Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет прикладних інформаційних технологій та електроінженерії
(назва факультету)
Кафедра комп'ютерно-інтегрованих технологій
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

магістр
(освітній ступінь (освітньо-кваліфікаційний рівень))

на тему:

Розробка та дослідження автоматизованої системи забезпечення безпеки адміністративного корпусу

Виконав: студент IV курсу, групи КТм-61
спеціальності (напряму підготовки) 151
Автоматизація та комп'ютерно-інтегровані технології
(шифр і назва спеціальності (напряму підготовки))

Дідуник О.А.
Дрозд М.В.
(підпис) (прізвище та ініціали)

Керівник (підпис) Митник М.М.
(прізвище та ініціали)

Нормоконтроль (підпис) Левицький В.В.
(прізвище та ініціали)

Рецензент (підпис) Трембач Р.Б.
(прізвище та ініціали)

м. Тернопіль – 2019

АНОТАЦІЯ

Дипломна робота складається з пояснювальної записки та графічної частини (ілюстративний матеріал – слайди).

Об’єм графічної частини дипломної роботи становить ___ слайдів.

Об’єм пояснювальної записки складає ___ друкованих сторінок формату А4 (210×297), об’єм додатків – ___ друкованих сторінок формату А4.

Дипломна робота складається з восьми розділів, в яких нараховується ___ рисунків та ____ таблиць з даними.

В роботі використано ___ літературних джерел.

Метою роботи було дослідити основні методи реалізації систем забезпечення безпеки адміністративного корпусу та розробити систему забезпечення комплексної безпеки. Також необхідно було забезпечити віддалене управління системою охорони та контроль проникнення

В результаті проведеної роботи було розглянуто та проаналізовано основні принципи побудови комплексних систем безпеки адміністративної будівлі. Наведено приклад реалізації такої системи. Обґрунтовано визначальні параметри, які в найбільшій мірі впливають на складність та надійність системи безпеки. Досліджено параметри системи на її відповідність нормам. Приведено принципи, приклади реалізації та елементи можливої оптимізації та здешевлення такої системи та роширення і функціональних можливостей.

Ключові слова: КОНТРОЛЬ ДОТУПУ, СИСТЕМА ОХОРОНИ, ВІДЕОНАГЛЯД, АВТОМАТИЗОВАНА СИСТЕМА, ДИСТАНЦІЙНИЙ КОНТРОЛЬ.

ЗМІСТ

ВСТУП

Дослідження питань ефективного забезпечення безпеки населення і промислових об'єктів в сучасних умовах є особливо актуальним у зв’язку з активізацією загроз міжнародного тероризму і техногенних катастроф, а також зростанням кваліфікованих злочинних посягань, економічною нестабільністю, комп'ютерними злочинами, промисловим шпигунством.

Рішення задач охорони об'єктів засноване на застосуванні комплексу технічних засобів сигналізації, які мають зафіксувати наближення або початок дій різних загроз - від пожежі і аварій до спроб проникнення на об'єкт або в комп’ютерну мережу.

При виборі і установці сигналізації на об’єктах приділяється особлива увага досягненню високої захищеності апаратури від її подолання. Існують різні способи реалізації цього завдання:

- контроль відкриття апаратних блоків;
- автоматична перевірка справності технічних засобів;
- захист доступу до управління апаратурою за допомогою кодів;
- архівування подій;
- захист інформаційних потоків між складовими частинами сигналізації методами маскування і шифрування та ін.

Таким чином, проектування ефективної системи сигналізації з урахуванням програмно-апаратних засобів її захисту від обходу зловмисником є найскладнішим багатоплановим завданням, рішення якого неможливо без глибоких і вичерпних знань про структуру, функціональні можливості та принципи роботи системи.

Охоронні сигналізації можна розділити на дві групи, в залежності від того, на яких об’єктах вони встановлюються:

- апаратура, що застосовується на об’єктах народного господарства, як правило, що охороняються спецпідрозділами охорони;

- апаратура, що застосовується на об'єктах, охорона яких, як правило, не перебуває під охороною спецпідрозділів охорони.

До першої групи належать технічні засоби, номенклатура яких строго обмежена, регламентується загальнодержавними нормативними документами, а інформація - відкрита і загальнодоступна.

До другої групи належать технічні засоби, номенклатура яких не обмежена, відомості про принципи та особливості побудови викладаються в друці, передача тривожної інформації виконується як на локальні звукові і світлові сигналізатори, так і на віддалені стаціонарні або на пульти по телефонних лініях, спеціальним радіоканалах, за допомогою систем мобільного та оптичного зв'язку.

Підвищення ефективності систем сигналізації на об'єктах в умовах різкого загострення криміногенної обстановки неможливе без розробки та впровадження наукоємних інтегрованих комплексних систем безпеки (ІКСБ). Проектування ІКСБ засноване на реалізації ідей системної концепції забезпечення комплексної безпеки об'єкта з паралельним вирішенням завдань автоматизації управління такими системами життєзабезпечення об'єкта, як енергопостачання, вентиляція, опалення, водопостачання, ліфтове обладнання, кондиціонування і т.д.

Проектування ІКСБ є одним з визначальних чинників, здатних скоротити збитки від настання протиправних дій, надзвичайних ситуацій, стихійних лих, а також витрати на усунення наслідків зазначених подій.

Таким чином, для вирішення прикладних проблем побудови ефективних систем захисту, необхідно розглянути наступні питання структурних і функціональних особливостей комплексних систем безпеки:

- загальні уявлення про охорону та захист об'єктів;

- основи системного підходу до вирішення проблем захисту та охорони;

- основи систематизації і класифікації об'єктів охорони, погроз, моделей порушників, технічних засобів охорони, тобто всього того, що потрібно знати і розуміти до того, як приступати до створення систем безпеки об'єктів;

- принципи формування зон забезпечення безпеки на об'єкті;

- принципи побудови, склад і особливості проектування систем охоронно-пожежної та тривожної сигналізації, телевізійних систем безпеки, систем контролю і управління доступом;

- загальні питання процедури проектування систем безпеки і оцінки їх ефективності.

Динаміка світового розвитку програмно-апаратних технічних засобів забезпечення комплексної безпеки об'єктів диктує необхідність не тільки вивчення сучасних засобів, а й відстеження тенденцій їх розвитку в перспективі. такий моніторинг дозволяє проводити попереджувальні розробки в області охоронної техніки, аналоги яких очікуються до появи найближчим часом.

1. АНАЛІТИЧНА ЧАСТИНА

1.1. Загальні положення та методики для організації захисту об’єктів

Здійснення заходів щодо забезпечення превентивної та адекватної безпеки населення і промислових об'єктів [6, 7] являє собою складний безперервний процес, а не одноразові або випадкові дії, які виконуються час від часу в міру виникнення необхідності і вносять неузгодженість в роботу різних служб. Безперервне і стабільне функціонування будь-якого об'єкта неможливо без організації надійного захисту, що включає в себе комплекс заходів, спрямованих на виявлення основних загроз і небезпечних ситуацій, оцінки збитку при здійсненні цих загроз і створення системи комплексної безпеки об'єкта при певних обмеженнях (наприклад, на вартість системи).

Безпека об'єкта, що захищається - це стан захищеності об'єкта від загроз заподіяння шкоди (шкоди) життю або здоров'ю людей; майну фізичних або юридичних осіб; державного або муніципального майна; технічним станом, інфраструктурі життєзабезпечення; зовнішнім виглядом, інтер'єру, ландшафтної архітектури; навколишньому природному середовищу.

Протикримінальна безпека об'єкта - це стан захищеності об'єкта, яке характеризується відсутністю недопустимого ризику або погроз різного типу і забезпечується комплексом захисних заходів. Для організації ефективного захисту необхідно розробити узагальнену системну концепцію безпеки, яка в кожному конкретному випадку повинна бути адаптована до конкретного об'єкта, виходячи з умов його функціонування, розташування, характеру діяльності, географічного положення, особливостей навколишнього середовища і інших факторів.

Концепція безпеки являє собою загальний задум організації технічних і організаційних заходів щодо захисту об'єкта від прогнозованих загроз. Виходячи з її положень, розробляється проект оснащення об'єкта інженерно-технічними, спеціальними і програмно-апаратними засобами безпеки.

Концепція забезпечення комплексної безпеки об'єкта призначена для вирішення наступних завдань:

- визначення цілей або предметів захисту, інакше, "кого або що захищати?" (Об'єкт - квартира, офіс, підприємство);

- визначення і оцінка загроз, інакше, "від якого посягання захищати?" (Випадковий хуліган, рецидивіст або організована група);

- розробка і реалізація адекватних заходів захисту, інакше, "чим і як захищати?" (Що повинна зробити охоронна система, щоб запобігти або зменшити шкоду).

Для цього необхідно провести аналіз уразливості об'єкта та існуючої системи захисту.

Уразливість (об'єкта) - це ступінь невідповідності вжитих заходів щодо захисту об'єкта прогнозованим загрозам або заданим вимогам безпеки. Цілями і завданнями проведення аналізу уразливості є:

а) визначення важливих для життєдіяльності об'єкта предметів захисту (найбільш ймовірних цілей злочинних акцій порушників);

б) визначення можливих загроз і моделей ймовірних виконавців погроз (порушників);

в) оцінка можливого збитку від реалізації прогнозованих загроз безпеки;

г) оцінка уразливості об'єкта та існуючої системи безпеки;

д) розробка загальних рекомендацій щодо забезпечення безпеки об'єкта.

Роботи проводяться методом експертних оцінок комісією, до складу якої входять фахівці відповідних служб замовника: безпеки, головного

технолога, головного інженера, пожежної охорони. Роботи проводяться із застосуванням методу математичного моделювання. Розглянемо існуючі класифікації об'єктів охорони, на яких розміщуються предмети захисту, можливі загрози і моделі ймовірних порушників.

1.2. Класифікація предметів та об’єктів охорони

Класифікація предметів захисту і об'єктів охорони

Об'єкт охорони – це підприємство, організація, житло, їх частина або комбінація, обладнані діючою системою охорони та безпеки.

Реалізацію життєво важливих інтересів будь-якого підприємства забезпечують його корпоративні ресурси. Ці ресурси повинні бути надійно захищені від прогнозованих загроз безпеки. Для промислового підприємства такими важливими для життєдіяльності ресурсами, а, отже, предметами захисту є:

- люди (персонал підприємства);

- майно: важливе або дефіцитне технологічне обладнання; секретна і конфіденційна документація; матеріальні та фінансові цінності; готова продукція; інтелектуальна власність (ноу-хау); кошти обчислювальної техніки; контрольно-вимірювальні прилади та ін.;

- інформація конфіденційна (на матеріальних носіях, а також циркулює у внутрішніх комунікаційних каналах зв'язку і інформації, в кабінетах керівництва підприємства, на нарадах і засіданнях);

- фінансово-економічні ресурси, що забезпечують ефективне і сталий розвиток підприємства (капітал, комерційні інтереси, бізнес-плани, договірні документи і зобов'язання і т.д.).

Втрата перерахованих ресурсів веде до наступних подій:

- значних матеріальних збитків;

- створення загрози для життя і здоров'я людей;

- розголошенню конфіденційної інформації або відомостей, що містять Державну або комерційну таємницю;

- банкрутства підприємства. Перераховані предмети захисту розміщуються на відповідних виробничих об'єктах підприємства в будівлях і приміщеннях. Ці об'єкти і є найбільш уразливими місцями, виявлення яких проводиться при обстеженні об'єкта.

Таким чином, формулюється відповідь на питання "що захищати?": життя і здоров'я громадян; майно, документи, грошові кошти та інші цінності фізичних та юридичних осіб, що знаходяться на стаціонарних та рухомих об'єктах, а також власне стаціонарні і рухомі об'єкти:

- будівлі, будівлі, споруди, їх окремі частини або приміщення; території, які вони займали, або прилеглі до них, окремі території, окремі предмети;

- транспортні засоби (автомобільний, залізничний, водний, повітряний транспорт).

Надійність захисту перерахованих об'єктів визначається наявністю інженерних засобів захисту на шляхах можливого проникнення порушників. Сукупність цих засобів визначає інженерно-технічних укріплення об’єкту. До інженерних засобів захисту відносяться різні паркани, огорожі, решітки, жалюзі, віконниці, замки, засуви, спеціальним чином укріплені двері, ворота, стіни, підлоги, стелі, віконні прорізи, повітроводи та інші елементи будівельних конструкцій. Інженерні засоби захисту збільшують час, необхідний порушнику для їх подолання, що робить більш імовірним можливість його виявлення і затримання, особливо якщо ці кошти використовуються в поєднанні з технічними засобами охорони (охоронною сигналізацією, системами охоронного телебачення і т.д.).

Таким чином, інженерно-технічна укріпленість об'єкта - це сукупність заходів, спрямованих на посилення конструктивних елементів будівель, споруд, приміщень та захищаються територій, які забезпечують необхідну і

достатню протидію несанкціонованому проникненню порушника в зону, яка захищається, злому і інших злочинних посягань.

Вимоги до інженерно-технічної укріпленості об'єкта захисту формулюються з урахуванням його категорії, його будівельними та архітектурно-планувальними рішеннями, режимом роботи і багатьма іншими факторами, які необхідно враховувати при проектуванні комплексної системи безпеки.

Категорія об'єкту, що охороняється - це комплексна оцінка об'єкта, що враховує його економічну чи іншу (наприклад, культурну) значимість, в залежності від характеру і концентрації зосереджених цінностей, наслідків від можливих злочинних посягань на них, складності забезпечення необхідної охорони.

Особливо важливий об'єкт - об'єкт, значимість якого визначається органами державної влади або місцевого самоврядування з метою визначення заходів щодо захисту інтересів держави, юридичних і фізичних осіб від злочинних посягань та запобігання шкоди, яка може бути завдана природі та суспільству, а також від виникнення надзвичайної ситуації.

Об'єкт життєзабезпечення - сукупність життєво важливих матеріальних, фінансових засобів і послуг, згрупованих за функціональним призначенням і використовуваних для задоволення життєво необхідних потреб населення (наприклад, у вигляді продуктів харчування, житла, предметів першої необхідності, а також в медичному, санітарно-епідеміологічному, інформаційному, транспортному, комунально-побутове забезпечення).

Об'єкт підвищеної небезпеки - об'єкт, на якому використовують, виробляють, переробляють, зберігають або транспортують радіоактивні, вибухо-, пожежонебезпечні, небезпечні хімічні і біологічні речовини, що створюють реальну загрозу виникнення джерела надзвичайної ситуації.

Залежно від категорії значущості всі об'єкти, їх приміщення та території поділяються на чотири групи: АІ і АІІ, БІ і БІІ.

Об'єкти групи АІ (особливо важливі об'єкти високої цінності або високої небезпеки):

- об'єкти особливо важливі, підвищеної небезпеки і життєзабезпечення, включені до Переліку об'єктів, які підлягають державній охороні;

- об'єкти, включені органами влади місцевого самоврядування до переліків об'єктів особливо важливих, підвищеної небезпеки і життєзабезпечення;

- об'єкти з виробництва, зберігання і реалізації наркотичних речовин, сильнодіючих отрут і хімікатів, токсичних і психотропних речовин та препаратів (бази аптекоуправління, аптеки, склади медрезерва, наукові, медичні та інші установи, закладу, у практиці яких використовуються ці речовини);

- ювелірні магазини, бази, склади та інші об'єкти, які використовують у своїй діяльності ювелірні вироби, дорогоцінні метали і камені;

- об'єкти і приміщення для зберігання зброї і боєприпасів, радіоізотопних речовин і препаратів, предметів старовини, мистецтва і культури;

- об'єкти кредитно-фінансової системи (банки, операційні каси поза касового вузла, додаткові офіси, пункти обміну валюти, банкомати);

- каси підприємств, організацій, установ, головні каси великих торгових підприємств;

- сейфові кімнати, призначені для зберігання грошових коштів, ювелірних виробів, дорогоцінних металів і каменів;

- інші аналогічні об'єкти і майнові комплекси.

Об'єкти групи АІІ (найбільш небезпечні приміщення на об'єктах групи АІ):

- сховища і склади грошових і валютних коштів, цінних паперів;

- сховища ювелірних виробів, дорогоцінних металів і каменів; сховища секретної документації, виробів;

- спеціальні сховища вибухових, наркотичних, отруйних, бактеріологічних, токсичних і психотропних речовин та препаратів;

- спеціальні фондосховища музеїв і бібліотек.

Об'єкти групи БІ (об'єкти роздрібної торгівлі та ін.):

- об'єкти зі зберіганням або розміщенням виробів технологічного, санітарно-гігієнічного та господарського призначення, нормативно-технічної документації, інвентарю та іншого майна;

- об'єкти дрібнооптової та роздрібної торгівлі (павільйони, намети, лотки, кіоски та інші аналогічні об'єкти).

Об'єкти групи БІІ (об'єкти категорії Б, що містять алкогольну продукцію або найбільш компактні лекоскидувані товари - електроніку, товари повсякденного попиту):

- об'єкти зі зберіганням або розміщенням товарів, предметів повсякденного попиту, продуктів харчування, комп'ютерної техніки, оргтехніки, відео- і аудіотехніки, кіно- і фотоапаратури, натуральних і штучних хутра, шкіри, автомобілів і запасних частин до них, алкогольної продукції з вмістом етилового спирту понад 13% обсягу готової продукції та іншого аналогічного майна.

Кожній групі об'єктів повинен відповідати певний клас захисту конструктивних елементів (огороджувальних конструкцій і елементів інженерно-технічного укріплення), а також технічних засобів забезпечення комплексної безпеки.

При цьому регламентується відповідність характеристик елементів першого класу мінімально необхідного ступеня захисту, другого класу - середньої, третього класу - високою і четвертого класу - спеціальної ступеня захисту об'єкта від проникнення. Чим нижче рівень вимог до інженерно-

технічної укріпленості об'єкта, тим менше коштів потрібно для організації його ефективної охорони.

В області протикримінального захисту також розроблений технічний регламент, що описує класифікацію об'єктів в залежності від передбачуваних загроз і встановлює різні класи захисту відповідно до виявленими рівнем загрози.

Залежно від ступеня потенційної небезпеки, а також можливих наслідків у разі реалізації кримінальних загроз об'єкти поділяються на три основні групи:

- критично важливі і потенційно небезпечні об'єкти;

- соціально значущі об'єкти;

- об'єкти зосередження матеріальних цінностей.

Крім того, в залежності від виду і розмірів збитку, який може бути нанесений об'єкту, що знаходиться на ньому людям та майну в разі реалізації кримінальних загроз прийнята наступна класифікація:

- клас I (висока значимість) - збиток придбає федеральний або міжрегіональний масштаб;

- клас II (середня значимість) - збиток придбає регіональний або міжмуніципальний масштаб;

- клас III (низька значимість) - збиток придбає муніципальний або локальний масштаб.

Залежно від класу об'єкта і виду знаходиться (зберігається) на ній знаходиться встановлюють класи захисту об'єктів. Подальший аналіз потенційних загроз і вразливих місць об'єкта дозволяє проектувати адекватну систему охорони з використанням рекомендованих видів обладнання, які відповідають встановленому класу значущості і групі небезпеки об'єкта.

Таким чином, облік класифікацій об'єктів за ступенем їх значущості, а також за розмірами потенційного збитку від реалізації загроз необхідний для

наближеної оцінки можливих витрат на оснащення об'єктів інженерно-технічними, спеціальними і апаратно-програмними засобами захисту.

1.3. Основи формування комплексу технічних засобів забезпечення безпеки

Питання "чому і як захищати?" вирішується здатністю існуючої безпеки або яка розробляється ефективно попереджати, запобігати загрозі та ліквідувати їх наслідки. Реалізація концепції безпеки передбачає кілька напрямків забезпечення захищеності об'єкта - це економічна, науково-технічна, технологічна, екологічна, інформаційна, інженерно-технічна безпека та ін. Всі вони є елементами єдиної системи комплексної безпеки даного об'єкту.

Комплексне забезпечення безпеки об'єкта, що захищається визначається нормативними документами як діяльність по створенню умов і забезпечення ресурсів для запобігання та / або зменшення наслідків для об'єкта, що захищається від загроз різної природи виникнення і різного характеру прояви.

Концепція безпеки є сполучною елементом в рамках створення комплексної безпеки об'єкта і визначає основні напрямки її модернізації та розвитку. Необхідно опрацювати наступні пункти:

1) Цілі і завдання системи безпеки.

2) Опис об'єктів захисту.

3) Опис потенційних загроз.

4) Опис основних принципів організації і функціонування системи безпеки.

5) Вимоги до основних підсистем безпеки.

При цьому стан захищеності об'єкта формується і підтримується обґрунтованим в рамках концепції безпеки набором засобів (організаційних,

інформаційних, фінансових, кадрових та ін.). Одним з таких засобів є комплекс технічних засобів забезпечення безпеки (ТЗЗБ). Цілі, завдання, склад комплексу ТЗЗБ, а також характеристики та вимоги по експлуатації обладнання ТЗЗБ формулюються в процесі реалізації комплексу інженерно-технічної безпеки, який є головним при створенні ефективної системи захисту.

У загальному випадку комплексна безпека будь-якого об'єкта повинна включати в себе наступні елементи:

- організаційні заходи забезпечення безпеки;

- фізичну охорону;

- технічні засоби забезпечення безпеки.

До заходів організаційного характеру при побудові і функціонуванні системи безпеки об'єктів відносяться:

- організація на об'єкті контрольно-пропускного режиму;

- спеціально розроблені правила поведінки співробітників об'єктів, відвідувачів і співробітників служби безпеки як в штатних, так і в позаштатних ситуаціях;

- порядок здачі приміщень під охорону і зняття їх з охорони;

- порядок дії співробітників, відвідувачів і служби охорони за сигналами тривоги і при виникненні надзвичайних ситуацій;

- розробка системи документообігу служби охорони (журнали реєстрації, порядок зберігання і знищення оперативних і архівних документів і т.п.);

- освоєння персоналом охорони основних принципів функціонування технічних засобів охорони на об'єкті, правил експлуатації, відповідно до тактики охорони об'єкта, формування навичок і вміння вирішувати охоронні завдання в специфічних умовах;

- навчання персоналу об'єкта правилам користування технічними засобами охорони;

- ознайомлення відвідувачів об'єктів з правилами поведінки;

- укладання та переукладання договорів на охорону об'єкта, післягарантійне і сервісне обслуговування технічних засобів охорони;

- своєчасне і в повному обсязі фінансове і матеріально-технічне забезпечення діяльності охорони і функціонування технічних засобів охорони;

- своєчасне адміністративне реагування керівництва об'єкта на випадки порушення вимог безпеки, внутрішньооб'єктного і пропускного режиму, виникнення нештатних ситуацій.

Фізична охорона об'єктів забезпечується наявністю:

- стаціонарних постів;

- обхідних маршрутів (патрульних постів);

- супроводжуючих постів;

- постів спостереження;

- груп оперативного реагування (груп затримання). До складу комплексу ТЗЗБ об'єкта повинні входити такі технічні підсистеми:

- охоронної і тривожної сигналізації;

- пожежної сигналізації;

- контролю і управління доступом;

- охоронні телевізійні;

- огляду і пошуку;

- пожежної автоматики (пожежогасіння, протидимного захисту);

- оповіщення та управління евакуацією;

- засоби оперативного зв'язку з об'єктом;

- захисту інформації;

- інженерно-технічної укріпленості;

- інженерного забезпечення об'єкта (електроосвітлення та електроживлення; газопостачання; водопостачання; каналізації; підтримки мікроклімату - теплопостачання, вентиляції, кондиціонування).

Склад і кількість об'єктових ТЗЗБ можуть варіюватися в залежності від призначення і значимості об'єкта, що захищається і конкретних умов з комплексного забезпечення його без пеки. Захист об'єкта може здійснюватися як в комплексі, так і по частинах, наприклад, створенням тільки системи охоронної сигналізації. Це може бути обумовлено малою вірогідністю реалізації будь-яких загроз або відносно низькою цінністю частини об'єкта захисту.

Системи контролю і управління доступом (СКУД), системи охоронні телевізійні (СОТ) і системи оповіщення можуть застосовуватися для посилення захисту об'єкта і оперативного реагування.

Для захисту окремих конструктивних елементів об'єкта і його уразливих місць можливе використання тільки СКУД або СОТ, при наявності в них пристроїв, що виконують аналогічні функції систем охоронної і тривожної сигналізації (наприклад, контроль відкривання дверей, автоматичне взяття / зняття з охорони за ідентифікатором, застосування обнаружителей руху, передача зображення в пункт централізованої охорони (ПЦО)).

У подібних випадках доцільно передбачити можливість подальшого розвитку системи захисту шляхом розширення і вдосконалення окремих елементів її частин, а також додаванням нових підсистем.

1.4. Загальні принципи побудови систем безпеки

Розглянемо принципи побудови СБ об'єкта, на основі яких встановлюються вимоги до створення та організації функціонування СБ в цілому і складових її ТСОБ. При побудові СБ об'єкта необхідно керуватися такими принципами:

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

2) зонального побудови або зональним принципом (СБ повинна передбачати організацію та створення зон обмеженого доступу і охоронюваних зон, що забезпечують "ешелоновану" захист охоронюваних об'єктів і їх критичних елементів);

3) равнопрочності (повинен бути забезпечений необхідний рівень ефективності СБ для всіх виявлених в процесі аналізу уразливості типів порушників і способів вчинення злочинних дій);

4) адаптивності (СБ 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).

Дотримання принципів побудови СБ дозволяє забезпечити ефективність захисту об'єктів, яка визначається здатністю технічних підсистем КСБ і ІСБ протистояти нештатних ситуацій на об'єкті з урахуванням виявлених загроз і моделей порушників.

Властивість адекватності технічної підсистеми дозволяє не допустити помилок в її структурному побудові і уникнути невиправданої технічної надмірності при реалізації.

Розглянемо більш докладно зональний принцип побудови СБ, який дозволяє раціонально зробити вибір і розподіл технічних засобів підсистем для охорони об'єкта і його критичних зон (елементів).

Під критичними зонами (елементами) об'єкта розуміють приміщення, їх конструктивні елементи, ділянки, реалізація загрози в відношення яких (або дія її наслідків) 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 по кожній конкретній зоні.

У загальному випадку зона захищається визначається як таке, що безпосередньо за захисною конструкцією простір, механічно огороджене від несанкціонованого доступу та інших позаштатних дій.

Так як конкретні завдання і умови функціонування ТСОБ залежать від структури об'єкта захисту, то під охороною зона може бути визначена як частина об'єкту, що охороняється, контрольована одним шлейфом охоронної сигналізації (для комплексів охоронної сигналізації), одним шлейфом пожежної сигналізації (для установок пожежної сигналізації), одним шлейфом охоронно-пожежної сигналізації або сукупністю шлейфів охоронної та пожежної сигналізації (для комплексів охоронно-пожежної сигналізації).

Шлейф сигналізації - це ланцюг (електрична, радіоканальні, оптоволоконная або інша), що з'єднує вихідні вузли сповіщувачів, що включає в себе допоміжні (виносні) елементи і сполучні лінії і призначена для передачі на прилад приймально-контрольний або на пристрій об'єктове системи передачі сповіщень інформації від сповіщувачів про контрольовані ними параметрах, а в деяких випадках - для подачі електроживлення на сповіщувачі.

Рубіж охоронної сигналізації - це шлейф або сукупність шлейфів або променів (для сигналізації, що використовує передачу повідомлень 36 по радіоканалу), контролюючих охоронювані зони території, будівлі або приміщення (периметр, обсяг або площа, самі цінності або підходи до них) на шляху можливого руху порушника до матеріальних цінностей, при подоланні яких видається відповідне повідомлення про проникнення.

Під рубежом охорони розуміється сукупність охоронюваних зон, контрольованих кордоном сигналізації. При організації зонування об'єкта повинно забезпечуватися посилення захисту від периферії до центру, тобто

до критичних елементів, що визначають категорію об'єкта. Якщо при оцінці ефективності СБ з'ясовується, що існуючих охоронюваних зон недостатньо для нейтралізації потенційних загроз, то можуть організовуватися додаткові рубежі захисту всередині існуючих зон.

Основу планування і технічного оснащення зон безпеки становить принцип рівнозахищеності 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, межі зон безпеки не повинні мати незахищених ділянок. Властивість адаптивності СБ дозволяє своєчасно і гнучко враховувати динаміку потенційних і реальних загроз і небезпек об'єкту. Таким чином, технічна підсистема КСБ і ІСБ повинна володіти адекватністю по відношенню до спектру загроз і небезпек об'єкту з урахуванням контрольних зон в своїй підконтрольній області та адаптивністю до змін умов функціонування об'єкта.

1.5. Умови функціонування систем безпеки

Обсяг і склад устаткування, використовуваного в кожній з систем, що входить в комплекс ТЗЗБ об'єкта, визначаються необхідним рівнем забезпечення безпеки об'єкта та його персоналу. Варіант спільного використання декількох СБ на об'єкті може бути обраний на основі компромісу між вартістю втрат від потенційних загроз і витратами на реалізацію цього варіанту. Пріоритетними для кожної СБ є вимоги, що забезпечують безпеку для життя людей, і пожежну безпеку об'єкта. Тому основним технічним вимогою до СБ є забезпечення необхідної

функціональної і апаратної надійності, пожежної безпеки та завадостійкості. Під надійністю СБ розуміється її властивість виявляти із заданою вірогідністю проникнення (спробу проникнення) на об'єкт, що охороняється (зону об'єкта).

Основні умови функціонування СБ можуть бути сформульовані наступним чином.

1. Жодна з підсистем у складі РБ не повинна порушувати режим функціонування об'єкта, а саме:

- функції спільно діючих систем повинні доповнювати один одного, не надаючи взаємного заважає впливу на працездатність своїх складових частин;

- в спільно діючих системах повинні забезпечуватися алгоритмічна сумісність і роздільна реєстрація вступників від них службових і тривожних сигналів;

- вимоги до експлуатаційної надійності, чутливості і завадостійкості однією з підсистем не повинні поступатися аналогічним вимогам, що пред'являються до інших працюючим спільно з нею підсистем, щоб не знижувати загальний рівень безпеки об'єкта в цілому;

- вихід з ладу однієї або декількох підсистем або каналів зв'язку не повинен призводити до виходу з ладу всієї СБ України.

2. СБ повинна управлятися як централізовано, так і децентралізовано з контролем рівня доступу персоналу до системи. Склад системи управління і контролю функціонування спільно діючих ПСБ повинен визначатися їх призначенням.

Слід надавати перевагу автоматичним засобам управління та контролю, як дублюючі допускаються ручні. Доцільність дублювання визначається вимогами щодо забезпечення експлуатаційної надійності систем. Засоби управління і контролю повинні мати захист від можливих помилкових дій персоналу.

3. СБ повинна зберігати справний стан при впливі факторів навколишнього середовища і відновлювати працездатний стан після закінчення їх дії.

4. СБ не повинна виходити з ладу при відключенні електроенергії на об'єкті та зберігати працездатний стан при відключенні мережевого або іншого основного джерела електроживлення протягом часу переривання електроживлення. Сигналізації не повинні видавати помилкових тривог при перемиканні джерел електроживлення з основного на резервний і назад.

5. Всі події, що відбуваються в системі, повинні протоколюватися.

6. Система повинна контролювати, тестувати і захищати себе від несанкціонованого доступу до управління.

7. Спільно діючі об'єктові системи різного функціонального призначення вимагають різного реагування на видані ними сигнали аварії, тривоги; при цьому:

- сигнали від різних спільно діючих систем, що передаються для реєстрації автоматично, повинні фіксуватися приладами управління окремо (дотримання цієї умови дозволяє запобігти небезпеці "помилкового виклику служби", тобто реагування однієї служби об'єкта на сигнали, призначені для іншої служби і / або прийняття персоналом об'єкта дій, неадекватних виникла обстановці);

- види і інтенсивність сигналів систем різного призначення повинні бути різними (при цьому звукові аварійні, тривожні сигнали не повинні перешкоджати використанню мовної, в тому числі телефонного зв'язку).

8. Система не повинна створювати загроз об'єкту забезпечення безпеки. У кожному конкретному випадку охорони розглянутий список може бути обмежений або доповнений додатковими умовами.

1.6 Структура комплексної системи безпеки

Будемо розглядати задачу забезпечення протикримінального захисту об'єкта силами чотирьох основних нероздільних підсистем комплексу ТЗЗБ, окремо виконують свої функції: системи охоронної і тривожної сигналізації, системи пожежної сигналізації, системи контролю і управління доступом, системи охоронної телевізійної.

Комплекс доповнюють різні допоміжні пристрої, наприклад, системи електроживлення, охоронного освітлення, оповіщення, запобігання і ліквідації загроз і інші системи, які забезпечують життєздатність і надійне функціонування основних підсистем ТЗЗБ.

Кожна з основних підсистем ТЗЗБ може розглядатися як КСБ, яка відпрацьовує свій комплекс загроз і включає в себе сукупність технічних засобів охорони. Технічні засоби охорони (ТЗО) є базовим поняттям, що позначає апаратуру, яка використовується в складі комплексів ТЗЗБ об'єктів від несанкціонованого проникнення.

ТЗО - це конструктивно завершений, яке виконує самостійні функції пристрій, що входить до складу систем охоронної, тривожної сигналізації, контролю і управління доступом, охоронного телебачення, освітлення, оповіщення та інших систем, призначених для охорони об'єкта. При цьому структура КСБ виконується за класичною схемою і складається з наступних елементів:

- СЗОІУЦ - система збору та обробки інформації та управління центральна - сервер, де зберігаються і обробляються всі бази даних системи; контрольні панелі, пульти, консолі управління; в загальному випадку входить до складу центрального пульта спостереження поряд з автоматизованими робочими місцями (АРМ) операторів, адміністраторів систем, постів охорони та служби безпеки;

- робочі станції окремих систем (при необхідності), які здійснюють обмін даними та командами зі своїми периферійними пристроями та виробляють попередню обробку інформації;

- СЗОІУП - система збору та обробки інформації та управління периферійна - пристрої (контролери, розширювачі, пульти управління), безпосередньо на апаратному рівні взаємодіють зі своїми сповіщувачами, датчиками або виконавчими пристроями, а на інформаційному рівні зв'язують їх по локальному інтерфейсу (RS-485, RS-232) з робочими станціями або з сервером;

- ЗВЗ - засоби виявлення загроз - сповіщувачі охоронної, тривожної, пожежної сигналізації, зчитувачі, клавіатури, відеокамери в залежності від призначення даної КСБ;

- СПП - система передачі повідомлень - канали і засоби передачі службових і / або тривожних сповіщень і повідомлень, візуальної і акустичної інформації про об'єкт і стані КСБ;

- локальна комп'ютерна мережа, інформаційно зв'язує в єдиний комплекс окремі компоненти системи;

- ПЗ - мережеве, системне і прикладне програмне забезпечення сервера і робочих станцій, а також вбудоване програмне забезпечення системних контролерів, контрольних панелей і модулів;

- СГБЗ - система гарантованого безперебійного електроживлення, яка включає в себе:

- електрощитову КСБ, підключену до мережі 220В і містить всі необхідні вхідні і вихідні силові автомати;

- джерела безперебійного живлення, що забезпечують безперервне і якісне електроживлення всієї апаратури КСБ протягом заданого часу;

- розведену по всьому об'єкту окрему мережу живлення з розміщенням при необхідності окремих ІБП в спеціально виділених приміщеннях, нішах або шафах, які перебувають під охороною.

- допоміжні пристрої, які забезпечують виконання системою охорони ряду функцій і включають в себе:

- ЗО - засоби оповіщення;

- ЗВІ - засоби відображення інформації;

- ЗРД - засоби реєстрації даних;

- ЗПЛЗ - засоби протидії та ліквідації загроз.

З огляду на важливість для КСБ кожного елемента узагальненої структурної схеми, можна виділити три основні групи ТЗО, без яких неможлива реалізація системи безпеки: пристрої виявлення загроз, система збору та обробки інформації і управління, а також кошти, пов'язані з тим чи іншим способом передачі інформації про стан системи по каналах зв'язку, доведення її до споживача (користувачів системи, спеціальних служб і т.д.).

Перераховані засоби забезпечують реакцію КСБ на виявлену подію. Розглянемо більш детально склад і особливості деяких елементів структурної схеми КСБ.

Засоби виявлення загроз (СВЗ) У загальному випадку являють собою елементи апаратури ТЗО, які виконують функцію реагування на зовнішній вплив. Наприклад, сейсмічне СВЗ реагує на коливання грунту, викликане рухом живої істоти (людини, тварини) або неживої (автомобіля, трактора) предмета.

Основу функціонування СВЗ становить фізичний принцип дії його чутливого елемента (наприклад, електромагнітний, вібраційний, радіотехнічний, ємнісний, оптичний і т.д.).

Чутливий елемент - це первинний перетворювач, що реагує на вплив на нього (пряме чи непряме) об'єкта виявлення і сприймає зміну стану навколишнього середовища.

Засіб виявлення - це пристрій, призначений для автоматичного формування сигналу з заданими параметрами (сигналу тривоги, інакше - сигналу спрацьовування або оповіщення) внаслідок вторгнення або

подолання об'єктом виявлення чутливої зони (інакше - зони виявлення) даного пристрою. В області забезпечення протикримінального захисту нормативні документи оперують поняттям засіб виявлення проникнення і визначають його для охоронної і тривожної сигналізації як автоматичні і неавтоматичні (тривожна сигналізація) охоронні сповіщувачі.

Сповіщувач (технічний засіб виявлення) - це пристрій для формування сповіщення про тривогу при проникненні (спробі проникнення) або ініціювання сигналу тривоги споживачем. Виходячи із загальної структури КСБ, в кожній з підсистем можна виділити ті пристрої, які є засобами виявлення різних загроз і діють на основі аналізу тих чи інших фізичних параметрів контрольованого об'єкта (в залежності від призначення і виконуваних функцій підсистеми).

До засобів виявлення загроз відносяться такі пристрої:

1. Для систем охоронної і тривожної сигналізації (СОТС) - охоронні і тривожні сповіщувачі, що формують сигнали при різних видах несанкціонованого проникнення в захищені зони. Формування сповіщення про тривогу відбувається при виявленні давачами наступних дій:

- рух або присутність об'єкта в контрольованій зоні;
- руйнування будь-яких конструкцій - стекол, стін і т. д.;
- зміщення предметів, рам, дверей і т. д.;
- перетин контрольованої зони та ін.

2. Для СВТ - пристрої спостереження (відеокамери), що дозволяють візуально стежити за станом об'єкту, що охороняється в різних умовах: вдень під час нормальної роботи об'єкта (наприклад, магазину) фіксувати ситуацію під час нападу на об'єкт, вночі в період охорони реєструвати зміни в зображенні і попереджати про це.

Чинним стандартом відеокамера (ВК) визначається як з точки зору фізичного принципу дії її чутливого елемента, так і з точки зору її становища в структурі сигналізації.

Відеокамера - це пристрій для перетворення оптичного зображення в електричний відеосигнал. ВК є первинним джерелом відеосигналу в складі системи охоронної сигналізації [12].

3. Для пожежної сигналізації - пожежні сповіщувачі, які представляють собою датчики виявлення загоряння і виробляють сигнали при появі ознак пожежі (при підвищенні температури вище допустимої, при збільшенні концентрації диму і т.п.).

Визначення пожежних сповіщувачів засноване на його функціональне призначення: пожежний сповіщувач - це технічний засіб, призначений для формування сигналу про пожежу.

4. Для СКУД - приймальні пристрої ідентифікації доступу, в якості яких використовуються кодонабірні пристрою PIN-коду (клавіатури), для яких рішення про доступ приймається при введенні правильного коду, а також зчитувачі, які розшифровують інформацію, записану на ідентифікаторах різного типу і встановлюють права людей, майна, транспорту на переміщення в зоні, що охороняється (об'єкті). Для підвищення рівня безпеки контролю доступу може використовуватися подвійна технологія, що припускає спільне використання клавіатури для введення PIN-коду і зчитувача будь-якого типу (в залежності від необхідного рівня забезпечення безпеки і фінансових або організаційних обмежень). В цьому випадку код служить для підтвердження факту санкціонованого використання ідентифікатора.

5. Для систем захисту інформації - датчики виявлення витоку інформації, що видають сигнал про спроби несанкціонованого отримання інформації з об'єкта захисту. Це можуть бути передавачі підслуховуючих пристроїв, встановлені в приміщенні або підключення до телефонної лінії; визначники підключення до телефонної лінії та ін.

6. Для систем життєзабезпечення - датчики контролю навколишнього середовища, що видають інформацію про стан середовища проживання

людини, що дозволяють виявляти ситуації, небезпечні для життя або здоров'я людини, або попереджати про можливість виникнення такої ситуації (наприклад, витік газу , підвищення радіаційного фону чи протікання). Прикладом можуть служити пристрої для контролю чистоти повітря в вентиляційних системах, дозиметри для виявлення підвищення радіаційного фону.

7. Датчики контролю стану СБ, які контролюють стан і працездатність системи і формують тривожні сигнали при порушенні режиму роботи або спроби втручання в елементи системи для виведення її з ладу. При цьому система повинна постійно контролювати свою працездатність (здійснювати самоконтроль), повідомляти про несправності і охороняти себе від спроб несанкціонованого втручання (наприклад, від спроб відкрити корпус детектора або заблокувати його).

2. ТЕХНОЛОГІЧНА ЧАСТИНА

2.1. Принципи роботи комплексної системи безпеки адміністративного об’єкту

Для роботи адміністративного об’єкту необхідно забезпечити його безпеку. Комплексна система безпеки повинна забезпечувати наступні елементи контролю:

- контроль доступу до критичних приміщень (вирішується за рахунок встановлення турнікетів або дверних модулів, що здатні провести ідентифікацію особи по відбитку, магнітній картці або коду);
- контроль несанкціонованого проникнення (встановлення давачів руху, як правило інфрачервоного типу, давачів биття скла, магнітних давачів на основі герконових реле або будь-якого інакшого типу);
- контроль пожежної безпеки за допомогою теплових диференційних давачів та димових давачів згідно діючих норм;
- контроль критичних зон корпусу за допомогою систем відео нагляду.

Слід відмітити, що створення такої системи являє собою складне комплексне рішення, яке повинно добре спланувуватись, зокрема прокладка кабельних систем на стадії ремонтних та штукатурних робіт. Наприклад, якщо наперед не було передбачено встановлення додаткових кабельних систем для резерву або встановлення додаткового обладнання з метою корекції системи безпеки, то додаткові лінії для збільшення, наприклад кількості давачів або відеокамер в певній зоні необхідно монтувати нові траси в коробах. Це у свою чергу портить зовнішній вигляд приміщення, характер його сприйняття, а окрім того збільшує імовірність проникнення зловмисника до кабельної системи комплексної безпеки. Тому всі види

кабелі бажано проводити у штукатурці. Проте такий підхід має і негативну сторону. Монтаж кабелів у стінах утруднює доступ до них при поломці останніх, що приводить до потреби розбивати штукатурку і ремонт. Тому планування розміщення давачів для забезпечення комплексної системи повинно проводитись дуже ретельно і продумано, адже корекція таких рішень може відбитися на значних затратах фінансів. У роботі авторами буде розглянуто можливість створення безпровідних давачів для корекції критичних точок безпеки. Проте такі елементи відносно легко перехоплюються і зловмисники мають ширший діапазон для обходу системи.

Розглянемо основні методики та принципи побудови таких систем.

Загальний вигляд адміністративного корпусу, який буде розглянуто в роботі для створення комплексної системи безпеки приведено на рис 2.1.

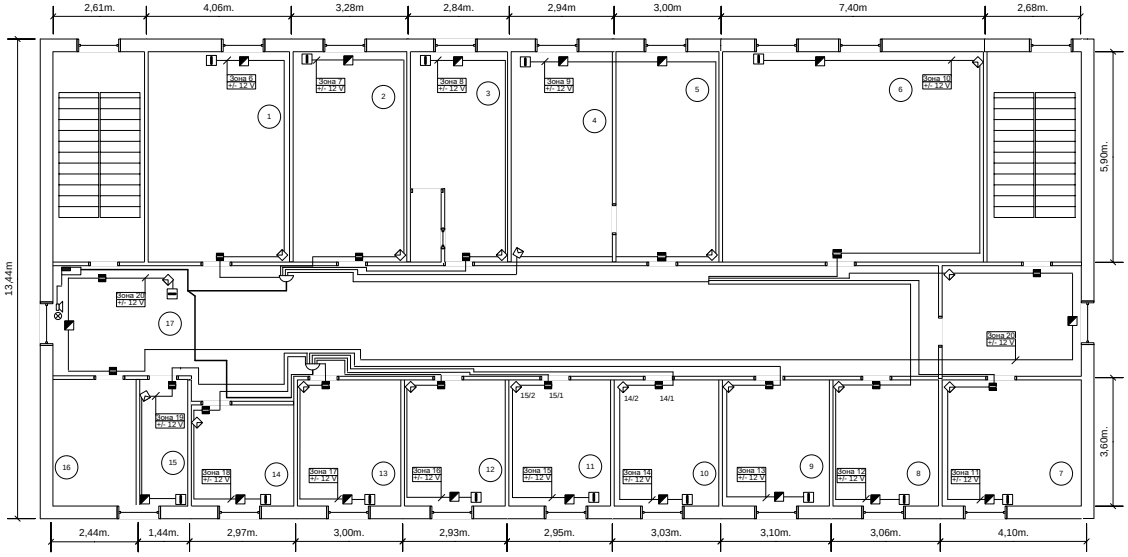


Рисунок 2.1 – план приміщення адміністративного корпусу для організації системи охорони

Основним підходом будем вважати наступний. Необхідно виходити з того, що система повинна забезпечити контроль в особливо критичних зонах. В цих місцях встановлюємо відеонагляд. Також відеокамеру необхідно встановити у центральному коридорі для візуального нагляду за усіма особами, які заходять у будівлю. Це забезпечить більшу імовірність

виявлення зловмисників. Охоронні давачі проникнення необхідно встановлювати в усіх приміщеннях на усіх вікнах і дверях для отримання статистики відкривання та закривання віко і дверей. Тим більше ці види давачів є найбільш дешевими і простими у встановлення та використанні. Давачі руху також будуть встановлюватися в усіх кімнатах, проте кількість буде визначатися виходячи з того, що необхідно зменшити кількість «мертвих» зон та забезпечити максимальний контроль руху в приміщенні.

Обладнання з контрольованим входом – дверні модулі будемо встановлювати лише на дверях в приміщеннях, де є обмежений доступ персоналу. Звичайно ж чим інтелектуальніший такий модуль, тим він і дорожчий. Найпростіший модуль працює з магнітним зчитувачем або кодом. Проте вказані елементи ідентифікації легко викрасти або скопіювати. Але такі пристрої надійні в роботі та прості в користуванні. Сканер відбитків пальців є найбільш складним та, на нашу думку, найбільш надійним пристроєм контролю доступу, але відповідно і найбільш дорогим. Тому кількість давачів, їхній тип спочатку планується, а потім бажано провести процес оптимізації. При цьому враховуються фінансові можливості замовника та вартість втрат при крадіжці.

Що стосується загальної характеристики системи безпеки, то керівний склад також має можливість віддалено контролювати, що відбувається у корпусі при його відсутності. Тобто при розробці системи безпеки необхідно передбачити вивід певних елементів на мобільні девайси.

Отже, проаналізувавши всі аспекти можна стверджувати, що розробка комплексної системи безпеки має багато факторів, таких як вартість, інтелектуальність обладнання, автоматичний та ручний контроль, наявність дистанційної передачі даних. Всі ці параметри необхідно враховувати. На сьогоднішні час присутньо багато видів обладнання, які при належному підході дозволяють реалізувати конкретні рішення в рази дешевше від готових аналогів.

2.2 Підсистема протипожежної безпеки

Відповідно до вимог найпершою системою, яка має бути присутня в адміністративних приміщеннях є система протипожежного захисту. Власне кажучи протипожежні служби не дадуть допуск до експлуатації будівель, якщо протипожежний захист не буде встановлено та ця система не буде відповідати діючим нормам.

Вимоги до проектування таких систем регламентуються документом «СИСТЕМИ ПРОТИПОЖЕЖНОГО ЗАХИСТУ ДБН В.2.5-56:2014» [5]. В ньому описано, які повинні бути системи протипожежного захисту, пожежогасіння та оповіщення при пожежах.

Керівництво може проводити встановлення таких систем самостійно, але у відповідності з нормами у погодження з пожежними службами або скористатися послугами спеціалізованих підприємств, які виконують роботи такого типу. Проте при підготовці комплексних систем бажано їх всіх поєднати, що ускладнює процес встановлення давачів та системи оповіщення.

Види давачів, які реагують на тепло або дим обираються відповідно до вимог від ДСТ EN 54-1 до ДСТУ EN 54-24. Давачі теплового типу використовують, якщо при виникненні пожежі може виділятися велика кількість тепла, димові, якщо можлива наявність диму, давачі полум’я, якщо в зоні можлива поява вогню температурою вище 600 °С.

Для адміністративного корпусу, тобто такої будівлі, де знаходиться велика кількість людей, немає спеціального обладнання, необхідно встановлювати давачі диму та теплові. Причому аналізуючи норми наукраще встановлювати диференційні теплові давачі та датчики диму. Вони діють найшвидше і покривають велику площу. Давачі такого типу монтуються на стелі і в такому випадку бажано, щоб проводи ішли не у стіні. Це пов’язано з

тим, що полум’я може пошкодити кабель, а це і єбажаним, оскільки давачі працюють на розрив лінії (тип NC).

2.3. Підсистема відео нагляду

При організації систем відео нагляду якихось вимог та норм немає. Якщо власники будівлі замовляють послуги на встановлення в іншої організації, то вона сама приймає рішення щодо розміщення елементів та кабельної системи.

Кількість відеокамер та їхній тип обирається вільно, виходячи з того, скільки які зони бажано бачити та які необхідно контролювати. Тип камер та обладнання обирається, виходячи з ціни та якості зображення, дальності дії та надійності в роботі.

Системи відео нагляду бувають трьох типів (по виду сигналу): аналогові, цифрові та комбіновані. Цифрові камери передають зображення набагато чіткіше за є більш завадостійкими, проте це відбивається на їхній вартості.

Також камери розділяються на ті, які передають зображення в кольорі та чорно біле (монохромні). Відповідно це також відбивається на їх вартості. Слід також відмітити, що при зберіганні записів з камер кольорові займають набагато більше місця, ніж монохромні. На нашу думку інформативність у них однакова. Слід відмітити, що для сприймання кольорового зображення використовують більш складні матриці та електроніку підтримки, що відбивається на вартості. При вибору типу відеокамери також враховується якість розкадровки, що відбивається на об’ємі файлу запису. Проте для аналізу обличчя необхідно максимальну якість. До того ж при аналітичній обробці зображень з метою ідентифікації також вимагається максимальна якість. На думку авторів монохромне зображення є більш інформативним і легше для сприйняття органами зору.

Що стосується виконання, то камери можуть бути виконаними наступним чином:

- в корпусі (самі найбільш функціональні);
- купольного типу (має механізми повороту, можна керувати нею віддалено);
- малогабаритні (володіють малими розмірами, як правило використовуються для резервної зйомки з метою знайдення зловмисника). Встановлення таких камер необхідно додатково погоджувати юридично, оскільки самовільне встановлення спецзасобів стеження карається законом;
- безкорпусні (виконанні у вигляді встановленого на плату об'єктиву зі схемотехнікою підтримки). Як правило використовуються для специфічних застосувань при встановлення в додаткові пристрої;
- з сферичним об'єктивом (отримують зображення сферичного типу, яке може охопити великий простір. Проте отриманий запис складний для аналізу та при необхідності аналізу треба застосовувати додаткову обробку. Однак одна така камера може замінити дві або три корпусного типу.

Слід відмітити, що для реалізації відеоспостереження ефективним засобом відстеження подій є запис зображень відеокамер. Системи реєстрації зображень на сучасний час, як правило, працюють по принципу затирання найбільш давнього запису. Чим довша тривалість запису, тим більший об'єм вінчестера необхідно забезпечити. Переважно реєстратори обирають по типу: мультиплексори та квадратори. Перші виводять зображення для 4-32 камер одразу, а другі – для 4 камер. Квадратори в більшості випадків витіснені мультиплексорами. Оскільки практично не відрізняються по вартості. Їх також можна налатувати на вивід певних зображень та захистити паролем, щоб персонал не міг самовільно виводити на екран зображення інших камер.

На даний час доцільним є використання можливості мобільного контролю за відеонаглядом та станом об’єкту з будь-якої точки земної кулі за допомогою систем мобільного зв’язку. Функціонал таких систем обмежений, проте дає певні перспективи.

2.4. Підсистема контролю проникнення

Захист від несанкціонованого доступу має свою специфіку. Насамперед необхідно забезпечити контроль за будь-яким проникненням сторонніх осіб з метою крадіжок в нічний проміжок часу. Для забезпечення цього встановлюються давачі руху, розбивання скла та відкривання дверей.

При цьому бажано сигнали усіх давачів виводити на екран комп’ютера чи іншого девайсу для охоронного персоналу, тоді досвідчений працівник зможе чітко зорієнтуватися в ситуації, що відбувається. Також необхідно забезпечити відповідну індикацію тривожного стану.

В якості засобів для вирішення цієї задачі використовують:

- магнітні зчитувачі або скануючі пристрої різних типів;
- давачі руху, як правило інфрачервоного типу;
- звукові давачі, як реагують на частоту биття скла;
- магнітні контактні давачі, побудовані на герконовому вузлі.

На двері та вікна доцільно встановлювати герконові вузли, вони є найбільш дешевими та надійними, проте вимагають підводу провідників до самого вузла. Паралельно до них встановлюється давач биття скла, адже якщо зловмисник розбив скло, герконове реле не спрацює.

Для контролю об’єму приміщення та рухів у ньому використовують також різні типи сповіщувачів. До них відносять:

- теплові пасивні давачі – вловлюють інфрачервоні випромінювання людського тіла;

- оптико- електричні давачі активного випромінювання. Вони складаються з випромінювача і приймача. При наявності перепони (наприклад людина пройшла між приймачем та випромінювачем) вони вловлюють втрату сигналу та видають справцювання;
- давачі, принцип роботи яких заснований на ефекті Доплера;
- комбіновані рухові давачі. В них поєднані кілька давачів з іншими принципами роботи. Такі пристрої володіють високою завадозахищеністю, оскільки порівнюють дані, отримані кількома методами.

Для забезпечення контролю приміщень необхідно встановити давачі руху та розбиття скла. для забезпечення повного контролю в кожному приміщенні, де є наявні вікна встановлюємо давачі розбивання скла. для розуміння розташування давачів руху розглянемо схему їхнього покриття.

Стандартний переріз зони покриття давача руху приведено на рис 2.2.

Розмір зони може змінюватися в залежності від типу давача, проте кут розтвору як правило більше 110 градусів і забезпечується повне перекриття зони з висоти 2,1 метра, що відповідає висоті більшості приміщень. Слід також відмітити, що налаштування давачів безпеки також необхідний процес. Вони перемикаються в режим індикації (він світиться червоним, коли спрацював) і проводиться налаштування його розміщення з метою покриття якомога більшої зони, при умова, що давач відреагує на рух. Потім режим індикації вимикають, щоб зловмисники не могли проводити попередню оцінку зон давачів.

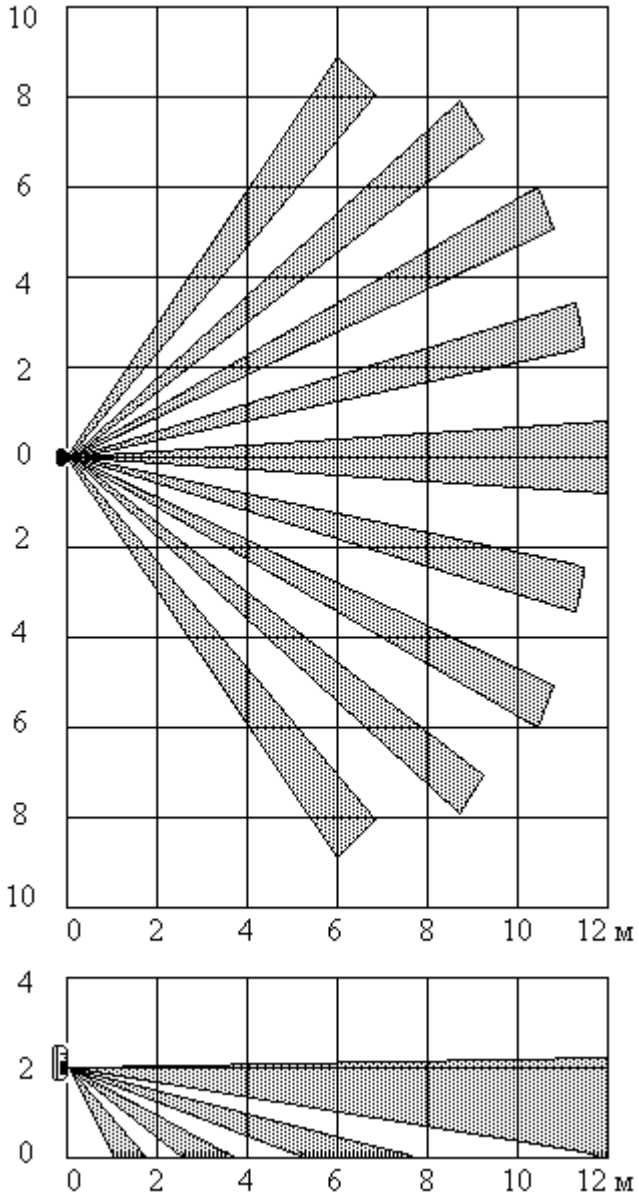


Рисунок 2.2 – Стандартна зона покриття для більшості давачів.

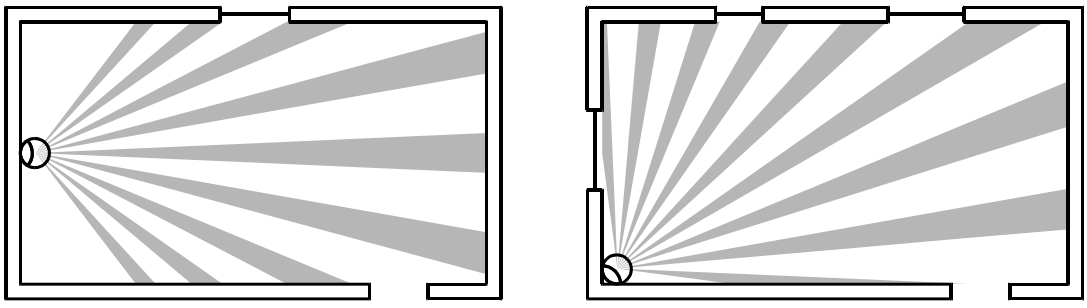


Рисунок 2.3 – Приклади встановлення давачів руху.

Аналізуючи рис. 2.3 можна зробити висновок, що найкращим розташуванням давачів є схема розташування одни напроти одного в різних кутах.

Приклад такої реалізації показано на рис. 2.4.

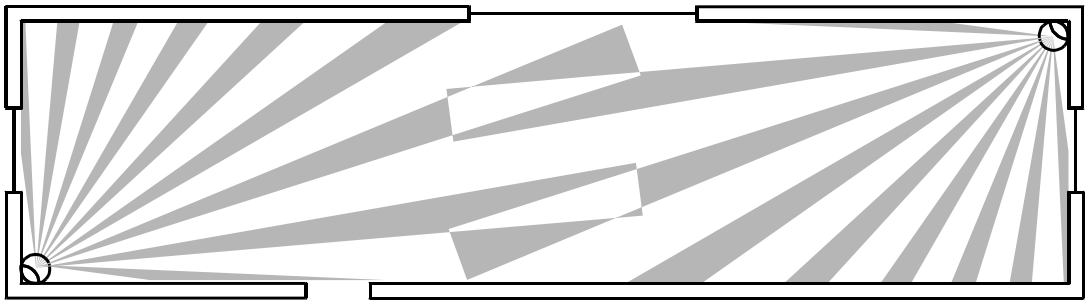


Рисунок 2.4 – оптимальне розташування давачів

При такому розташуванні вони контролюють один одного та перекривають усі зони в приміщенні, що є найбільш ефективним способом. Проте не завжди вдається реалізувати таку схему.

3. КОНСТРУКТОРСЬКА ЧАСТИНА

В загальному комплексну систему забезпечення безпеки будівлі можна представити у наступному вигляді:

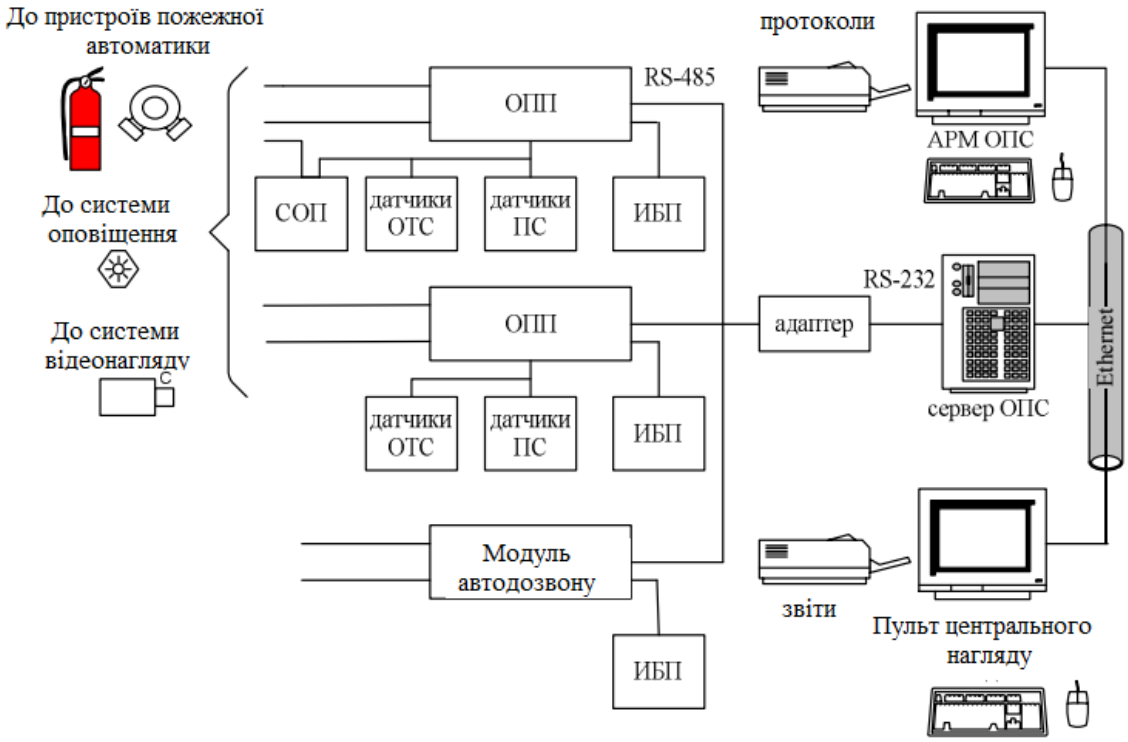


Рисунок 3.1 – Одна з типових структур пожежно-охоронної системи сигналізації:

АРМ – автоматизоване робоче місце; ОПП – охоронно-протипожежна панель; ПС – пожежна сигналізація; СОП – систем охорони периметру; ОТС – охоронно-тривожна сигналізація.

Аналізуючи таку реалізацію і принципи та методи створення таких систем ми пропонуємо наступну реалізацію такого підходу, яка представлена на рис. 3.2.

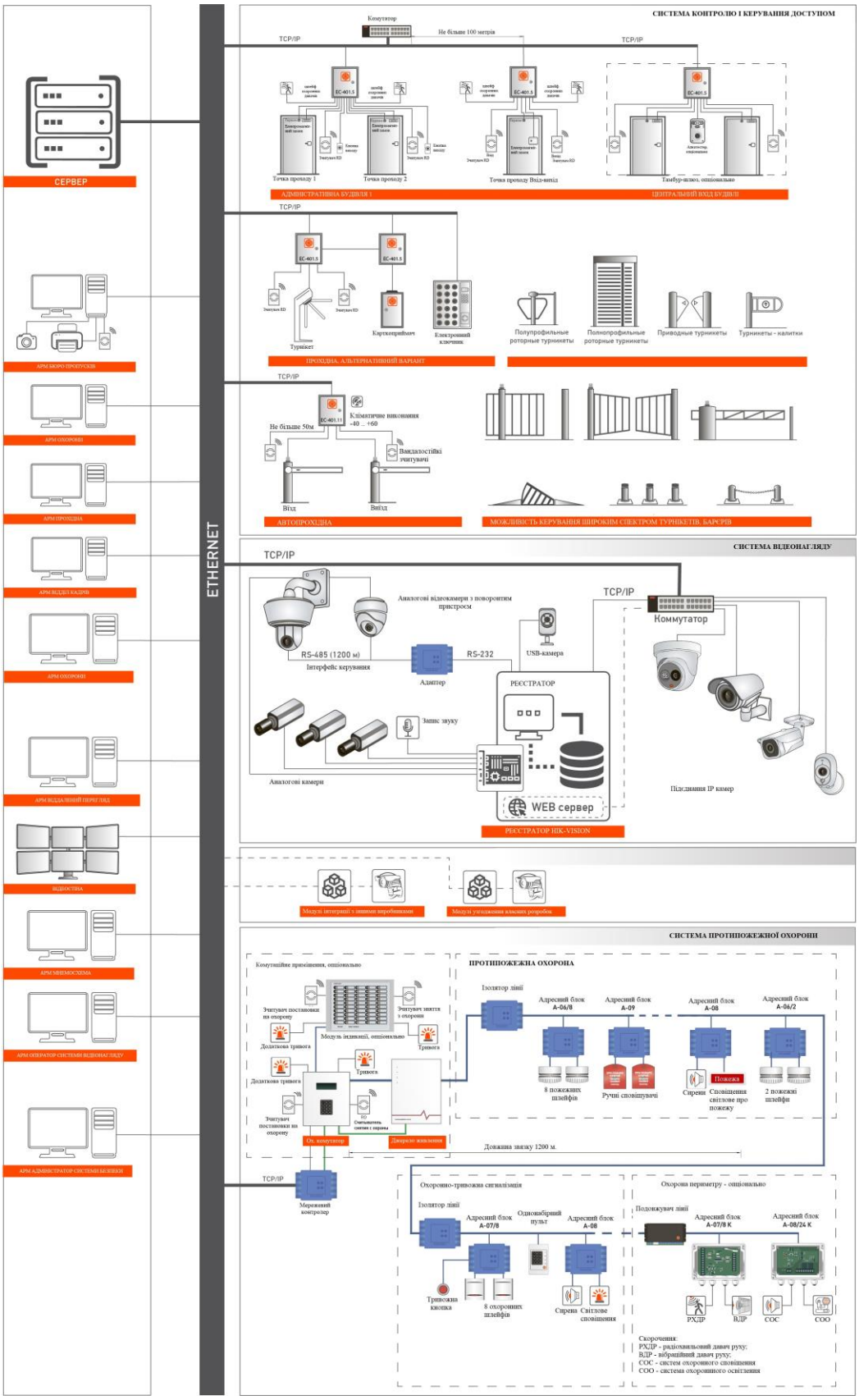


Рисунок 3.2 – Розроблена структура комплексної системи безпеки

3.1. Система під’єднання камер та структура системи відеоспостереження

Для організації відеонагляду згідно приведеної схеми необхідно уточнити, які саме приміщення повинні перебувати під відеонаглядом. Як правило встановлення камер у всіх приміщеннях є сильно дорогим та, з психологічної точки зору, створює тиск на персонал, особливо коли це стосується виконання творчої роботи. Люди не почувають себе вільно.

Як правило відеонагляд необхідно встановити за входом у будівлю та за критичними об’єктами. В приміщеннях високого ступеня контролю відеонагляд встановлюють таким чином, щоб камери контролювали одна одну. Аналізуючи велику кількість виробників відеоспостереження найбільш надійними пристроями є системи відеонагляду фірми HIK-Vision.

Загальна структурна схема реалізації відеонагляду приведена на рис 3.3

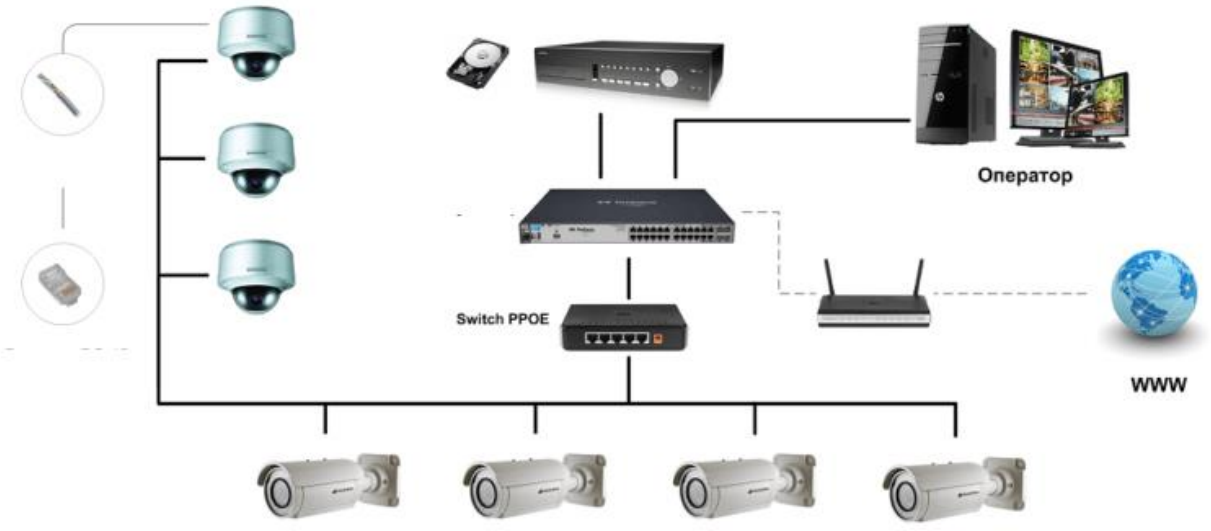


Рисунок 3.3 – Функціональна схема реалізації системи відеонагляду

В якості базових елементів обираємо камери типу DS-2CD2042WD-I.

Це є пристрої внутрішнього виконання, які мають у своїй конструкції 4 мм об’єктив, та інфрачервону підсвітку. Це забезпечує ефективну дальність дії до 30 метрів. Вони мають можливості під’єднання по IP адресі, що спрощує реалізацію такої системи. По витій парі реалізовано передачі живлення та зображення. Також слід відмітити, що до зображення камери можна отримати доступ з локальної мережі, ввівши мережеву адресу та код доступу. Якщо необхідно отримати доступ до запису показів камери, то можна з будь-якого комп’ютера мережі зайти на реєстратор та отримати необхідну інформацію. Також вказана камера володіє індикатором руху, тобто з метою економії місця на диску реєстратора вона може записувати лише в режимі визначення руху. Загальний вигдяд камери та інтерфейс налаштування зон спостереження приведено на рис 3.4.

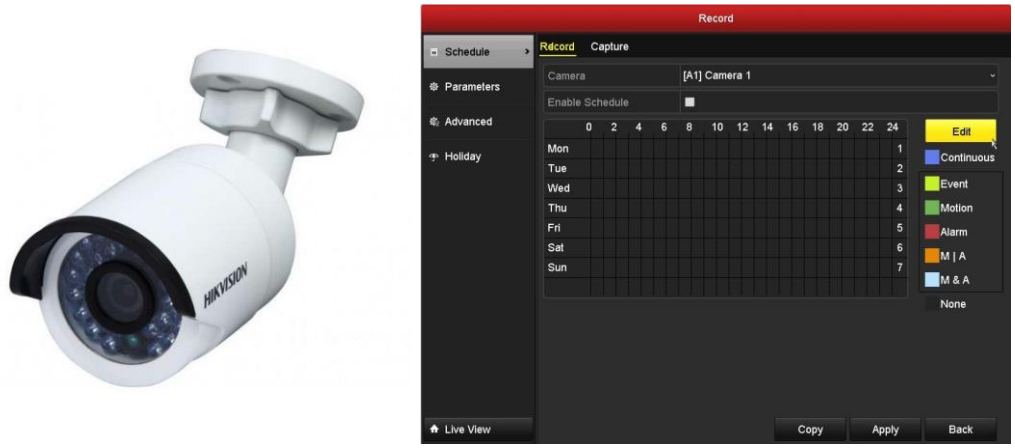


Рисунок 3.4 – Вигляд обраної камери та вікно налаштування методів запису.

По плану приміщень згідно додатку 1 в нашому випадку необхідно встановити 6 камер спостереження.

Слід відмітити, що налаштування самої камери є інтуїтивно зрозумілими, тому приводити розширений її опис немає доцільності.

В якості реєстратора записів обрано пристрій типу DS-7608NI-Q1.

Від дозволяє обслуговувати 8 пристроїв відеонагляду з якістю зображення 4К. Також для такого пристрою було обрано жорсткий диск об’ємом 2 терабайти, що забезпечить запис відеонагляду на протязі 15 днів. Цього на нашу думку абсолютно достатньо для забезпечення контролю.

Реєстратор також під’єднується в локальну мережу, має власну мережеву адресу. До нього можна під’єднатися з будь-якого ПК в мережі або з мобільного девайсу.

Для того, щоб зайти на реєстратор або камеру необхідно в браузера на пк ввести мережеву адресу пристрою і кладка перейде у вікно входу системи HIK-Vision. По адресу і паролю користувач може отримати доступ до записів камер, на які має дозвіл.

Також хорошою опцією є можливість спостерігати за об’єктом, станом запису віддалено через інтернет. Проте тут є кілька нюансів. Реалізувати перегляд можна реалізувати через хмарний сервіс HIK-Connect, який до речі є безкоштовним, або через виділену «білу» айпі адресу у провайдера. Другий випадок вимагає серйозної реалізації налаштувань фаєрволів на вхідних роутерах для запобігання вірусних атак.

Для реалізації виходу в інтернет або доступу до системи відеонагляду, для контролю пожежної сигналізації, а також для можливості слідкування за об'єктом бажано замовити у провайдера відкриту IP адресу для виходу в інтернет. Така послуга дасть можливість автоматизовано керувати об'єктом віддалено. Системи відеоспостереження дозволяють отримати доступ до відеокамер через хмарні сервіси такі як HIK-connect або інші доступні хмарні сервіси. Проте передача даних через такі сервіси є обмеженою, швидкодія в них як правило нижча і присутня певна затримка при передачі зображення.

Тому більш ефективним способом контролю за системою відеонагляду є доступ до реєстратора або камер за допомогою використання відкритої IP адреси. При цьому необхідно налаштувати вхідний роутер таким чином щоб приховати внутрішнє розташування та порти доступу до відеокамер та

реєстратора. Їх повинен знати лише оператор віддаленого керування. Для цього на роутері необхідно підняти Firewall та налаштувати переадресацію портів. Система відеонагляду вимагає для доступу ззовні забезпечити прокидку портів. Стандартними портами є 80, 554, 8000, 443. Проте якщо залишити такі порти стандартними віруси ззовні легко зламають реєстратор. тому при прописані прокидки портів на роутері необхідно їх змінити на інакші випадкові, які будуть знати лише люди, які мають відношення до системи відеонагляду.

Способи програмування роутера та реєстратора будуть розглянуті в спеціальній частині.

3.2. Система охоронної сигналізації та протипожежної охорони

Впровадження системи протипожежного захисту є важливою задачею оскільки дозволяє швидко і ефективно реагувати на виникнення пожежі, що приводить до зменшення матеріальних втрат. Адже пожежа наносить надзвичайно велику шкоду майну підприємства. Тому запобігання пожежі та створення засобів оповіщення при його виникненні для забезпечення евакуації людей є важливою задачею при створенні інтегрованих систем безпеки адміністративних корпусів. Оскільки в адміністративних корпусах працюють люди, то вимоги до пожежної безпеки особливо жорсткі.

Для запобігання пожежі застосовують теплові та димові давачі. Найдешевшими є теплові давачі типу ІП, як спрацьовують при температурі 70 °С. Проте, якщо температура на стелі досягає такого значення пожежу місцево зупинити практично неможливо. Тому не дивлячись на дещо більшу вартість необхідно обирати теплові давачі диференційного типу, які реагують на миттєву різку зміну температури і при цьому набагато краще визначають

пожежу. Це у свою чергу дозволяє вчасно прореагувати та зменшити втрати підприємства.

В нашому випадку було обрано давачі типу ТПТ-4. Його ціна коливається в районі 130 грн за штуку. Даний давач має індикацію охоронного режиму, що дозволяє легко перевірити його роботоздатність. Працює по двопроводовому зв’язку, з діапазоном гарантованого спрацювання 54-70 ℃. Загальний вигляд давача приведено на рис. 3.5.

Рисунок 3.5 – Давач ТПТ-4.

Для реакції на дим було обрано давачі типу ИКП-8, ціною 135 грн. Він проводить визначення наявності диму в приміщенні при допомозі інфрачервоного випромінювача. При відсутності диму приймач не бачить випромінювача, він направлений не в його сторону. Проте при появі диму сигнал випромінювача внаслідок заломлення попадає на чутливий елемент, що викликає спрацювання. В деяких випадках такі давачі дозволяють швидше прореагувати на пожежу. Даний тип давача також має діодну індикацію охоронного режиму. Загальний вигляд давача приведено на рис 3.6. Даний давач здатен

Рисунок 3.6 – загальний вигляд давача диму

Вказані типи давачів під’єднуються до центрального пульта пожежної охорони з індикацією стану ліній та можливістю передачі параметрів на ПК для організації центрального пульта охорони.

Пожежну централь було обрано типу ТІРАС – 4П.1

Рисунок 3.7 – Загальний вигляд централі

Дана централь підримує усі необхідні давачі, дозволяє контролювати їхні параметри і передавати результат на персональний комп’ютер. Також має вбудований модуль GSM для передачі даних по мобільних мережах.

Що стосується системи охорони, то для неї було обрано давачі руху SWAN SQUAD, від 250 грн за штуку. В основі пристрою – чотириелементна оптична лінза з PIR- сенсором. Даний пристрій володіє хорошою стійкістю до видимого світла та надійний в роботі. Його параметрів цілком достатньо для реалізації роботи системи безпеки адмінкорпусу. Дальність спостереження 18*18 метрів, чого є цілком достатньо. Загальний вигляд давача та схема його під’єднання показані на рис. 3.8 та 3.9.

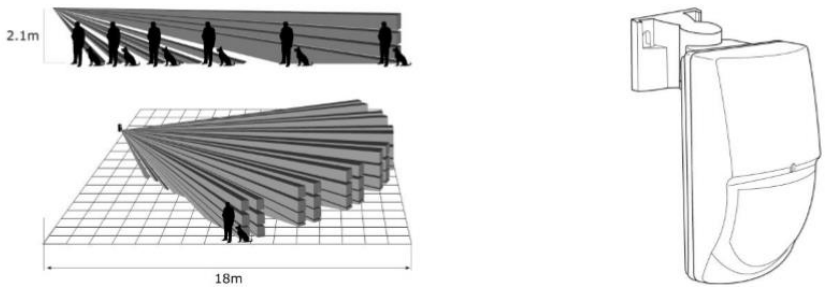


Рисунок 3.8 – загальний вигляд та зона покриття давача

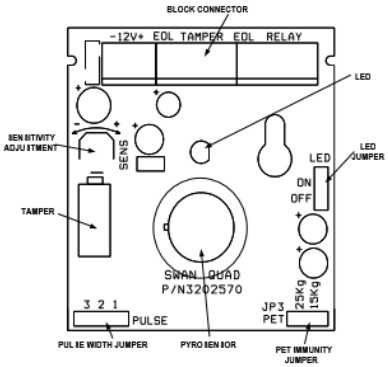


Рисунок 3.9 – Схема під’єднання SWAN SQUAD

В якості давача биття скла обрано пристрій типу INDIGO (акустичний давач). Його встановлювали в кожній кімнаті, де є в наявності вікно. Цього цілком достатньо, щоб виявити проникнення зловмисників через розбиття скла. Цей пристрій служить для визначення чи розбито скло, як багатошарове, так і нормальної товщини. Може вловлювати як генерацію звуку внаслідок удару (генерується хвиля низької частоти), так і внаслідок розбитого скла (генерується хвиля високої частоти). При чосу після реєстрації удару давач вмикає систему визначення високої частоти, щоб підтвердити проникнення, якщо хвиля не виникла, спрацювання не відбудеться. Тобто виключається спрацювання від того, що щось впало на підлогу або від інших джерел звуку. Також давач володіє плавним регулюванням чутливістю сегментів.

На вікна і двері також встановлювали герконові блоки, які розмикаються при відкриванні дверей чи вікна. Це забезпечує контроль оператора за станом дверей та вікон, особливо в нічний час.

Всі елементи під’єднані до пульта центральної охорони ОРІОН 16Т3-2. З пульта сигнал про стан об’єкту та охоронних і пожежних давачів виводиться на екран монітору охоронців, а також з мобільного девайсу ззовні також можна переглянути стан об’єкту.

3.3. Альтернативні системи для вирішення проблемних моментів в системах охорони

У даному розділі буде розглянуто кілька можливих реалізацій охоронних рішень, які за своєю реалізацією є досить надійними, проте володіють дуже низькою вартістю та простотою реалізації. Оскільки система охорони розробляється для адміністративного корпусу, то система буде працювати в нормальних умовах (температура не буде меншою нуля, вологість буде в допустимих межах). Впровадження такої системи вимагає деяких затрат інженерної праці та деяких елементів виготовлення, таких як пайки на макетній платі, створення корпусу для системи керування, тощо. Проте при наявності часу і відповідного персоналу, затрати на впровадження системи охорони можна скоротити в рази.

Тому у даному розділі ми спроектуємо систему охорони, засновану на популярній, дешевій та відносно надійній платформі Arduino. Розглянемо метод реалізації системи охороно по бездротовому принципу. Така реалізація може бути використана як варіант вирішення додаткових задач, коли основна система охорони вже встановлена і необхідно додати ще кілька давачів, а провести нову кабельну систему є накладно. В такому випадку на допомогу приходить бездротова реалізація.

В нашому випадку система буде використовувати будь-який інфрачервоний давач руху, методи встановлення яких та їхнє покриття було розглянуто в розділі 2. Слід відмітити, що давачі руху в більшості випадків виконані модульно, тобто не важливо, яке виконання, від давача до пульта приходить лінія NC типу. При ідентифікації руху вона розриває коло. Цю подію необхідно обробити та видати керуючий сигнал тривоги. В нашому випадку отриманий сигнал буде передаватися бездротовим шляхом.

На рис. 3.10 приведено необхідне обладнання для реалізації системи.

В даному випадку ми розглядаємо проектний варіант, проте в подальшому бредборд замінюється друкованою платою, доробляються корпуси для системи керування та розміщення давачів, тощо.

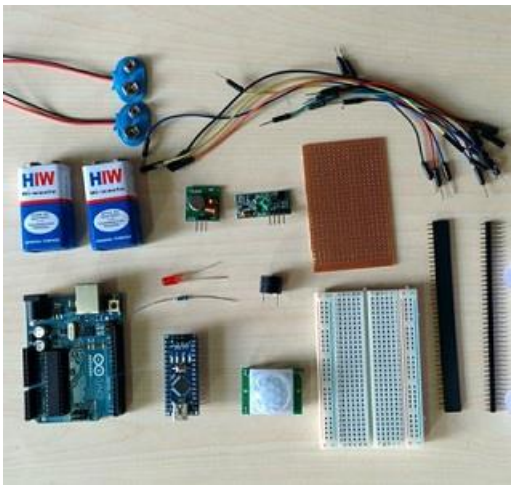


Рисунок 3.10 – Компоненти, необхідні для реалізації системи

Частина системи, яка буде виконувати передавальну функцію може бути виконана на будь-якій платформі, в нашому випадку це Arduino Nano.

Для бездротової преедачі будемо використовувати будь-який РЧ пристрій передавання. Розглядувана плата має 14 цифрових входів-виходів та п’ять аналогових входів. Вихід давача руху будемо під’єднувати до D2, а лінію даних радіопередавача – до входу D12. На рис. 3.11 представлена схема з’єднань для передавальної частини системи.

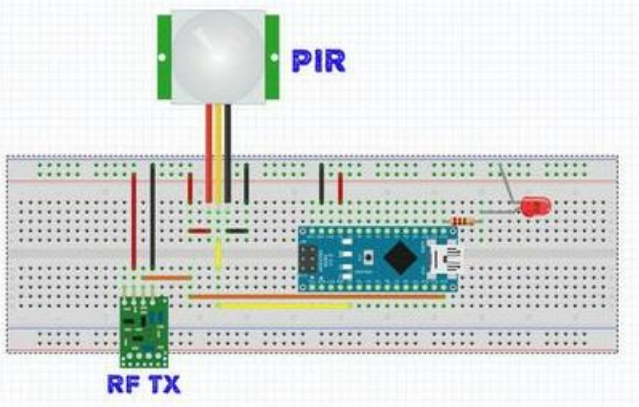


Рисунок 3.11 – Схема під’єднання передавальної частини пристрою

Частина, яка повинна приймати сигнал, має в своєму складі 2 плату типу Arduino, пристрій РЧ приймання, п’єзоелемента і світлодіоду. П’єзоелемент можна встановлювати опціонально, якщо необхідно генерувати звук при спрацюванні давача або генерації режиму тривоги. Якщо необхідно під’єднати сирену, тоді портібно додатково встановлювати блок живлення для неї, як правило 12В. Схема цієї частини приведена на рис. 3.12

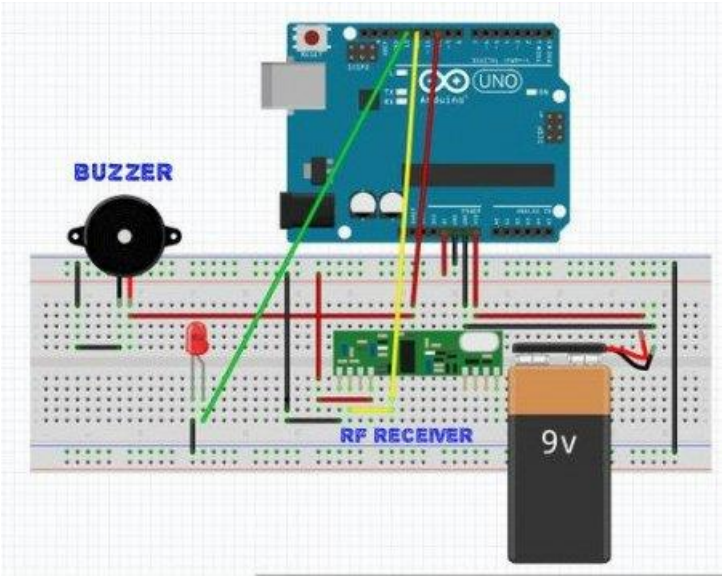


Рисунок 3.11 – Реалізація приймаючого пристрою

Приклад коду для даної реалізації

Лістинг 1

```
#include <VirtualWire.h>

int led_pin = 13;
int transmit_pin = 12;
int pir_pin = 2;
int val = 0;
int pir_state = LOW;

void setup()
{
   Serial.begin(9600);
   vw_set_tx_pin(transmit_pin);
   vw_setup(4000); // Скорость передачи
   pinMode(led_pin, OUTPUT);
   pinMode(pir_pin,INPUT);
}

void loop()
{
  char msg[1] = {'0'};
  // Получаем значение с датчика
  val = digitalRead(pir_pin);
  // Меняем сообщение, если движение замечено
  if (val == 1)
  {
      msg[0] = '1';
      digitalWrite(led_pin, HIGH); // Зажигаем светодиод для индикации передачи
      vw_send((uint8_t *)msg, 1);
      vw_wait_tx(); // Ждем, когда сообщение уйдет
      if (pir_state == LOW)
      {
      Serial.println("Motion detected!");
      pir_state = HIGH;
      }
   }
 else
 {
   msg[0] = '0';
   digitalWrite(led_pin, LOW);
   vw_send((uint8_t *)msg, 1);
   vw_wait_tx(); // Ждем, когда сообщение полностью уйдет
   if (pir_state == HIGH)
   {
      Serial.println("Motion ended!");
      pir_state = LOW;
   }
  }
}
```

Нижче наведено код програми типовий для реалізації приймача

Лістинг 2

```
#include <VirtualWire.h>

// Pins definition
const int led_pin = 13;
const int receive_pin = 12;
int pinSpeaker = 10;

void setup()
{
   Serial.begin(9600); // Только для отладки
   vw_set_rx_pin(receive_pin);
   vw_setup(4000); // Скорость передачи
   // Старт ФАПЧ приемника
   vw_rx_start();
   // Настройка выводов для пьезозуммера и светодиода
   pinMode(led_pin, OUTPUT);
   pinMode(pinSpeaker, OUTPUT);
}

void loop()
{
   uint8_t buf[VW_MAX_MESSAGE_LEN];
   uint8_t buflen = VW_MAX_MESSAGE_LEN;

   // Проверка, получено ли сообщение
    if (vw_get_message(buf, &buflen))
    {
      if(buf[0]=='1')
     {
     Serial.println("Motion ended!");
     digitalWrite(led_pin,0);
     playTone(0, 0);
     delay(300);
     }
   }
}

// Длительность в миллисекундах, частота в герцах
void playTone(long duration, int freq)
{
    duration *= 1000;
    int period = (1.0 / freq) * 1000000;
    long elapsed_time = 0;
    while (elapsed_time < duration)
    {
    digitalWrite(pinSpeaker,HIGH);
    delayMicroseconds(period / 2);
    digitalWrite(pinSpeaker, LOW);
    delayMicroseconds(period / 2);
    elapsed_time += (period);
   }
}
```

Така реалізація є досить простою в реалізаці і коштує дуже дешево, проте дозволяє безпровідно передавати сигнал тривоги, не вимагає прокладання додаткових комунікацій, може під’єднати до 8 давачів руху або биття скла, герконових блоків.

Далі розглянемо схему подібної реалізації для створення ситеми охорони із застосування GSM передавача, тобто при сигналі тривоги система може відправляти СМС про тривожний стан. Система GSM передачі є досить дорогою і тому важливим є також розглянути досить дешеві аналоги, які в певних випадках дозволять здешевити вартість впровадження системи, а при провадженні вимагають лише певних інтелектуальних затрат.

І знову для реалізації системи будемо використовувати плату Arduino. Система буде використовувати технологі. GSM, загальний вигляд якої приведено на рис. 3.12

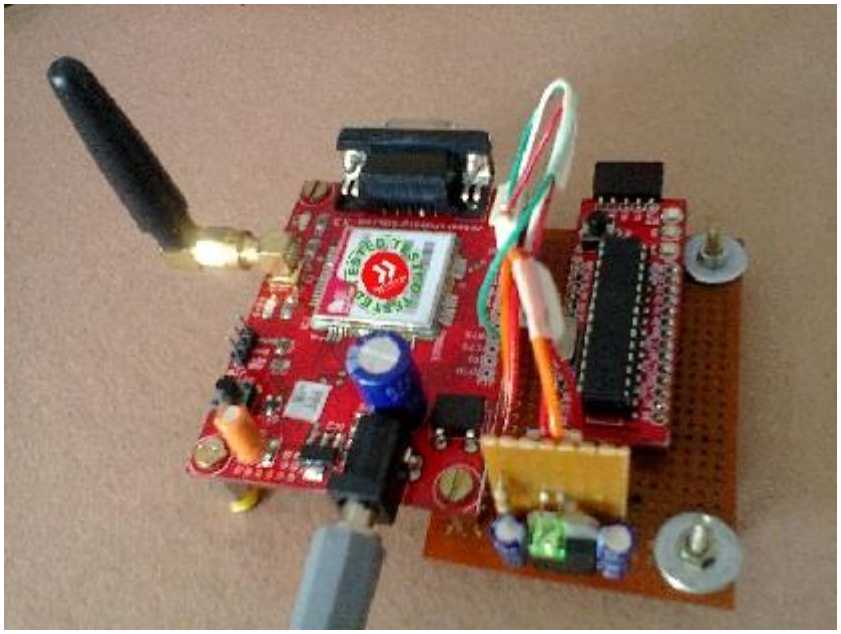


Рисунок 3.12 – загальний вигляд GSM модуля для організації охорони

До самої плати Arduino під’єднується модуль, який визначає проникнення. При генерації сигналу від нього на мобільний девайс користувача висилається мобільне повідомлення. На рис. 3.13 представлена блок-схема реалізації системи.

В якості основних елементів системи є модуль GSM/GPRS SIM900A та мікроконтролерна плата на базі Atmega. На наступному рисунку приведено базову реалізацію під’єднання модулів.

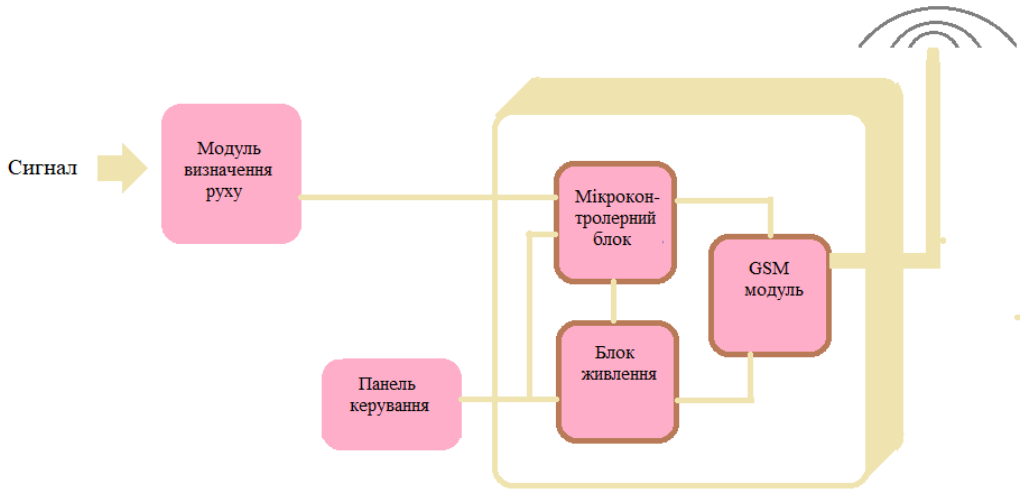


Рисунок 3.14 – Блок схема реалізації модульної системи охорони

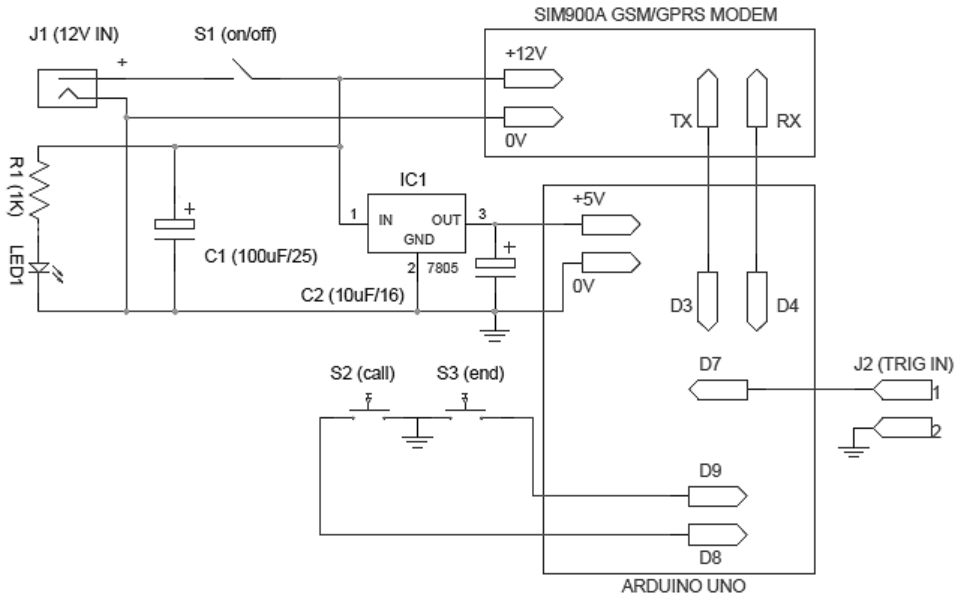


Рисунок 3.15 – принципова схема з’єднань GSM системи

Функціонування системи, власне кажучи, дуже просте . Коли подається живлення, система переходить у режим очікування. Однак, власне кажучи, коли регулюючий джампер закритий, попереджувальне повідомлення автоматично посилається на визначений номер користувача. Будь-який датчик виявлення може бути підключений до, власне кажучи, вхідної розетки. Слід зазначити, власне кажучи, що низький рівень на штирі 1 роз'єму активний і включає систему безпеки.

Лістинг керуючої програми приведено нижче.

```
#include <NewSoftSerial.h>
NewSoftSerial mySerial(3,4); // выводы RX и TX настроить на связь с модулем GSM
#define msg_key 7
#define call_key 8
#define end_key 9
String number ="0000000000"; // Сюда вместо нулей нужно вписать 10-значный мобильный номер
void setup()
{
Serial.begin(9600);
mySerial.begin(9600);
pinMode(msg_key,INPUT);
pinMode(call_key,INPUT);
pinMode(end_key,INPUT);
digitalWrite(msg_key,HIGH);
digitalWrite(call_key,HIGH);
digitalWrite(end_key,HIGH);
}
void loop()
{
//отправлять sms каждый раз, когда срабатывает msg_key
if (digitalRead(msg_key)==LOW) // Проверка, нажата ли кнопка отправки sms
{
mySerial.println("AT+CMGF=1"); // Устанавливаем режим в качестве тектового режима
delay(150);
mySerial.println("AT+CMGS=\"+00"+number+"\""); // Укажите номер адресата в международном формате, заменив нули
delay(150);
mySerial.print("Warning! Intruder Alert!"); // Введите сообщение
delay(150);
mySerial.write((byte)0x1A); // Символ конца сообщения 0x1A : эквивалент Ctrl+z
delay(50);
mySerial.println();
}
//Совершить вызов, когда сработает call_key
```

```
mySerial.println("ATD+91"+number+";"); //Определяем номер для вызова
while(digitalRead(call_key)==LOW);
delay(50);
}
//Сброс вызова
else if (digitalRead(end_key)==LOW) // Проверка, нажата ли уже кнопка сброса вызова
{
mySerial.println("ATH");
while(digitalRead(end_key)==LOW);
delay(50);
}
}
```

Отже, загальна структура системи відеонагляду, протипожежного захисту та охоронної сигналізації приведені на рис. 3.16, 3.17, 3.18 відповідно.

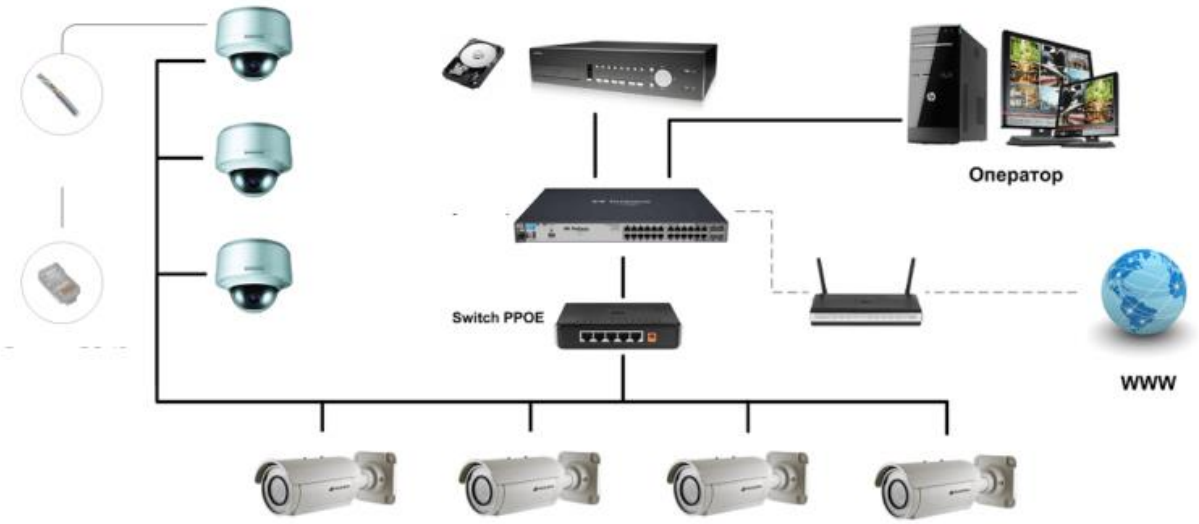


Рисунок 3.16 – Функціональна структура системи відеонагляду

Рисунок 3.17 – Структура системи доступу

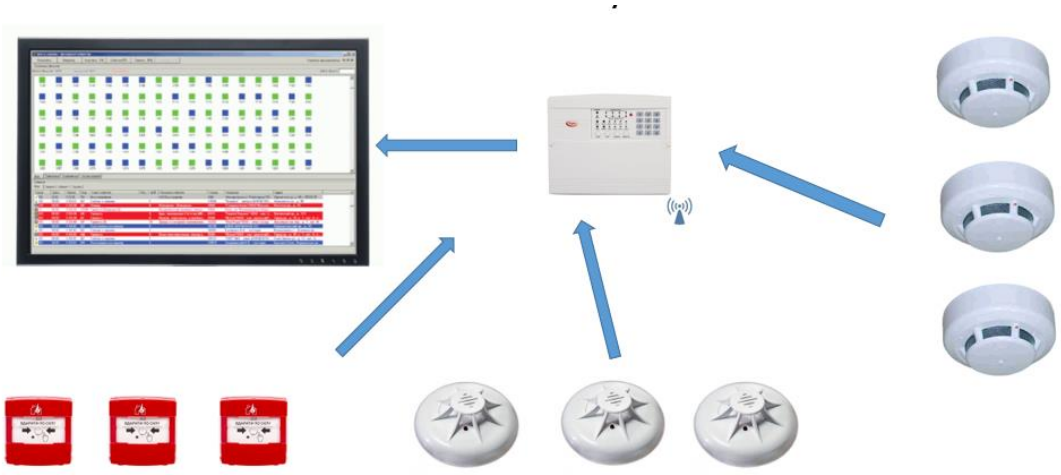


Рисунок 3.18 – Реалізація системи протипожежного захисту

4. НАУКОВО-ДОСЛІДНА ЧАСТИНА

4.1 Дослідження розподілу звукового сигналу

Необхідно відзначити, що наявність звукових сигналів є першим елементом захисту від проникнення або при виникненні критичних ситуацій. Звук сирени викликає стресові відчуття у зловмисника, та оповіщає всіх про наявність критичної ситуації. У зв'язку з цим при реалізації системи охорони необхідно провести дослідження встановлених сирен та засобів оповіщення на поширення звуку.

Такі дослідження проводяться натурно або з використанням вимірювачів звуку. Діапазон частот повинен відповідати людським і коливатись в межах 30-130 дБ від 30-8000 Гц. Слід відмітити, що сила звуку обирається в межах до больових відчуттів, тобто до 120 дБ.

Вимірювання звукових параметрів необхідно проводити в приміщеннях при закритих дверях, щоб визначити зони поширення звуку з максимальними завадами. Вимірювання звукових поширень бажано проводити кілька разів, у нашому випадку 3 рази.

Результати моделювання поширення звуку приведені в табл. 4.1

Відповідно до нормативних документів для коректної роботи системи оповіщення рівень звуку таких пристроїв повинен бути не менше 65 дБ. Аналізуючи дані вказаної таблиці можна стверджувати , що рівень оповіщення відповідає нормативним вимогам. Як вже говорилось максимальний рівень звуку в 120 дБ не був зареєстрованим.

Результати вимірювань по приміщеннях приведені у додатку 2

Слід відмітити, що в деяких випадках доцільно встановлювати додаткові сирени в критичних місцях для забезпечення стресу зловмисникам. Такі додаткові звукові джерела встановлюються в місцях, де імовірність

появи зловмисника максимальна при мінімальній імовірності появи робочого персоналу. Злочинця така звукова сирена налякає, а при хибних спрацюваннях (а такі будуть при первинному впровадженні системи) викличе мінімальний дискомфорт в персоналу.

Таблиця 4.1

Результати досліджень поширення звуку для оповіщення про небезпеку

№ кімнати	Результати вимірювань			Середнє значення
	1	2	3	
301	76	77	76	76
302	78	77	76	77
303	69	69	71	70
304	71	72	70	71
307	71	74	74	73
310	68	69	69	69
311	87	89	88	88
312	66	68	67	67
313	71	70	70	70
314	75	72	76	74
315	73	75	71	73
316	74	75	73	74
317	72	75	71	73
318	78	76	77	77
319	77	78	77	77
320	90	89	92	90
321	90	91	90	90

В подальшому для запобігання збоям необхідно провести базовий розрахунок затрат потужності на обслуговування системи сповіщення.

4.2. Оптимізація затрат живлення на обслуговування системи давачів проникнення

При роботі системи охорони її режим може бути різний, проте він буде знаходитись між двома граничними станами. Оскільки інфрачервоні давачі руху працюють по принципу нормально замкнутих контактів (їх можна і переналаштувати, проте такий режим є фективнішим, оскільки запобігає перерізанню дротів) то в режимі, коли об’єкт під охороною струм споживання буде максимальний, тому що синальні лінцюги замкнуті. Коли ж усі давачі спрацювали, струм споживання буде мінімальним. Проте такий випадок як правило неможливий. Отже, підсумовуючи сказане можна стверджувати, що система завжди знаходиться десь між двома станами: охорона бех тривог (максимальне споживання), всі давачіспрацьовані проте сирени не задіяні (мінімальне споживання).

Слід відмітити, що для розрахунків достатньо розглянути режим максиального навантаження, щоб забезпечити необхіну потужність на функціонування системи. Згідно з правилами електроніки та електротехніки найбільш оптимальним для проведення таких розрахунків є реалізація схеми заміщення, яка приведена на рис 4.1.

В даному випадку весь опвр розбивається на дві складові – опір кабельної системи до кожного давача Rk, та опір давача Rзв.

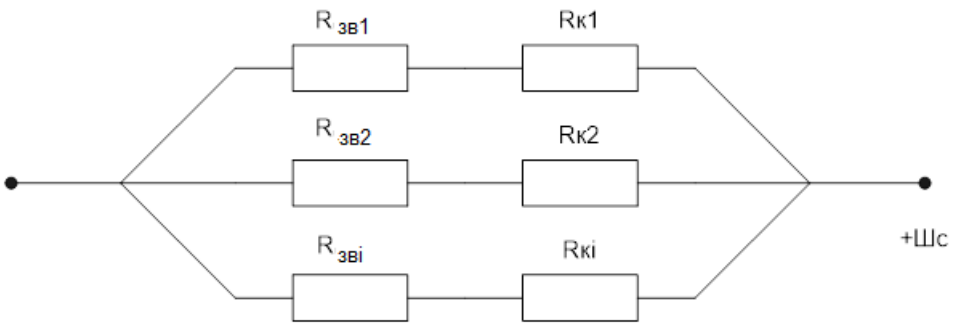


Рисунок 4.1 – Еквівалентна сзема заміщення для розрахунку потужності.

Відповідно до типу обраних давачів, аналізуючи їхні технічні характеристики можна стверджувати, що споживання в режимі спрацювання – 8 мА, а в режимі охорони – 15 мА. Для давача розбивання скла дані наступні тривожний стан 14 мА, охоронний стан – 24 мА. Ці дані отримані для дженела живлення 12 В, яке в більшоств випадкі є стаціонарним для такої системи.

Слід відмітити, що в подальшому при розрахунку рівнів сигналів необхідно було розраховувати втрати в системі кабелів. При використанні стандартних кабелів січенням 4*05 мм, електричний опір приблизно становитиме 148 ом/км.

Для розрахунку опору кабеля використовуємо формулу:

$$R_К = R_{УД} \cdot L \tag{4.1}$$

Тут перша складова – питомий опір, а друга – довжина провідника відповідно.

Отже, після розрахунків, маємо для давача 6-2:

$R_К = 0{,}148 \cdot 6 = 0.87\,\text{Ом}$

Напруга живлення:

$$U_{iППИ} = U_{НОМ} - I_{ПИТ} \cdot R_К \tag{4.2}$$

Звідки, напруга на давачі руху:

$U_{6-2ПИТ} = 12 - 0{,}016 \cdot 0.87 = 11{,}97\,\text{В}$

Наруга на сповіщувачі розбиття скла:

$U_{6-2ПИТ} = 12 - 0{,}025 \cdot 2.03 = 11{,}89\,\text{В}$

Виходячи з подібного принципу було розраховано рівні сигналів, необхідні для коректної роботи системи в максимально навантаженому режимі, результати яких для представленої схеми приведені в табл. 4.2.

Таблиця 4.2

Рівні сигналів та навантаження на систему в макмимальному режимі роботи

№№ сповіщувача	Довжина кабеля, КСПВ 4х0,5 м	Опір сигнального кабеля КСПВ 4х0,5, Ом	Опір кабеля живлення КСПВ 4х0,5, Ом	Струм через сповіщувач, мА	Напруга в сповіщувачі, В
6-2	6	0,87	0,87	16	11,9722
6-3	14	2,03	2,03	25	11,8985
7-2	8	1,16	1,16	16	11,9629
7-3	16	2,32	2,32	25	11,884
8-2	10	1,45	1,45	16	11,9536
8-3	18	2,61	2,61	25	11,8695
9-2	12	1,74	1,74	16	11,9443
9-3	20	2,9	2,9	25	11,855
10-2	14	2,03	2,03	16	11,935
10-3	22	3,19	3,19	25	11,8405
11-2	18	2,61	2,61	16	11,9165
11-3	26	3,77	3,77	25	11,8115
12-2	16	2,32	2,32	16	11,9258
12-3	24	3,48	3,48	25	11,826
13-2	14	2,03	2,03	16	11,935
13-3	22	3,19	3,19	25	11,8405
14-2	13	1,885	1,885	16	11,9397
14-3	21	3,045	3,045	25	11,8478

В результаті було розраховано всі струми і визначено сумарний, який споживає система в режимі повної охорони та в режимі спрацювання. У першому режимі цей параметр становить 658 мА, в другому – 495 мА.

В подальшому необхідно розрахувати споживану потужність для системи в різних режимах. Вона розраховується як добуток струму на напругу живлення:

$$P_i = U_{ПИТ} \cdot I_{ПИТ} \tag{4.3}$$

Отже, для давача руху маємо:

$P_{6-2} = 11{,}97 \cdot 0{,}016 = 0{,}19$ Вт в охоронному режимі,

$P_{6-2} = 11{,}97 \cdot 0{,}016 = 0{,}19$ Вт в тривожному режимі.

Для давача розбивання скла в двох режимах відповідно маємо:

$P_{6-3} = 11{,}97 \cdot 0{,}025 = 0{,}297$ Вт

$P_{6-3} = 11{,}97 \cdot 0{,}015 = 0{,}179$ Вт

Втрати потужності у провідниках:

$$P_{iППО} = R_K \cdot I_{ПИТ}{}^2 \tag{4.4}$$

Відповідно маємо:

$P_{6-2ПОТ} = 0{,}87 \cdot 0{,}016^2 = 4{,}45$ мВт

$P_{6-2ПОТ} = 0{,}87 \cdot 0{,}016^2 = 4{,}45$ мВт

Сумарна потужність споживана системою 8,14 Вт. Відповідно необхідно забезпечити сумарну потужність від безперебійного блоку живлення10 Вт для давачів та додати споживання усіх встановлених сирен.

5. СПЕЦІАЛЬНА ЧАСТИНА

5.1. Налаштування доступу до системи відеонагляду через хмарний сервіс

У даному розділі опишемо підключення за допомогою персонального комп'ютера до відеореєстратора Hikvision через хмарний сервіс, для віддаленого перегляду відео через інтернет. Підключення та перегляд відео виконано за допомогою програмного забезпечення iVMS. Обладнання що використовується: комплект відеоспостереження на 4 камери Worldvision KIT-4x1080P-DOME підключений до хмари EZVIZ.

Клієнтська програма для відеоспостереження iVMS-4200 є універсальним програмним забезпеченням для роботи з пристроями Hikvision. При першому запуску найкраще відразу увімкнути російську мову.

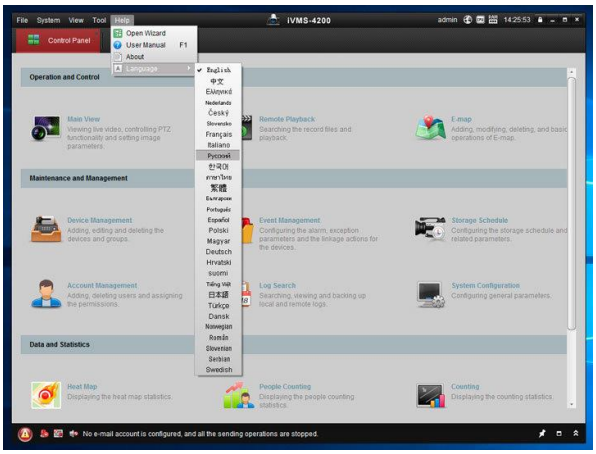


Рисунок 5.1 – Зміна мови системи

Програма попередить, що змінить мову тільки після перезапуску.

Перезавантажуємо програму. Відкривається «Панель управління».

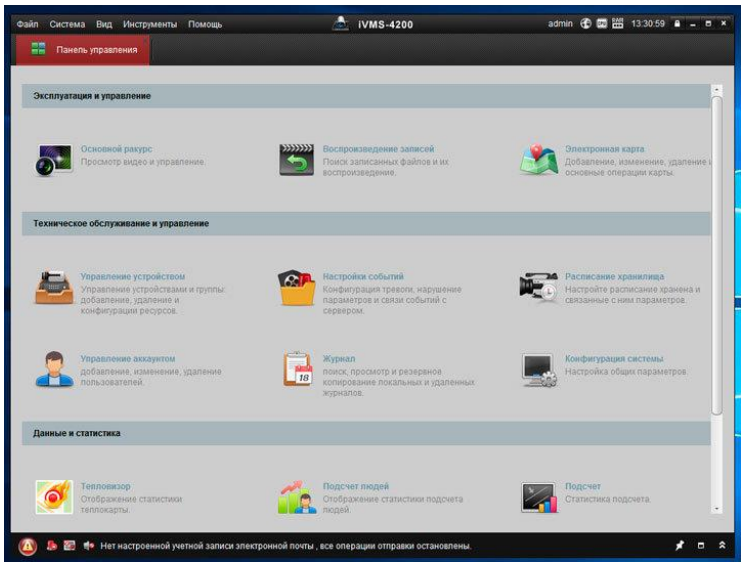


Рисунок 5.2 – Панель керування

Входимо в розділ Управління пристроєм.

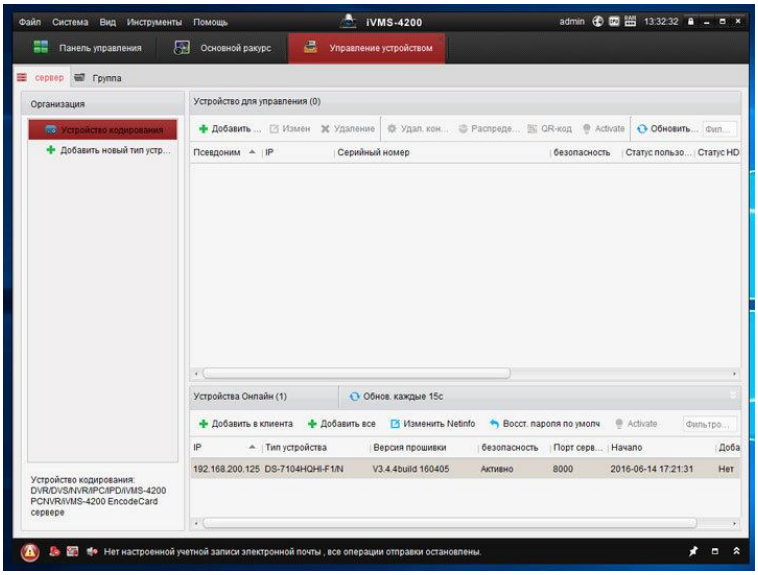


Рисунок 5.3 – Розділ «Управління пристроєм»

Для додавання пристрою за IP адресою натискаємо кнопку «Додати». Якщо відеореєстратор знаходиться в локальній мережі, програма знайде його автоматично і відобразить його характеристики в нижній частині вікна. В цьому випадку для підключення все одно потрібно додати в параметри підключення пароль. Натискаємо подвійним клацанням миші на рядку реєстратора.

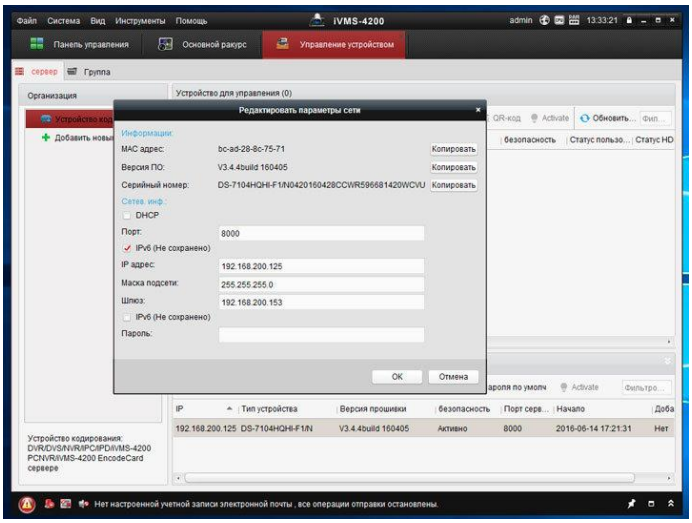


Рисунок 5.4 – Налаштування мережі

iVMS-4200 підключення до хмари.

Замість цього давайте підключимо реєстратор, заведений в хмару. Для цього вибираємо в поле Організація (в лівій частині вікна) Новий тип пристрою, відзначаємо у спливаючому вікні Пристрій в EZVIZ хмарі P2P, натискаємо «ОК».

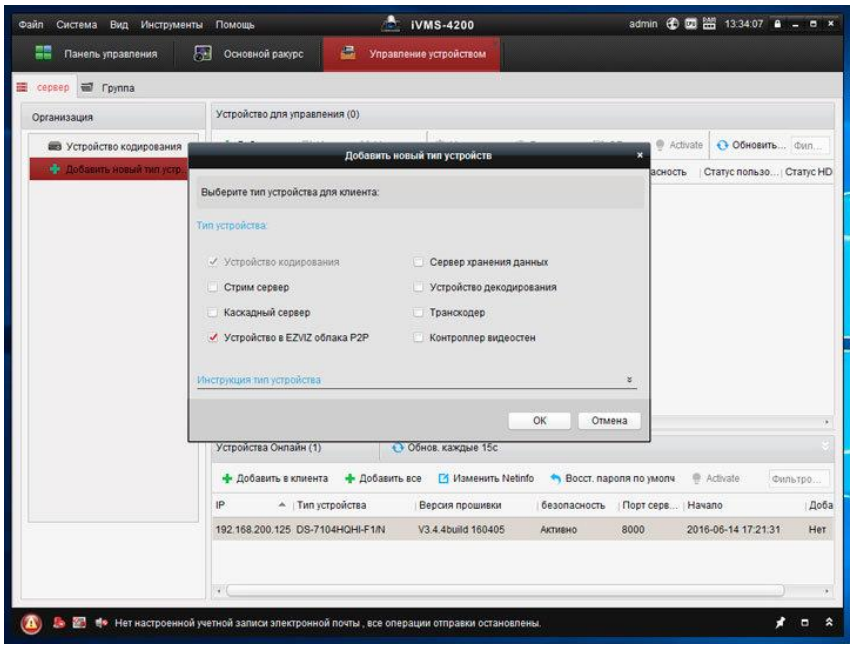


Рисунок 5.5 – Вікно додавання нового пристрою.

Потрапляємо у вікно хмарного облікового запису.

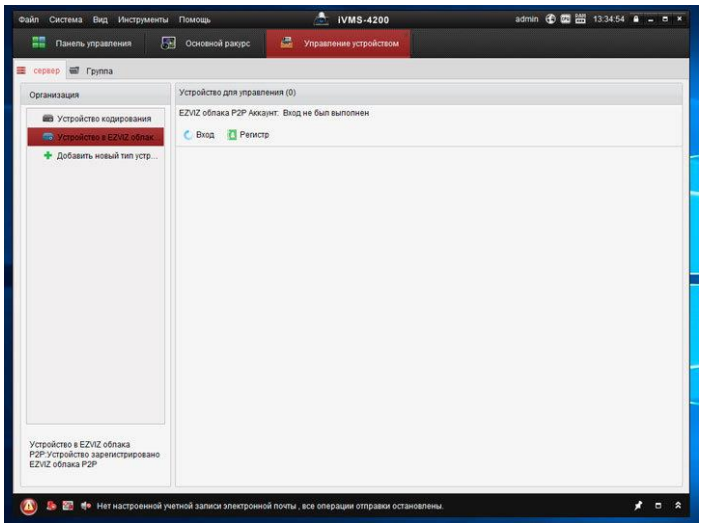


Рисунок 5.6 – Вікно керування пристроєм

Тут можна виконати реєстрацію нового хмарного облікового запису не заходячи на сайт сервісу (Реєстрація через iVMS-4200 відбувається аналогічно реєстрації через сайт або через мобільні додатки, див. Опис раніше).

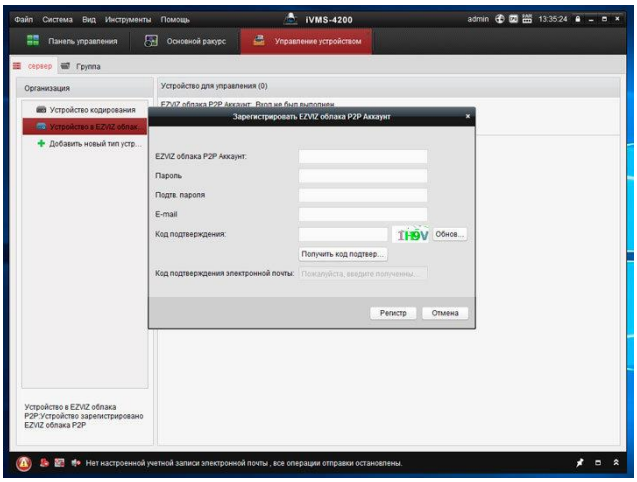


Рисунок 5.7 – Реєстрація P2P акаунту

Або під'єднатися до раніше створеного облікового запису.

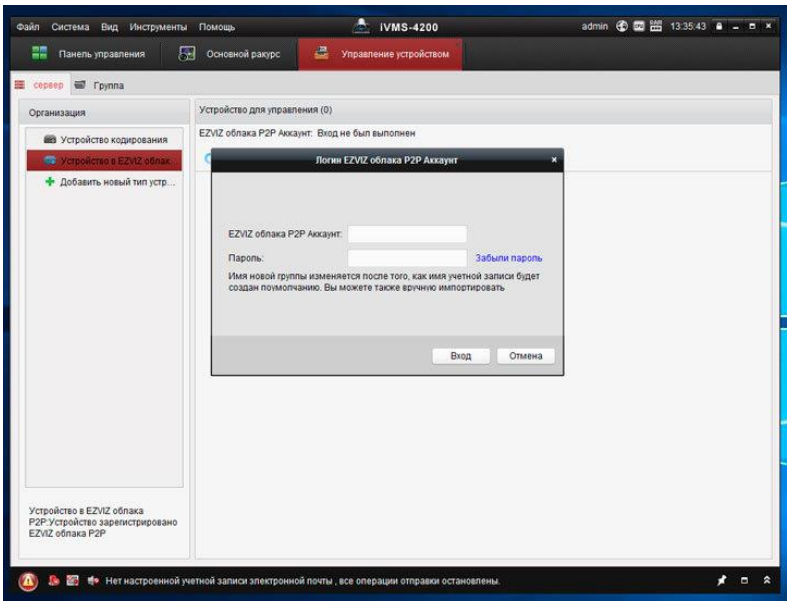


Рисунок 5.8 – Форма вводу паролю

Якщо обліковий запис новий, або в нього не заведений реєстратор, натискаємо «Додати пристрій». У цьому випадку програма запросить серійний номер реєстратора і код підтвердження, зазначені на нижньому боці корпусу.

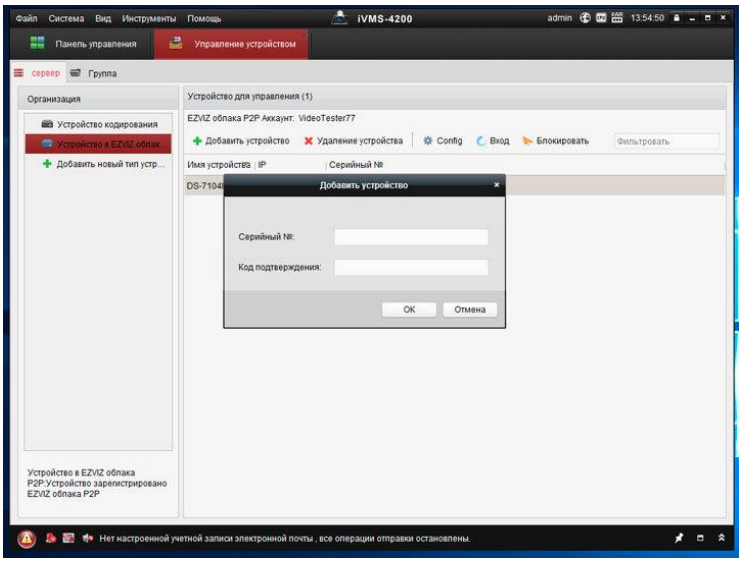


Рисунок 5.9 – Додавання пристрою

Якщо реєстратор доданий, його назва, IP адреса і серійний номер відображаються у вікні.

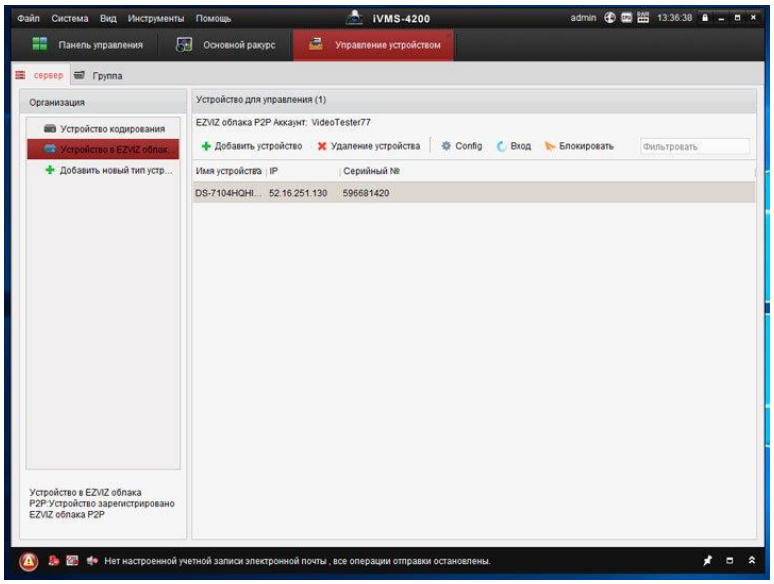


Рисунок 5.10 – Вікно керування пристроями

iVMS-4200 перегляд відео

Повертаємося до вкладки Панель управління і входимо в розділ Основний ракурс.

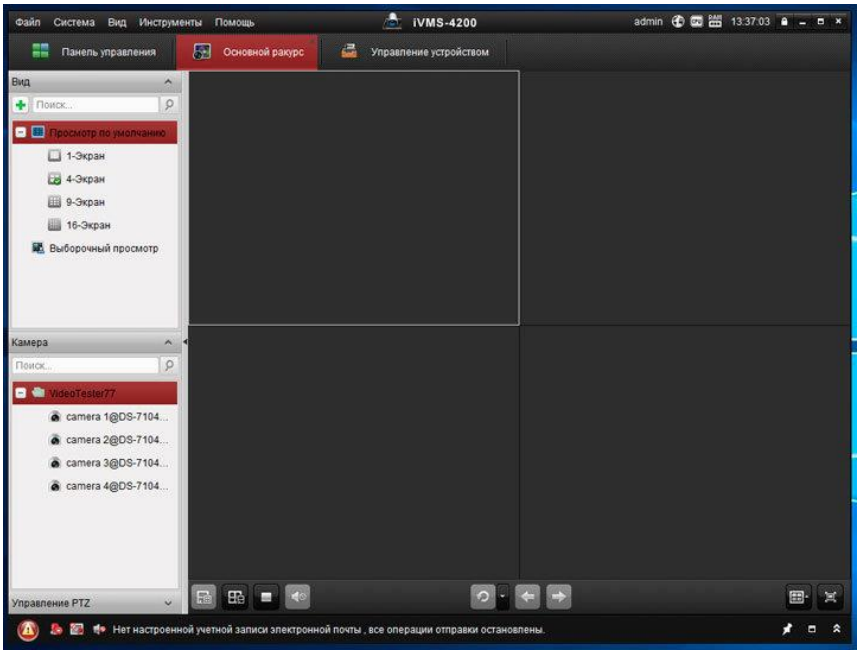


Рисунок 5.11 – Вкладка Основний ракурс

Внизу зліва відображено назву хмарного облікового запису і чотири канали підключеного до неї реєстратора. Мишкою перетягуємо камери в область перегляду.

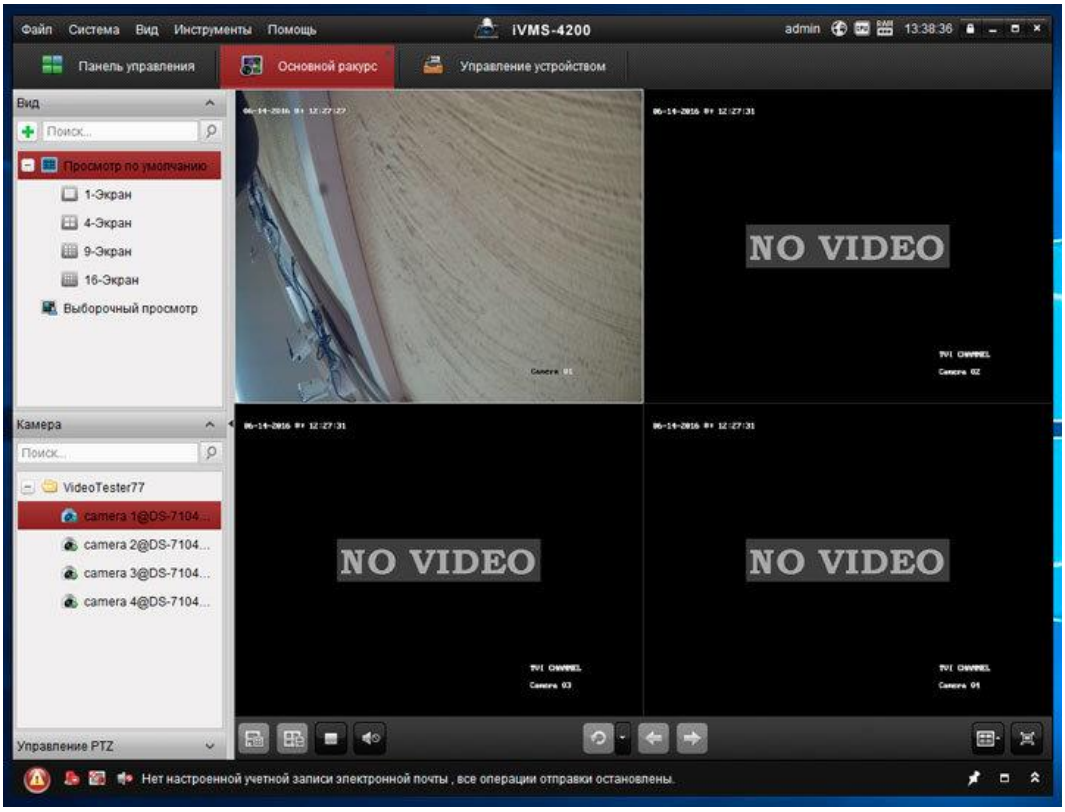


Рисунок 5.12 –Вікно перегляду пристрою через хмарний сервіс

Доступ до архіву здійснюється через Панель управління > Відтворення записів. Навігація по архіву доступна як щодо подій - поле Фільтрувати в правій частині вікна, так і по часовій шкалі - нижня частина вікна.

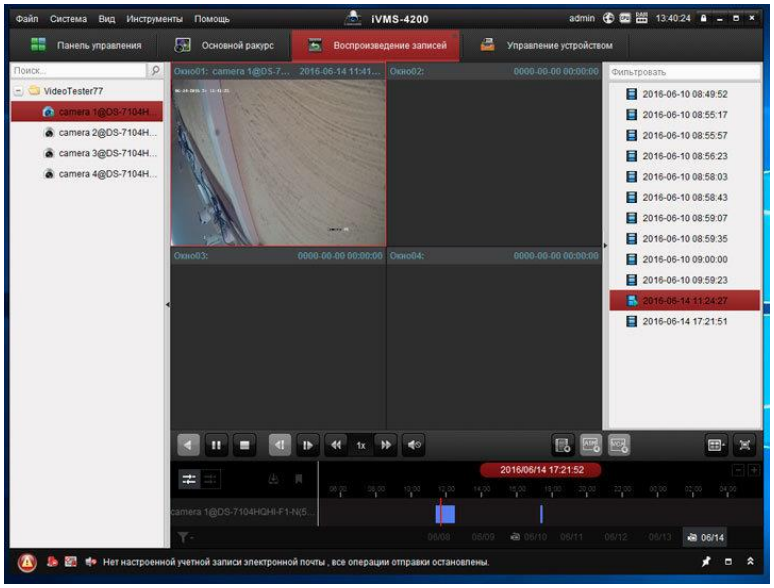


Рисунок 5.13 – Перегляд кількох пристроїв

5.2. Налаштування роутера для доступу до системи безпеки по зовнішній IP адресі

Mikrotik – це популярний бренд роутерів, який широко поширений в СНД і Європі. Завдяки своїй дешевизні і відмінним характеристикам, маршрутизатор нітрохи не поступається своїм китайським побратимам. Сам роутер функціональний як в технічному плані, так і в системному – присутні множинні налаштування і модулі.

Налаштування роутера Mikrotik заслуговує на окрему увагу, завдяки великій кількості дій для створення мережі, також і при експлуатації виникає чимало нюансів. Так як присутній великий спектр налаштувань, то має місце і деяка плутанина.

Настройка роутера починається з розбору функціоналу, вираженого в кількості вільних портів.

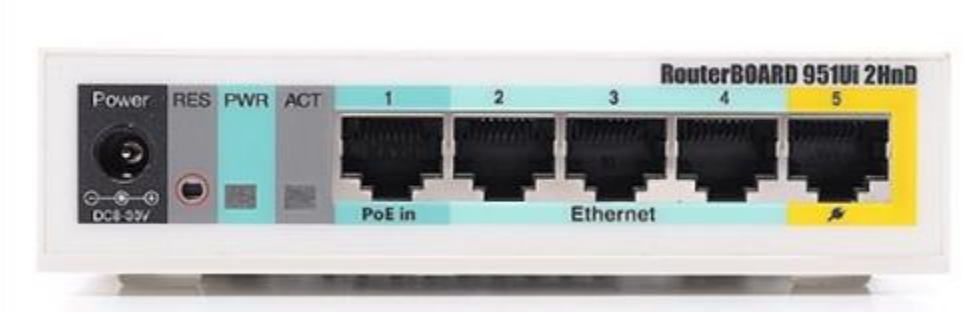


Рисунок 5.14 – вигляд задньої панелі роутера

Отже, ззаду роутера ви побачите кількість портів, кожен виконує свою задачу, а саме:

- перший «Power» – живлення, саме зарядний поставляється комплектом;
- втоплена кнопка скидання;
- перший з Ethernet портів краще використовувати для WLAN кабелю, але обмежень немає;

- ряд нехитрих LAN портів для експлуатації, в якості свіча і локальної мережі.

Налаштування Wi-Fi роутера має головним завданням бездротової вихід в мережу і на нього ми звернемо головний акцент. Маршрутизатор нестандартний, але гнучкий, тому раз приділивши час, ви зможете на довго забути про необхідність міняти параметри.

Сам пристрій відкриває 3 шляхи настройки:

Winbox – полегшена для розуміння утиліта, пристосована для Windows, є офіційною програмою від виробника;

Webfig – безпосередньо web сторінка. Скористатися інтерфейсом легко, введіть шлях 192.168.88.1 і натиснувши Enter ви зіткнетеся з нутрощами пристрою.

Звичайно ж Telnet.

Найбільш простий і звичний спосіб, як увійти в налаштування роутера і комфортно їх міняти – Winbox.

Тепер необхідно відкрити утиліту, перейти на вкладку Neighbors, і трохи почекати, щоб програма визначила наш роутер. Для синхронізації потрібно зайняти 3-и поля: спочатку вводиться MAC-адресу, потім логін і в кінці пароль. Виконуючи перше з’єднання ваша пара для входу матиме вигляд, де login – admin, a password – порожній рядок. Перший параметр MAC-адресу заповнюється динамічно при виборі роутера.

Нас вітає настройка роутера у вигляді вікна ознайомлення і перераховані основні конфігураційні параметри. Ви їх або застосовуєте, або скидає, залежить унікальності ситуації.

Об’єднання портів.

У більшості настройка домашнього роутера виключає подібну дію, адже воно передбачено за замовчуванням, але це не справедливо по відношенню до Mikrotik. Перевагою маршрутизатора є те, що тут немає жорстких рамок, тобто ви зможете підключити WLAN до будь-якого Ethernet

порту, також майстер-порт може бути встановлений будь-хто. Завдяки гнучкості вам надається більший спектр налаштувань. Щоб в подальшому працювати з усіма портами як LAN мережею і роздавати на них Wi-Fi вам необхідно зробити з них бридж, для цього:

Дотримуйтесь в розділ Interfaces;

Виберіть порт Ethernet 3 і подвійний клік по ньому;

Знаходимо, що розкривається з ім’ям «Master Port» і вкажіть його. Можна визначити будь-який, в нашому випадку 2;

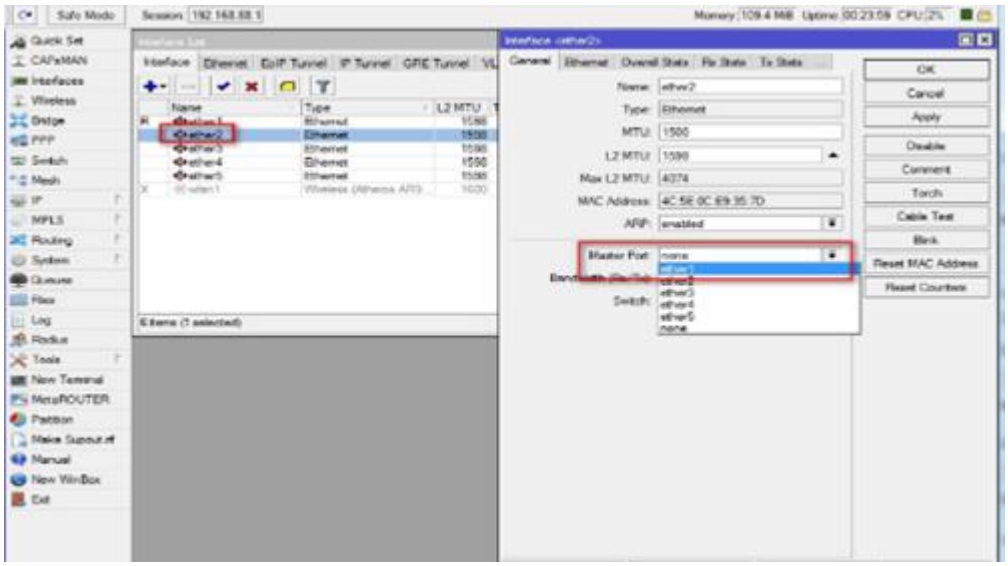


Рисунок 5.15 – Об’єднання портів в режим свіча

Здійсніть цю ж процедуру і для інших портів.

Тепер потрібно об’єднати міст з Wi-Fi інтерфейсом, тут вам необхідно виконати наступні дії:

- перейдіть в розділ «Bridge» і натисніть на плюс в меню;
- вкажіть ім’я та натисніть «Ок»;
- створиться новий елемент, тепер перейдіть у вкладку «ports»;
- рнову клік по додати і виберіть в розділі «Interface» наш майстер порт;

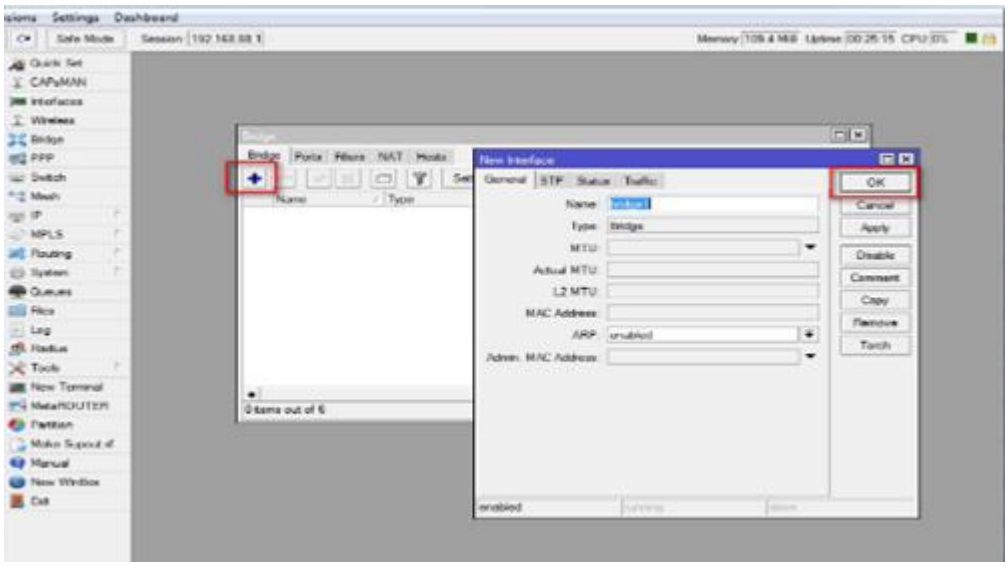


Рисунок 5.16 – Вкладка Bridge

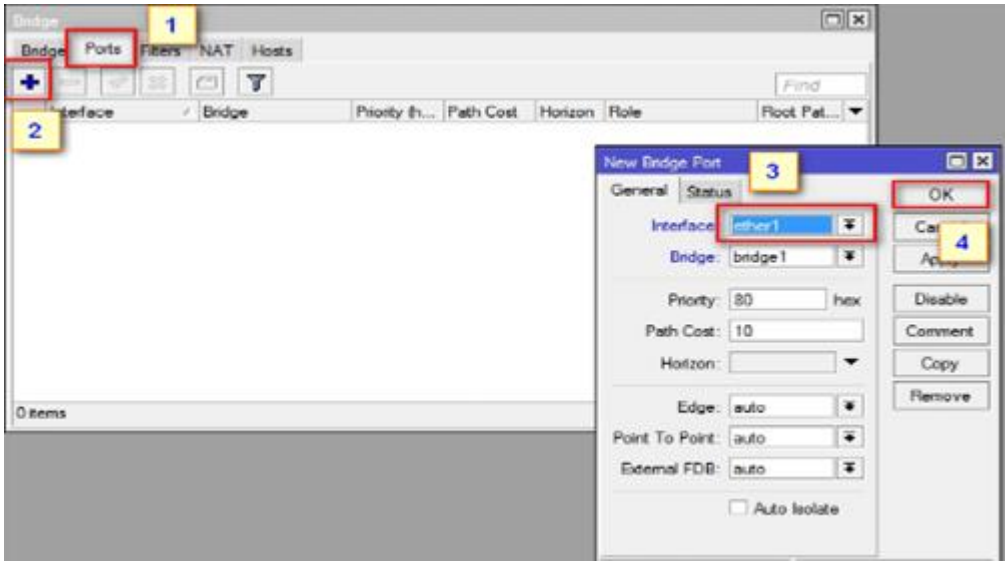


Рисунок 5.17 – Вікно додавання портів у брідж

Вас відключить від роутера і це нормально, знову увійдіть і перейдіть в цей же меню, тільки тепер додайте інтерфейс wlan, основне джерело трафіку.

Щоб налаштувати роутер підключення, важливо загострити увагу на типі придбання опцій підключення. Налаштування змінюються відповідно до специфічністю провайдера. Існують статичні мережі і динамічні (DHCP). Значно більш сучасною і актуальною стандарт DHCP використовується частіше, але існують серверні станції, де потрібні постійні IP. Виставте індивідуальні зміни в пристроях.

На ПК:

Перейдіть до робочої панелі «Центр управління мережами і загальним доступом», потрапити сюди можна просто натиснувши ПКМ на значок підключення в області повідомлень;

Продовжуйте слідувати в «Зміна параметрів адаптера»;

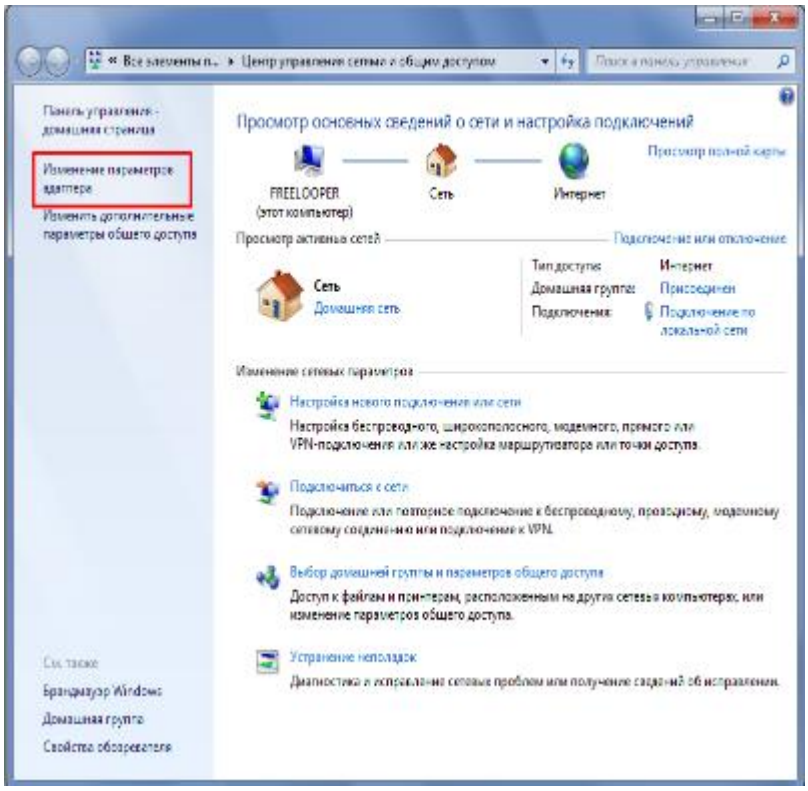


Рисунок 5.18 – Налаштування мережі на ПК

ПКМ по активного підключення і «Властивості»;

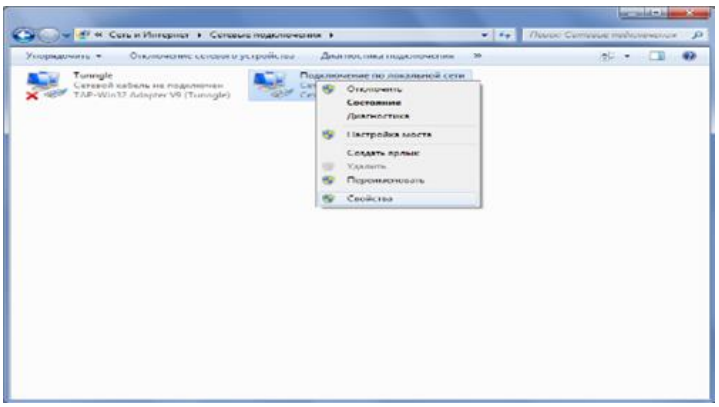


Рисунок 5.19 – Вибір мережевого адаптера на ПК

Клацніть двічі по протоколу TCP / IPv4;

Встановіть отримати IP / DNS автоматично або задайте значення вручну, отримавши у саппорт.

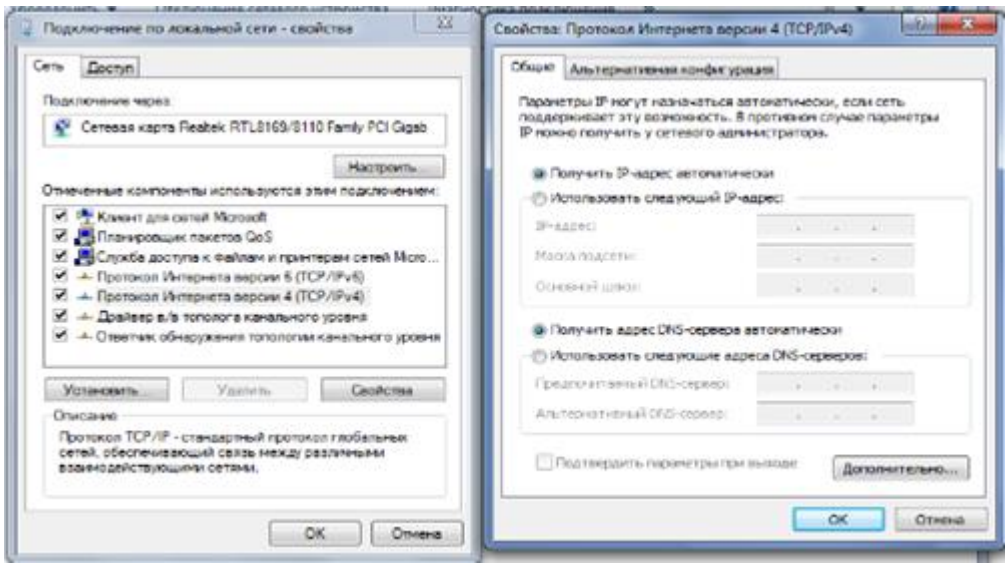


Рисунок 5.20 – Налаштування DHCP

Аналогічно і на роутері:

- в утиліті Winbox рухайтеся в каталог «IP»;
- перейдіть розділ «DHCP Server» і клікніть на Setup;
- у першому вікні вкажіть міст;

На наступних етапах можна натискати Next, якщо у вас немає особливого завдання налаштування мережі.

Встановлення точки доступу wlan.

Існує залишковий нюанс в питанні, як правильно налаштувати роутер, і ми станемо свідками активації виходу в мережу – ініціалізація точки доступу. Вам потрібно:

- перейдіть в розділ «Wireless»;
- виділіть наше WLAN підключення і натисніть на галочку;
- виберіть вкладку «Security profiles»;
- подвійний клік по Default і для рядка «Mode» задаємо значення «dynamic keys»;
- встановіть прапори біля WPA / 2 PSK;

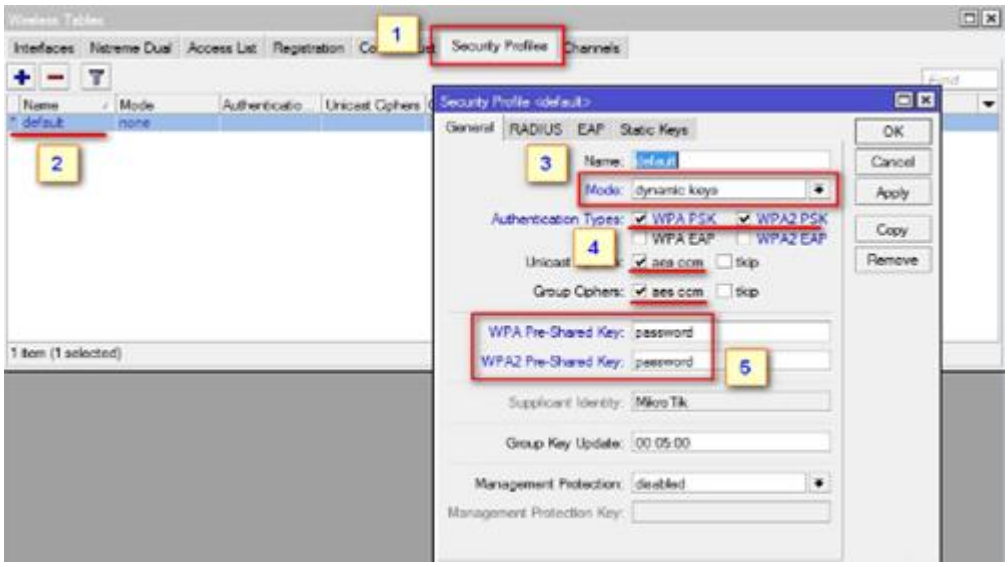


Рисунок 5.21 – Налаштування паролів для захисту вайфаю

- заповнюємо обидва поля з паролями для мережі;
- збережіть параметри.

Тепер залишилася остання маніпуляція з wlan підключенням, від вас вимагається використовувати подвійне натискання і відкрити його. Потім міняємо перший рядок «Mode» на «ap bridge», а другу «Band» на 2GHz-B / G / N. Встановити пароль можна, якщо перейти на вкладку «System» і вибрати «Users».

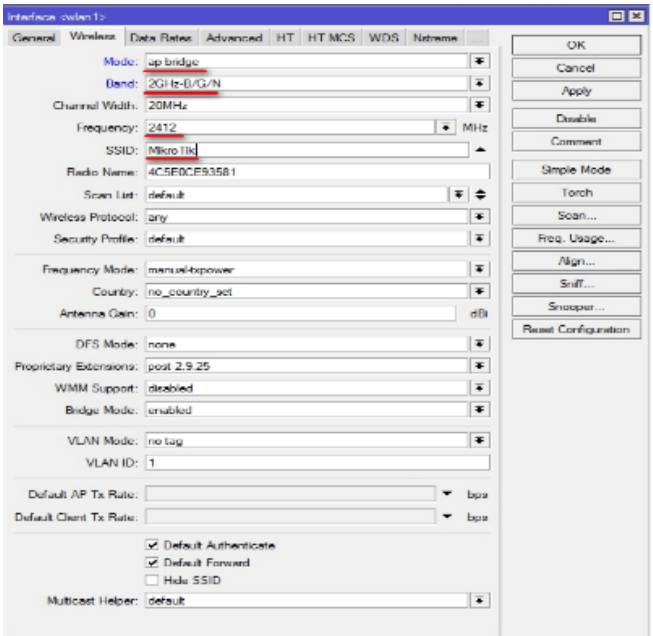


Рисунок 5.22 – Фінальні налаштування параметрів безпеки

5.3 Опис налаштування IVMS для мобільних пристроїв

Сьогодні у кожного з нас є можливість контролювати свою квартиру, офіс або будь-яке інше приміщення перебуваючи практично у будь-якій точці земної кулі. За допомогою камери Hikvision і безкоштовного мобільного додатку IVMS 4500, розробленого фахівцями Hikvision Digital Technology, ви завжди будете в курсі того, що відбувається на підконтрольній вам території. Головне, все правильно налаштувати й знати що до чого.

1. Додавання пристрою у додаток

Завантажуємо додаток IVMS-4500 з Play Market (для Android) або App Store (для iOS), запускаємо його і бачимо меню програми. Додаємо камеру або реєстратор у вкладці "Пристрої".

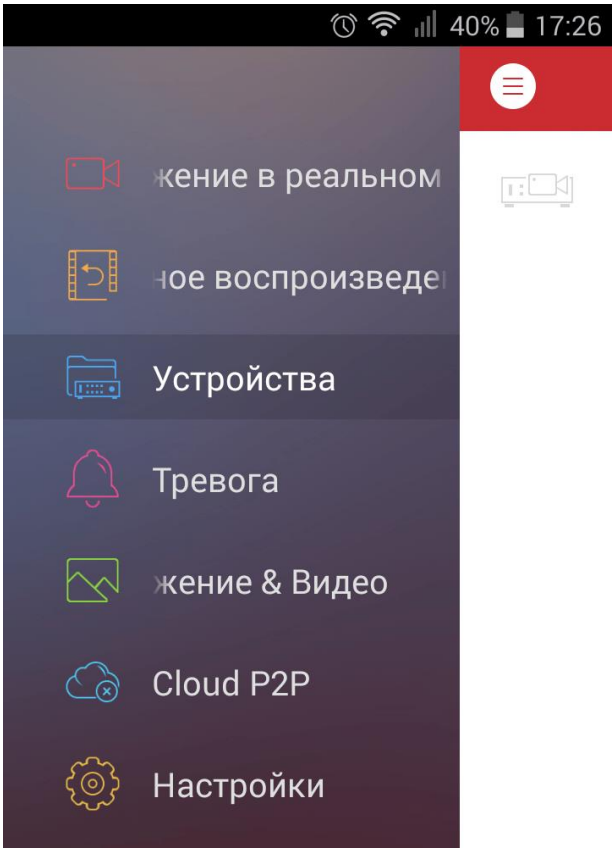


Рисунок 5.23 – Вибір типу під’єднання слідкуючих пристроїв

Для цього у вікні натискаємо на кнопку "+" і вибираємо ручне додавання.

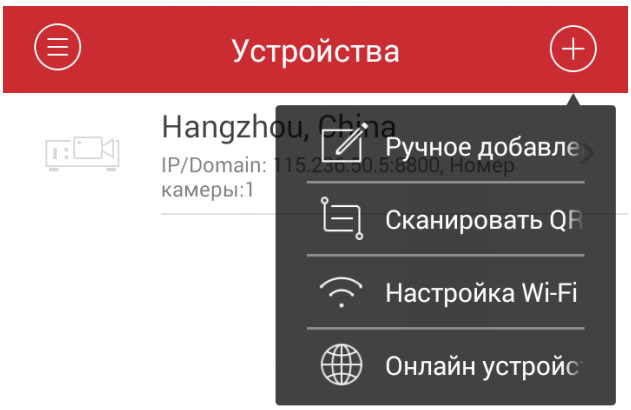


Рисунок 5.24 – Додавання пристрою

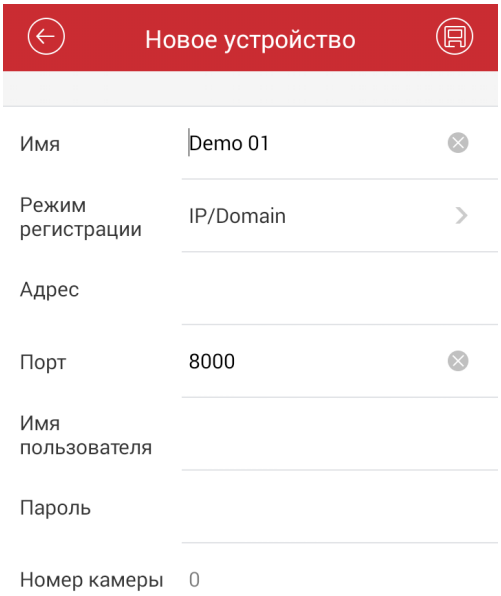


Рисунок 5.25 - Параметри додавання нового пристрою

У вікні нового пристрою вводимо:

бажане ім'я пристрою, наприклад, "Стоянка 1";

у полі "Адреса" - IP-адресу (статичну);

у полі "Порт" вводимо порт, який "прокинутий" на роутері (він же порт пристрою);

у полі "Ім'я користувача" - логін (стандартно - "admin");

у полі "Пароль" вводимо пароль, який ви задали камері чи реєстратору під час активації.

Якщо все було зроблено правильно, то під час натискання на кнопку "Почати показ у реальному часі"

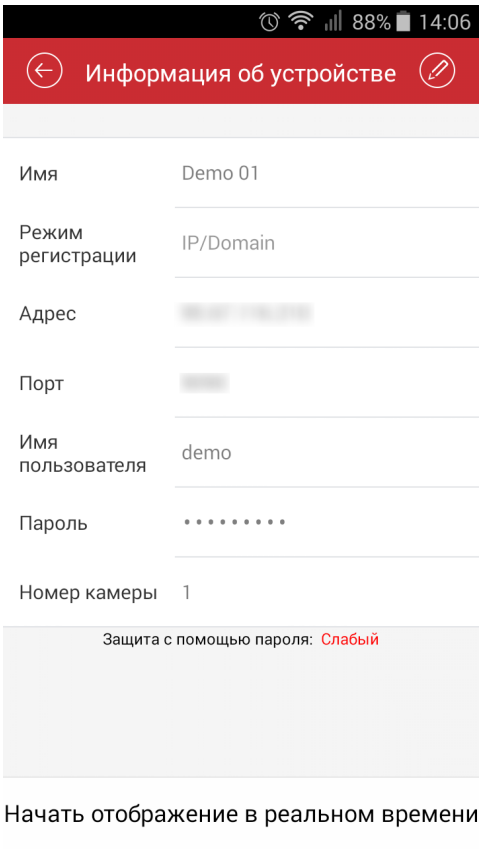


Рисунок 5.26 – Вікно вибору трансляції пристроїв

У вкладці, що відкрилася, ви побачите відео з камери.

2. Перегляд архіву та інші можливості

Окрім перегляду відео у реальному часі, додаток має ще кілька функцій, зручних для користувача, наприклад, перегляд архіву. Увійти до віддаленого відтворення можна через головне меню програми.

Для перегляду архіву через мобільний пристрій попередньо потрібно налаштувати камеру або реєстратор на запис в інтерфейсі самого пристрою, через ПЗ додатки IVMS 4200 або в інтерфейсі браузера на комп'ютері.

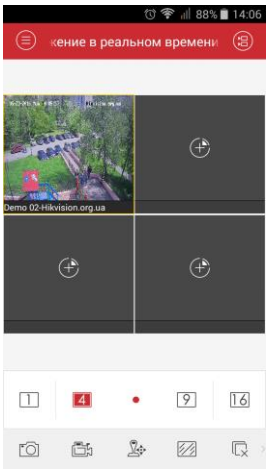


Рисунок 5.27 – Вікно перегляду відеокамер

Якщо ви вже зробили це, то у вкладці "Віддалене відтворення" під час вибору потрібної вам камери, зобразитися архів записів з цієї камери.

При подвійному натисканні на зображення воно розгорнеться у весь екран.

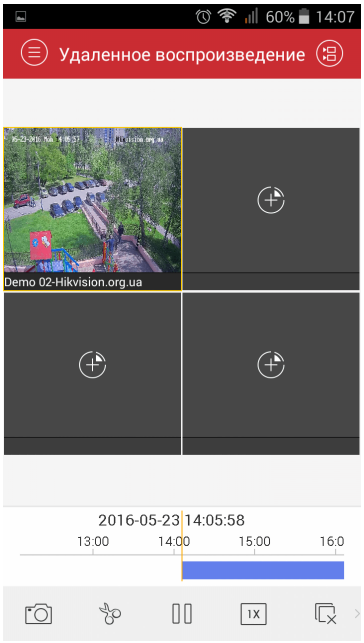


Рисунок 5.28 – Вікно віддаленого перегляду

За допомогою пересування доріжки відеозапису вправо або вліво ви зможете переглядати запис за певний відрізок часу.

3. Зображення та відео

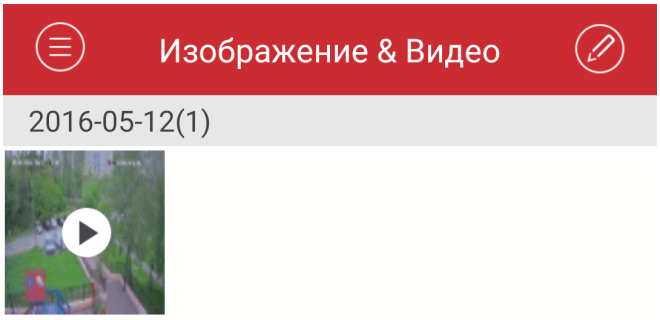


Рисунок 5.29 – Вікно перегляду зображень та відео

У цьому розділі будуть показуватися відео і фото, які ви можете зробити за допомогою кнопки запису в меню камери у розділі "Показ у реальному часі".

4. Cloud P2P (EZVIZ)

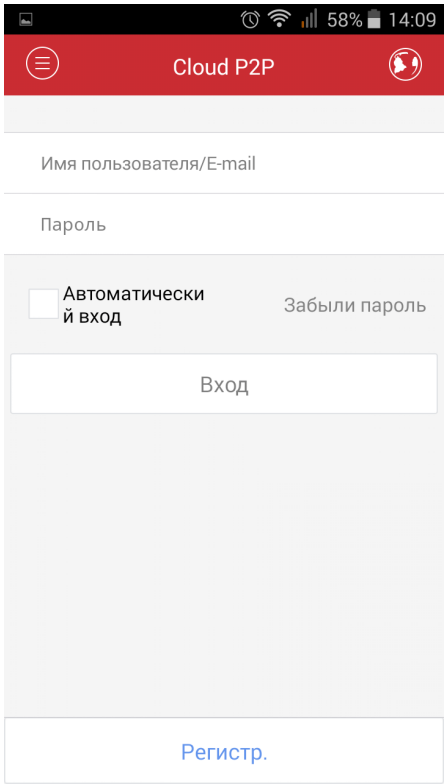


Рисунок 5.30 – Реєстрація для перегляду через хмару

Тут ви зможете переглядати камери через хмару EZVIZ у разі, якщо у вас немає статичної IP-адреси.

5. Налаштування

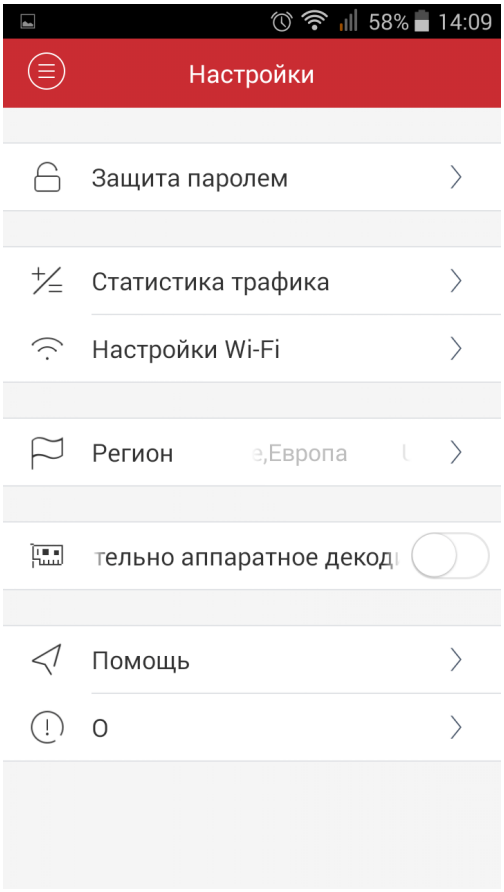


Рисунок 5.31 – Додаткові налаштування додатку

У цьому розділі знаходяться додаткові налаштування: захист паролем, статистика трафіку, налаштування Wi-Fi та інше. Натиснувши на кнопку "Допомога" можна переглянути інструкцію використання програми англійською мовою.

6. ОБГРУНТУВАННЯ-ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

6.1. Розрахунок норм часу на виконання науково-дослідної роботи

Реалізація проекту інформаційної системи управління доступом з використанням інформаційних технологій розпізнавання образів складається з низки послідовних та взаємопов’язаних етапів.

Норми часу на виконання науково-дослідницької роботи розраховуватимуться на основі середнього часу виконання стадії в годинах, що наведені в таблиці 5.1 разом із інформацією про виконавців і сумарною кількості затраченого часу.

Таблиця 6.1

Операції технологічного процесу та їх час виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	Підготовча стадія	Проектний менеджер Інженер-програміст	10
2	Технічна пропозиція	Проектний менеджер Інженер-програміст	10
3	Створення технічного завдання	Проектний менеджер Інженер-програміст	20
4	Проектування системи	Інженер-програміст	200
5	Практична реалізація	Інженер-програміст	200
6	Тестування системи	Тестувальник	20
7	Верифікація системи	Тестувальник Інженер-програміст Проектний менеджер	20
8	Створення документації	Інженер-програміст	50
9	Заключна стадія	Проектний менеджер	20
Разом			650

Кожен із етапів реалізації проекту характеризується метою та змістом, оцінкою часу виконання, кількістю та спеціалізацією виконавців, а також приблизною оцінкою вартості.

Реалізація інформаційної системи управління безпекою об’єкту складається із підготовчого етапу, етапу технічної пропозиції, створення технічного завдання, проектування системи, практичної реалізації, тестування, верифікації та заключного етапу.

В підсумку на реалізацію проекту інформаційної системи управління доступом з використанням інформаційних технологій розпізнавання образів необхідно 650 людино-годин, залучення трьох спеціалістів та виконання дев’яти різноманітних стадій реалізації проекту.

6.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Визначення витрат на оплату праці та відрахувань на соціальні заходи прямо залежить від кількості витраченого працівниками часу на роботу, ставки в годину чи місяць, кількість відрахувань на соціальні заходи встановлених в законному порядку на час розрахунку.

В результаті розрахунку потрібно визначити основну та додаткову заробітну плату, витрати на соціальні заходи та на основі цих даних визначити сумарні витрати на оплату праці.

Основна заробітна плата нараховується за виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично відпрацьований час.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Наймані працівники для розробки інформаційної системи управління доступом з використанням інформаційних технологій розпізнавання образів працюють згідно контракту, який в якому вказано їхню погодинну ставку. Тобто розрахунок заробітної плати працівників відбуватиметься на базі тарифної ставки та кількості відпрацьованих годин.

У штаті найманих працівників для розробки інформаційної системи залучено проектного менеджера, інженера-програміста і тестувальника.

Тарифні ставки учасників процесу розробки інформаційної системи:

Проектний менеджер – 150 грн./год.

- Інженер-програміст – 130 грн./год.
- Тестувальник – 100 грн./год.

Основна заробітна плата розраховується за формулою 5.1:

$$З_{осн.} = Т_с * К_г \text{ ,} \qquad (6.1)$$

де $Т_с$ – тарифна ставка, грн.; $К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт в виконує три спеціаліста, то основна заробітна плата буде розраховуватись за даною формулою 6.1;

$З_{осн.}$ = 150*80 + 130*530 + 100*40 = 84900 грн.

Додаткова заробітна плата становить 10–15 %% від суми основної заробітної плати й визначається за формулою 6.2.

Коефіцієнт додаткових виплат працівникам становить 0,1.

$$З_{дод.} = З_{осн.} * К_{допл.} \quad (6.2)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам

$З_{дод} = 84900*0,1 = 8490$ грн.

Звідси загальні витрати на оплату праці (фонд заробітної плати) визначаються за формулою 6.3:

$$В_{о.п.} = З_{осн.} + З_{дод.} \quad (6.3)$$

$В_{о.п.} = 84900 + 8490 = 93390$ грн.

З цієї суми утримуються обов'язкові відрахування на заробітну плату:

- Єдиний соціальний внесок (ЄСВ), що становить 22%%;
- Військовий збір (ВЗ), що становить 1,5%%;

Сума відрахувань становить 23,5%% від фонду оплати праці та визначається за формулою 5.4:

$$B_{с.з.} = Ф_{оп} * 0,235 \quad (6.4)$$

де $Ф_{оп}$ – фонд оплати праці, грн.

$B_{с.з.} = 93390*0,235 = 21946,25$ грн.

Усі витрати обчислюються детально наведені в таблиці 6.2 та обчислюються за формулою 6.5:

$$В_{зп} = ФЗП + ФОП \quad (6.5)$$

$В_{зп}$ = 93390 + 21946,25= 115336,65 грн.

Таблиця 5.2 – Розрахунки витрат на оплату праці

№з/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на плату праці, грн. (6=3+4+5)
		Тарифна ставка, грн.	Кількість відпрацьованих год.	Фактично нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1.	Проектний менеджер	150	80	12000	525	-	-
2.	Інженер-програміст	130	530	68900	2600	-	-
3.	Тестувальник	100	40	4000	300	-	-
Разом		380	650	84900	8490	21946,25	115336,25

Опираючись на розрахунки витрат на оплату та зведену таблицю результатів 6.2 видно, що всього витрати на плату праці становлять 115336,25 грн.

6.3 Розрахунок матеріальних витрат

Матеріальні витрати є невід’ємною частиною розробки інформаційної та визначаються як добуток кількості витрачених матеріалів та їх ціни за формулою 6.6:

$$M_{ві} = q_i \cdot p_i \,, \qquad (6.6)$$

де: q_i – кількість витраченого матеріалу і–го виду; p_i – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 6.7:

$$З_{м.в.} = \sum M_{ві} \,. \qquad (6.7)$$

Результати проведених розрахунків наведено у таблиці 6.3.

Таблиця 6.3 – Результати розрахунків матеріальних витрат.

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Фактично витрачено матеріалів	Ціна одиниці, грн.	Загальна сума витрат, грн.
1	CD диски	шт.	2	7,45	14,90
2	Папір для друку	листів	500	0,15	75,00
3	Чорнила для принтера	шт.	1	80,00	80,00
Всього					169,90

Згідно проведених розрахунків, матеріальні витрати становлять 169,90 грн.

6.4 Розрахунок витрат на електроенергію

Однією із статей витрат є витрати на електроенергію під час проходження усіх етапів реалізації кінцевого продукту.

Затрати на електроенергію одиниці обладнання визначаються за формулою 6.8:

$$З_в = W*T*S, \qquad (5.8)$$

де W – необхідна потужність, кВт; T – кількість годин на реалізацію розробки; S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів. Отже, 1 кВт з ПДВ коштує 2,42 грн.

Потужність комп'ютерів для реалізації кінцевого продукту – 400 Вт, кількість годин роботи обладнання згідно таблиці 6.1 – 650 годин.

Визначимо витрати на електроенергію згідно формули 6.11:

$З_в$ = 0,4 *650*2,42 = 629,20 грн.

Згідно формули затрати на електроенергію становлять 629,20 грн.

6.5 Розрахунок суми амортизаційних відрахувань

Для будь якої діяльності характерною є властивість зношування на зниження якості властивостей інструментарію та фондів за допомогою яких ведеться діяльність.

Для вирішення проблеми із відновленням даних фондів використовується амортизація, що являє собою процес трансформації вартості основних фондів на вартість продукції, яка щойно була створена, задля повного відновлення основних фондів.

Для визначення амортизаційних відрахувань використовується формула 6.9:

$$А = (Б_В * Н_А) / 100\% \qquad (5.9)$$

де, $Б_В$ – балансова вартість обладнання, грн;

$Н_А$ – норма амортизаційних відрахувань в рік, %%;

– річний робочий фонд часу, год;

– фактичний час роботи обладнання по написанню програми, год.

Комп’ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 %% (квартальна – 15 %%).

Річний робочий фонд становитиме 2352 годин, так як робочий день становить 8 годин, а кількість робочих днів в місяці становить 24,5 годин.

Для даної розробки засобом розробки є комп’ютер. Його сума становить 18500 грн. Отже, амортизаційні відрахування будуть рівні:

$A = 18500 \cdot 5\%\% / 100\%\% = 925$ грн.

Згідно проведених обчислень амортизаційні відрахування становлять 925 грн.

5.6 Обчислення накладних витрат

Накладні витрати пов’язані з обслуговуванням виробництва, утриманням апарату управління спілкою та створення необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб’єкта, накладні витрати можуть становити 20–60 %% від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п} * 0{,}2 \ldots 0{,}6 \,, \qquad (5.10)$$

де $H_в$ – накладні витрати.

Отже, накладні витрати становлять згідно формули 6.10:

$H_в = 93390 * 0{,}2 = 18678$ грн.

Накладні витрати згідно розрахунку формули, становить 18678 грн.

5.7 Складання кошторису витрат та визначення собівартості науково-дослідницької роботи

Результати проведених вище розрахунків наведено у таблиці 6.4.

Таблиця 5.4

Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В %% до загальної суми
Витрати на оплату праці	93390	0,69
Відрахування на соціальні заходи	21946,25	0,15
Матеріальні витрати	169,9	0,01
Витрати на електроенергію	256,52	0,01
Амортизаційні відрахування	925	0,01
Накладні витрати	18678	0,13
Собівартість	135365,7	100

Собівартість ($C_в$) програмного продукту розрахуємо за формулою:

$$C_в = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_в + A + H_в \, . \qquad (6.11)$$

Отже, собівартість розробки системи дорівнює:

Св = 135365,70 грн.

Загальний кошторис витрат та визначення собівартості науково-дослідницької роботи становить 135365,70 грн.

5.8 Розрахунок ціни розробки системи

Ціну науково-дослідної роботи можна визначити можна визначити за формулою:

$$Ц = (С_В * (1 + Р_{рен}) + К * В_{н.і.}) / К * (1+ПДВ) \quad (6.12)$$

де $Р_{рен.}$ – рівень рентабельності, 30 %%; $К$ – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних систем); $В_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту); *ПДВ* – ставка податку на додану вартість, (20 %%).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти К та Ві.н , оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = С_В * (1+Р_{рен}) * (1+ПДВ) \quad (6.13)$$

Звідси ціна на роботу складе:

$Ц$ = 135365,70 * (1 + 0,3) * (1 + 0,2) = 211170,49 грн.

Загальний розрахунок ціни програмного продукту становить 211170,49 грн.

5.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність ($E_р$) полягає у відношенні результату виробництва до затрачених ресурсів:

$$Е_р = П / С_В \quad (6.14)$$

де $П$ – прибуток; $С_в$ – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц – С_в . \quad (6.15)$$

Розраховуємо плановий прибуток:

$П_{пл}$ = 211170,49 – 135365,70 = 75804,79 грн.

Отже, формула для визначення економічної ефективності набуде вигляду:

$$Е_р = П / С_В \quad (6.16)$$

Тоді,

$E_р$ = 75804,79 / 135365,70 = 0,56.

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень ($T_р$):

$$T_P = 1/E_P \quad (6.17)$$

Термін окупності дорівнює:

T_p = 1 / 0,56 = 1,79 р.

Згідно формул плановий прибуток від розробки становить 75804,79 грн., економічна ефективність дорівнює 0,56, а термін окупності становить 1,79 року що вважається доцільним та економічно вигідним.

7 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

7.1 Організація охорони праці при роботі з системою управління

Охорона праці розглядає проблеми забезпечення здорових і безпечних умов праці. Виявляє і вивчає можливі причини нещасних випадків, професійних захворювань, аварій, вибухів, пожеж і розробляє систему заходів і вимог з метою виключення цих причин і створення безпечних і сприятливих для людини умов праці.

Завдання охорони праці є зведення до мінімуму імовірності пошкодження або захворювання працівників з одночасним забезпеченням комфорту при максимальній продуктивності праці.

Навчання працівників безпеці праці проводять відповідно до вимог ГОСТ 12. 0.004 - 79, який встановлює порядок і види навчання. На всіх підприємствах і в організаціях незалежно від характеру і ступеню небезпеки виробництва навчання працівників проводять при підготовці нових робітників, проведенні різноманітних видів інструктажів і підвищенні кваліфікації.

Контроль за своєчасним і якісним навчанням виконує відділ охорони праці чи інженер з охорони праці, або ІТП, на якого наказом керівника підприємства покладено ці обов'язки. Ті, що вперше поступають на роботу, навчання проходять згідно з "Типовим положенням про підготовку і підвищення кваліфікації робітників". В журналі обліку навчальної роботи реєструють навчальну тему, за якою проводилось навчання.

Інструктаж працюючих поділяють на вступний, початковий, на робочому місці, повторний, позаплановий і початковий.

Вступний інструктаж з усіма, хто поступає на роботу незалежно від їх освіти і стажу роботи по даній професії, проводить інженер з охорони праці за програмою, затвердженою головним інженером підприємства, про проведення вступного інструктажу з обов'язковим підписом того, хто проводив інструктаж і того, хто його отримував.

Початковий інструктаж на робочому місці, повторний, позаплановий і поточний проводить керівник робіт.

Початковий інструктаж на робочому місці проводять при прийомі на роботу нових робітників за інструкцією з охорони праці, розробленою для окремих професій або видів робіт. Всі робітники після цього інструктажу і перевірки знань 2-5 змін (залежно від навичок і стажу роботи) працюють під наглядом бригадира чи майстра, потім оформляється допуск до їх самостійної праці.

Повторний інструктаж проходять всі працівники незалежно від кваліфікації, освіти і стажу роботи через три місяці. Його проводять з метою перевірки знання робітниками правил і норм з охорони праці.

Позаплановий інструктаж проводять коли змінилися правила охорони праці або технологічний процес, обладнання, інструмент та інші фактори, що впливають на безпеку праці; коли працівники порушують правила охорони праці, що можуть призвести чи призвели до травм, аварій чи пожежі, вибуху. Його проводять індивідуально чи з групою робітників однієї професії за програмою початкового інструктажу на робочому місці. При його реєстрації вказують причину, яка спричинила його проведення.

Умови праці мають велике значення практично для всіх виробничих показників - продуктивності праці, якості робіт, безпеки працівників та інше.

Санітарно-гігієнічні умови праці характеризуються показниками виробничого середовища - рівнем освітлення, мікрокліматичними

параметрами, загазованістю і запиленістю повітряного середовища, рівнем шуму і вібрації, наявністю іонізуючого випромінювання та інше.

7.2 Електробезпека

Електричні установки, з якими доводиться мати справу практично всім працюючим по встановленню та налагодженню засобів автоматизації, виявляють для людини велику потенційну небезпеку, яка збільшується у зв'язку з тим, що органи чуття людини не можуть на відстані виявити присутність електричної напруги на обладнанні.

Степінь ураження електричним струмом залежить від цілого ряду факторів: значення сили струму, електричного опору тіла людини та тривалості протікання через неї струму, виду та частоти струму, індивідуальних властивостей людини та умов навколишнього середовища.

Конструкція електроустановок має відповідати умовам їх експлуатації та забезпечувати захист персоналу від дотику з струмоведучими та рухомими частинами, а обладнання - від попадання всередину посторонніх твердих тіл та води.

Конструкція, вид виконання, спосіб встановлення, клас ізоляції застосовуваних провідників, кабелів, пристроїв та іншого електрообладнання відповідають вимогам електробезпеки. За ступенем ураження людей електричним струмом котельня відноситься згідно ПУЕ 1.1.13 до категорії приміщень з підвищеною небезпекою (висока температура, можливість одночасного дотику до металевих елементів технологічного обладнання або металоконструкцій будинку та металевих корпусів електрообладнання).

У нормальному режимі роботи обладнання - можливість ураження працівників електричним струмом виключена. Але на випадок аварії для запобігання ураження струмом людей передбачене захисне заземлення.

Згідно ПУЕ 1.7.65 допустимий опір заземлення повинен бути не більшим 10 Ом.

При виконанні монтажних робіт використовуються переносні електроінструменти (електродрилі, електрошліфувальні установки, тощо). Для забезпечення безпечної праці корпуси однофазних електроприймачів повинні занулюватись.

Захист людини від ураження електричним струмом в мережах з зануленням здійснюється тим, що при замиканні одної з фаз на занулений корпус в ланці цієї фази виникає струм короткого замикання, що діє на струмовий захист (плавкий запобіжник, автомат), в результаті чого відбувається відключення аварійної ділянки від мережі. Крім того, ще до спрацювання захисту струм короткого викликає перерозподіл напруги в мережі, що приводить до зниження напруги корпусу відносно землі. Таким чином, занулення зменшує напругу дотику та обмежує час, на протязі якого людина, що доторкнулася до корпусу, може попасти під дію напруги.

Для того, щоб забезпечити швидке (на протязі декількох секунд) відключення аварійної ділянки, струм короткого замикання повинен бути достатньо великим. Відповідно до вимог ПУЕ струм короткого замикання повинен не менше ніж в три рази перевищувати номінальний струм плавкої вставки найближчого запобіжника або номінальний струм нерегульованого розчеплювача автоматичного вимикача. При використанні автоматичних вимикачів, що мають тільки електромагнітний розчіплювач (відсічку), струм короткого замикання повинен перевищувати значення струму встановлення миттєвого спрацювання в 1,25-1,4 рази в залежності від номінального струму.

В однофазних електроприймачів, що включені між фазним та нульовим робочим проводами, занулення корпусів слід виконувати з допомогою окремого (третього) провідника, який повинен з'єднувати корпус електроприймача з нульовим захисним проводом. В таких випадках

під'єднувати корпуси електроприймачів для забезпечення електробезпеки до нульового робочого проводу недопустимо, оскільки при його розриві (перегоранні запобіжника) всі під'єднані до нього корпуси виявляться під фазною напругою відносно землі.

В мережі з зануленням недопустимо використовувати заземлення окремих електроприймачів, не під'єднавши їх перед цим до нульового захисного провідника. В цьому випадку при замиканні фази на заземлений, але не приєднаний до нульового захисного провідника корпус створюється коло струму через заземлення цього корпусу та заземлення нейтралі джерела струму. Такий випадок небезпечний, оскільки засоби захисту не зможуть відключити такий електроприймач через мале значення струму і тому небезпечна напруга на всіх корпусах може зберігатися тривалий період, поки заземлений приймач не буде відключений вручну.

Важливо відмітити, що якщо занулений корпус одночасно заземлений, то це тільки покращує умови безпеки, оскільки забезпечує додаткове заземлення нульового захисного проводу.

Для ізоляції людини від частин електроустановок, що знаходяться під напругою, використовуються основні та допоміжні ізолюючі засоби, а саме слюсарно-монтажний інструмент з ізольованими ручками, коврики, ізолюючі підставки, тощо.

У приміщеннях, де знаходяться вимірювальні прилади, необхідно забезпечити виконання заходів по боротьбі з статичною електрикою (тобто прилади повинні бути заземлені). Найпростішим засобом є підтримка відносної вологості повітря на рівні 50 - 60 % за допомогою побутового електрозволожувача.

Підлогу слід виконувати відповідно до ГОСТ 12.4.124-83, використовуючи антистатичне покриття на проходах і біля робочих місць.

Робітникам рекомендовано носити одежу з природних матеріалів або з комбінованих - природних і штучних волокон. Для зняття електростатичних зарядів з одежі слід використовувати антистатики побутового призначення.

Оскільки корпуси приладів виконані з металу, то для усунення небезпеки ураження людини електричним струмом (можливий пробій на корпус приладу) використовується захисне заземлення.

7.3 Розрахунок заземлення

Розрахуємо систему заземлення для електроустаткування, яке працює від напруги 220 В.

$$R_{заз} \le \frac{U}{I_p} = \frac{220}{66} = 3.3 \le 4 Ом$$

Визначаємо опір грунту: $\rho = \kappa_н * \rho_н$ = 2*200 = 400 Ом м,

де $\kappa_н$ - коефіцієнт підсилення;

$\rho_н$ — питомий опір грунту (вибирається з довідкової літератури).

Визначаємо опір одиночного вертикального заземлювача:

$$R_B = \frac{\rho}{2\pi l}(\ln\frac{21}{d} + \frac{1}{2} * \frac{4t+1}{4t-1})$$

де t - відстань від середини заземлювача до поверхні грунту, м;

l,d - довжина і діаметр стержня заземлювача, м;

R_B = 96 Ом.

Визначаємо опір сталевої полоси, що з'єднує стержневі заземлювачі:

$$R_П = (\rho / 2\pi l) * \ln(l^2 / dt) = 61 \text{ Ом.}$$

Визначаємо орієнтовне чмсло стержневих заземлювачів:

$$n = R_B /[r_B]\eta_B = 96/4*1 = 24 \text{ шт;}$$

r_B - допустимий по нормам опір заземляючого пристрою,

$\eta_в$- коефіцієнт використання вертикальних заземлювачів (для орієнтовного розрахунку приймається рівним 1).

Приймаємо розміщення вертикальних заземлювачів по контуру з відстанню між стальними заземлювачами рівним 21. З довідкової літератури визначаємо $\eta_в$= 0,66 і $\eta_г$ = 0,39.

Визначаємо необхідну кількість вертикальних заземлювачів

$$n = R_в /[r_в]\eta_в = 96/(4*0.66) = 36$$

Розраховуємо загальний розрахунковий опір аземлюючого пристрою R з врахуванням з'єднувальної полоси

$$R = R_в R_п /(R_в \eta_г + R_п \eta_в n) = 3.9 \text{ Ом.}$$

Розрахунок проведено правильно, оскільки виконується умова $R \leq [r_в]$.

Розрахунок штучного заземлення:

Приймаємо, що опір захисного заземлення не повинен перевищувати 4 Ом:

$$R_{ЗЗ} = \frac{R_c R_п}{R_c + R_п} \leq 4 Ом$$

де $R_{ЗЗ}$ – опір захисного заземлення;

R_c – опір стержневих заземлювачів;

$R_п$ - опір поперечних заземлювачів.

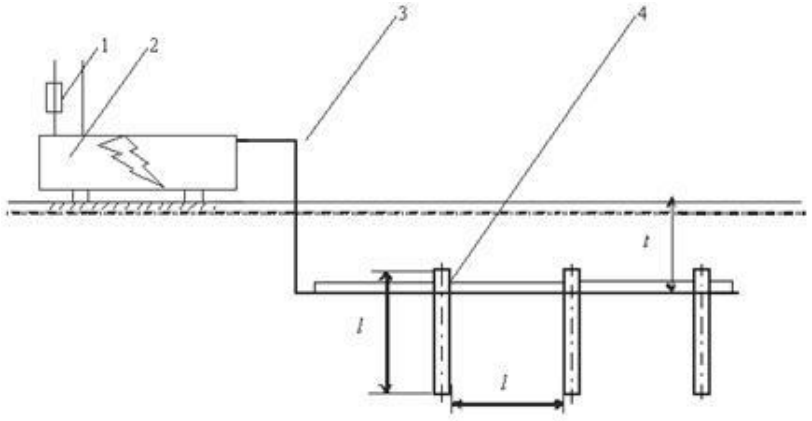


Рисунок 7.1 - Пристрій заземлення

4 – плавка вставка; 2 – електроустановка; 3 – з'єднувальна штаба; 4 – трубчатий заземлювач

Опір одиночного стержневого заземлювача розтіканню електричного струму:

$$R_{oc} = \frac{\rho_p}{2\pi l}(\ln\frac{2l}{d} + \ln\frac{4h'+l}{4h'-l})$$

де h – відстань від поверхні грунту до заземлювача і становить 0,8 м;

l – довжина стержневого заземлювача 3 м;

d – діаметр стержневого заземлювача 50 мм.

$$R_{oc} = \frac{750}{2\cdot 3.14\cdot 3}(\ln\frac{2\cdot 3}{0.05} + \ln\frac{4\cdot 0.8+3}{4\cdot 0.8-3}) = 39.8\cdot(0.18+3.43) = 143.8Ом$$

Опір одиночного поперечного заземлювача:

$$R_{on} = \frac{\rho_p}{2\pi l}\ln\frac{2l^2}{bh'}$$

де l – довжина поперечного заземлювача 2,5 м;

b – ширина полоси заземлювача 30 мм;

ρ_p - розрахунковий опір грунту: для поперечних електродів 1000 Ом·м, для стержневих електродів 750 Ом·м.

$$R_{on} = \frac{1000}{2\cdot 3{,}14\cdot 2{,}5}\ln\frac{2\cdot 2{,}5^2}{0{,}03\cdot 0{,}8} = 63.7\cdot 6{,}25 = 398.1Ом$$

В наслідок взаємовпливу вводимо коефіцієнт використання заземлювачів:

$$\eta = \frac{R_0}{nR_o}$$

де $R_д$ – допустимий опір заземлення, що становить 4 Ом;

R_o – опір одиночного заземлювача.

З цієї формули методом ітерацій підбирають n, при якому η =1:

n	**R_n**	**R_c**	**R_o**	**ŋ**
1	398,1	143,8	105,6	26,1
5	398,1	143,8	105,6	5,2
10	398,1	143,8	105,6	2,6
15	398,1	143,8	105,6	1,7
20	398,1	143,8	105,6	1,3
25	398,1	143,8	105,6	1,1
26	398,1	143,8	105,6	1,0
27	398,1	143,8	105,6	0,9

Отже приймаємо кількість одиночних заземлюючих електродів рівною 26.

8 ЕКОЛОГІЯ

8.1 Екологізація виробництва

Екологізація виробництва передбачає наявність взаємозв'язку і взаємозумовленості будь-яких дій з урахуванням екологічних вимог до розвитку НТП. У зв'язку з цимуправління господарством країни і його функціонування повинні здійснюватися на основі раціонального природокористування та застосування нової технології, прогресивної організації маловідходних і безвідходних виробництв.

Екологізація виробництва — це розширене відтворення природних ресурсів шляхом вдосконалення технології, організації матеріального виробництва, підвищення ефективності праці в екологічній сфері.

Шляхи впровадження екологізації

Екологізація народного господарства, підприємств промисловості та АПК припускає інтенсивний розвиток НТП і переклад його на еколого-економічні, економіко-організаційні та еколого-технічні відносини.

Перший напрямок екологізації народного господарства можна здійснювати повсюдно в широких масштабах на діючих основних фондах народного господарства за допомогою екологізації всієї виробничо-господарської діяльності, не перериваючи її. При цьому в основному вирішуються завдання, які не потребують докорінної перебудови основних фондів, але дозволяють досягти суттєвих результатів щодо зниження забруднення навколишнього середовища та ресурсозбереження.

Другий напрямок екологізації господарства здійснюється при відтворенні основних його фондів.

8.2 Зниження енергоємності та енергозбереження.

Енергозбереження стосується зменшення споживання енергії за рахунок використання меншої кількості енергетичних послуг. Енергозбереження відрізняється від енергоефективності, яке стосується використання меншої кількості енергії в тій самій послузі. Наприклад, менше користуватись авто – енергозбереження, а пересісти на авто з меншою витратою паливаенергоефективність. Але і енергозбереження, і енергоефективність є техніками зменшення використання енергії.

Оптимізація освітлення

- максимальне використання денного світла (збільшення кількості, площі та прозорості вікон);
- оптимальне розміщення джерел штучного світла (місцеве, направлене освітлення);
- використання освітлювальних приладів лише за необхідністю;
- підвищення світловіддачі наявних джерел світла (заміна люстр, відбивачів тощо);
- використання приладів управління освітленістю (датчики руху, акустичні датчики, датчики освітленості, таймери, дистанційне керування, дімери);
- запровадження автоматичної системи диспетчерського управління зовнішнім освітленням (АСДУ НО);
- установка інтелектуальних розподілених систем управління освітленням.

Електропривід

- оптимальний підбір потужності електродвигуна;
- використання частотно-регульованого приводу.

Заходи по зниженню втрат тепла та підвищенню ефективності систем теплопостачання:

джерело теплопостачання

- зменшення витрат енергії та тепла на власні потреби;
- використання сучасного обладнання з вищим ККД теплогенерації, напр. конденсаційні котли;
- використання вузлів обліку теплової енергії;
- використання ко- і три- генерації.

теплові мережі

- ізоляція мереж для зниження втрат тепла у довкілля;
- скорочення шляху теплоносія від виробника до споживача теплової енергії (напр., міні-котельня у будинку)
- оптимізація гідравлічних режимів тепломереж;
- зменшення протікань.

споживачі

- належна ізоляція опалюваних приміщень;
- використання систем місцевого регулювання опалювальних приладів;
- переведення будинків в режим нульового споживання тепла для опалення (температура всередині підтримується за рахунок внутрішнього тепловиділення та гарної ізоляції);
- використання вузлів обліку теплової енергії.

Економія води

- встановлення приладів обліку використання води;
- використання води лише коли дійсно необхідно;
- встановлення установка зливних бачків, які мають функцію вибору інтенсивності зливу;
- встановлення автоматичних регуляторів витрат води, аераторів, сенсорних датчиків

8.3 Джерела електромагнітних полів, іонізуючого випромінення та методи їх знешкодження.

Розрізняють природні та штучні джерела електромагнітних полів (ЕМП). У процесі еволюції біосфера постійно перебуває під впливом ЕМП природного походження (природний фон): електричне та магнітне поля Землі, космічні ЕМП, передусім ті, що генеруються Сонцем. У період науково-технічного прогресу людство створило і все ширше використовує штучні джерела ЕМП. У теперішній час ЕМП антропогенного походження значно перевищують природний фон і є тим несприятливим чинником, чий вплив на людину з року в рік зростає. Джерелами, що генерують ЕМП антропогенного походження, є телевізійні та радіотрансляційні станції, установки для радіолокації та радіонавігації, високовольтні лінії електропередач, промислові установки високочастотного нагрівання, пристрої, що забезпечують мобільний та сотовий телефонні зв'язки, антени, трансформатори і т. ін. По суті, джерелами ЕМП можуть бути будь-які елементи електричного кола, через які проходить високочастотний струм. Причому ЕМП змінюється з тою ж частотою, що й струм, який його створює.

Ще на стадії проектування повинне бути забезпечене таке взаємне розташування опромінюючих та опромінюваних об'єктів, якеб зводилоб до мінімуму інтенсивність опроміненя. Потрібно зменшити імовірність проникненя людей у зони з високою інтенсивністю ЕМП, скоротити час перебування під опроміненям. Потужність джерел випромінювання мусить бути мінімально потрібною.

Важливе значення мають інженерно-технічні методи захисту: колективний, локальний та індивідуальний. Колективний захист спирається на розрахунок поширення радіохвиль в умовах конкретного рельєфу місцевості. Економічно найдоцільніше використовувати природні екрани –

складки місцевості, лісонасадження, нежитлові будівлі. Встановивши антену нагорі, можна зменшити інтенсивність поля, яке опромінює населенний пункт, у багато разів.

При захисті від випромінювання екрана повинне враховуватись затухання хвилі при проходженні через екран (наприклад, через лісову смугу). Для екранування можна використовувати рослинність. Спеціальні екрани у вигляді відбивальних щитів дорогі і використовуються дуже рідко.

Закритими називаються будь-які джерела іонізуючого випромінювання, будова яких виключає проникнення радіоактивних речовин у навколишнє середовище при передбачених умовах їхньої експлуатації і зносу.

Основними принципами забезпечення радіаційної безпеки при роботі із закритими джерелами іонізуючого випромінювання є:

• зменшення потужності джерел до мінімальних значень ("захист кількістю");

• скорочення часу роботи з джерелом ("захист часом");

• збільшення відстані від джерел до людей ("захист відстанню");

• екранування джерел випромінювання матеріалами, що поглинають іонізуюче випромінювання ("захист екраном").

Відкритими називаються такі джерела іонізуючого випромінювання, при використанні яких можливе потрапляння радіоактивних речовин у навколишнє середовище.

ВИСНОВКИ

У процесі виконання роботи було обґрунтовано важливість впровадження системи інтегрованої комплексної безпеки адміністративної будівлі. Встановлення такої системи має багато факторі та елементів. На першому етапі було розроблено структуру системи, обрано обладнання для отримання даних (давачі), обладнання для збору даних (реєстратори, централі), та обладнання для реалізації віддаленого контролю. При цьому було вирішено наступні питання:

- В результаті проведеної роботи було розглянуто та проаналізовано основні принципи побудови комплексних систем безпеки адміністративної будівлі;
- Наведено приклад реалізації такої системи;
- Обґрунтовано визначальні параметри, які в найбільшій мірі впливають на складність та надійність системи безпеки;
- Досліджено параметри системи на її відповідність нормам;
- Приведено принципи, приклади реалізації та елементи можливої оптимізації та здешевлення такої системи та розширення її функціональних можливостей.

Запропонована система забезпечує реалізацію контролю безпеки будівлі з можливістю активного контролю за її станом та віддаленого керування.

ПЕРЕЛІК ПОСИЛАНЬ

1. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 1. [навчальний посібник] (Лист МОНУ №1/11-8052 від 28.05.12р.) - Львів, "Магнолія 2006", 2013. – 256 с.

2. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 2. [навчальний посібник] (Лист МОНУ №1/11-11650 від 16.07.12р.) - Львів, "Магнолія 2006", 2014. – 312 с.

3. Микитишин А.Г., Митник, П.Д. Стухляк. Комплексна безпека інформаційних мережевих систем: навчальний посібник – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 256 с.

4. Микитишин А.Г., Митник М.М., Стухляк П.Д. Телекомунікаційні системи та мережі : навчальний посібник для студентів спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017 – 384 с.

5. ДБН В.2.5-56-2014 Системи протипожежного захисту. Редактор А.О. Лучковська. – Київ: Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України, 2015. – 134 с.

6. Петров, С.В. Обеспечение безопасности организаций и производственных объектов: практическое пособие для руководителей и работников предприятий и организаций / С.В. Петров. – Москва : ЭНАС, 2007. – 221 с.

7. Гафнер, В.В. Опасности социального характера и защита от них : учебное пособие : / В.В. Гафнер, С.В. Петров, Л.И. Забара. – 2-е изд., стер. – Москва : Флинта, 2016. – 320 с.

8. Алешин Б.С., Бондаренко А.В., Волков В.Г., Драб Э.С., Цибулькин Л.М. Оптические приборы наблюдения, обработки и распознавания объектов

в сложных условиях / Москва: Государственный Научно Исследовательский Институт авиационных систем, 1999. — 140 с.

9. Волф У., Цисис Г. (ред.) Справочник по инфракрасной технике в 4-х томах. Том 1 - Физика ИК-излучения Пер. с англ., Москва, Мир, 1995, 606 с. - ISBN 5-03-002924-9.

10. Синилов В. Г. Системы охранной, пожарной и охранно-пожарной сигнализации : учебник для нач. проф. образования / В. Г. Синилов. — 5-е изд., перераб. и доп. — М. : Издательский центр «Академия», 2010. — 512 с.

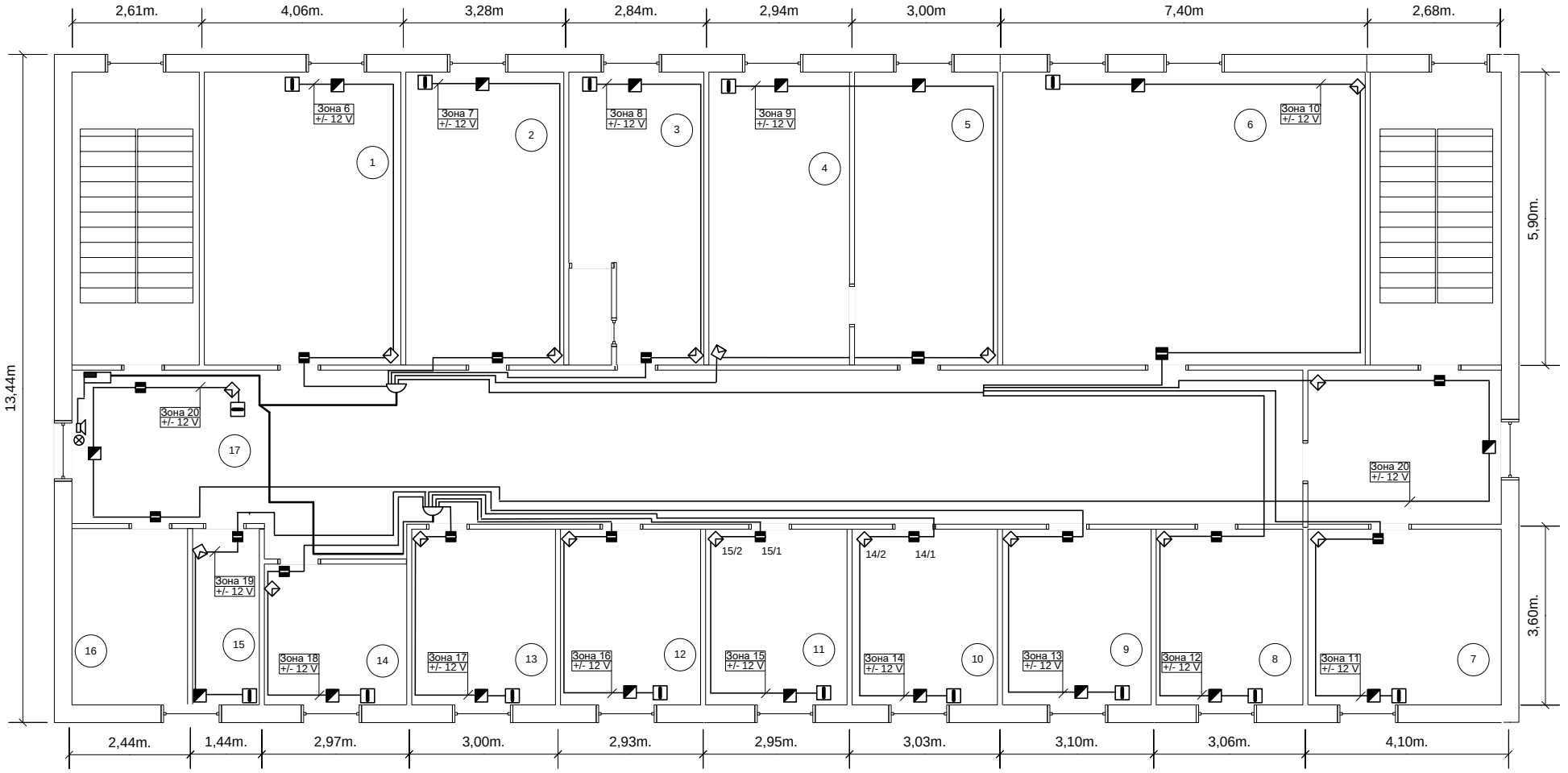
11. https://ajax.systems/ru/.

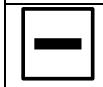
12. https://pp-tsilkovita-bezpeka.prom.ua/.

ДОДАТКИ

Додаток 1.

Схема розташування давачів сигналізації



	Коробка комутаційна КК-20
 □	Коробка комутаційна КК-2П
	Коробка комутаційна КК-2П з кінцевиком
	Давач розбивання скла
	Давач руху
	Герконовий блок
	Концентратор

Додаток 2

Результати вимірювань звукового сигналу в приміщеннях при аналізі системи оповіщення