Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування вищого навчального закладу)

Навчально-науковий інститут інформаційних технологій і робототехніки
(повне найменування інституту, назва факультету (відділення))

Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

бакалавр
(освітній рівень)

на тему **Проектування комплексної системи безпеки фінансової установи**

Виконав: студент 4 курсу, групи 401-ТТ
спеціальності 172 «Телекомунікація та радіотехніка»
(шифр і назва напряму підготовки, спеціальності

Андрійко В. Г.
(прізвище та ініціали)
Керівник Шефер О. В.
(прізвище та ініціали)
Рецензент Обіход Я. Я.
(прізвище та ініціали)

Полтава - 2021 рік

РЕФЕРАТ

кваліфікаційної роботи "Проектування комплексної системи безпеки фінансової установи"

Робота містить 74 сторінки, 25 ілюстрацій, 22 таблиці, 10 використаних джерел, 2 додатка.

Ключові слова: фінансова установа, система безпеки, схема, охоронна і пожежна сигналізація, відеоспостереження, контроль.

Об'єктом розробки кваліфікаційної роботи є процес забезпечення комплексної системи безпеки фінансової установи.

Предметом розробки кваліфікаційної роботи є система безпеки фінансової установи.

Метою кваліфікаційної роботи є розробка проекту системи комплексної безпеки для приміщень офісу фінансової установи.

У роботі передбачено розрахунок вартості та кількості всього необхідного обладнання для реалізації найякіснішого та найпростішого для розуміння проекту.

Робота має практичну цінність і її результати після більш детальної доробки можуть бути використані для забезпечення захисту будь-якої фінансової установи.

ANNOTATION

qualification work «Design of a comprehensive security system of a financial institution»

The work contains 74 pages, 25 illustrations, 22 tables, 10 sources used, 2 applications.

Keywords: financial institution, security system, scheme, fire alarm, video surveillance, control.

The object of development of qualification work is the process of ensuring a comprehensive security system of a financial institution.

The subject of development of qualification work is the security system of the financial institution.

The purpose of the qualification work is to develop a project of a comprehensive security system for the office of a financial institution.

The paper provides for the calculation of the cost and quantity of all necessary equipment for the implementation of the highest quality and easiest to understand the project.

The work has practical value, and its results after more detailed revision can be used to ensure the protection of any financial institution.

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інститут Навчально-науковий інститут інформаційних технологій і робототехніки
Кафедра Автоматики, електроніки та телекомунікацій
Ступінь вищої освіти Бакалавр
Спеціальність 172 «Телекомунікації та радіотехніка»

ЗАТВЕРДЖУЮ
Завідувач кафедри автоматики, електроніки та телекомунікацій
_____О.В. Шефер
" 11 " травня 2021 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРУ СТУДЕНТУ
Андрійку Владиславу Григоровичу

1. Тема роботи: *«Проектування комплексної системи безпеки фінансової установи»***.**
Керівник роботи Шефер Олександр Віталійович, д.т.н., доцент
Затверджена наказом вищого навчального закладу від 03.03.2021 року № 158 – фа.
2. Строк подання студентом проекту (роботи) 15.06.2021 р.
3. Вихідні дані до проекту (роботи): Площа, чутливість датчиків, резервне живлення, інерційність.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Аналіз потенційних загроз та безпеки фінансової установи. Методи забезпечення комплексної безпеки. Проектування комплексної системи безпеки фінансової установи.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів):
   1) схема системи контролю та управління доступом;
   2) схема розміщення камер;
   3) схема периметру території, що захищається;
   4) схема пожежної сигналізації;
   5) схема охоронної сигналізації.
6. Дата видачі завдання 11.05.2021 р.

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів кваліфікаційної роботи бакалавра	Термін виконання етапів роботи			Примітка (плакати)
1	Аналіз потенційних загроз та безпеки фінансової установи	18.05.21		25%	
2	Методи забезпечення комплексної безпеки	25.05.21	I	50%	
3	Проектування комплексної системи безпеки фінансової установи	05.06.21		80%	
4	Оформлення кваліфікаційної роботи бакалавра	15.06.21	II	100%	

Студент _____ Андрійко В.Г.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Шефер О.В.
(підпис) (прізвище та ініціали)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 7
ВСТУП 8
1. АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ТА БЕЗПЕКИ ФІНАНСОВОЇ УСТАНОВИ 11
1.1. Класифікація можливих загроз фінансової установи 11
1.2. Висновки до розділу та постановка задач проектування 14
2. МЕТОДИ ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСНОЇ БЕЗПЕКИ 15
2.1. Структура і склад технічного забезпечення систем безпеки 15
2.2. Технічні засоби відеоспостереження 16
2.3. Системи контролю доступу в приміщеннях 19
2.4. Засоби контролю стану об'єкту, що охороняється 20
2.5. Взаємодія приймально-контрольних приладів з комп'ютером і зовнішніми пристроями 22
2.6. Інтегровані охоронні системи 25
2.7. Класифікація принципів побудови комплексних охоронних систем 27
2.8. Висновки до розділу 29
3. ПРОЕКТУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ БЕЗПЕКИ ФІНАНСОВОЇ УСТАНОВИ 30
3.1. Розробка підсистеми контролю та управління доступом 30
3.2. Розробка підсистеми відеоспостереження 39
3.3. Система охоронно-пожежної сигналізації 47
3.4. Висновки до розділу 63
ВИСНОВКИ 64
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 65
ДОДАТОК А 66
ДОДАТОК Б 70

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

СКД – система контролю доступу;

ПЗ – програмне забезпечення;

СКБ – система комплексної безпеки;

ТК – технічні кошти;

ТЗЗІ – технічні засоби захисту інформації;

МУ – муніципальне утворення;

ПКП – приймально-контрольний прилад;

СОС – система охоронної сигналізації;

БЖД – безпека життєдіяльності;

ДРП – джерело резервного живлення;

АКБ – акумуляторна батарея;

ТВЛ – телевізійні лінії;

ПК – персональний комп’ютер;

АС – автоматизована система;

НСД – несанкціонований доступ;

КД – керівні документи;

ЗК – загальні критерії;

ЗОТ – засоби обчислювальної техніки;

ІТ – інформаційні технології;

ІОС – інтегрована охоронна система;

СКУД – система контролю та управління доступом;

АРМ – автономне робоче місце;

ІСБ – інтегрована система безпеки;

ЛОМ – локальна обчислювальна мережа.

ВСТУП

Метою кваліфікаційної роботи є розробка проекту системи комплексної безпеки (СКБ) для приміщень офісу фінансової установи.

Приміщення, за своєю специфікою, є часто відвідуваними об'єктами і потребують правильного розмежування доступу в приміщення, в засобах, що забезпечують безпеку життєдіяльності (БЖД), а так само в засобах захисту інформації від несанкціонованого доступу. В дане приміщення впроваджуються додаткові охоронні системи, що містять в собі системи контролю доступу (СКД).

Система комплексної безпеки, в загальному понятті, являє собою автоматизовану систему (АС) взаємопов'язаних комплексів програмно-апаратних та технічних засобів (ТЗ) безпеки, метою яких є своєчасне виявлення, інформування, запобігання вторгнення і ліквідацію загроз, пов'язаних з небезпекою для людини, майна і інформації. В технічно обґрунтованих випадках інтегровані системи безпеки (ІСБ) повинні допускати можливість їх використання в складі *системи комплексної безпеки* в якості базової технічної підсистеми. Так як, за технічним завданням, система комплексної безпеки складається з інтегрованої системи охорони, то в проекті буде зроблено великий акцент саме на розробку інтегрованої системи охорони.

Різноманітність технічних засобів охорони на сучасному ринку і різноманіття рішень по їх застосування підштовхує сучасність до уніфікації. Виробники відзначають, що технічні засоби безпеки повинні використовуватися спільно, оскільки саме такий підхід дає максимальний ефект. Виходячи з цього, доцільним рішенням при побудові комплексної системи безпеки є створення інтегрованої охоронної системи.

Інтегрована охоронна система являє собою комплексну багатофункціональну систему безпеки, що поєднує в собі функції всіх традиційних автономних систем. Система передбачає об'єднання на базі сучасних інформаційних технологій і програмно апаратної інтеграції

декількох підсистем, функціонально та інформаційно пов'язаних один з одним, а так само їх роботу за єдиним алгоритмом.

Можливі два шляхи вирішення проблеми інтеграції компонентів охоронної системи:

- апаратний;
- програмний.

Апаратна інтеграція часто утруднена в зв'язку з використанням виробниками різноманітних інтерфейсів і стандартів, що обмежує гнучкість систем з апаратної інтеграцією.

Програмний метод інтеграції позбавлений цієї особливості. Інтеграція на рівні драйверів тим більш зручна, що на сьогоднішній день більшість виробників технічних засобів охорони забезпечують свої продукти програмними модулями, що дозволяють організовувати взаємодію з комп'ютерами.

В даний час найбільш перспективним середовищем інтегрування (ТК) охорони є локальна мережа, що охороняється. Основними перевагами використання даної технології в якості бази для інтеграції технічних засобів є її повсюдна поширеність і наявність різноманітних засобів забезпечення інформаційної безпеки.

Актуальність теми проекту підтверджується гострою необхідністю в захисті від впливу загроз на різні сфери життя і діяльності людини в приміщенні, яке займає фінансова установа.

У сучасному світі захист людини, майна, інформації займає одне з перших місць серед потреб людини і суспільства в цілому. Поява і створення нових загроз, розвиток вже існуючих, змушують людей впроваджувати і розробляти нові охоронні системи. Поява різних технічних засобів охорони дає можливість забезпечити цілісність, доступність і конфіденційність інформації, послабити або усунути вплив загроз на людину і його майно в будь-яких сферах життєдіяльності.

Зараз, установа будь-якої організаційно-правової форми, не обходиться без заходів, спрямованих на впровадження, розвиток і підтримку систем безпеки в своїх організаціях. Завдання дипломного проекту повністю обумовлені його метою.

Для досягнення результатів необхідно:

- визначити клас захищеності об'єкта;
- провести огляд сучасних СКБ;
- розглянути принципи побудови охоронних систем;
- розробити структуру охоронної системи;
- програмного забезпечення для її організації;
- побудувати імітаційну модель запропонованої структури;
- розробити програмне забезпечення для створення інтегрованої охоронної системи.

1. АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ТА БЕЗПЕКИ ФІНАНСОВОЇ УСТАНОВИ

1.1. Класифікація можливих загроз фінансової установи

Побудована АС повинна забезпечувати захист від усіх видів загроз, інакше утворюється «дірка» в захисті, тому необхідно перерахувати всі можливі загрози, щоб максимально було вирішено питання щодо захисту. Єдиної і загальноприйнятої класифікації загроз безпеки АС поки не існує. Однак можна класифікувати ці загрози з різних аспектів їх реалізації, способу їх здійснення і об'єкту атаки [1].

Класифікація загроз по цілі:

- несанкціоноване читання інформації, несанкціоновані зміни інформації, несанкціоноване знищення інформації;
- повне або часткове руйнування операційної системи (під руйнуванням операційної системи розуміється цілий комплекс руйнівних впливів від короткочасного виведення з ладу ("завішування") окремих програмних модулів системи до фізичного стирання з диска системних файлів).

Класифікація загроз за принципом:

- використання відомих (легальних) каналів отримання інформації, наприклад, загроза несанкціонованого читання файлу, доступ користувачів до якого визначено некоректно;
- дозволений доступ користувачеві, якому відповідно до адекватної політики безпеки доступ повинен бути заборонений;
- використання прихованих каналів отримання інформації, наприклад: загроза використання зловмисником недокументованих всіх можливостей операційної системи;
- створення нових каналів отримання інформації за допомогою програмних закладок.

Класифікація загроз за характером впливу:

- активний вплив;
- несанкціоновані дії зловмисника в системі;
- пасивний вплив;
- несанкціоноване спостереження зловмисника за процесами, що відбуваються в системі.

Класифікація загроз на кшталт використовуваної зловмисником слабкості захисту [1]:

- неадекватна політика безпеки, в тому числі і помилки адміністратора системи;
- помилки і недокументовані можливості програмного забезпечення операційної системи, в тому числі і так звані люки;
- випадково або навмисно вбудовані в систему "службові входи", що дозволяють обходити систему захисту. Зазвичай люки створюються розробниками програмного забезпечення для тестування і налагодження, і іноді розробники забувають їх видалити або залишають спеціально;
- раніше впроваджена програмна закладка [1].

Класифікація загроз за способом впливу на об'єкт атаки:

- безпосередній вплив;
- перевищення користувачем своїх повноважень, робота від імені іншого користувача;
- використання результатів роботи іншого користувача (наприклад, несанкціоноване перехоплення інформаційних потоків, ініційованих іншим користувачем).

Класифікація загроз за способом дій зловмисника (порушника):

- в інтерактивному режимі (вручну);
- у пакетному режимі (за допомогою спеціально написаної програми, яка виконує негативні впливи на операційну систему без безпосередньої участі користувача-порушника).

Класифікація загроз по об'єкту атаки:

- операційна система в цілому;
- об'єкти операційної системи (файли, пристрої тощо);
- суб'єкти операційної системи (користувачі, системні процеси і т.д.);
- канали передачі даних.

Класифікація загроз по використовуваних засобів атаки:

- штатні засоби операційної системи без використання додаткового програмного забезпечення; програмне забезпечення третіх фірм (до цього класу програмного забезпечення відносяться як комп'ютерні віруси та інші шкідливі програми (exploits), які можна легко знайти в інтернеті, так і програмне забезпечення, спочатку розроблене для інших цілей: отладчики, мережеві монітори і сканери і т.д .);
- спеціально розроблене програмне забезпечення [1].

Класифікація загроз об'єкта операційної системи на момент атаки:

- зберігання;
- передача;
- обробка.

Класифікація фізичних загроз:

- знищення або руйнування засобів обробки інформації і зв'язку;
- розкрадання носіїв інформації;
- розкрадання програмних або апаратних ключів і засобів криптографічного захисту даних;
- вплив на персонал [2].

Класифікація радіоелектронних загроз:

- впровадження електронних пристроїв перехоплення інформації в технічні засоби і приміщення;
- перехоплення, розшифровка, підміна і знищення інформації в каналах зв'язку [2].

1.2. Висновки до розділу та постановка задач проектування

На підставі зазначених небезпек сформовано СКБ, вирішальну поставлену задачу. Для забезпечення безпеки, СКБ повинна захищати від усього спектра можливих загроз і зловмисників. Основною слабкою ланкою і основною загрозою безпеці є людський фактор.

При побудові СКБ слід керуватися основними принципами організації захисту: системністю, комплексністю, безперервністю захисту, розумною достатністю, гнучкістю управління та застосування, відкритістю алгоритмів і механізмів захисту і простотою застосування захисних заходів і засобів.

2. МЕТОДИ ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСНОЇ БЕЗПЕКИ

2.1. Структура і склад технічного забезпечення систем безпеки

Галузь техніки, присвячена розробці та виробництву комплексних систем безпеки, в даний час активно розвивається в зв'язку з розвитком технологій, зокрема, комп'ютерних та усвідомленням необхідності комплексного підходу до вирішення завдань забезпечення безпеки. Практика показує, що застосування окремих спеціалізованих систем або підсистем для забезпечення безпеки недостатньо. Повне рішення проблеми можливо лише на основі інтеграції всіх засобів забезпечення безпеки в єдину об'єднану систему безпеки, тобто створення комплексної системи безпеки об'єкта.

Завдання захисту об'єкта може вирішуватися не тільки в комплексі, але і по частинах, наприклад, створенням тільки системи охоронної, охоронно-пожежної або пожежної сигналізації. Однак доцільно комплексне вирішення цього питання або, облік можливості подальшого розширення системи захисту як за рахунок розширення і вдосконалення окремих елементів її частин, так і додавання нових систем (наприклад, системи відео спостереження та системи контролю доступу до системи охоронної сигналізації) [3].

Основні складові технічного забезпечення комплексних систем безпеки (даний розподіл умовно і в реальній системі такого чіткого поділу може і не бути):

- Засоби охоронної сигналізації;
- Засоби контролю доступу;
- Засоби захисту інформації;
- Засоби відеоспостереження;
- Засоби контролю технологічних процесів;
- Засоби зв'язку;
- Засоби пожежної сигналізації;

2.2. Технічні засоби відеоспостереження

У сучасному світі існує величезна кількість систем відеоспостереження, які включають в себе різні технічні засоби і пропонують різний набір функцій. Поняття ідеальної системи існувати не може, так як охопити весь спектр необхідних функцій дуже складно. Для більш детального аналізу спочатку розберемо типи систем і їх компонентів [3].

Типи систем відеоспостереження: У різних джерелах типи систем описуються по-різному. Але, можна виділити три великих типи систем відеоспостереження:

1. Аналогова;
2. Цифрова;
3. Комбінована (напів-цифрова).

Типова аналогова система відеоспостереження складається з камери, провідної мережі для передачі сигналу, роздільник екрану монітора, записуючого пристрою і моніторів. Зазвичай відео фіксація в таких системах проводитися на касету відеомагнітофона, яка може вмістити до 960 годин сигналу. У зв'язку з цим система вимагає постійного обслуговування – заміни та чищення відео-головок, зміни та архівації касет. З появою цифрових технологій, дана система застаріла. ***Недоліки*** системи полягають в обмеженості функцій і в необхідності постійного обслуговування, а ***переваги*** в простоті налаштування, роботи і обслуговуванні.

Напів-цифрова система прийшла на зміну аналогової. Головна відмінність її в підвищенні функціональності. З появою відео-реєстраторів пропала необхідність використовувати відеокасети. Зменшився час пошуку необхідних відео-фрагментів. До цифрових відео-реєстраторів можна підключити аналогові відеокамери і монітори за рахунок аналогових інтерфейсів. З'явилася можливість включення запису за розкладом або по сигналу від охоронного сповіщувача. Так само стало можливим копіювати відео-архів на ПК через USB або локальну мережу. ***Недоліки*** системи

полягають у складності налаштування і в необхідності кваліфікованого обслуговування системи спеціалістами. ***Переваги*** напів-цифрової системи полягають в можливості використання аналогових камер і моніторів, в отриманні стабільно високоякісного зображення, в доступі до записаного архіву по локальній мережі або через інтернет. Так само в можливості запису інформації на жорсткий диск [3].

Цифрова (зараз більш популярна) система відеоспостереження має головні компоненти – це IP-камери і відео-сервери, які встановлюють зв'язок через стандартні комп'ютерні мережі, Інтернет або з використанням бездротових технологій. Такі системи легко можуть входити в системи комплексної безпеки. У такій системі функція запису виконується мережевим відео-реєстратором, в якості якого виступає стандартний комп'ютерний сервер зі спеціалізованим програмним забезпеченням. ***Перевагами*** цифрових систем є висока якість відеозапису, можливість масштабування записаних кадрів, можливість інтеграції з системами безпеки, онлайн трансляція і перегляд відео по локальній мережі і інтернету, можливість запису фрагментів на зовнішні носії та інше. ***Недоліками*** системи є ті ж, що і в напів-цифрової, а саме складність настройки і те, що обслуговування системи має здійснюватися кваліфікованими фахівцями.

Типи камер відеоспостереження:

Спочатку всі камери відеоспостереження розрізняються на дві великі групи за типом обробки сигналу – аналогові і цифрові (мережеві). Головна відмінність цифрових камер від аналогових, що запис відео ведеться відразу ж в цифровому форматі, і воно не вимагає додаткової оцифровки. Так само камери діляться за призначенням на зовнішні (вуличні) камери, які повинні працювати при будь-яких погодних умовах і бути вандалостійкими і на камери внутрішнього спостереження, призначені для цілодобового спостереження за приміщенням. Камери діляться по передачі кольору на кольорові і монохромні (чорно). Переваги чорно-білих камер полягають у тому, що зображення істотно менше займає місця на жорсткому диску, зображення більш

деталізовано і самі камери коштують дешевше, в порівнянні з кольоровими. Перевага кольорової камери полягає в тому, що зображення приємніше для очей і несе в собі велику інформативність [4].

За виконанням, виробники камер виділяють досить багато типів камер. Основні типи, які можна виділити:

- корпусні (мають широкий спектр функцій, дозволяють використовувати змінні об'єктиви, можуть мати кілька режимів роботи і забезпечують високу якість зображення);
- купольні (плюси камери в тому, що вона обертається усередині купола і забезпечує круговий огляд (швидкість повороту у камер розрізняється), а так само за матовим склом купола не видно на кого в даний момент націлений об'єктив. Камери компактні і легко монтуються);
- мініатюрні (камери невеликих розмірів, що дозволяє їх використовувати, в тому числі і для прихованого відеоспостереження. Якість зображення у таких камер досить висока);
- без корпусні (модульні) (камера являє собою плату з встановленим на ній об'єктивом. Камера мініатюрного розміру, що дозволяє встановити її в будь-яке місце);
- відеоглазкі (головна перевага такої камери - це використання ширококутний об'єктив, який дає кут огляду, рівний 180 градусам. кут огляду інших відеокамер (не рахуючи купольні) 90 градусів і менше) [4].

Коротко про обладнання обробки відеосигналів. Воно обробляє відеозображення, що отримується з декількох камер системи відеоспостереження, і передає його на монітори відеоспостереження. Можна виділити два типи:

- квадратори;
- мультиплексори.

Квадратори зазвичай встановлюють на системи з невеликою кількістю відеокамер. Вони поділяють екран на 4 частини і виводять зображення в

режимі реального часу від підключеної до певного каналу камери. Мультиплексори можуть виводити зображення з 4 до 32 камер і виконувати запис цих зображень на окремий або вбудований відео-реєстратор.

2.3. Системи контролю доступу в приміщеннях

При необхідності контролю доступу в обширний комплекс приміщень в якості системи обробки інформації та управління доцільно використовувати комп'ютер. Засоби контролю стану об'єкта для вирішення поставленого завдання [5]:

- Охоронні сповіщувачі;
- Пристрої спостереження;
- Пристрої контролю стану системи захисту.

Часто також пожежні сповіщувачі:

- Як засоби відображення інформації поряд з монітором комп'ютера, де стан об'єктів, що охороняються відображається централізовано, доцільно використовувати й індикаторні лампи або світлодіоди для відображення інформації на місцях;
- Як засоби контролю доступу найчастіше використовуються сканери магнітних карт, ключів і інших носіїв ідентифікатора користувача;
- Як засоби оповіщення на охоронних об'єктах і пультах охорони найбільш широко поширеними є сирени, дзвінки, миготливі лампи, мовні повідомлення;
- Як засоби передачі повідомлень, зазвичай виступають повідомлення по телефону, sms-повідомлення [5].

Для протоколювання подій зручно використовувати базу даних на комп'ютері. При побудові системи контролю доступу в приміщення слід приділити увагу наступним питанням:

- Необхідно забезпечити джерелами безперебійного живлення всі компоненти охоронної системи.

- Крім засобів централізованого управління - комп'ютера, в ряді випадків слід передбачити наявність засобів управління на місцях.

Наприклад, в разі, коли система з ПКП і підключених до нього сповіщувачів входить в охоронний комплекс в якості одного з вузлів. У разі використання комп'ютера в якості системи обробки інформації та управління слід приділити особливу увагу інформаційній безпеці і завадостійкості операційної системи і програмного забезпечення [6].

2.4. Засоби контролю стану об'єкту, що охороняється

Найбільш поширеними засобами контролю стану приміщення, що охороняється є охоронні сповіщувачі. Вони включають в себе:

1. Охорона вікон:

- Акустичні сповіщувачі. Формують тривожний сигнал як реакцію на послідовність звуків прогину і руйнування скла (звук прогину: 45кГц, руйнування: 1 кГц - lМГц.).
- Омічні. Виконуються зазвичай у вигляді смужок фольги, що наклеюються на вікна і порушуваних при руйнуванні скла.
- Активні п'єзоелектричні сповіщувачі. У протилежних кутках скла встановлюють передавач, що випускає механічні коливання, що поширюються в склі вікна, і приймач. При виникненні в склі ушкоджень сигнал від передавача не доходить до приймача.

2. Охорона дверей:

- Магнітоконтактні сповіщувачі. Як правило, такі сповіщувачі побудовані на герконовому вузлі.
- Електроконтактні сповіщувачі. Використовуються рідше, оскільки призначені для масивних дверей.

3. Контроль обсягу приміщення:

- Пасивні оптико-електронні (інфрачервоні) сповіщувачі (PIR-детектори). Вловлюють інфрачервоні (і теплові) випромінювання людини.

- Активні оптико електронні сповіщувачі. До їх складу входять випромінювачі і приймачі. При проходженні людини сигнал від передавача не доходить до приймача.
- Допплерівські датчики руху Засновані на ефекті Допплера.
- Комбіновані сповіщувачі. В одному корпусі зібрані два датчика різних типів (наприклад, PIR- детектор і допплерівський обнаружитель переміщення). Використання двох первинних датчиків працюють на різних фізичних принципах дозволило значно підвищити перешкодозахищеність сповіщувача. Це обумовлено тим, що перешкоди для одного типу датчика не є перешкодами для датчика іншого типу. Сигнал тривоги формується тільки в тому випадку якщо спрацьовування одного датчика підтверджується спрацьовуванням іншого.

При використанні комп'ютера в якості засобу обробки інформації та управління можливе використання мікропроцесорних (далі PC-сумісних) сповіщувачів, безпосередньо підключених до комп'ютера.

Мікропроцесорні сповіщувачі мають більш складні алгоритми обробки сигналу (які можуть враховувати не тільки частоту, амплітуду сигналу і інтервали між сигналами, але і тривалість сигналу, його форму і співвідношення амплітуд сигналів). Завдяки цьому знижується ймовірність помилкових спрацьовувань.

Як засоби контролю доступу найчастіше використовуються сканери магнітних карт, ключів і інших носіїв ідентифікатора користувача. Часто такі пристрої підключають до комп'ютера з метою протоколювання надходить з них інформації. Передана інформація зазвичай містить:

1. Порядковий номер події;
2. Ідентифікатор користувача;
3. Інформацію про те, чи наданий доступ в приміщення.

2.5. Взаємодія приймально-контрольних приладів з комп'ютером і зовнішніми пристроями

Для організації взаємодії приймально-контрольного приладу з комп'ютером необхідно мати інформацію про тип вихідного ланцюга приймально-контрольного приладу, пристроях управління, інтерфейсі і протоколі передбаченому виробником для взаємодії з комп'ютером.

Основні типи вихідних ланцюгів приймально-контрольних для передачі повідомлень про тривогу і службових повідомлень:

1. Бінарний вихід тривоги – вихідний ланцюг, що працює в бінарному режимі (включений / виключений) [7].

2. Вихід тривоги підвищеної інформативності вихідного ланцюга, що виконує ті ж функції, що і бінарний вихід тривоги, але дозволяє розрізняти сигнали тривоги, що зініціюються різними шлейфами, наприклад, за допомогою використання різних режимів роботи оповіщувача (безперервно / переривчасто).

3. Бінарні виходи стану – вихідні ланцюги, що працюють в бінарному режимі і призначені для передачі інформації про певні зміни стану системи охорони, наприклад при проникненні, несправності, пожежі і т.д. включаються різні виходи.

4. Інформаційний вихід стану вихідного ланцюга для передачі інформації про стан системи охорони на пульт централізованого спостереження по телефонній лінії. Для передачі інформації використовується вбудований (або підключається) модем, який здійснює передачу повідомлень з використанням того чи іншого стандартного формату. Такі ПКП можуть передавати інформацію про всі зміни стану системи (тривога, відновлення, зняття з охорони / постановка на охорону з вказівкою користувача, результати тестування і т.д.) [7].

5. Мережева шина для організації роботи декількох ПКП в мережі з виведенням інформації про стан системи на комп'ютер.

Пристрої управління ПКП:

1. Електромеханічний ключ, магнітні та типові карти, радіо брилки та ін. Пристрої, призначені для постановки системи на охорону або зняття з охорони; перевагою даних пристроїв є простота використання, а недоліком – ту обставину, що в разі крадіжки або втрати ключа (карти, радіо-брелка) існує небезпека несанкціонованого доступу до системи;

2. Вбудована в ПКП клавіатура, призначена для управління системою за допомогою набору певного коду або пароля і відповідних команд управління; контроль доступу забезпечується за допомогою системи паролів, які можуть перепрограмувати користувачем з відповідним рівнем доступу до системи;

3. Виносні клавіатури, призначені для виконання тих самих функцій, що і вбудовані клавіатури; конструктивно виконані у вигляді окремих пристроїв, що забезпечують дистанційне, в тому числі бездротове, управління системою;

4. Дистанційне керування з комп'ютера, що використовується для управління і відображення інформації в складних системах охоронної, охоронно-пожежної або пожежної сигналізації; управління системою з комп'ютера можна запустити паралельно з використанням виносних або вбудованих клавіатур [7].

Додаткові технічні засоби, що використовуються для реєстрації і протоколювання системних подій:

1. Розширювачі пам'яті (накопичувачі файлів). Деякі моделі ПКП дозволяють підключати додаткові пристрої розширення пам'яті і накопичення даних. Це дає можливість значно збільшити кількість запам'ятовуються подій, а також підвищити їх інформативність. Накопичувач може бути підключений до комп'ютера для перегляду і перенесення інформації в базу даних.

2. Комп'ютер. Для реєстрації системних подій на жорсткому диску комп'ютера або безпосереднього виведення інформації на принтер ПКП повинен бути оснащений стандартними висновками. Реєстрація подій з використанням комп'ютера зручна, оскільки це дозволяє вести постійно

оновлювану базу даних подій, полегшує обробку інформації, дає широкі можливості її візуалізації [7].

Види повідомлень про зміни в стані системи:

- повідомлення про тривогу (в тому числі дані про те, в якій системі який з шлейфів порушений);
- повідомлення користувачів (дані про те, який користувач зняв систему з охорони або поставив її на охорону);
- повідомлення про відновлення шлейфів сигналізації після порушення або несправності;
- повідомлення про результати тестування системи сигналізації.

Передані відомості зазвичай містять:

- ідентифікаційний номер об'єктового ПКП;
- коди тривожних повідомлень (тривога, пожежа і т.д.);
- номера порушених зон; - коди службових повідомлень (постановка на охорону, зняття з охорони та ін.);
- допоміжну інформацію (який користувач виконав операцію з управління системою і т.п.).

Взаємодія ПКП з комп'ютером дозволяє створювати програмне забезпечення для вирішення наступних основних завдань:

- управління ВКП (віддалена постановка на охорону, зняття з охорони і т.п.);
- програмування ПКП;
- контроль працездатність ПКП і каналу зв'язку;
- формування бази даних користувачів;
- ведення протоколу системних подій;
- зручна візуалізація інформації [7].

2.6. Інтегровані охоронні системи

В даний час існує безліч технічних рішень охоронних систем. Здебільшого технічні засоби охорони добре сумісні лише з продуктами тієї ж фірми-виробника, можливість же поєднання продуктів різних виробників затруджена, що дуже незручно, оскільки виключає можливість поєднання технічних засобів різних фірм найбільш вдалих з точки зору поєднання технічних і економічних характеристик. Аналіз різних технічних рішень охоронних систем і їх можливостей виявив необхідність створення механізму інтеграції технічних засобів охорони різних виробників в єдину систему на основі локальної мережі охороняється об'єкт. Використання вже існуючих на об'єкті комунікацій (локальної мережі) вельми доцільно як з економічної, так і з організаційної точки зору. Таке рішення дозволяє звести до мінімуму обсяг монтажних робіт, необхідних для створення охоронної системи.

Дослідження переваг і недоліків різних моделей архітектури охоронних систем показало, що інтегровані охоронні системи крім економічної і організаційної доцільності мають високий ступінь спадкоємності, оскільки дозволяють поєднувати інтегровані мережеві рішення з традиційними моделями охоронних систем [8].

У порівнянні з простою сукупністю окремих систем і засобів захисту застосування інтегрованих систем безпеки забезпечує наступні переваги:

- можливість більш точної реакції на події, що відбуваються;
- оптимальна, заздалегідь продумана реакція на поточну ситуацію;
- значне зниження ризику, пов'язаного з "людським фактором";
- помилками і можливими недобросовісними діями обслуговуючого персоналу і співробітників фірми;
- зменшення витрат на обладнання;
- зниження витрат на монтаж та експлуатацію системи безпеки;
- скорочення обслуговуючого персоналу і витрат на його навчання і зміст.

В рамках інтеграційної гілки розвитку архітектури охоронних систем, у перебігу останніх років була створена і рекомендована до впровадження система «Оріон» компанії Bolid (Рис.2.1) [9].

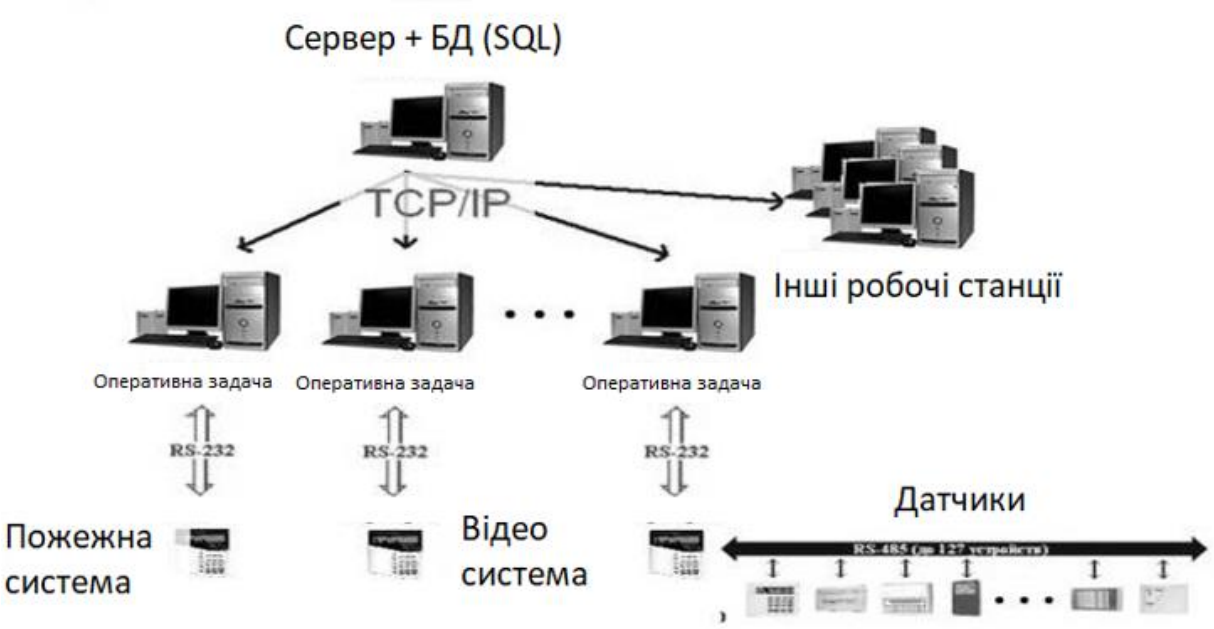


Рисунок 2.1 – Архітектура системи «Оріон» компанії Bolid

Сервер може бути організований звичайним комп'ютером, що значно зменшує витрати на систему. Але, якщо в установи будуть виділені додаткові кошти на інтегровану систему охорони, тобто можливість встановити спеціалізоване ПЗ фірми Болід – «ОріонПРО». Комп'ютер, який вирішує оперативне завдання, передає зібрані дані на сервер, який може бути встановлений в будь-якому місці, наприклад, в кабінеті директора [9].

Оператори – будь-які комп'ютери, на яких визначено доступ і перелік завдань, які вони можуть вирішувати. В основному це комп'ютери пункту охорони. В результаті вивчення цієї системи були виявлені такі недоліки, як:

1. Якщо на обладнанні використовується ВО «Оріон», з протоколом «Оріон», то до цього ж порту можна підключити обладнання, яке працює на інших протоколах.
2. Недостатньо висока інформаційна захищеність.

3. Базування програмних компонентів комплексу на це дозвіл платному ПЗ, необхідність закупівлі у компанії розробника ряду специфічних апаратних засобів.
4. Для кожного окремого випадку розміщення системи на об'єкті, що охороняється потрібна спеціалізована настройка, що зобов'язує наявність професійного фахівця, який працює з системою.

2.7. Класифікація принципів побудови комплексних охоронних систем

З точки зору архітектури та складу, поєднуваних в охоронній системі компонентів, принципи побудови комплексних охоронних систем можна розділити на наступні групи [1]:

1. Відокремлені охоронні системи: автономні та централізовані.

2. Інтегровані охоронні системи з апаратної і програмної інтеграцією компонентів.

Автономні відокремлені охоронні системи створюються з обладнання строго певної фірми-виробника і розширюються за допомогою її ж продукції. Дана охоронна система ізольована від комунікацій об'єкту, що охороняється. Як правило, рішення таких систем пропонуються в готовому вигляді (Рис. 2.2).

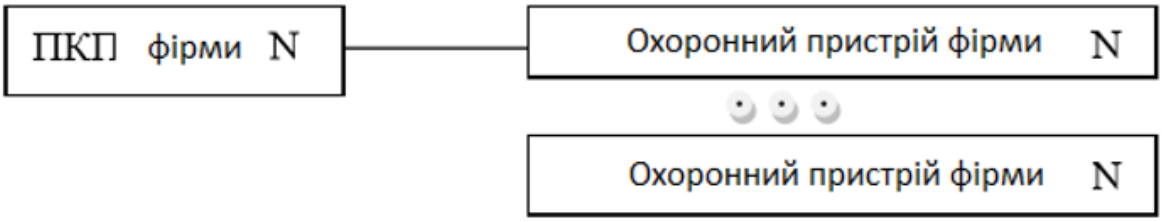


Рисунок 2.2 – Узагальнена схема автономної охоронної системи

Централізовані охоронні системи можуть бути створені з обладнання різних фірм-виробників. Дана охоронна система ізольована від комунікацій об'єкту, що охороняється. Як правило, в ролі засобу протоколювання даних (іноді обробки) і управління є комп'ютер (Рис. 2.3) [1].

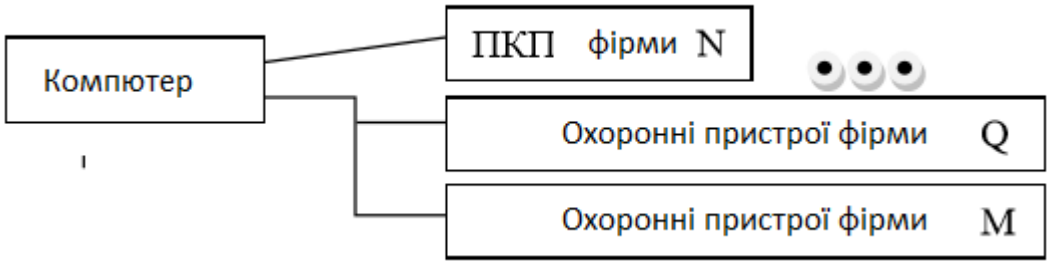


Рисунок 2.3 – Узагальнена схема централізованої відокремленої охоронної системи.

Інтегровані охоронні системи з апаратною інтеграцією компонентів побудовані на принципі: існуючі технічні рішення певних виробників інтегруються в комунікації об'єкту, що охороняється переважно за рахунок апаратних засобів. Координація дій компонентів здійснюється охоронним сервером (Рис. 2.4) [1].

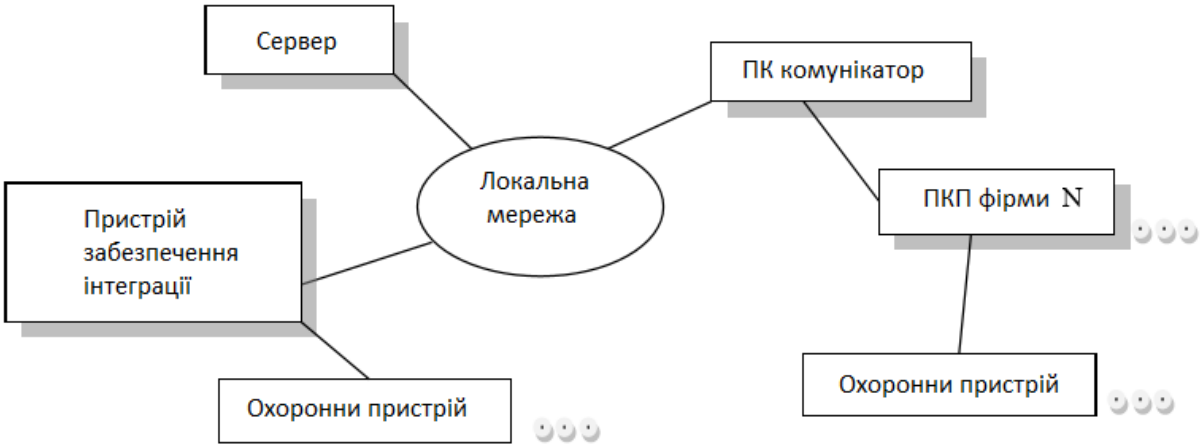


Рисунок 2.4 – Узагальнена схема інтегрованої охоронної системи з апаратною інтеграцією компонентів.

Інтегровані охоронні системи з програмної інтеграцією компонентів. Існуючі технічні рішення певних виробників інтегруються в комунікації об'єкту, що охороняється переважно за рахунок програмних засобів. Охоронну систему такого типу можна трактувати як систему, яка працює за єдиним алгоритмом, організовану з ряду складових відокремлених охоронних систем з рознесенням ряду функцій (оповіщення, протидія загрозам) по вузлах

системи і відповідними механізмами координації (і синхронізації) роботи вузлів і забезпечення необхідної відмовостійкості. До цього типу належить дана розроблена охоронна система (Рис. 2.5) [1].

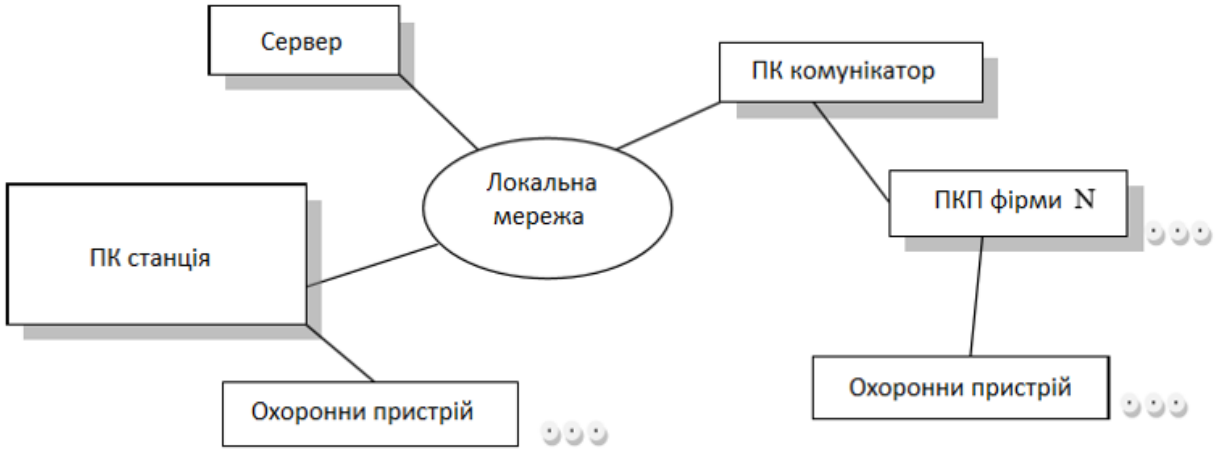


Рисунок 2.5 – Узагальнена схема інтегрованої охоронної системи з програмної інтеграцією компонентів

2.8. Висновки до розділу

У цьому розділі розглянуто принципи побудови охоронних систем різних типів, їх структура, склад, способи взаємодії компонентів. У зв'язку з тим, що для побудови системи безпеки виділяється обмежена кількість коштів, що призводить до необхідності мати велику гнучкість системи і сумісність з різними технічними засобами охорони, обрана для побудови інтегрована охоронна система з програмної інтеграцією. ІСБ з програмної інтеграцією має ряд переваг, серед яких можливість більш точної діагностики стану об'єкта, що охороняється і реакції на події, що відбуваються, і так само суттєве зниження витрат на обладнання, монтаж та експлуатацію системи. Це є одним з ключових чинників для створення системи в обмежених фінансових умовах. Аналіз різних технічних рішень охоронних систем і їх можливостей виявив необхідність інтегрувати різноманітні технічні засоби охорони в єдину мережу на основі локальної мережі об'єкту, що охороняється.

3. ПРОЕКТУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ БЕЗПЕКИ ФІНАНСОВОЇ УСТАНОВИ

3.1. Розробка підсистеми контролю та управління доступом

Об'єкти, що підлягають оснащенню системою контролю і управління доступу:

1. КПП;
2. Бухгалтерія;
3. Відділ безпеки;
4. Серверна;
5. Кабінет керівника;
6. Приміщення для проведення конфіденційних переговорів.

Системою контролю та управління доступу вирішуються наступні завдання:

- контроль і управління доступом співробітників і відвідувачів на територію об'єкта;
- контроль і управління доступом співробітників і відвідувачів в ряд приміщень;
- автоматичне ведення баз даних доступу в межах об'єкта, що захищається.

В організації на постійній основі працює 20 співробітників. Середня кількість прибуваючих в організацію клієнтів – 5 осіб на годину.

Тип ідентифікаторів користувачів: безконтактні карти MIFARE Classic 4k. На картах постійних користувачів (співробітників підприємства) розміщується фотографія, логотип компанії і інша інформація про співробітника. На тимчасових картах клієнтів не розміщується ніякої інформації про відвідувача.

Територія підприємства обладнана одним КПП для персоналу. Максимальне навантаження на прохідну – 120 людей / рік.

Для управління СКУД використовується одне автоматизоване робоче місце, розташоване на пості охорони. АРМ поста охорони захищено від несанкціонованого доступу і шкідливого програмного забезпечення за допомогою DeviceLock і антивірус Касперського 6.0. З'єднання з іншими АРМ по ЛОМ відсутня.

Система контролю і управління доступом узгоджена з системою відеоспостереження і системою охоронно-пожежної сигналізації за допомогою інтегрованої системи безпеки ІСБ-1.

Структура пріоритетності зон, що захищаються:

Вищий пріоритет: Кабінет директора, приміщення для проведення конфіденційних переговорів.

Середній пріоритет: бухгалтерія, відділ безпеки, серверна.

Нижчий пріоритет: КПП.

Опис роботи системи

Співробітники підприємства проходять КПП, підносячи постійний пропуск до зчитувача карт на турнікеті. Факт ідентифікації особистості записується на АРМ СКУД (реєструється час ідентифікації та П.І.Б. співробітника).

Відвідувачі підприємства отримують тимчасовий пропуск при пред'явленні посвідчення особи. Процедура видачі пропуску фіксується в електронному журналі обліку виданих перепусток. Після видачі пропуску, відвідувач може пройти на територію підприємства. При виході, відвідувач зобов'язаний здати тимчасовий пропуск на КПП. У журналі робиться відмітка про вибуття відвідувача, і здачі пропуску.

Доступ до бухгалтерії мають тільки бухгалтер, старший бухгалтер і керівник підприємства. Їх постійний пропуск запрограмований відповідним чином, щоб вони могли отримати доступ до кабінету бухгалтерії.

Доступ до відділу безпеки і серверної мають головний адміністратор, начальник відділу безпеки і керівник підприємства. Їх постійний пропуск

запрограмований відповідним чином, для отримання доступу до кабінету відділу безпеки і серверної.

Доступ до приміщення для проведення конфіденційних переговорів мають керівник відділу безпеки і керівник підприємства. Їх постійний пропуск запрограмований відповідним чином, для отримання доступу до приміщення для проведення конфіденційних переговорів.

Доступ до кабінету керівника підприємства має тільки керівник підприємства. Доступ здійснюється за допомогою пред'явлення відповідного пропуску.

Система підтримує можливість подальшого розширення, шляхом установки додаткових зчитувачів.

Функціональні можливості системи контролю та управління доступом:

- реєстрацію і протоколювання тривожних і поточних подій;
- пріоритетне відображення тривожних подій;
- управління роботою пристроями, в точках доступу по командам оператора;
- завдання тимчасових режимів дії ідентифікаторів;
- захист технічних і програмних засобів від несанкціонованого доступу;
- автоматичний контроль справності засобів, що входять в систему, і ліній передачі інформації;
- установку режиму вільного доступу з пункту управління при аварійних ситуаціях і надзвичайних подіях;
- блокування проходу по точках доступу командою з пункту управління.

Для даного проекту було обрано турникет-трипод ZKTeco TS1000 Pro (Рис. 3.1) і вхідні двері Siberia, бо їхніх характеристик цілком достатньо для реалізації всіх потреб проекту. Обрані механізми (Табл. 3.1 – 3.2) – це якісні

пристрої, які будуть працювати довгий час, незважаючи на невисоку собівартість. Надійний захист забезпечений.

Рисунок 3.1 – Турнікет-трипод ZKTeco TS1000 Pro

Таблиця 3.1 – Турнікет-трипод ZKTeco TS1000 Pro

Характеристика	Параметр
Напруга живлення	AC110В/220В
Ширина проходу	500 мм
Вага	34 кг
Пропускна здатність	30 людей/хв
Енергоспоживання	15-68 Вт
Габаритні розміри турнікета (довжина * ширина * висота)	520*310*1010мм
Робочий діапазон температур	-28…+60°C
Напрацювання на відмову	1 млн. проходів
Ціна	21283 грн

Таблиця 3.2 – Вхідні двері Siberia

Характеристика	Параметр
Верхній замок	КАЛЕ 257L сувальдний + нічна засувка
Нижній замок	Електронний з відбитком пальця
Протизнімачі	3 шт
Оздоблення всередині	МДФ вологостійкий фрезерований (22 мм)
Оздоблення зовні	Метал 1.8 мм з молдингом
Вага	135 кг
Товщина	75мм
Розміри (ширина * висота)	960*2050мм
Ціна	9899 грн

КПП:

Кількість користувачів: 20 постійних, і відвідувачі.

Виконано у вигляді турнікета, пристроєм для читання карт. На КПП є ручний металодетектор (Рис. 3.2). Характеристик даного металодектора цілком достатньо для перевірки відвідувачів (Табл. 3.3). Протоколюється пропуск відвідувачів через прохідну. Присутня система відеоспостереження. Турнікет і зчитувач карт підключені через шлейф мережевого контролера доступу пристрою ІСБ-1. Є резервне живлення 12В.

Рисунок 3.2 – Ручний металодетектор Garrett Super Scanner V

Таблиця 3.3 – Ручний металодетектор Garrett Super Scanner V

Характеристика	Параметр
Налаштування чутливості	Самокалібрування (мікропроцесор усуває необхідність переналаштування чутливості)
Робоча частота	2 кГц
Довжина	42 см
Вага	0,5 кг
Товщина	75мм
Живлення	Батарея 9 В (Крона)
Ціна	7056 грн

Бухгалтерія:

Кількість користувачів: 3 постійних, відвідувачі.

Рубіж виконаний у вигляді сталевих дверей з двома замками. Перший замок відкривається відповідної картою доступу. Другий замок механічний, відкривається ключем. Ключ є у бухгалтера, головного бухгалтера, заступника керівника і керівника підприємства. Запасні ключі зберігаються в сейфі в кабінеті керівника. Присутнє відеоспостереження. Є аудіодомофон для прийому відвідувачів. Відбувається протоколювання проходів відвідувачів для даних дверей. Є резервне живлення 12В.

Відділ безпеки:

Рубіж виконаний у вигляді сталевих дверей з двома замками. Перший замок відкривається відповідної картою доступу. Другий замок механічний, відкривається ключем. Ключ є у начальника відділу безпеки, головного адміністратора, заступника керівника та керівника підприємства. Запасні ключі зберігаються в сейфі в кабінеті керівника. Присутнє відеоспостереження. Є аудіодомофон для прийому відвідувачів. Відбувається протоколювання проходів відвідувачів для даних дверей. Є резервне живлення 12В.

Серверна:

Рубіж виконаний у вигляді сталевих дверей з двома замками. Перший замок відкривається відповідної картою доступу. Другий замок механічний, відкривається ключем. Ключ є у начальника відділу безпеки, головного адміністратора, заступника керівника та керівника підприємства. Запасні ключі зберігаються в сейфі в кабінеті керівника. Відбувається протоколювання проходів відвідувачів для даних дверей. Є резервне живлення 12В.

Кабінет керівника:

Рубіж виконаний у вигляді сталевих дверей з двома замками. Перший замок відкривається відповідної картою доступу. Другий замок механічний, відкривається ключем. Ключ є у заступника керівника і керівника підприємства. Запасний ключ зберігаються в сейфі в кабінеті керівника. Присутнє відеоспостереження. Відбувається протоколювання проходів відвідувачів для даних дверей. Є резервне живлення 12В.

Приміщення для проведення конфіденційних переговорів:

Рубіж виконаний у вигляді тамбурних дверей з двома замками. Перший замок відкривається відповідної картою доступу. Другий замок механічний, відкривається ключем. Ключ є у керівника підприємства, заступника керівника підприємства, системного адміністратора і начальника відділу безпеки. Запасний ключ зберігаються в сейфі в кабінеті керівника. Є можливість застосування ручного металодетектора. Присутнє відеоспостереження. Є аудіодомофон. Відбувається протоколювання проходів відвідувачів для даних дверей. Є резервне живлення 12В.

Устаткування:

Мережевий контролер доступу є основною частиною інтегрованої системи безпеки ІСБ-1, тому було обрано саме контролер ZKTeco (Рис. 3.3), адже він не тільки якісний, а й дозволить обробляти більше інформації при розширенню фірми. Це можна побачити в його характеристиках (Табл. 3.4).

До мережевих контролерів доступу підключається необхідне додаткове обладнання: зчитувачі, інтерфейсні модулі і т.д.

Рисунок 3.3 – Мережевий контролер доступу ZKTeco

Таблиця 3.4 – Мережевий контролер доступу ZKTeco

Характеристика	Параметр
Вбудована пам'ять карток	30 000
Вбудована пам'ять подій	100 000
Напруга живлення	9.6-14В
Кількість шин	8
Вага	0,25 кг
Допустима вологість	10%...80% без конденсата
Діапазон робочих температур	0°C - + 55°C
Ціна	7969 грн

Мережевий охоронний контролер.

Контролер призначений для створення розподілених мережевих охоронних систем, що працюють під управлінням ПК. Контролери працюють в складі інтегрованої системи, розширюючи її охоронні функції і служать для сполучення СКУД і системи ОПС, тому вони були обрані вже з провіреної компанії ZKTeco (Табл. 3.5).

Таблиця 3.5 – Мережевий охоронний контролер ZKTeco

Характеристика	Параметр
Напруга живлення	12В
Кількість шин	8
Ціна	3499 грн

Для розробленої СКУД було обрано мережевий зчитувач EM-Marine ZKTeco (Рис. 3.4). Бюджетність, простота і ціна цього пристрою тримається на висоті (Табл. 3.6).

Рисунок 3.4 – Мережевий зчитувач EM-Marine ZKTeco

Таблиця 3.6 – Мережевий зчитувач EM-Marine ZKTeco

Характеристика	Параметр
Підтримка ідентифікаторів	Mifare Classic 1К и 4К; Mifare UltraLight; Mifare ProX;
Напруга живлення	9-24В
Температура	-40 - +60°С
Розміри	103 х 48 х 19 мм
Дальність читання	30-80мм
Ціна	900 грн

Також було використано інтерфейс сполучення (Табл. 3.7).

Таблиця 3.7 – Інтерфейс сполучення

Характеристика	Параметр
Інтерфейс підключення:	USB
Кількість ліній RS-485	1
Живлення	Від USB-порта

Всі, раніше описані, пристрої були використані в попередньо розробленій схемі СКУД (Рис. 3.5).

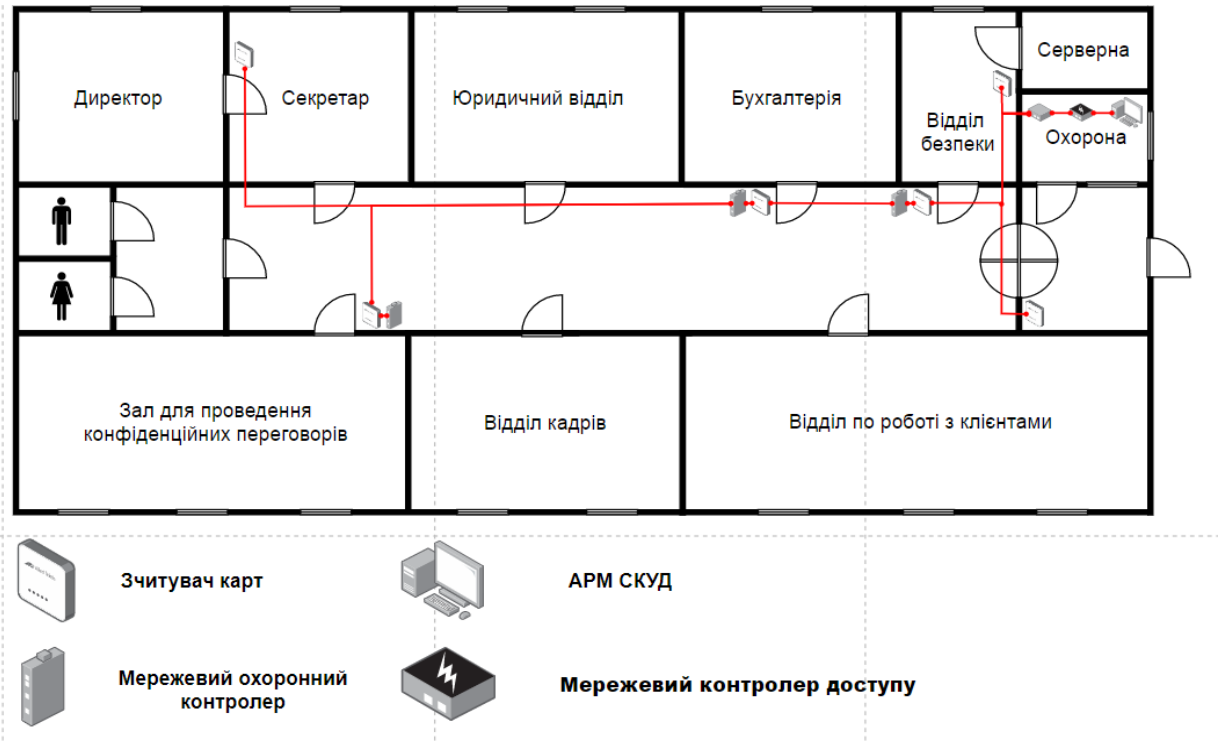


Рисунок 3.5 – Схема системи контролю та управління доступом

3.2. Розробка підсистеми відеоспостереження

Основні положення:

Зони огляду:

1. КПП. Мета спостереження в денному і нічному режимі: ідентифікація особистості. Денне освітлення: світлодіодні лампи потужністю 9Вт. Нічне освітлення: світлодіодні лампи меншої інтенсивності. Температура в приміщенні змінюється від 18 до 25 °С, завдяки автономному опаленню.

2. Головний коридор. Мета в спостереженні в денному і нічному режимі: упізнання особистості. Денне освітлення: Світлодіодні лампи. Нічне освітлення: Світлодіодні лампи меншої інтенсивності. Температура в приміщенні змінюється від 18 до 25 °С, завдяки автономному опаленню.

3. Кабінет секретаря. Спостереження ведеться тільки в нічний час, або за запитом секретаря або керівника. Контролюється двері кабінету генерального директора. Мета спостереження: ідентифікація особистості. Денне освітлення: світлодіодні лампи. Нічне освітлення: світлодіодні лампи меншої інтенсивності. Температура в приміщенні змінюється від 18 до 25 °С, завдяки автономному опаленню.

4. Вулиця. Цілі спостереження в денному і нічному режимі: впізнання особистості і транспортного засобу, ніч – впізнання особистості і транспортного засобу. Денне освітлення: природне. Нічне освітлення: вбудований ІК прожектор камери спостереження, штучне освітлення від прилеглих будівель. Температура від -20 до +30°С, видимість може бути затруджена через опади та інші погодні явища. Сейсмічна активність відсутня.

Завдання, які вирішуються:

1. Контроль несанкціонованого доступу співробітників і (або) порушників на територію об'єкта.
2. Контроль несанкціонованого доступу співробітників або порушників на територію (або з території) об'єкта через огородження або заборонені зони.
3. Захист людей та матеріальних цінностей в межах контрольованої зони.
4. Ідентифікація особи відвідувача або співробітника при проходженні КПП, або при відвідуванні кабінету генерального директора.

5. Виявлення автомобілів, що в'їжджають на територію контрольованої зони.
6. Автоматична фіксація і зберігання протягом певного часу запису протиправних або інших подій за тривожним повідомленням.
7. Виявлення та фіксування інших протиправних дій.

Пости спостереження і керування комплексом.

Присутній один пост спостереження, пост охорони. Розташований на КПП, при вході на територію, що охороняється.

Система відеоспостереження узгоджена з інтегрованою системою безпеки ІСБ-1. Одна АРМ відеоспостереження розташована на посту охорони.

Можливість відео-реєстрації: безперервна, по сигналу оператора, за таймером, детектор руху.

Можливий перегляд одночасно всіх відеокамер комплексу.

Камери можуть виконувати охоронні функції в якості детектора руху.

Система відеоспостереження узгоджена з інтегрованою системою безпеки. Одне АРМ відеоспостереження розташоване в кімнаті охорони.

Загальні вимоги до системи відеоспостереження:

• кольорова, чорно-біла, комбінована камера;

• термін зберігання відеозаписів в архіві;

• необхідність в доповненні системи відеоспостереження системою автоматизованого управління доступом у приміщення і на об'єкти;

• необхідність фіксації аудіо інформації з охоронюваних об'єктів;

• можливість розширення системи;

• наявність і розташування щитів електроживлення поблизу місць установки устаткування і на постах спостереження;

• наявність резервного або дублюючого живлення;

• можливість подальшого розширення шляхом додавання нових телекамер і постів спостереження (охорони).

Термін зберігання відеозаписів в архіві 5 днів.

Можливість розширення: система може бути розширена шляхом додавання нових постів спостережень, телекамер, відео-реєстраторів та інтерфейсів синхронізації з ПК.

Живлення: Електричний щит розташований в кімнаті охорони. Також присутній резервне живлення 12В.

Система відеоспостереження: Присутній комбінована система відеоспостереження. Всередині приміщення застосовуються кольорові камери, для вуличного спостереження застосовуються чорно-білі камери, з вбудованим інфрачервоним прожектором.

Відеоспостереження ведеться з 3 камер всередині приміщення, і з 3 вуличних камер. Пост спостереження обладнаний двома відео-реєстраторами, які з'єднані з інтегрованою системою безпеки за допомогою спеціального інтерфейсу і відповідного програмного забезпечення. Відео-реєстратори додатково оснащені жорсткими дисками для зберігання відео-архіву. Камери можуть виконувати охоронні функції в якості детектора руху. Відео-реєстратор може записувати відео-потік в різних режимах: при наявності руху, за сигналом оператора, за таймером. Інформація з камер виводиться на екран монітора оператора.

Характеристики камер внутрішнього спостереження (Табл. 3.8).

Таблиця 3.8 – Характеристики внутрішнього спостереження

	КПП	Коридор	Секретар
Фокусна відстань об'єктива (мм)	13,5	3	13,5
Формат матриці відеокамери	1/3	1/3	1/3
Висота установки камери (м)	2,5	3	3
Кут нахилу камери (градус)	35	15	25
Роздільна здатність (твл)	420	420	420
Відстань до об'єкта (м)	2,5	9,2	4

Характеристики камер зовнішнього спостереження (Табл. 3.9).

Таблиця 3.9 – Характеристики зовнішнього спостереження

Характеристика	Величина
Фокусна відстань (мм)	3
Формат матриці відеокамери	1/3
Висота установки камери (м)	6
Кут нахилу камери (градус)	25
Роздільна здатність (твл)	600
Відстань до об'єкта (м)	25

Технічні характеристики камер, використаних в даному проекті:

У приміщенні були використані відеокамери inter Vision IVR-734C (Рис. 3.6). Це мініатюрні відеокамери, які мають сертифікат відповідності. Їх характеристик достатньо для спостереження в будівлі. Також, потрібно зазначити, їхню гарну якість і невелику вартість (Табл. 3.10).

Рисунок 3.6 – Відеокамера inter Vision IVR-734C

Таблиця 3.10 – Характеристики камери inter Vision IVR-734C

Характеристика	Значення параметру
1	2
Передача кольору	Кольорова
Матриця	ПЗС матриця 1/3”

Продовження таблиці 3.10

1	2
Вбудований об'єктив	3.6 мм
Розширення	420 Твл
Чутливість	0,05 Лк
Відношення сигнал / шум	46 дБ
Тип камери	Цифрова
Наявність синхронізації	Зовнішня
Температурний режим	-10…+50°C
Кут огляду	90° стандартний, додаткові кути 110°, 78°, 56°, 35°, 25°, 15°
Напруга живлення	12В
Ціна	3250 грн

Зовні були використані відеокамери Vision Hi-Tech VN51BH-H4IR (Рис. 3.7). Дані відеокамери, які мають сертифікат відповідності, зроблені в ударостійкому і вологонепроникному корпусі. Їх характеристик достатньо для комфортного спостереження на подвір'ї. Також, потрібно зазначити, що відео, які фіксує Vision Hi-Tech – чорно-білі і це дуже великий плюс, адже їх розмір значно менший від розміру кольорових відео, і це дає змогу зберігати більше відзнятого матеріалу. (Табл. 3.11).

Рисунок 3.7 – Відеокамера Vision Hi-Tech

Таблиця 3.11 – Характеристики відеокамери Vision Hi-Tech

Характеристика	Значення параметру
Передача кольору	Чорно-біла
Матриця	ПЗС матриця 1/3”
Розширення	600 Твл
Вбудований об'єктив	4.3мм
Кут огляду	90° стандартний, додаткові кути 78°, 56°, 44°, 25°, 21°
Напруга живлення	12В
Температурний режим	-45 …+70°С
Примітка	Є вбудований ІК прожектор, з дальністю підсвічування до 30 метрів.
Корпус	Вологонепроникний, ударостійкий
Ціна	3499 грн

Для продуктивної роботи був вибраний якісний і багатофункціональний відео-реєстратор HIKVISION DS-7608NI-Q1 (Рис. 3.8). Він добре справляється з поставленими задачами, завдяки непоганим характеристикам (Табл. 3.11).

Рисунок 3.8 – Відео-реєстратор HIKVISION

Таблиця 3.12 – Характеристики відео-реєстратора HIKVISION

Характеристика	Параметр
Вид накопичувача	Цифровий
Робоча вологість	не більше 90%
Розширення	600 ТВЛ
Діапазон робочих температур	-10° + 55°C
Режим запису	Постійний, тривога, таймер, детектор руху
Розміри	315 x 240 x 48 мм
Вага	1 кг, без HDD
Кількість каналів запису	8
Живлення	12В
Ціна	3080 грн

Як засіб перегляду зображень, одержуваних з камер, використовуємо відео-монітор LG BK550Y (на посту охорони). Характеристик вибраного пристрою цілком достатньо для перегляду відеофайлів і роботи в цілому (Табл. 3.13) [10].

Таблиця 3.13 – Характеристики монітора LG BK550Y

Характеристика	Параметр
Розширення	1920 x 1080
Яскравість	250 кд/кв.м
Контрастність	1000:1
Кількість кольорів	5 мільйонів
Живлення	220В
Співвідношення сторін	16:9
Ціна	4899 грн

Розмежування прав користувачів відбувається на програмному рівні. Камери з'єднані з відео-реєстраторами, які перебувають на посту охорони, за допомогою коаксіального кабелю. Будуємо схему розміщення відеокамер (Рис. 3.9).

Рисунок 3.9 – Схема розміщення камер

3.3. Система охоронно-пожежної сигналізації

Загальні відомості про об'єкт:

Системою охоронно-пожежної сигналізації обладнуються:

- Коридор (загальнодоступна зона).
- Відділ по роботі з клієнтами.
- Відділ безпеки.
- Серверна.
- Пункт охорони.
- Відділ кадрів.
- Бухгалтерія.
- Юридичний відділ.
- Секретар.

- Кабінет керівника.
- Приміщення для проведення конфіденційних переговорів.

До категорії особливо важливих приміщень відносяться:

- Кабінет керівника, обладнаний сховищем цінностей (вогнетривкий сейф).
- Приміщення для проведення конфіденційних переговорів.
- Відділ безпеки.
- Серверна.

Найбільш уразливими місцями для несанкціонованого доступу на об'єкт із-за меж зони, що захищається, є вікна та віконні прорізи.

Кліматичні умови. Температура в приміщенні змінюється від 18 до 25°С, вологість від 20 до 80%. Температура в серверній змінюється від 5 до 10°С.

Умови на вулиці: світлова обстановка – сонячне світло, температура від -30 до +40°С, видимість може бути утруднена через опади та інші погодні явища. Сейсмічна активність відсутня.

Периметр території, що захищається 87,9м. Площа території, що захищається 450,125 $м^2$.

Місця і способи складування цінностей на території, що захищається (Рис. 3.10).

Основні цінності (матеріальні, цінні папери, грошові) зберігаються в вогнетривкому сейфі в кабінеті керівника. Доступ до сейфа має тільки керівник підприємства.

У відділі безпеки встановлений сейф, в якому зберігаються пристрої резервного копіювання інформації. Доступ до сейфа має головний адміністратор і начальник служби безпеки. Найбільш вразливі місця для проникнення порушника на ці об'єкти є вікна і двері.

Рисунок 3.10 – Схема периметра території, що захищається

Електроживлення системи ОПС здійснюється від двох незалежних джерел.

Основне живлення здійснюється від електричного щита, розташованого в пункті охорони, через понижуючий трансформатор. Резервне живлення передбачено від двох акумуляторних батарей 12В.

Електропроводка пожежної сигналізації виконуються кабелем, який не поширює горіння, що прокладається в монтажних коробах.

Пост охорони з цілодобовим чергуванням розташований в приміщенні для охорони, при вході на об'єкт, що охороняється. Пост охорони обладнаний пультом централізованого спостереження, синхронізованого з інтегрованою системою безпеки. Обладнаний телефоном, телефонна коробка знаходиться на пості охорони.

Найменування приміщення з цілодобовим чергуванням, куди подаються сигнали системи – це пост охорони.

Функціональні можливості системи:

Зонами охорони є приміщення, що містять матеріальні цінності, крім місць загального користування (коридори, туалети).

Зони охорони:

- Коридор.

- Відділ по роботі з клієнтами.
- Відділ безпеки.
- Серверна.
- Пункт охорони.
- Відділ кадрів.
- Бухгалтерія.
- Юридичний відділ.
- Секретар.
- Кабінет керівника.
- Приміщення для проведення конфіденційних переговорів.

Пріоритетними зонами захисту є кабінет керівника, приміщення для проведення конфіденційних переговорів і приміщення служби безпеки.

Опис системи пожежної сигналізації:

Пожежною сигналізацією обладнані всі приміщення, за винятком туалетів. Застосовуються два три типи пожежних сповіщувачів: димовий, тепловий і ручний. Ручні сповіщувачі встановлені на шляхах евакуації. Димові сповіщувачі встановлені в коридорі і в інших приміщеннях. Кабінет директора і приміщення для конфіденційних переговорів додатково обладнані тепловими сповіщувачами. У разі отримання на пульт сигналу «Пожежа», автоматично подається сигнал тривоги, за допомогою системи оповіщення про пожежу, яка включає в себе 4 комбіновані сирени (звукова і світлова сирена). На стінах коридору вказано шляхи евакуації при пожежі. Додатково, раз у три місяці, проводяться навчальні тривоги.

Опис системи охоронної сигналізації:

Відділ по роботі з клієнтами, відділ кадрів, бухгалтерія, юридичний відділ і кабінет секретаря обладнані датчиками руху, призначеними для виявлення проникнення в приміщення через вікна. Контролюється можливість несанкціонованого проникнення через двері, так як коридорний простір проглядається камерами спостереження, що дає можливість оператору

зреагувати на можливий прояв загрози. Так само, важливим є факт, що зловмисникові, щоб покинути територію, необхідно пройти або через пункт КПП, або вилізти через вікно, яке контролюється датчиками руху. У разі виявлення подається сигнал на пульт оператора, який приймає рішення про подальші дії (виклик охорони по тривожній кнопці, або затримання порушника силами особового складу охорони).

Приміщення для проведення конфіденційних переговорів, кабінет керівника і відділ безпеки обладнані акустичними датчиками розбиття скла і Магнітоконтактними сповіщувачами на відкриття дверей. Серверна також обладнана Магнітоконтактним сповіщувачем. Дані приміщення є пріоритетними об'єктами захисту, тому при їх проектуванні враховувалося, що спроба проникнення повинна бути виявлена на ранніх етапах. Акустичні датчики реагують на розбиття скла, що дозволяє виявити спробу проникнення до того, як зловмисник проникне в приміщення, і швидше зреагувати.

Магнітоконтактні сповіщувачі реагують при спробі відкриття дверей, що так само дає можливість виявити спробу проникнення до потрапляння порушника в приміщення, що охороняється. У разі виявлення спроби проникнення подається сигнал на пульт оператора, який приймає рішення про подальші дії.

Опис видів сигналів:

«Пожежа». При отриманні сигналу «Пожежа», автоматично включається звукова і світлова сирена, турнікети переводяться в режим вільного пропускання відвідувачів, проводиться евакуація персоналу і викликається пожежна служба.

«Прийнято під охорону». Об'єкт приймається під охорону після закінчення робочого дня. В даному режимі вмикаються всі охоронні сповіщувачі.

«Знятий з охорони». Об'єкт знімається з охорони на початку робочого дня. В даному режимі вимикаються всі охоронні сповіщувачі, крім

сповіщувачів в кімнаті для проведення конфіденційних переговорів, і кабінеті керівника.

«Тривога». Сигнал подається при спрацьовуванні датчиків руху, або при виявленні зловмисника за допомогою системи охоронного відеоспостереження.

«Злом». Сигнал подається при спрацьовуванні датчиків розбиття скла і магнітоконтактних сповіщувачів. Сигнал означає, що виявлена спроба проникнення в приміщення, що охороняються.

«Несправність». Сигнал подається при пропажі сигналів від сповіщувачів.

Пункт охорони оснащений тривожною кнопкою для виклику співробітників приватного охоронного підприємства «Кербер». Розрахунковий час прибуття 4-5 хвилин.

Система охоронно-пожежної сигналізації інтегрована в загальну систему безпеки, і співпрацює з системою охоронного відеоспостереження і системою управління контролем доступу, за допомогою інтегрованої системи безпеки.

Можливість розширення системи присутнє. Для розширення системи знадобиться установка додаткових технічних засобів виявлення, сигнальних ліній, джерел резервного живлення і приймально-контрольних приладів.

Обладнання системи пожежної сигналізації:

Для реалізації системи пожежної сигналізації був вибраний автоматичний димовий пожежний сповіщувач Satel TSD-1 (Рис. 3.11). Технічних характеристик якого більш чим достатньо для розробленої схеми. Переваги: Гарна якість і невисока ціна (Табл. 3.14).

Рисунок 3.11 – Димовий сповіщувач Satel TSD-1

Таблиця 3.14 – Характеристики сповіщувача Satel TSD-1

Характеристика	Параметр
Напруга живлення	12В
Інерційність спрацювання	Не більше 5с
Середнє напрацювання на відмову	Не менше 60000ч
Вага	164 г
Пороги температур виклику тривоги	+54…+65 °С
Діапазон робочих температур	-10…+55 °С
Чутливість сповіщувача	85 дБ/м
Сертифікат відповідності	Відповідає вимогам пожежної безпеки
Ціна	985 грн

Для реалізації системи пожежної сигналізації був вибраний автоматичний тепловий пожежний сповіщувач ИПК-9/1 (Рис. 3.12). Низька ціна, непогані характеристики і якісна його робота – це все, що потрібно для системи безпеки (Табл. 3.15).

Рисунок 3.12 – Тепловий сповіщувач ИПК-9/1

Таблиця 3.15 – Характеристики теплового сповіщувача ИПК-9/1

Характеристика	Параметр
Напруга живлення	12В
Інерційність спрацювання	Не більше 8с
Термін предатності	Не менше 10 років
Номінальна температура спрацьовування	+54...+85 °С
Сертифікат відповідності	Відповідає вимогам пожежної безпеки
Ціна	171 грн

Для реалізації системи пожежної сигналізації був вибраний ручний пожежний сповіщувач СПР «Тірас» (Рис. 3.13). Низька ціна, непогані характеристики і якісна його робота – це все, що потрібно для розробленої системи безпеки (Табл. 3.16).

Рисунок 3.13 – Ручний сповіщувач СПР «Тірас»

Таблиця 3.16 – Характеристики ручного сповіщувача СПР «Тірас»

Характеристика	Параметр
Напруга живлення	8-28В
Діапазон робочих температур	-10°…+55°С
Сигнал тривоги - варіант 1	Збільшення імпедансу
Сигнал тривоги - варіант 2	Зменшення опору
Сигнал тривоги - варіант 3	Розрив лінії ШС
Сигнал тривоги - варіант 4	Блокування лінії ШС діодом
Сертифікат відповідності	Відповідає вимогам пожежної безпеки
Ціна	336 грн

Далі було обрано для проекту звуковий сповіщувач (сирену) Atis LD-95 (Рис. 3.14). Це економний, достатньо функціональний пристрій, який сповістить персонал про пожежу і зробить це швидко і якісно завдяки своїм характеристикам (Табл. 3.17).

Рисунок 3.14 – Сирена Atis LD-95

Таблиця 3.17 – Характеристики сирени Atis LD-95

Характеристика	Параметр
Напруга живлення	12В
Діапазон робочих температур	-30°…+55°С
Інтенсивність звуку	До 100дБ
Типи сигналів	Світло і звук
Ціна	105 грн

Обладнання системи охоронної сигналізації:

Для охоронної сигналізації використано магнітоконтактний сповіщувач SATEL B-4 S (Рис. 3.15). Обраний датчик отримав безліч позитивних відгуків і його характеристики якраз підходять для даного проекту. Плюс хороша якість і невисока вартість (Табл. 3.18).

Рисунок 3.15 – Магнітний сповіщувач SATEL B-4 S

Таблиця 3.18 – Характеристики магнітного сповіщувача SATEL B-4 S

Характеристика	Параметр
Напруга живлення	12В
Ступінь захисту від зовнішніх впливів	Не нижче IP66
Діапазон комутованих напруг	До 100 В
Діапазон комутованих струмів	До 400 мА
Поріг спрацювання	75 - 80 мм
Сертифікат відповідності	Наявний
Додатково	Контроль розтину корпусу
Ціна	697 грн

Також для цієї ж системи був використаний акустичний сповіщувач руху об’єктів і розбиття скла SATEL NAVY (Рис. 3.16). Якісний пристрій, який не тільки добре виконує свою роботу завдяки своїм характеристикам

(Табл. 3.19), а й коштує недорого. Даний сповіщувач було поміщено в приміщення, де потребується більша охорона.

Рисунок 3.16 – Сповіщувач руху і розбиття скла SATEL NAVY

Таблиця 3.19 – Характеристики акустичного сповіщувача SATEL NAVY

Параметр	Характеристика
Напруга живлення	12В
Висота інсталяції	2.4 м
Мінімальна контрольована площа скла	10 $см^2$
Робоча вологість	Не більше 93%
Діапазон робочих температур	-10…+55°С
Сертифікат відповідності	Наявний
Вага	100 г
Перешкодостійкість	Стійкість до акустичних шумів, електростатичних розрядів, перешкод по мережі живлення, впливу електромагнітних полів і захист від тварин вагою до 15 кг
Додатково	Цифрова компенсація температури, контролює рух об’єктів поблизу
Ціна	573 грн

У приміщення, потребуючих меншої захищеності, було вмонтовано об’ємний охоронний пасивний оптико-електронний сповіщувач COLT10DL (датчик руху) (Рис. 3.17). Даний пристрій хоча і не перевершує технічні характеристики SATEL NAVY, але його характеристик цілком достатньо для якісної охорони (Табл. 3.20). І знову ж, по вартісним затратам можна виграти.

Рисунок 3.17 – Датчик руху COLT10DL

Таблиця 3.20 – Характеристики датчика руху COLT10DL

Характеристика	Параметр
Напруга живлення	12В
Дальність дії	10 м
Висота інсталяції	2 - 2,4 м
Діапазон робочих температур	-10…+50°С
Кут зони виявлення	90°
Сертифікат відповідності	Наявна
Додатково	Несприйнятливий до руху тварин масою до 10 кг
Ціна	252 грн

Для керування системою охоронної безпеки був обраний охоронний точковий електроконтактний ручний сповіщувач (ППКОП) Orion NOVA L

(Рис. 3.18). Незважаючи на його високу вартість, його характеристики і робота просто на висоті, так що це гарний вибір для таких задач (Табл. 3.21)[10].

Рисунок 3.18 – ППКОП Orion NOVA L

Таблиця 3.21 – Характеристики ППКОП Orion NOVA L

Характеристика	Параметр
Кількість базових зон	16
Макс. кількість зон в системі	64
Базові виходи	6
Групи	32
Користувачі	64
Клавіатури	8
Виносні пристрої розширення	8

Продовження таблиці 3.21

Інтерфейси	RS-485 (2шт.), mini-USB, Touch Memory
Вихідний струм	850 мА
Протокол зв'язку з ПЦН	NOVA і SUR-GARD
Канали зв'язку	GPRS (2 SIM), Ethernet (з модулем M-NET+), Wi-Fi (з модулем M-WIFI)
АКБ, що підключається	7 або 9 А*г
Розміри	280x280x85 мм
Сертифікат відповідності	Наявна
Ціна	5 442 грн

На основі всіх раніше отриманих обладнань розроблено схему пожежної і охоронної сигналізації (Рис. 3.19 – Рис. 3.20).

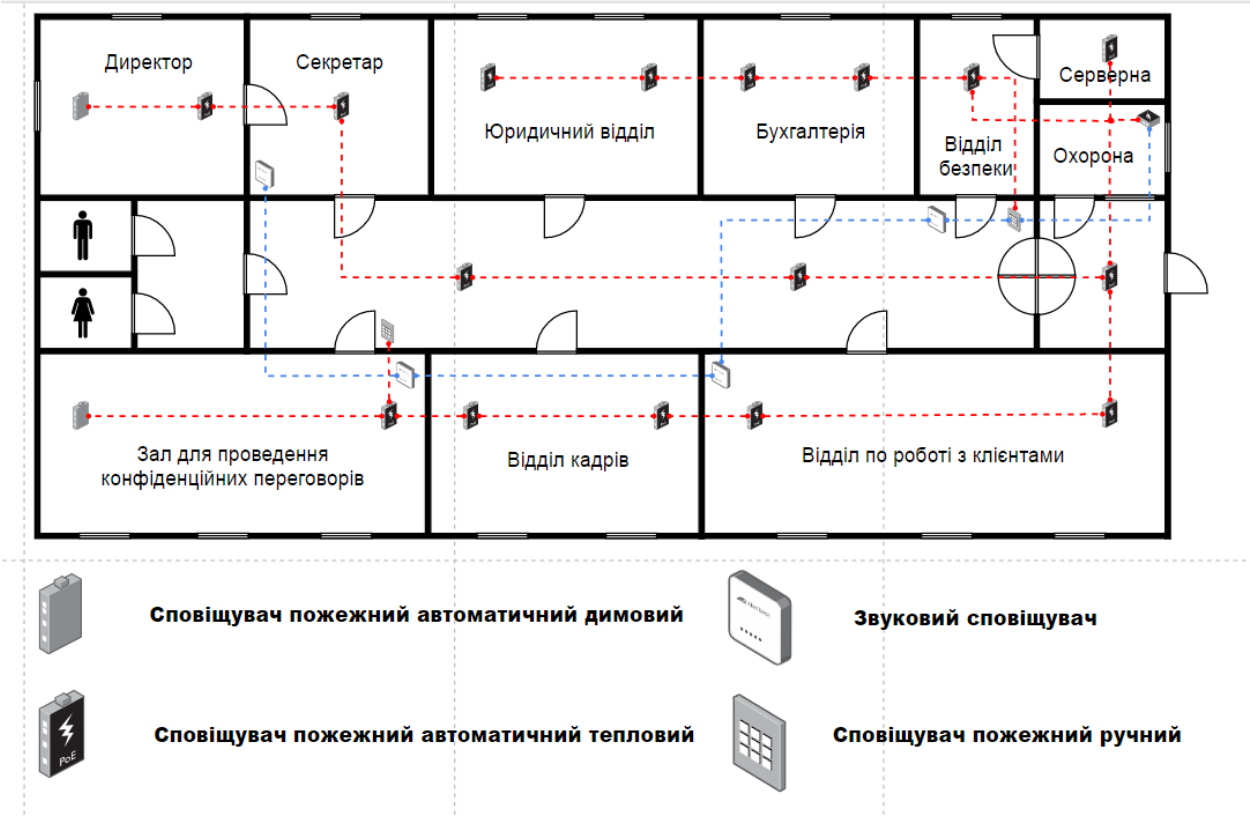


Рисунок 3.19 – Схема пожежної сигналізації

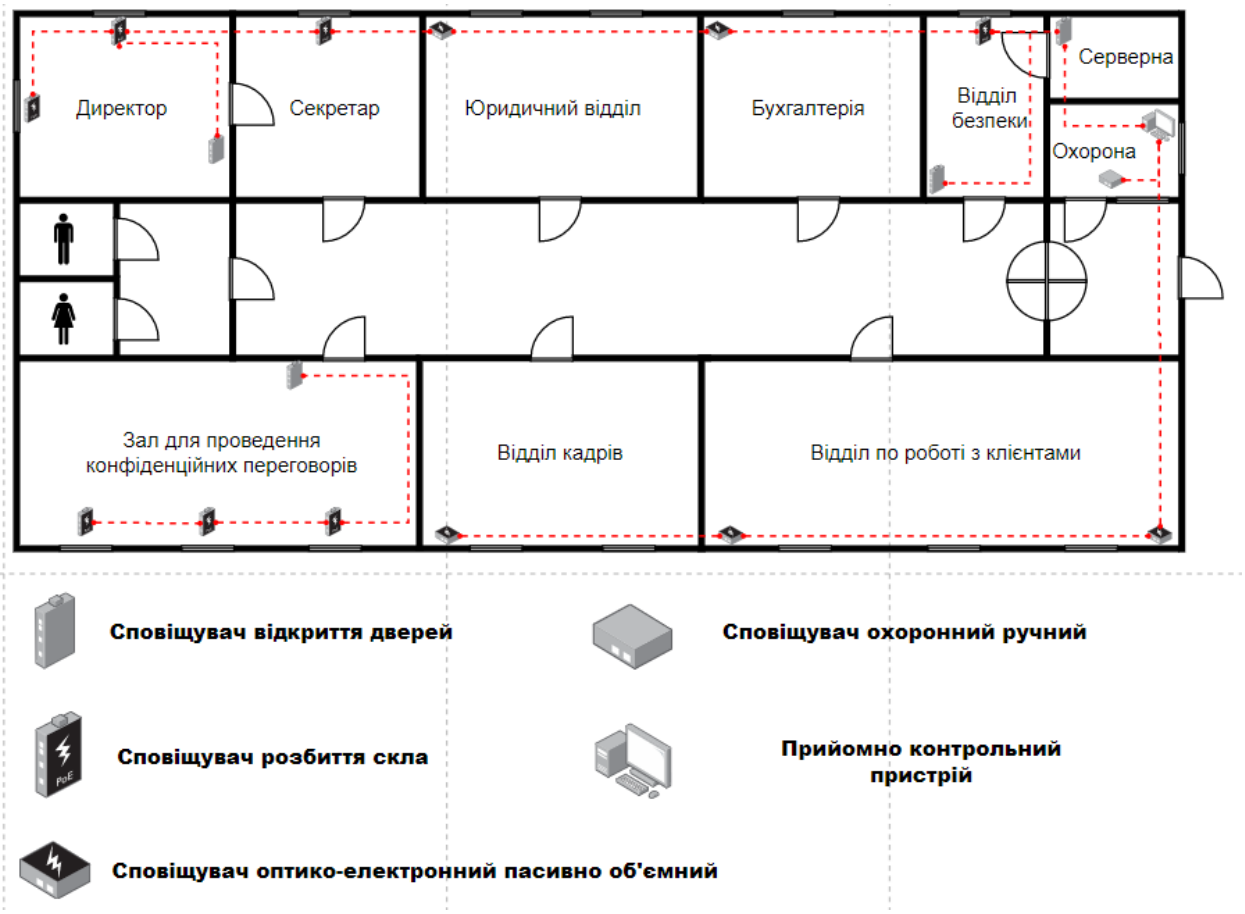


Рисунок 3.20 – Схема охоронної сигналізації

Проведено розрахунок фінансових витрат на обладнання (Табл. 3.22), яке потрібно для реалізації проекту. Як можна побачити, вони не досить великі, адже була вибрана вся техніка гарної якості, а головне – недорога.

Таблиця 3.22 – Фінансові витрати на обладнання

№	Назва приладу	Вартість, грн	Кількість
1	2	3	4
1	Турнікет-трипод ZKTeco TS1000 Pro	21 283	1
2	Вхідні двері Siberia	9 899	1
3	Ручний металодетектор Garrett Super Scanner V	7 056	1

Продовження таблиці 3.22

1	2	3	4
4	Мережевий контролер доступу ZKTeco	7 969	1
5	Мережевий охоронний контролер ZKTeco	3 499	3
6	Мережевий зчитувач EM-Marine ZKTeco	900	5
7	Відеокамера inter Vision IVR-734C	3 250	3
8	Відеокамера Vision Hi-Tech	3 499	3
9	Відео-реєстратор HIKVISION	3 080	1
10	Монітор LG BK550Y	4 899	1
11	Димовий сповіщувач Satel TSD-1	985	2
12	Тепловий сповіщувач ИПК-9/1	171	16
13	Ручний сповіщувач СПР «Тірас»	336	2
14	Сирена Atis LD-95	105	4
15	Магнітний сповіщувач SATEL B-4 S	697	4
16	Сповіщувач руху і розбиття скла SATEL NAVY	573	7
17	Датчик руху COLT10DL	252	5
18	ППКОП Orion NOVA L	5 442	1
19	Інтерфейс сполучення, мишка, системний блок, клавіатура	10 500	1
20	Всі прилади разом	119 229	62

Дана система безпеки спроектована таким чином, що затрати на її реалізацію досить маленькі. Звичайно, можна було спроектувати і на більшу вартість, але немає ніякого сенсу так витрачатись, адже функціонал СКБ буде такий самий як і на запропоновану вартість. Якщо зробити її ще дешевшою, то ми урізаємо її функціонал. Тобто буде гірша якість зйомки, неефективна система охорони і система пожежної безпеки, послаблена інформаційна безпека, а головне – це погана згуртованість всіх систем безпеки. Тому 119 229 гривень – це найоптимальніша вартість для даної СКБ.

3.4. Висновки до розділу

У даному розділі була розроблена комплексна система захисту фірми. При розробці СКБ були враховані особливості організації, такі як її невеликий розмір, але велика кількість оброблюваної конфіденційної інформації. З урахуванням цих особливостей були прийняті наступні рішення:

1. поєднати політику безпеки з політикою інформаційної безпеки і політикою менеджменту безпеки підприємства;
2. використовувати в якості перепусток смарт-карти;
3. використовувати базові постійні пропуску співробітників для доступу до деяких особливо охоронних відділів;
4. делегувати силову охорону об'єкта групі швидкого реагування;
5. поєднати автоматизовану систему, і вжити заходів щодо захисту загальної системи, а також, безліч інших організаційних і конструкторських рішень.

ВИСНОВКИ

В роботі розглянуті принципи захисту побудови охоронних систем різних типів, їх структура, склад, способи взаємодії їх компонентів.

В результаті аналізу існуючих технічних засобів охорони і тенденцій їх розвитку встановлено, що застосування інтегрованих систем безпеки забезпечує ряд переваг в порівнянні з використанням простої сукупності окремих систем і засобів захисту. Запропоновано структуру інтегрованої охоронної системи на основі локальної комп'ютерної мережі. Таке рішення дозволяє поєднувати існуючі мережеві рішення з традиційними моделями охоронних систем. Інтеграція в систему технічних засобів охорони (ПК-сумісні охоронні сповіщувачі або приймально-контрольні прилади)

В результаті виконання роботи отримані наступні практичні результати:

- Узагальнення всіх можливих загроз;
- Розглянуто сучасні СБ;
- Спроектовано КСБ фінансової фірми і розраховано затрати на придбання всього необхідного обладнання.

Запропонована в роботі інтегрована охоронна система, при максимальному використанні техніки і комунікацій, що існують на об'єкті, що охороняється, надає безпеку, що відповідає необхідним для підприємства вимогам, система може бути рекомендована до використання і на інших підприємствах, де безпека є одним з необхідних елементів діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Програмно-апаратні засоби забезпечення інформаційної безпеки. Захист в операційних системах: Посібник для вузів / Проскурін В.Г., Крутов С.В., Мацкевич І.В. - М .: Радіо та зв’язок, 2000. - 168 с.

2. Стандарт безпеки. Скородумов Б. Л., Іванов В. М.. 2001.

3. Пристрої для захисту об'єктів та інформації, Довідковий посібник. Андріанов В. И., Соколов А. В. 2-ге вид., 2000. - 256 с.

4. Системи відеоспостереження. Основні вимоги до систем відеоспостереження [Електронний ресурс]: – Режим доступу: http://www.tvgarant.ru/text12.

5. Мережеві системи контролю і управління доступом "Системи безпеки, зв'язку та телекомунікацій" Крахмальов А. К., N2 23, 1987.

6. Засоби і системи контролю і управління доступом. Класифікація. Загальні технічні вимоги. методи випробувань. В.И. Андріанов, А.В. Соколов 2008.

7. Технічні засоби безпеки. Частина 1. Охоронна і охоронно-пожежна сигналізація. Системи відео-контролю. Системи контролю і управління доступом. Кірюхіна Т.Г., Членів А.Н.. НОУ "Такір", 2002 - 216 с.

8. Технічні основи охорони фірми - «Світ зв’язку. Connect.» N2 Малянов В.Н., 2001. - 4с.

9. Системи безпеки Bolid. Інтегрована система охорони «Оріон» [Електронний ресурс]: - Режим доступу: http://bolid.ru/production/orion/

10. Інтернет-магазин «Розетка»: доступ до [Електронний ресурс]: – Режим доступу: https://rozetka.com.ua/promo/birthdayparty/.

ДОДАТОК А

ANALYSIS OF POTENTIAL THREATS AND SECURITY OF THE FINANCIAL INSTITUTION

Classification of possible threats of a financial institution

The built AS must provide protection against all types of threats, otherwise a "hole" is formed in the protection, so it is necessary to list all possible threats to maximize the protection issue. There is no single and generally accepted classification of security threats to the AS. However, these threats can be classified from various aspects of their implementation, the method of their implementation and the object of attack.

Classification of threats by purpose:

- unauthorized reading of information, unauthorized changes in information, unauthorized destruction of information;
- complete or partial destruction of the operating system (the destruction of the operating system means a set of destructive effects from short-term failure ("hanging") of individual software modules of the system to physical erasure from the disk of system files).

Classification of threats according to the principle:

- use of known (legal) channels for obtaining information, for example, the threat of unauthorized reading of a file, access to which is incorrectly defined;
- allowed access to a user who, in accordance with an adequate security policy, should be denied access;
- use of covert channels to obtain information, for example: the threat of an attacker using undocumented all the features of the operating system;
- creating new channels for obtaining information using software bookmarks.

Classification of threats by the nature of the impact:

- active influence;
- unauthorized actions of the attacker in the system;

- passive influence;
- unauthorized monitoring of the attacker on the processes occurring in the system.

Classification of threats such as the security vulnerability used by the attacker:

- inadequate security policies, including system administrator errors;
- errors and undocumented capabilities of the operating system software, including so-called hatches;
- accidentally or intentionally built into the system "service entrances" that allow protection of the security system. Usually people create software developers for teaching and adaptation, and other developers forbid them to remove or leave specifically;
- previously implemented software bookmark.

Classification of threats according to the method of impact on the object of attack:

- direct impact;
- the user exceeds his authority, work on behalf of another user;
- use of the results of another user's work (for example, unauthorized interception of information flows initiated by another user).

Classification of threats by the method of action of the attacker (violator):

- in interactive mode (manually);
- in batch mode (using a specially written program that has a negative impact on the operating system without the direct participation of the user-violator).

Classification of threats by object of attack:

- operating system as a whole;
- operating system objects (files, devices, etc.);
- operating system entities (users, system processes, etc.);
- data transmission channels.

Classification of threats by means of attack used:

- regular means of the operating system without the use of additional software; third-party software (this class of software includes both computer viruses and other malicious programs (exploits) that are easy to find on the Internet, and software originally designed for other purposes: debuggers, network monitors and scanners, etc.);
- specially designed software.

Classification of threats to the object of the operating system at the time of the attack:

- storage;
- transfer;
- processing.

Classification of physical threats:

- destruction or destruction of information processing and communication facilities;
- theft of media;
- theft of software or hardware keys and means of cryptographic data protection;
- impact on staff;

Classification of electronic threats:

- introduction of electronic devices for interception of information in technical means and premises;
- interception, decryption, substitution and destruction of information in communication channels.

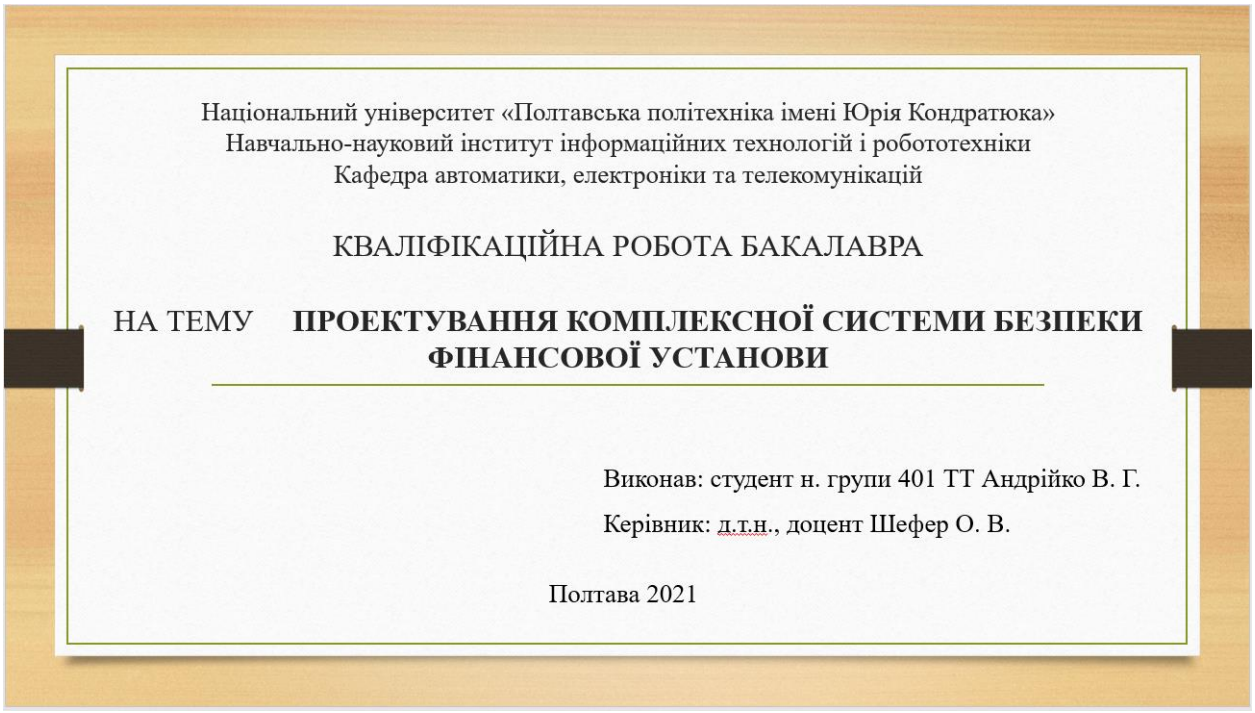
Conclusion to the section and setting designing tasks

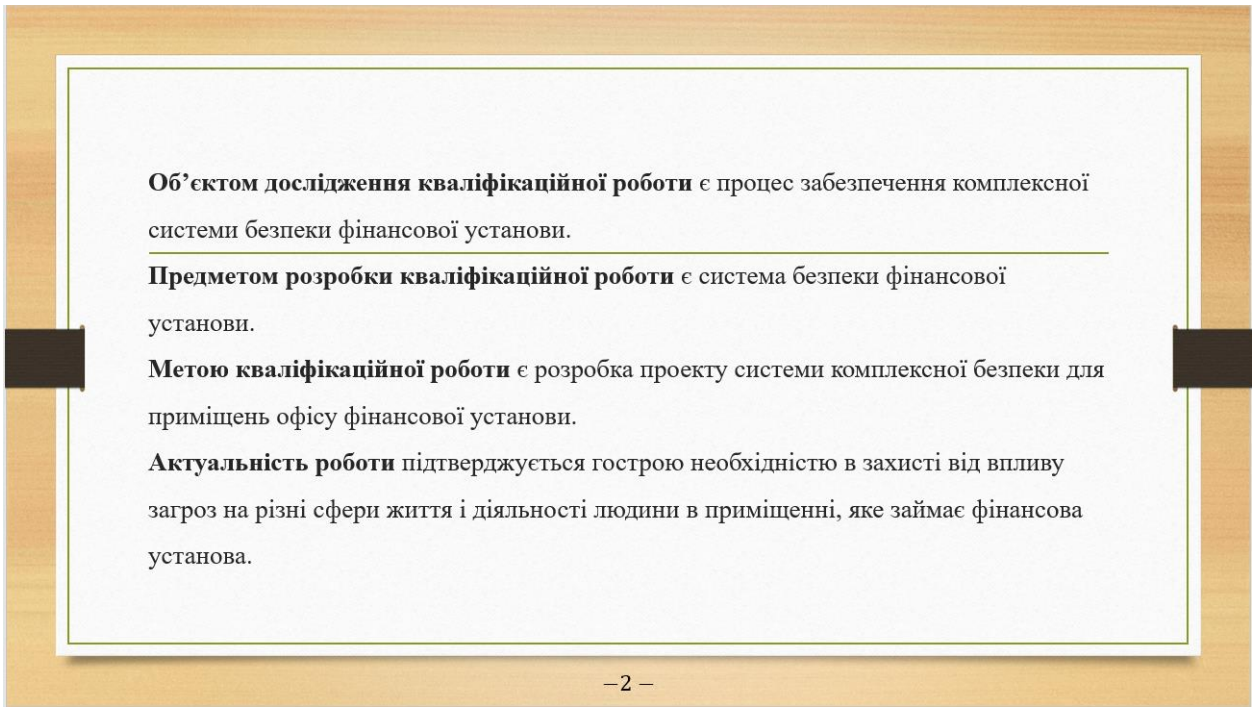
On the basis of the specified dangers ISS is formed, the set task is solved. To ensure security, ISS protects against the full range of possible threats and attackers. The main weakness and the main threat to security is the human factor.

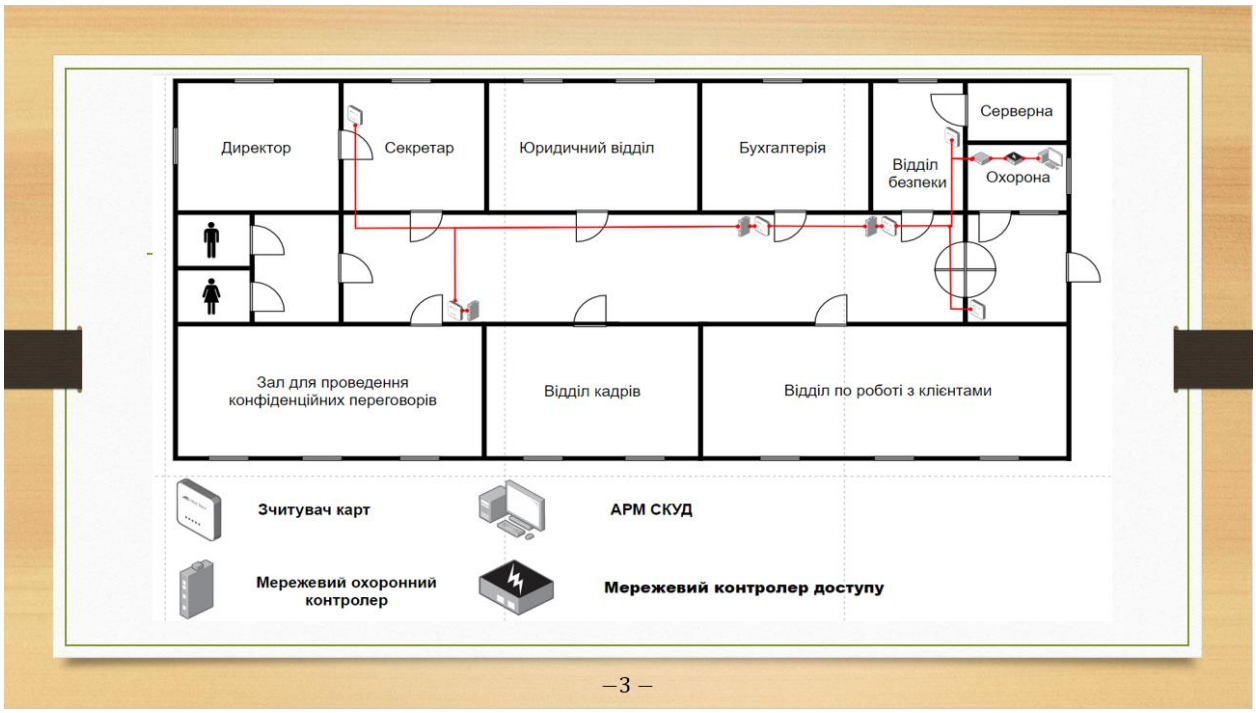
The construction of the ISS should be guided by the basic principles of protection: system, complexity, continuity of protection, reasonable sufficiency, flexibility of management and application, openness of algorithms and mechanisms of protection and ease of application of protective measures and means.

ДОДАТОК Б

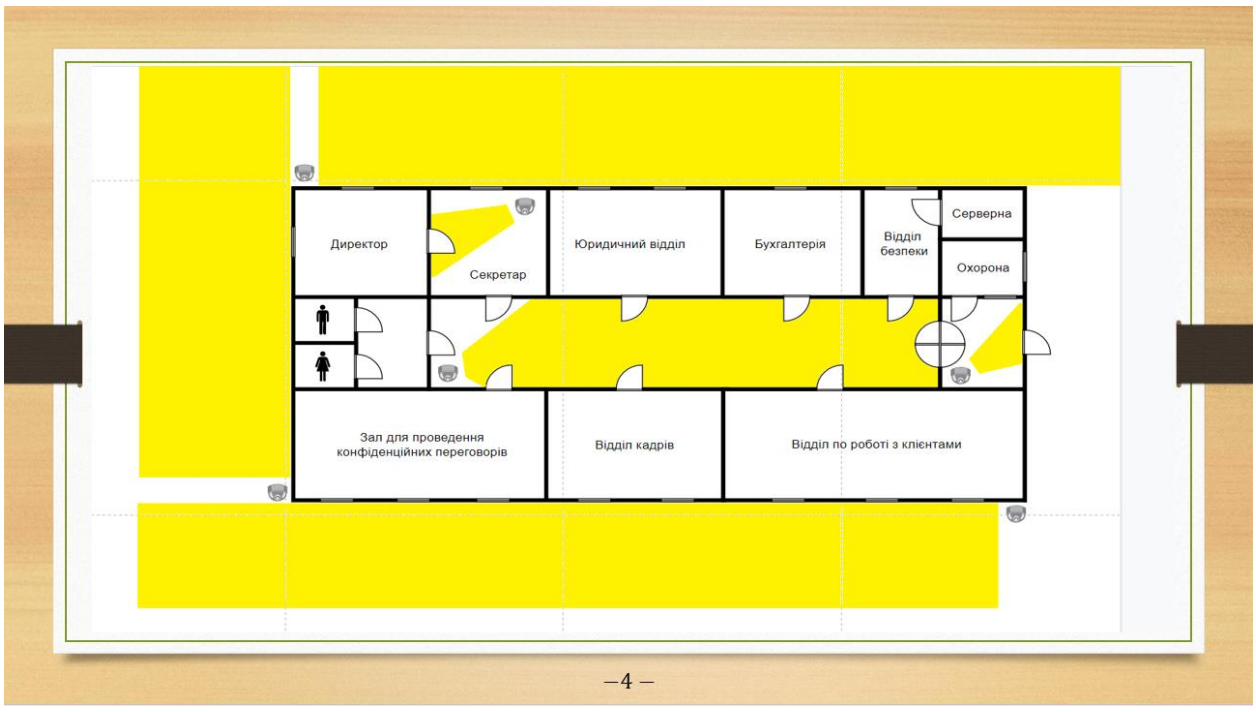
Презентація до роботи:



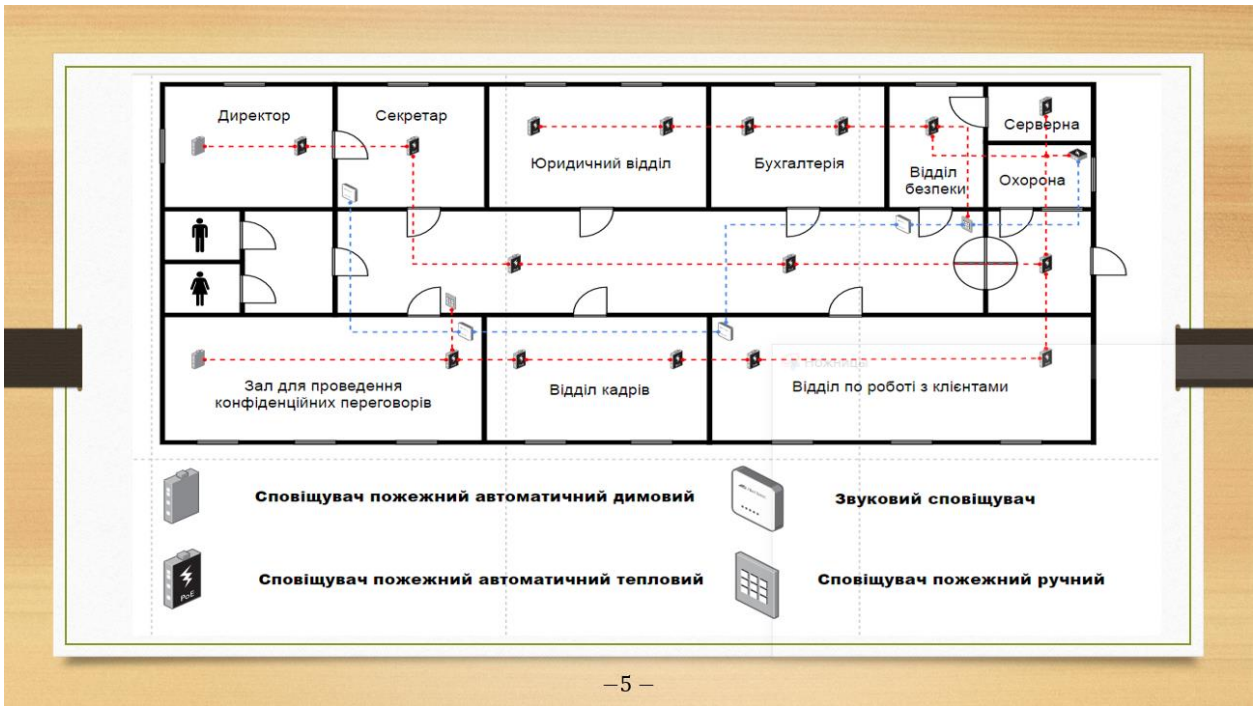



Директор
Секретар
Юридичний відділ
Бухгалтерія
Відділ безпеки
Серверна
Охорона
Зал для проведення конфіденційних переговорів
Відділ кадрів
Відділ по роботі з клієнтами
Зчитувач карт
АРМ СКУД
Мережевий охоронний контролер
Мережевий контролер доступу

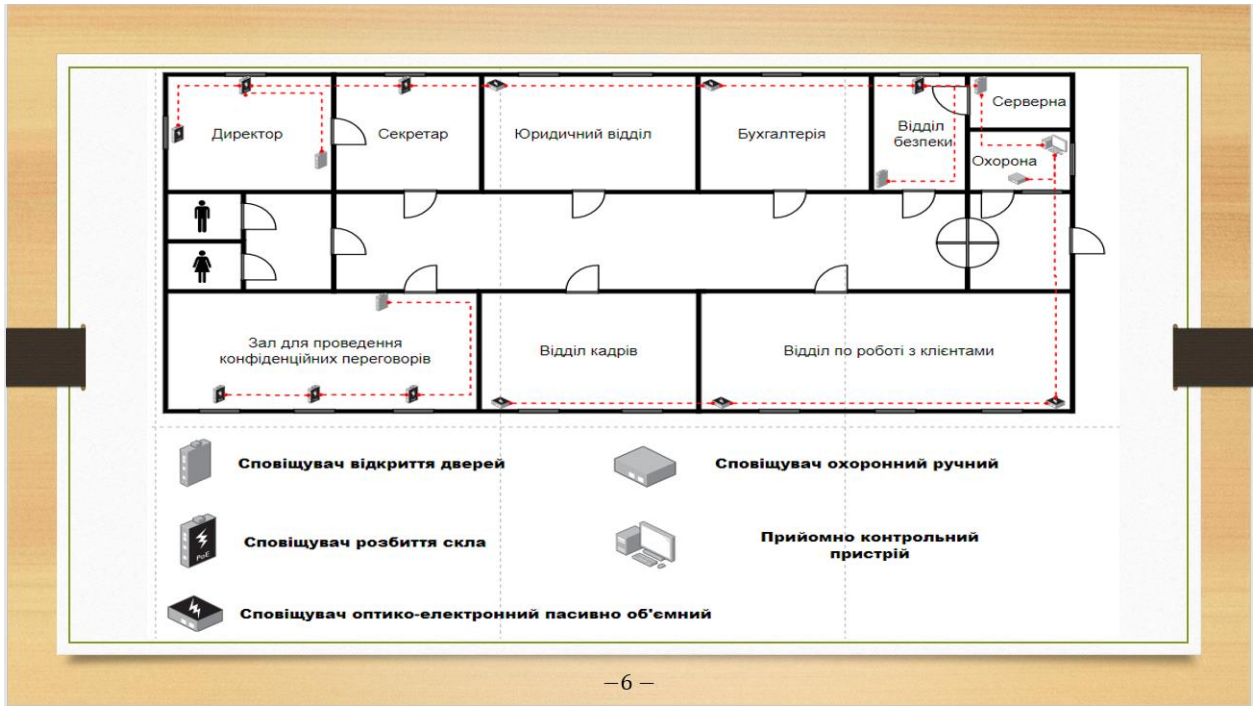
–3 –


Директор
Секретар
Юридичний відділ
Бухгалтерія
Відділ безпеки
Серверна
Охорона
Зал для проведення конфіденційних переговорів
Відділ кадрів
Відділ по роботі з клієнтами

–4 –


Директор
Секретар
Юридичний відділ
Бухгалтерія
Відділ безпеки
Серверна
Охорона
Зал для проведення конфіденційних переговорів
Відділ кадрів
Відділ по роботі з клієнтами
Сповіщувач пожежний автоматичний димовий
Звуковий сповіщувач
Сповіщувач пожежний автоматичний тепловий
Сповіщувач пожежний ручний

–5 –


Директор
Секретар
Юридичний відділ
Бухгалтерія
Відділ безпеки
Серверна
Охорона
Зал для проведення конфіденційних переговорів
Відділ кадрів
Відділ по роботі з клієнтами
Сповіщувач відкриття дверей
Сповіщувач охоронний ручний
Сповіщувач розбиття скла
Прийомно контрольний пристрій
Сповіщувач оптико-електронний пасивно об'ємний

–6 –

Фінансові витрати на обладнання

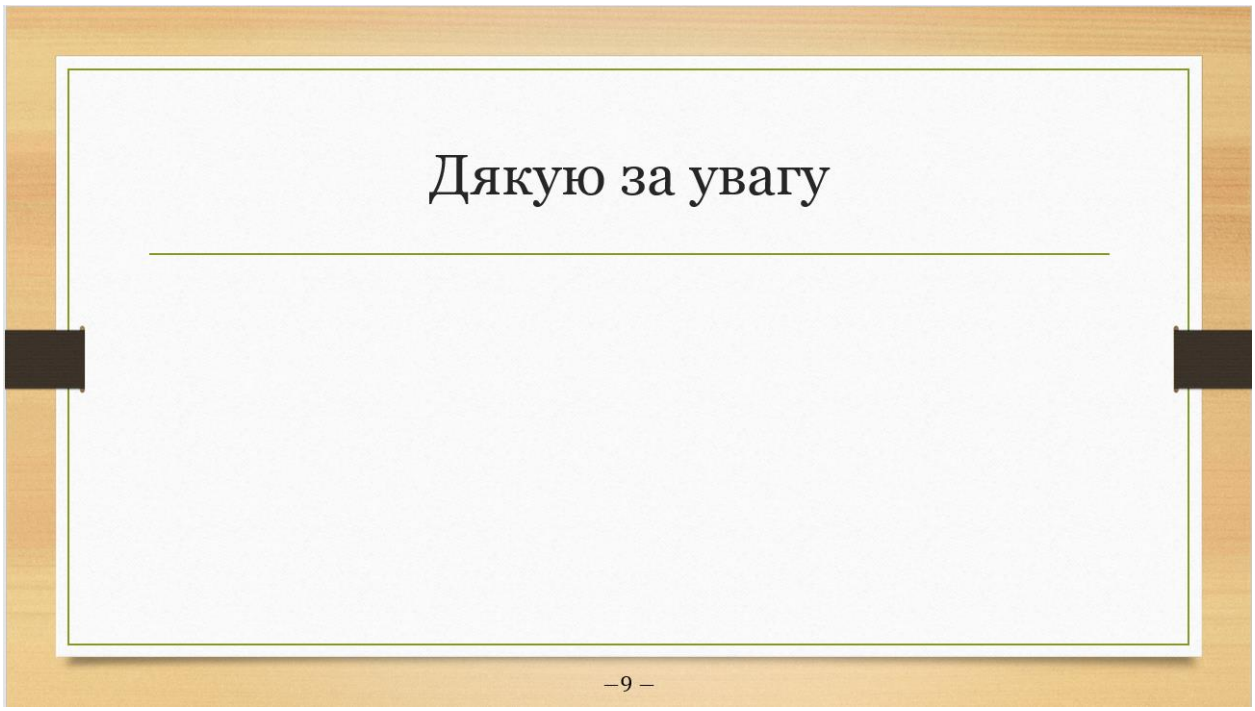
№	Назва приладу	Вартість, грн	Кількість	№	Назва приладу	Вартість, грн	Кількість
1	Турнікет-трипод ZKTeco TS1000 Pro	21 283	1	11	Димовий сповіщувач Satel TSD-1	985	2
2	Вхідні двері Siberia	9 899	1	12	Тепловий сповіщувач ИПК-9/1	171	16
3	Ручний металодетектор Garrett Super Scanner V	7 056	1	13	Ручний сповіщувач СПР «Тірас»	336	2
4	Мережевий контролер доступу ZKTeco	7 969	1	14	Сирена Atis LD-95	105	4
5	Мережевий охоронний контролер ZKTeco	3 499	3	15	Магнітний сповіщувач SATEL B-4 S	697	4
6	Мережевий зчитувач EM-Marine ZKTeco	900	5	16	Сповіщувач руху і розбиття скла SATEL NAVY	573	7
7	Відеокамера inter Vision IVR-734C	3 250	3	17	Датчик руху COLT10DL	252	5
8	Відеокамера Vision Hi-Tech	3 499	3	18	ППКОП Orion NOVA L	5 442	1
9	Відео-реєстратор HIKVISION	3 080	1	19	Інтерфейс сполучення, мишка, системний блок, клавіатура	10 500	1
10	Монітор LG BK550Y	4 899	1	20	Всі прилади разом	119 229	62

–7 –

Висновки

- Спроектована комплексна система безпеки фінансової установи
- Розраховані затрати на придбання всього необхідного обладнання

–8 –


Дякую за увагу
– 9 –