37,2
12	Спирт етиловий	л	0,04	70	2,8
	Разом				159,42

Таким чином, вартість основних і допоміжних матеріалів з урахуванням транспортно-заготовчих витрат складає

$$C_{м\ (нов)} = 1{,}12 \cdot 131{,}37 = 147{,}13 \text{ грн.}$$

$$C_{м\ (баз)} = 1{,}12 \cdot 159{,}42 = 178{,}55 \text{ грн.}$$

Зворотні відходи в новому та базовому технологічному процесі відсутні

$$C_{зв(нов)} = 0;$$

$$C_{зв(баз)} = 0.$$

Вартість покупних виробів та напівфабрикатів

Розрахунок вартості покупних виробів визначаємо за цеховими або заводськими даними з урахуванням транспортно-заготовчих витрат, які становлять 12% від вартості матеріалів та розраховуються за формулою

$$C_{пв}=(1+K_{тз})\cdot\sum_{i=1}^{n} H_{пві}\cdot Ц_{пві}, \qquad (3.2)$$

де $H_{пві}$ – витрати i-го виду на одиницю продукції; $Ц_{пві}$ – ціна одного виду покупного виробу.

Таблиця 3.3 – Вартість покупних виробів для нового приладу

№	Покупні вироби	Тип, марка	Кількість на одиницю виробу, шт	Ціна за штуку, грн	Загальна вартість, грн
1	Мікроконтроллер	ATmega168	1	136	136
2	GSM модуль	SIM900	1	320	320
3	Імпульсний стаб.напруги	LM2576T-ADJ	1	25	25
4	Матриця з потуж. транз. Дарлінгтона	ULN2003	1	6,1	6,1
5	Стабілізатор електричної напруги	7805	1	5,40	5,40
8	Транзистори	BC847	3	0,42	1,26

9	Кварцовий резонатор	HC-49U	1	3,36	3,36
10	Роз’єм антени	SMA	1	39	39
11	Котушки індуктивності	LDNP-101MC, MCDR1511NP-151K	1+1	16,50;26,50	43
12	Клеми	DG306-5.0-14P,DG306-5.0-04P	1+1	20+4,25	24,25
13	Мікрофон	BCM-9767P	1	10	10
14	Конденсатори	К73-17 4,7мкФ 6,3В	1	8	8
15	Конденсатори	К73-17 0,1мкФ, TECAP 0,22мкФ	5+1	3,4+1,44	18,44
16	Запобіжник	0216001.MXP	1	2,50	2,50
17	Кондесатори	27Ф,047мкФ, 47мкФ,2200мкФ,330мкФ,470мкФ 25В,1мкФ.	2+3+1+1+1+1+1	4;1,5;7;8;6,3;5,5;4,1;8,7;7,2;5,25.	64,55
18	Резистори	5,6кОм,4,7кОм,3,3кОм,10кОм,22Ом,100Ом,1кОм,2кОм,820Ом,39	3+3+5+4+3+2+3+1+1+4	0,30	8,7

		0Ом			
19	Стабілітрони	1N4726A 2,7B, 1N5338B 5,1B	1, 10	0,5, 3,8	38,5
20	Діоди	BAS40W, 1N4148, 1N5822, HER201	1+2+1+1	2,5;1;1,4 ;1,66	6.56
	Разом				760,62

Таблиця 3.4 – Вартість покупних виробів для базового приладу

№	Покупні вироби	Тип, марка	Кількість на одиницю виробу, шт	Ціна за штуку, грн	Загальна вартість, грн
1	Мікроконтроллер	PIC18F46K2	1	170	170
2	GSM модуль	SIM900	1	320	320
3	DTFM приймач	HOLTEK HT9170D	1	21	21
4	Матриця з потуж. транз. Дарлінгтона	ULN2003AG	1	35	35
5	Мультиплексор/демультиплексор	HEF4051BT	2	6,40	12,80

6	МОП транзистор	ST 4NF03L	1	20	20
7	Кварцевий резонатор	10.000, 3.5795450	1+1	31,9	40
8	Котушка індуктивності	SDR0503 150мкГн	1	10	10
9	FLASH пам’ять	SST 25VF016B	1	30	30
10	Конденсатори	К50-30,24,16	1+1+1	3,75;7;5,55	16,3
11	Кондесатори	SMD	17	0,5	8,5
12	Роз’єм антени	SMA	1	39	39
13	Стабілізатор току	L5973D	1	75	75
14	Клеми	15EDGK 12p	2	44,70	89,40
15	Тел. роз’єм	RJ12	1	1,50	1,50
16	Кнопка	TACT SMD	1	1	1
17	Резистор	Будь-який на 300 Ом	1	0,6	0,6
18	Резистори SMD	361Ом,289Ом,472Ом,153Ом,1RO,302Ом,104Ом,103Ом,189,682,333,220,112, 560,101,472,562,683	3+1+1+3+1+1+10+4+4+1+1+3+1+4+3+3+5+6	1	55
19	Діоди	Шотки типу 1N6263	9	1	9
20	Запобіжник	RUEF110	1	3	3
	Разом				957,10

Вартість покупних виробів нового та базового пристрою з урахуванням транспортно-заготовчих витрат складає

$$С_{пв(нов)} = 1,12 \cdot 760,62 = 851,9 \text{ грн.}$$

$$С_{пв(баз)} = 1,12 \cdot 957,1 = 1072 \text{ грн.}$$

Витрати на паливо та енергію

Витрати на паливо та енергію визначаємо, виходячи з потужності агрегатів, тривалості технологічного процесу та вартості одиниці енергії

$$C_e = A_e \cdot Ц_e \tag{3.3}$$

$$A_e = \frac{\sum_{i=1}^{n} C_{npi} \cdot W_i \cdot T_{пл} \cdot t_{шкі}}{T_{пл}}, \tag{3.4}$$

де $С_е$ - витрати на паливо та енергію;

$А_е$ – витрати енергії агрегатом, кВт/год, при виготовленні одного виробу;

C_{npi} – кількість агрегатів, за допомогою яких здійснюється обробка;

W_i – потужність агрегата, кВт;

$T_{пл}$ – плановий фонд часу агрегата;

n – число операцій, при виконанні яких затрачується енергія на технологічні цілі;

$Ц_e$ – вартість одного кВт/год електроенергії для промислового підприємства (ціна на ел.енергію з 01.12.16 р. 1,9616 грн/кВт.);

$T_{шкі}$ - норма штучно-калькуляційного часу i-ї операції.

У процесі виготовлення ПКП за новим технологічним процесом використовується електроенергія на

- експозиційну камеру РКТ – 100 Вт;
- установку травильну - 100 Вт;
- спеціальне обладнання КП – 7511 - 400 Вт;
- термошафу (сушку) – 400 Вт.

У процесі виготовлення ПКП за базовим технологічним процесом використовується електроенергія на

- світлокопіювальну камеру - 100 Вт;

- гальванічний осад міді - 600 Вт;

- спеціальне обладнання КП – 7511 - 400 Вт;

- термошафу (сушку) – 400 Вт.

Таким чином знайдемо C_e

$A_{e(нов)} = 0,1 \cdot 0,08 + 0,1 \cdot 0,2 + 0,4 \cdot 0,23 + 0,4 \cdot 1,0 = 0,52$ кВт;

$A_{e(баз)} = 0,1 \cdot 0,05 + 0,6 \cdot 0,25 + 0,4 \cdot 0,23 + 0,4 \cdot 1,0 = 0,65$ кВт.

$C_{e(нов)} = 0,52 \cdot 1,9616 = 1,02$ грн.

$C_{e(баз)} = 0,65 \cdot 1,9616 = 1,28$ грн.

Основна заробітна плата робітників

Основна заробітна плата робітників розраховується виходячи з повної норми часу на кожну операцію технологічного процесу, вимог до кваліфікації та годинної тарифної ставки.

Розцінки на операції визначаємо за формулою

$$q_i = t_{шкі} \cdot i, \quad (3.5)$$

де q_i - розцінка на i – ту операцію;

i - годинна тарифна ставка (ГТС) за розрядом робіт на i-й операції, грн.

Таблиця 3.4 – Розрахунок заробітної плати для виготовлення пристрою за новим технологічним процесом

№	Операція	Розряд	ГТС, грн/год	$t_{шкі}$, год	Розцінка, грн
1	Підготовка поверхні діелектрика	3	32	0,1	3,2
2	Свердління технологічних отворів	3	32	0,1	3,2
3	Фотолітографія	3	32	0,3	9,6

4	Хімічне травлення	3	32	0,25	8
5	Лакування	3	32	0,3	9,6
6	Свердління монтажних отворів	3	32	0,8	25,6
7	Установка конденсаторів	3	32	0,1	3,2
8	Установка резисторів	3	32	0,1	3,2
9	Установка транзисторів	3	32	0,3	9,6
10	Установка стабілітронів	3	32	0,3	9,6
11	Установка катушок	3	32	0,5	16
12	Пайка хвилею припою	3	32	0,7	22,4
13	Контроль пайки	3	32	0,5	16
14	Перевірка працездатності	3	32	1,0	32
15	Контроль ВТК	3	32	0,4	12,8
	Разом			5,75	184

Таблиця 3.5 – Розрахунок заробітної плати для виготовлення пристрою за базовим технологічним процесом

№	Операція	Розряд	ГТС, грн/год	$t_{шкі}$, год	Розцінка, грн
1	Підготовка поверхні діелектрика	3	32	0,1	3,2
2	Свердління технологічних отворів	3	32	0,1	3,2
3	Нанесення фоторезиста	3	32	0,4	12,8
4	Нанесення малюнка	3	32	0,3	9,6
5	Дублення	3	32	0,3	9,6
6	Свердління монтажних отворів	3	32	0,8	25,6

7	Установка конденсаторів	3	32	0,1	3,2
8	Установка резисторів	3	32	0,1	3,2
9	Установка транзисторів	3	32	0,3	9,6
10	Установка стабілітронів	3	32	0,3	9,6
11	Установка катушок	3	32	0,5	16
12	Пайка хвилею припоя	3	32	0,7	22,4
13	Контроль пайки	3	32	0,5	16
14	Перевірка працездатності	3	32	1,0	32
15	Контроль ВТК	3	32	0,4	12,8
	Разом			5,9	188,8

Основна заробітна плата включає доплату за відпрацьований час в другу зміну і в нічний час у розмірі 5% від розцінки і премію в розмірі 25% від розцінки, тоді витрати на основну заробітну плату можна розрахувати за формулою

$$C_{оз} = (1+K_{зм}+K_{пр}) \cdot \sum_{i=1}^{n} q_i \,, \qquad (3.6)$$

Де $K_{зм}$ та $K_{пр}$ – коефіцієнти, які враховують збільшення годинної ставки робітника, який працює у другу зміну і премії.

Використовуючи данні табл. 3.4 і 3.5, а також формули (3.5) та (3.6), знайдемо сумарні витрати на основну заробітну плату

$$C_{оз(нов)} = (1+0,05+0,25) \cdot 184 = 239,2 \text{ грн.}$$

$$C_{оз(баз)} = (1+0,05+0,25) \cdot 188,8 = 245,44 \text{ грн.}$$

Додаткова заробітна плата робітників

Додаткова заробітна плата робітників включає оплату відпусток, часу виконання державних обов'язків, оплату пільгових годин роботи підлітків і складає

$$C_{дз} = C_{оз} \cdot \frac{K_{дзп}}{100}, \quad (3.7)$$

де $K_{дзп}$ – прийнятий розмір додаткової заробітної плати, у відсотках. Приймемо $K_{дзп} = 20\%$.

Використовуючи формулу (3.7), розрахуємо додаткову заробітну плату робітників

$$C_{дз(нов)} = 0,2 \cdot 239,2 = 47,84 \text{ грн.}$$

$$C_{дз(баз)} = 0,2 \cdot 245,44 = 49,1 \text{ грн.}$$

Соціальне відрахування

Згідно з законом України «Про Збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування» ЄСВ складає 22% від основної та додаткової заробітної плати робітників та розраховується за формулою:

$$C_{сф} = (C_{оз} + C_{дз}) \cdot 0,22. \quad (3.8)$$

Використовуючи формулу (3.8) розрахуємо збори ЄСВ

$$C_{сф(нов)} = (239,2 + 47,84) \cdot 0,22 = 63,15 \text{ грн.}$$

$$C_{сф(баз)} = (245,44 + 49,1) \cdot 0,22 = 64,8 \text{ грн.}$$

Витрати на підготовку та освоєння виробництва

Витрати на підготовку й освоєння виробництва складають 5 % від основної заробітної плати робітників та розраховується за формулою:

$$C_{осв} = C_{оз} \cdot 0,05. \quad (3.9)$$

Використовуючи формулу (3.9) розрахуємо витрати на підготовку та освоєння виробництва

$$C_{осв(нов)} = 239,2 \cdot 0,05 = 11,96 \text{ грн.}$$

$$C_{осв(нов)} = 245,44 \cdot 0,05 = 12,27 \text{ грн.}$$

Амортизаційні відрахування

Нарахування амортизації здійснюється протягом строку корисного використання (експлуатації) об'єкта, який встановлюється підприємством при визнанні цього об'єкта активом (при зарахуванні на баланс), і призупиняється на період його реконструкції, модернізації, добудови, дообладнання та консервації.

Під терміном «основні фонди» слід розуміти матеріальні цінності, що використовуються у господарській діяльності платника податку протягом періоду, який перевищує 365 календарних днів з дати введення в експлуатацію таких матеріальних цінностей, та вартість яких поступово зменшується у зв'язку з фізичним або моральним зносом. Згідно Закону України від 17.07.2015 г. № 655-VIII вартість «основних фондів» від 6000 грн. Якщо вартість менша, а строк корисного використання більше року, то це МНМА. Розрахунок амортизаційних відрахувань здійснено згідно Постанови Кабінету Міністрів України від 01.06.2011 №869. Також відображено в обліковій політиці, що амортизація МНМА проводиться в першому місяці використання 100% вартості. Амортизація основних засобів проводиться прямолінійним способом. При застосуванні прямолінійного методу річна сума амортизації розраховується, як ділення вартості, що амортизується, на термін корисного використання об'єкта основних засобів.

В нашому випадку застосовується технічне обладнання, яке відноситься до групи №4 (строк корисного використання 5 років), та МНМА, яке відноситься до групи №11.

Таблиця 3.6 – Перелік технологічного обладнання для виготовлення приладу за новим технологічним процесом

№	Найменування обладнання	Первісна вартість, грн	Витрати на амортизацію за 1 рік, грн	Група ОФ
1.	Прес бороздковий	71792,00	14358,40	4
2.	Станок свердлильний	7320,00	1464,00	4
3.	Термошафа	1665,00	1665,00	11
4.	Стіл монтажний	13012,00	2602,40	4
5.	Установка для травлення	2715,00	2715,00	11
6.	Шафа витяжна універсальна	33824,00	6764,80	4
7.	Лінія гальванічна	35220,00	7044,00	4
8.	Ванна вініпласт на	1570,00	1570,00	11
9.	Ванна з підігрівом	3365,00	3365,00	11
10.	Установка для пайки хвилею припою	4680,00	4680,00	11
11.	Експозиційна камера	20000,00	4000,00	4
	Разом:	195163,00	50228,60	

Таблиця 3.7 – Перелік технологічного обладнання для виготовлення пристрою за базовим технологічним процесом

№	Найменування обладнання	Первісна вартість, грн	Витрати на амортизацію, грн	Група ОФ
1.	Прес бороздковий	71792,00	14358,40	4
2.	Станок свердлильний	7320,00	1464,00	4
3.	Термошафа	1665,00	1665,00	11
4.	Стіл монтажний	13012,00	2602,40	4
5.	Установка для травлення	2715,00	2715,00	11
6.	Шафа витяжна універсальна	33824,00	6764,80	4
7.	Лінія гальванічна	35220,00	7044,00	4

8.	Ванна вініпластна	1570,00	1570,00	11
9.	Ванна з підігрівом	3365,00	3365,00	11
10.	Установка для пайки хвилею припою	4680,00	4680,00	11
11.	Світлокопіювальна камера	14684,00	2936,80	4
12.	Гільйотинні ножиці	1623,00	1623,00	11
	Разом	206436,00	50788,40	

Використовуючи данні табл. 6.6. та 6.7, знайдемо сумарні амортизаційні відрахування

$$C_{ав\ (нов)} = 50228{,}60 \text{ грн.}$$

$$C_{ав\ (баз)} = 50788{,}40 \text{ грн.}$$

Сума амортизаційних витрат в собівартості виробу при виробництві 1000 одиниць на рік знаходиться за формулою

$$AB = AB_c / 1000, \qquad (3.10)$$

де AB_c – амортизаційні витрати на виготовлення 1000 одиниць виробу,

AB – амортизаційні витрати на виготовлення однієї одиниці виробу.

Використовуючи формулу 6.10., визначимо суму амортизаційних витрат в собівартості виробу при виробництві 1000 одиниць на рік

$$AB_{(нов)} = AB_c / 1000 = 50228{,}60 / 1000 = 50{,}23 \text{ грн.},$$

$$AB_{(баз)} = AB_c / 1000 = 50788{,}40 / 1000 = 50{,}79 \text{ грн.}$$

Витрати на утримання та експлуатацію обладнання

Витрати на утримання устаткування (поточний і капітальний ремонт, технічне переоздоблення) визначається з розрахунку 5% вартості основних фондів, розподілених на один виріб

$$C_{р\ (нов)} = C_{ав(нов)} \cdot 0{,}05 = 50{,}23 \cdot 0{,}05 = 2{,}51 \text{ грн.}$$

$$C_{р\ (баз)} = C_{ав(баз)} \cdot 0{,}05 = 50{,}79 \cdot 0{,}05 = 2{,}54 \text{ грн.}$$

Інші витрати

Інші витрати становлять 12% від ОЗП та включають в себе витрати операційної діяльності, які не ввійшли до складу попередніх розрахунків, зокрема витрати на відрядження, послуги зв'язку, виплату матеріальної допомоги, плата за розрахунково-касове обслуговування тощо.

$$C_{ін} = C_{оз(нов)} \cdot 0{,}12 = 239{,}2 \cdot 0{,}12 = 28{,}7 \text{ грн.}$$

$$C_{ін} = C_{оз(баз)} \cdot 0{,}12 = 245{,}44 \cdot 0{,}12 = 29{,}5 \text{ грн.}$$

Загальновиробничі витрати

Загальновиробничі витрати становлять 400% від основної заробітної плати

$$C_{знв(нов)} = C_{оз(нов)} \cdot 4 = 239{,}2 \cdot 4 = 956{,}8 \text{ грн.}$$

$$C_{знв(баз)} = C_{оз(баз)} \cdot 4 = 245{,}44 \cdot 4 = 981{,}76 \text{ грн.}$$

Виробнича собівартість визначається як сума вищевказаних статей калькуляції і розраховується за формулою

$$C_{вир} = C_м + C_{зв} + C_{пв} + C_е + C_{оз} + C_{дз} + C_{сф} + C_{осв} + C_{ав} + C_р + C_{знв} + C_{ін} \quad (3.11)$$

Розрахуємо виробничу собівартість за формулою (3.11)

$$C_{вир(нов)} = 147{,}13 + 0 + 851{,}9 + 1{,}02 + 239{,}2 + 47{,}84 + 63{,}15 + 11{,}96 + 50{,}23 + 2{,}51 + 956{,}8 + 28{,}7 = 2400{,}44 \text{ грн.}$$

$$C_{вир(баз)} = 178{,}55 + 0 + 1072 + 1{,}28 + 245{,}44 + 49{,}1 + 64{,}8 + 12{,}27 + 50{,}79 + 2{,}54 + 981{,}76 + 29{,}5 = 2688{,}03 \text{ грн.}$$

Статті витрат і відрахування за ними наведено в табл. 3.8 та 3.9.

Таблиця 3.8 – Кошторис витрат на виготовлення ПКП для пристрою за новим технологічним процесом

№	Вид витрат	Сума відрахувань, грн.	Частка, %
1	Основні та допоміжні матеріали	147,13	6,129
2	Покупні вироби	851,9	35,489
3	Електроенергія на технологічні цілі	1,02	0,042
4	Основна зарплата	239,2	9,965
5	Додаткова зарплата	47,84	1,993
6	Соціальне відрахування	63,15	2,631
7	Витрати на підготовку та освоєння виробництва	11,96	0,498
8	Амортизаційні відрахування	50,23	2,093
9	Витрати на утримання та експлуатацію обладнання	2,51	0,105
10	Інші витрати	28,7	1,196
11	Загальновиробничі витрати	956,8	39,859
	Виробнича собівартість	2400,44	100

Таблиця 3.9 – Кошторис витрат на виготовлення ПКП для пристрою за базовим технологічним процесом

№	Вид витрат	Сума відрахувань, грн	Частка, %
1	Основні та допоміжні матеріали	178,55	6,642
2	Покупні вироби	1072	39,880
3	Електроенергія на технологічні цілі	1,28	0,048
4	Основна зарплата	245,44	9,130

5	Додаткова зарплата	49,1	1,826
6	Відрахування на соціальне страхування	64,8	2,411
7	Витрати на підготовку та освоєння виробництва	12,27	0,460
8	Амортизаційні відрахування	50,79	1,889
9	Витрати на утримання та експлуатацію обладнання	2,54	0,094
10	Інші витрати	29,5	1,097
11	Загальновиробничі витрати	981,76	36,523
	Виробнича собівартість	2688,03	100

Як видно з табл. 3.8. та 3.9., найбільшу частку витрат на виготовлення виробу складають покупні вироби.

3.4 Розрахунок економічного ефекту

Перед проведенням розрахунку економічного ефекту необхідно визначити оптово-випускну ціну з урахуванням рентабельності підприємства.

Для цехів машинобудівних заводів, продукція яких має закінчений цикл і йде на реалізацію за межі підприємств, цехова ціна встановлюється рівною затвердженої оптово-відпускної ціни даного виробу. Оптово-відпускна ціна при цьому розраховується за формулою 3.12.

$$Ц_{опт} = C_{вир} \cdot \left(1 + \frac{P}{100}\right), \quad (3.12)$$

де P – рентабельність підприємства. На етапі сучасних ринкових відносин з огляду на специфіку господарської діяльності виробничої організації необхідно закладати рівень рентабельності не менше 15%, тоді оптово-відпускна ціна ПКП складе:

$$Ц_{опт(нов)} = 2400 \cdot (1 + 0{,}15) = 2760 \text{ грн.}$$

$$Ц_{опт(баз)} = 2688 \cdot (1 + 0{,}15) = 3091 \text{ грн.}$$

Розрахуємо економічний ефект за такою формулою

$$P_{еф} = \sum_{i=1}^{n} P_i \cdot d_i - \sum_{i=1}^{n} З_s \cdot d_i ,$$

(3.13)

де $P_{еф}$ – економічний ефект за період n років, *грн.*; P_i - результат в i-ому році, *грн.*; $З_i$ – витрати в i-ому році; d_i – коефіцієнт дисконтування.

Витрати за перший рік являють собою вартість устаткування, необхідного для виготовлення цього пристрою

$$З_{і(нов)} = 195163 \text{ грн.}$$

Використовуючи формулу (3.13) розрахуємо економічний ефект протягом 5 років за річного випуску 1000 штук. Результати розрахунків наведені в табл. 3.10.

Проєкт визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} – N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (6%);

$N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0{,}46 > (6 – 5)/100 = 0{,}46 > 0{,}01.$$

Термін окупності капітальних інвестицій $T_о$ показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_о = \frac{К}{Е} = \frac{1}{ROSI}$$

$$T_0 = 1 / 0{,}23 = 2{,}17 \text{ років.}$$

Таблиця 3.10 – Економічний ефект за 5 років для виготовлення приладу за новим технологічним процесом

Найменування	2017	2018	2019	2020	2021
Ціна виробу, грн	2760	2760	2760	2760	2760
Собівартість виробу, грн.	2400	2400	2400	2400	2400
Обсяг випуску, шт./рік	1000	1000	1000	1000	1000
Прибуток, грн/шт	360	360	360	360	360
Коефіцієнт дисконтування	1	0,9091	0,8264	0,7513	0,683
Результати від виробництва, грн.	360000	327276	297504	270468	245880
Капітальні витрати, грн.	195163	0	0	0	0
Економічний ефект, грн.	164837	327276	297504	270468	245880
Економічний ефект за 5 років					1305965

3.5 Висновок

Отже, згідно з наведеними розрахунками можливо зробити висновок, що застосування модифікованого приймально-контрольного пристрою є економічно доцільним.

Капітальні витрати, які складають 195163 грн, дозволяють отримати ефект величиною 1305965 грн. Відповідно до отриманих значень показників економічної ефективності можна зазначити, що такий підхід дозволить

отримувати 0,46 економічного ефекту на 1 грн. капітальних витрат (коефіцієнт повернення інвестицій ROSI складає 0,46 грн.). Термін окупності при цьому складатиме 2,17 років.

Величина економічного ефекту визначатиметься також розміром компанії, величиною вартості нематеріальних активів (об'єктів прав інтелектуальної власності) та кількістю об'єктів прав інтелектуальної власності, право на авторство яких може бути порушеним.

Таким чином, можемо зробити висновок, що окупність розробки та впровадження ПКП наступає вже на другий рік, тому впровадження виробництва такого ПКП є вигідним і економічно доцільним.

ВИСНОВКИ

Кваліфікаційна робота магістра розкриває особливості організації системи охорони периметру приватного об'єкту.

Проведено аналіз сучасних системи охорони периметру. Проаналізовані сучасні пристрої, що входять до систем захисту периметру. Зокрема, розглянуті системи відеоспостереження без урахування правил розташування систем спостереження, розрахунку кількості систем відеоспостереження та об'єднання їх у комплексну систему з урахуванням спеціального приймально-контрольного пристрою не можуть забезпечити підвищений рівень захисту об'єктів. Це обумовлено тим, насамперед, що характеристики таких систем не відповідають нормам при проєктуванні системи охорони приватного об'єкту.

На основі проведеного аналізу технічних засобів, які утворюють структуру сучасної системи охорони периметру, визначено, що розглянуті елементи відрізняються у схемо-технічному виконанні тим, що різні функції системи можна реалізувати на основі одного обладнання. Проведено вибір основних складових системи відеоспостереження та визначено її структуру. На основі структурної схеми визначені технічні особливості, які варто враховувати при проєктуванні аналогічних систем охорони об'єктів. Розроблені структурна та функціональна схеми приймально-контрольного пристрою. Проведено аналіз та обґрунтування електричної принципової схеми приймально-контрольного приладу системи захисту периметру приватного об'єкту, а також представлено модернізацію електричної принципової схеми приймально-контрольного приладу На основі спеціалізованого програмного забезпечення IP Video System Design Tool визначено основні етапи створення проєкту інтегрованої системи охорони периметру приватного призначення, проведено дослідження та обґрунтована кількість камер відеоспостереження і наведено рекомендації щодо налаштування та з'єднання елементів цієї інтегрованої системи охорони периметру на основі новітніх програмних і апаратних рішень. З'ясовано, що інструменти в розглянутих програмах дозволяють провести визначення місць розташування відеокамер, які

дозволять усунути у процесі створення реального проєкту «сліпі» зони по периметру охорони території. У процесі планування і проєктування системи відеоспостереження визначено, скільки і яких відеокамер було потрібно, де і як розмістити їх, визначено зони огляду, розраховані фокусна відстань об'єктивів і кількість пікселів на метр. При цьому, слід зазначити, що при збільшенні кута огляду камери зменшується якість зображення спостережуваних об'єктів. Тому визначено баланс між можливістю розпізнавання / ідентифікації людей в кадрі, розміром зони огляду, кількістю камер, типом встановлених камер. Також слід зазначити, що існуючі калькулятори об'єктивів не допоможуть визначити ефективність застосування мегапіксельних камер і не дозволять побачити заздалегідь, яке зображення в результаті буде бачити оператор системи. Крім розрахунків, пов'язаних з підбором камер, вибором об'єктивів і розташуванням, проведено розрахування обсягу відео архіву та оцінено навантаження на локальну мережу. Наведено методику оцінки ризиків IoT разом із системою оцінки ризиків, щоб підкреслити кількісний підхід. Це дослідження було зосереджено на ширшому домені IoT, досліджено приклади векторів Інтернету речей і проведено обчислення їх показників ризику.

Проведено дослідження та аналіз використання системи автоматизованого проєктування IP Video System Design Tool для визначення оптимальної кількості й місць розташування камер відеоспостереження приватної території;

Проведено розрахунок собівартості модернізованого ПКП за допомогою калькулювання, тобто визначено собівартість одиниці продукції за встановленою номенклатурою витрат з урахуванням місця їх виникнення. Доведено, що окупність розробки та впровадження ПКП наступає вже на другий рік, тому впровадження виробництва такого ПКП є вигідним і економічно доцільним.

ПЕРЕЛІК ПОСИЛАНЬ

1. Короткий огляд найбільш поширених систем сигналізації. [Електронний ресурс]. Режим доступу: https://xn--j1ahb.xn--j1amh/articles/kratkij-obzor-samyh-rasprostranennyh-sistem-signalizacii/ (Дата звернення 13.10.2023)

2. Охоронна сигналізація. [Електронний ресурс]. Режим доступу: https://xn--j1ahb.xn--j1amh/ohrannaya-signalizaciya/ (Дата звернення 13. 10. 2023)

3. Монтаж систем безпеки. [Електронний ресурс]. Режим доступу: https://securitypolice.com.ua/index.php/poslugu/tekhnichna-okhorona/montazh-system-bezpeky (Дата звернення 13.10.2023)

4. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

5. Магауенов Р.Г. Системи охоронної сигналізації: основи теорії і принципи побудови. Навчальний посібник для вузів. 2-вид. М.: Гаряча лінія – Телеком. 2008. 496 с.

6. Цифрові системи відеоспостереження [Електронний ресурс] – Режим доступу: https://www.vostok.dp.ua/ukr/infa1/sistemy_vidyeonablyudeniya/digital-video/ (Дата звернення 13.10.2023)

7. IP відеоспостереження – [Електронний ресурс] – Режим доступу: https://xn--80adgeboqrpy5j.com.ua/ip_videosposterejennya/ (Дата звернення 11.10.2023)

8. Video surveillance systems [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/228708805_Video_Surveillance_System

9. Системи IP-відеоспостереження. Огляд. [Електронний ресурс] - Режим доступу: https://valtek.com.ua/ua/systemintegration/security-control-system/video-surveillance/ip-systems-review (Дата звернення 11.10.2023)

10. Check Point Software Technologies опублікувала звіт Global Threat Index. – [Електронний ресурс] – Режим доступу: https://itpro.ua/post/check_point_software_technologies_opublikovala_otchet_global_threat_index/

11. Річний звіт з кібербезпеки у 2020 році. – [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/uk_ua/products/security/defending-against-critical-threats.html

12. Аналогові або цифрові камери відеоспостереження: на чому зупинитися? [Електронний ресурс] – Режим доступу: http://dovidkam.com/tehnika/analogovi-abo-cifrovi-kamerivi deosposterezhennya-na-chomu-zupinitisya.html (Дата звернення 11.10.2023)

13. Круглов Герман, Професійне відеоспостереження. Практика і технології аналогового і цифрового відеоспостереження, 2-е вид.: Пер. з англ. М.: Сек'юріті Фокус (Security Focus), 2010. 640 с.

14. Лукьяніца А.А., Шишкін А.Г. Цифрова обробка відеозображень. М.: «Ай-Ес-Ес Прес», 2009. 267 с.

15. Розрахувати необхідний обсяг жорсткого диска для системи відеоспостереження будинку [Електронний ресурс]. – Режим доступу: https://greenvision.ua/ua/service-support/ (Дата звернення 13.10.2023)

16. IP Video System Design Tool. [Електронний ресурс] – Режим доступу: https://www.jvsg.com/ (Дата звернення 11.10.2023)

17. Двинских В.І. Аналіз вразливості системи охорони. оцінки показників уразливості. Офіційний сайт охоронно-інформаційного агентства Каскад-Сервіс. Харків: 2009. 78 с.

18. Волковіцький В.Д., Волхонський В.В. цифрові системи ТВ спостереження. Безпека, достовірність, інформація. СПб.: 2009 38-47 с.

19. Ворона В.А., Тихонов В.А. Системи контролю і управління доступом. М.: Гаряча лінія - Телеком, 2010. 272 с

20. Гедзберг Ю.М. Охоронне телебачення. М.: Гаряча лінія - Телеком, 2005. 312 с.

21. Синилов В. Г. Системи охоронної, пожежної та охоронно-пожежної сигналізації. Підручник для поч. проф. освіти. 5-е вид. М.: Видавничий центр «Академія» 2010. 512 с.

22. Казанський С.В. Надійність електроенергетичних систем. Навчальний посібник / С.В.Казанский, Ю.П. Матеєнко, Б.М.Сердюк. – К.: НТУУ «КПІ», 2011. – 216с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	3	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	24	
6	А4	Спеціальна частина	33	
7	А4	Економічний розділ	20	
8	А4	Висновки	2	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація Клименко_СВ.ppt

2 Диплом Клименко_СВ.doc

ДОДАТОК В. Відгук керівника економічного розділу

Клименко Світлана Володимирівна у кваліфікаційній роботі представила опис об'єкту, а саме приймально-контрольний пристрій, а також опис модифікованого пристрою. Проведено розрахунок собівартості приймально-контрольного пристрою. Проведено розрахунок економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень. При виконанні кваліфікаційної роботи Клименко С.В. виявила достатні теоретичні та практичні знання та належним чином виконала усі розрахункові завдання. Календарний графік щодо виконання економічного розділу витримувався. Завдання економічного розділу виконані у повному обсязі. Економічний розділ кваліфікаційної роботи Клименко Світлани Володимирівни заслуговує оцінки _____

Керівник розділу,
к.е.н., доц. _____ Пілова Д.П.
(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-22з-1 Клименко С.В.

на тему: «Розробка та дослідження системи охорони периметру»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 100 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на розробку та дослідження системи охорони периметру. Охоронні системи дозволяють цілодобово контролювати як приватні, так і території комунальної власності, допомагати при виявленні протиправних дій, направлених на приватну або комунальну власність, забезпечувати своєчасне попередження про різноманітні позаштатні ситуації. Дані системи мають дуже широке застосування у більшості сфер нашого життя, що свідчить про актуальність теми кваліфікаційної роботи.

При виконанні роботи авторка продемонструвала добрий рівень теоретичних знань і практичних навичок. На основі аналізу принципів побудови сучасних систем охорони периметру, а також аналізу збору, обробки та передачі інформації, аналізу загроз та ризиків в системах охорони периметру сформульовані задачі, вирішенню яких присвячений спеціальний розділ. У спеціальному розділі запропоновано опис приватного об'єкту, який потребує захисту охорони периметру, розроблено структурну та функціональну схеми, проведено вибір та обґрунтування електричної принципової схеми приймально-контрольного пристрою системи захисту периметру, наведена методика оцінки ризиків кібербезпеки, проведено розрахунок надійності охоронної системи, проведено дослідження та аналіз безпеки системи охорони периметру.

Наукова новизна результатів полягає у розробці модифікованого приймально-контрольного пристрою системи захисту периметру приватного будинку, а також представленій методиці оцінки ризиків кібербезпеки та

застосування сучасних додатків для проєктування та монтажу відеосистем охорони приватної прибудинкової території.

Практична цінність роботи полягає у тому, що було запропоновано використання системи автоматизованого проєктування IP Video System Design Tool, яке дозволило швидко знайти оптимальну кількість і розташування камер відеоспостереження приватної території, виконати розрахунок системи відеоспостереження, оцінити довжину кабелів і відобразити на плані місцевості зони ідентифікації, розпізнавання, детектування, змоделювати перешкоди в 2D і 3D для виявлення мертвих зон.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Клименко С.В. заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
д.т.н., професор **В.І. Корнієнко**