МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітньо-професійна програма: «Безпека комп'ютерних систем і мереж»

Група: 4КБ-02

Дипломний проект

здобувача освіти денної форми навчання
КБ.02.09.000.ДП

КОНДРАТЮКА ДЕНИСА В'ЯЧЕСЛАВОВИЧА

м. Одеса
2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітньо-професійна програма: «**Безпека комп'ютерних систем і мереж»**

Група: **4КБ-02**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту на тему:

Проектування комплексної системи безпеки підприємства на основі обладнання Hikvision

Проектний матеріал складається з пояснювальної записки на 77 сторінках та графічного (презентаційного) матеріалу на 17 аркушах (слайдах)

Дипломник _____ (Кондратюк Д.В.)

Керівник _____ (Стайкуца С.В.)

Консультанти:

з економічного розділу_____ (Канський М.Ю.)

з розділу охорони праці та техніки безпеки_____ (Чорновол Н.І.)

з нормоконтролю _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Голова циклової комісії _____ (Кривченко Ю.В.)

Завідувач відділення _____ (Краснокутська К.Г.)

Захист «28» червня 2025 р. Протокол ЕК № 7

Оцінка ЕК 4 (добре) / 75 б

Секретар ЕК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *комп'ютерних систем* Комісія *КТ та ПІ*

Спеціальність *123 «Комп'ютерна інженерія»*

Освітньо-професійна програма *«Безпека комп'ютерних систем і мереж»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР _____

Беркань І.В.

"09" 05 2025 р.

ЗАВДАННЯ

на дипломний проект

Здобувачеві (здобувачці) освіти *Кондратюку Денису В'ячеславовичу*

(прізвище, ім'я, по батькові)

1. Тема проекту *Проектування комплексної системи безпеки на основі обладнання Hikvision*

затверджена наказом по коледжу від "14" листопада 2025 р. № 246

2. Термін здачі закінченого проекту _____

3. Вихідні данні до проекту (роботи) *1. Комплексні системи безпеки; 2. Системи відеоспостереження; 3. Системи контролю та управління доступом; 4. Охоронна сигналізація; 5. Ринок комплексних систем безпеки України; 6. Розробити технічне завдання на проектування комплексної системи безпеки; 7. Представити результати роботи на план схемі об'єкту..*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Історія появи комплексних систем безпеки; Загальні принципи роботи систем відеоспостереження; Поняття СКУД; Компонентний скла та типи СКУД; Рубежі захисту охоронних систем; Порівняння технологічних рішень брендів обладнання для реалізації проекту;Популярні виробники обладнання на ринку України; Формування технічного завдання; Проектування комплексної системи безпеки; Опис обладнання проекту

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Теорія візуального спостереження; Види систем відеоспостереження та їх компоненти; Відеоаналітика; Системи контролю та управління доступом; Типи порталів контролю доступу; Елементи контролю доступу; Охоронна сигналізація; Компонентний склад системи охорони; Загальний стан ринку безпеки України; Порівняння ключових характеристик обладнання; Висновки порівняльного аналізу; Технічне завдання на проектування комплексної системи безпеки; Спроектована комплексна система безпеки на основі Hikvision; Висновки

6. Консультанти по проекту (роботі), із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Основний розділ	*Стайкуца С.В.*		
Економічний розділ	*Канський М.Ю.*		
Розділ охорони праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання 29.04.25р.

Керівник _____ *Стайкуца С.В.*
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1.	*Вступ. Історія комплексних систем безпеки*	*14.05.2025*	Виконано
2.	*Системи відеоспостереження*	*17.05.2025*	Виконано
3.	*Види систем відеоспостереження та їх компоненти*	*20.05.2025*	Виконано
4.	*Системи контролю та управління доступом, компоненти та склад СКУД.*	*22.05.2025*	Виконано
5.	*Охоронна сигналізація*	*01.06.2025*	Виконано
6.	*Рубежі захисту, компоненти та особливості проектування охоронної сигналізації*	*03.06.2025*	Виконано
7.	*Популярні виробники обладнання та їх технологічнірішення*	*06.06.2025*	Виконано
8.	*Складання технічного завдання на проектування*	*10.06.2025*	Виконано
9.	*Обладнання проекту*	*11.06.2025*	Виконано
10.	*Аналіз роботи комплексної системи безпеки*	*12.06.2025*	Виконано
11.	*Виконання економічних розрахунків*	*13.06.2025*	Виконано
12.	*Розробка заходів з охорони праці*	*14.06.2025*	Виконано
13.	*Виконання графічної частини проекту*	*16.06.2025*	Виконано

Дипломник _____
(підпис)

Керівник _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			КБ 02. 09 000. 00 ДП	Дипломний проект		
А4			КБ 02. 09 000. 00 ДП ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	КБ 02. 09 000. 00 ДП		
Розробив		Кондратюк Д.В.			Проектування комплексної системи безпеки підприємства на основі обладнання Hikvision	Літ.	Аркуш 3 / Аркушів 77
Перевірив		Стайкуца С.В.				Н Д П	
Н. Контр.		Петрашова В.І.		16.06.25		ВСП "ОТФК ОНТУ" гр.4КБ-02	
Затверд.		Кривченко Ю.В.		18.06			

ЗМІСТ

ВСТУП

У сучасному світі питання безпеки об’єктів критичної інфраструктури, підприємств, офісів та приватних володінь набуло особливої актуальності. Зростання рівня загроз – від крадіжок до спроб несанкціонованого доступу до інформаційних або фізичних ресурсів – потребує застосування ефективних технічних рішень для захисту об’єктів. Одним із ключових напрямів забезпечення фізичної безпеки є впровадження комплексних систем безпеки, що поєднують в собі відеоспостереження, системи охоронної сигналізації та контролю доступу.

Історичний розвиток технологій безпеки демонструє еволюцію від простих механічних та аналогових рішень до багатофункціональних, цифрових і мережевих систем, що інтегрують у собі елементи автоматизації, аналітики та штучного інтелекту. Сучасні системи безпеки мають не лише реагувати на події, а й активно запобігати загрозам, проводити аналіз ситуацій у реальному часі та взаємодіяти з іншими технічними підсистемами підприємства.

У даній дипломній роботі розглядається побудова комплексної системи безпеки для підприємства, що займається обслуговуванням систем фізичного захисту. Основна мета проєкту – проектування ефективної та масштабованої інтегрованої системи, що охоплює підсистеми охоронної сигналізації, системи контролю та управління доступом (СКУД), а також сучасного цифрового відеоспостереження на основі IP-технологій.

Результатом дипломної роботи є структуровано обґрунтований підхід до впровадження сучасної системи безпеки на основі перевірених рішень і технологій, що дозволяє забезпечити високий рівень захисту персоналу, ресурсів та інфраструктури підприємства.

1 ОСНОВНИЙ РОЗДІЛ

1.1 Історія комплексних систем безпеки

Мандруючи історією електронних систем безпеки, зверніть особливу увагу на еволюцію систем сигналізації та контролю доступу, адже саме в нездатності цієї галузі адаптуватися до нових технологій було закладено насіння сьогоднішніх і завтрашніх систем.

Спочатку були системи сигналізації. У 1851 році в Бостоні була встановлена перша система сигналізації телеграфного типу McCulloh loop. Ці системи посилали струм силою 20 міліампер по петлі дроту і відстежували силу струму в дроті. Якщо струм змінювався, це призводило до зміни стану реле або переміщення пера на паперовій стрічці, надсилаючи закодоване повідомлення. Вони також широко використовувалися в поліції та пожежних частинах.

Перші домофонні системи датуються 1940-ми роками. Перші картки контролю доступу з магнітною смугою з'явилися в 1960-х роках.

У 1961 році лондонська поліція почала використовувати системи відеоспостереження (CCTV) для контролю за діяльністю на залізничних станціях. Все це були дискретні, індивідуальні системи. Наприклад, не було перемикачів камер, але кожна камера підключалася до окремого монітора. Відеозапис не проводився, оскільки це було занадто дорого. Запис тривог здійснювався за допомогою ручних нотаток. Ідея полягала в тому, щоб бути в курсі проблем зі злочинністю, стримувати злочинців і допомагати тим, хто цього потребує.

Це було перше покоління електронних систем безпеки. За сьогоднішніми мірками, це були дуже базові системи. Перше покоління систем контролю доступу все ще використовується сьогодні у вигляді однодверних готельних карткових систем (рис. 1.1)

У першому поколінні технологій безпеки системи відеоспостереження та домофони були рідкістю. Системи відеоспостереження в основному обмежувалися однією камерою, зображення з якої виводилося на один монітор.

У тих небагатьох системах, які мали більше однієї камери, зазвичай для кожної камери використовувався окремий монітор. Там, де домофони взагалі використовувалися, вони, як правило, або встановлювалися на замовлення, або були розширенням бізнес-домофонів.

Рисунок 1.1. Зчитувач карток першого покоління

Друге покоління систем контролю доступу об'єднувало вісім зчитувачів карток у мережу зі спеціальним комп'ютером, який був приблизно розміром з величезний ранній електронний настільний калькулятор (рис. 1.2)

Рисунок 1.2. Карткова система доступу другого покоління

Зазвичай він мав пару клавіатур, дисплей з трубкою ніксі та паперову стрічку завдовжки 3 дюйми. Коли людина підносила картку до вхідних дверей установи, можна було почути, як дзижчить паперова стрічка, а ніксі-трубки показували щось на кшталт 1CO3-AG. Потім людина зверталася до книги, яка вказувала, що картці CO3 було надано доступ до дверей.

Друге покоління сигналізацій замінило складні для читання лічильники і паперові стрічки кольоровими лампами і звуковим сигналом (рис. 1.3).

Рисунок 1.3. Сигналізація другого покоління

Кожна сигналізація мала три кольорові лампи - зелену для безпеки, червону для тривоги і жовту, коли її обходили. Був перемикач для обходу сигналізації. Друге покоління почалося приблизно в 1945 році і триває до сьогодні.

Системи відеоспостереження все ще мало використовувалися, але системи внутрішнього зв'язку ставали дещо більш-менш зрозумілими.

Третє покоління почалося в 1968 році і тривало приблизно до 1978 року. Системи третього покоління об'єднували сигналізацію та контроль доступу в одній системі. До 64 зчитувачів карток і до 256 точок тривоги підключалися окремо до міні-комп'ютера PDP-8 або IBM Series 1 з оперативною пам'яттю, терміналом «beehive» і лінійним принтером. Базова система на 16 зчитувачів карток могла коштувати понад 100 000 доларів. У цей час системи відеоспостереження почали використовуватися корпораціями, а також з'явилося кілька прикладів систем внутрішнього зв'язку.

Рисунок 1.4. Система сигналізації та контролю доступу третього покоління

У 1971 році Intel представила перший 4-розрядний мікропроцесор 4044, розроблений дизайнером Тедом Хоффом (Ted Hoff) для японської компанії з виробництва калькуляторів. Процесор мав понад 2300 транзисторів - більше, ніж у ENIAC, який займав цілу кімнату і вимагав спеціальної системи кондиціонування тільки для комп'ютера. Невдовзі з'явилися 8-розрядні мікропроцесори 6502 та 8088. Вони стали основою для нового покоління технологій систем сигналізації та контролю доступу, які отримали назву систем розподілених контролерів.

До 1974 року кожен польовий пристрій сигналізації та контролю доступу окремо підключався до міні-комп'ютера, де плутанина проводів підключалася до спеціально виготовлених друкованих плат. Всі ці дроти були дорогими і часто непідйомними для більшості організацій.

У 1974 році з'явилася одна з перших систем сигналізації та контролю доступу на базі мікрокомп'ютерів з розподіленим контролером (компанія Cardkey). Вона вперше дала можливість мультиплексувати сигнали тривоги та

зчитувачі карток на контролерні та мережеві панелі в розподілену систему. Це була радикальна зміна.

Нарешті, вартість кабелів, яка була основною статтею витрат у ранніх системах, була різко знижена. Найперші системи четвертого покоління все ще об'єднували всі ці контролери в центральний міні-комп'ютер, комп'ютерний термінал і лінійний принтер (рання система Cardkey 2000). Комп'ютери часто мали інтерфейс, який називали «користувацьким». Коли людина підносила картку до вхідних дверей, термінал все одно слухняно показував щось на кшталт «1CO3-AG», а лінійний принтер балакав те саме повідомлення. Консьєрж шукав цей код у книжці. Корпорації почали ширше використовувати домофони та системи відеоспостереження, хоча ціни на них все ще були непомірно високими для більшості користувачів, а базові камери коштували до 1200 доларів за штуку.

У цей період також відбулися значні досягнення у сфері відеоспостереження. Вперше стало можливим використовувати лише кілька відеомоніторів для перегляду багатьох камер, тому що камери нарешті стали перетворюватися на послідовні перемикачі, які послідовно перемикали зображення з камери на камеру. По мірі розвитку галузі, витрати різко знизилися, а системи стали набагато зручнішими для користувачів.

Системи відеоспостереження зазнали значного прогресу. По-перше, поява побутових відеомагнітофонів допомогла знизити ціну зберігання відео до практичного рівня. На початку 1990-х років відео мультиплексували, розбиваючи 30 кадрів на секунду, які використовував відеомагнітофон, між різними камерами так, щоб кожна камера записувала зображення два або більше разів на секунду на одну касету. Це дозволило ще більше заощадити на зберіганні відео.

У цей час в індустрії систем сигналізації та контролю доступу міні-комп'ютери поступилися місцем персональним комп'ютерам і мережевим системам на базі серверів. Відставали від них домофонні технології, для яких не існувало єдиного галузевого стандарту і була низька сумісність між виробниками, а об'єднувати будівлі або об'єкти в мережу було складно. У

більшості систем інтерком використовувався мінімально, як правило, для полегшення доступу до віддалених воріт і дверей.

Однак до середини 1990-х років виробники зрозуміли, що організації хочуть інтегрувати різні системи, і почали об'єднувати сигналізацію, контроль доступу, відеоспостереження та домофони у справді інтегровані системи. Ці системи могли виявляти вторгнення, автоматично викликати відповідну відеокамеру для перегляду місця тривоги, а якщо поблизу знаходився домофон, вони могли іноді ставити його в чергу на відповідь. Вони також відображали не лише відео, але й карту, що показувала місце тривоги, щоб допомогти оператору пульта краще зрозуміти, що він або вона бачить на відеомоніторі. Це була перша спроба того, що пізніше стало відомим як комплексна система безпеки.

Ці системи були здатні виявляти і реагувати в режимі реального часу на події, що виникають у сфері безпеки. Однак інтерфейси систем були дуже пропрієтарними і незграбними. Досягнення зв’язку між будь-якими двома брендами і моделями систем, як правило, не поширювалося на інші бренди і моделі. Кожного разу, коли була потрібна інтеграція, це завжди була інша технологія.

Проблема систем сигналізації та контролю доступу полягала в тому, що їхні виробники думали, що вони виробляють системи сигналізації та контролю доступу. Насправді вони виробляли програмовані логічні контролери (ПЛК), які були оснащені базою даних систем сигналізації та контролю доступу.

Це важлива відмінність, тому що, не розуміючи цього, вони чіплялися за архітектуру EPROM. Хоча ПЗП вирішували ранні проблеми галузі, пов'язані з високою вартістю пам'яті, в міру того, як вартість пам'яті падала, галузь обмежувала свої системи тими функціями, які її дизайнери уявляли собі для кожної коробки і реалізовували в ПЗП в коробці контролера. Однак корпоративні та державні клієнти мали особливі потреби, які можна було задовольнити лише шляхом внесення змін до логічної структури контролера. Наприклад, якщо клієнту була потрібна локальна сигналізація, яка б спрацьовувала на дверях, якщо вони залишалися відчиненими занадто довго вдень, але він хотів, щоб ці

двері спрацьовували на пульті відразу після закінчення робочого дня, йому продавали блок адаптера, який виконував цю функцію для кожних дверей. Більшість виробників відреагували на такі потреби, створивши довгий список адаптерних плат і коробок, щоб їхні системи могли задовольнити кожну унікальну потребу. Для тих виробників, які не випускали великий асортимент цих продуктів, існували сторонні виробники, які це робили.

Ця стратегія добре служила виробничій спільноті, але не дуже добре служила клієнтам через додаткове апаратне забезпечення та спеціальне обладнання, необхідне для виконання абсолютно логічних функцій, потрібних середньостатистичному клієнту. Наприклад, якщо клієнт хотів отримати підтвердження тривог на периметрі від двох систем виявлення (потрібно, щоб обидві спрацювали, щоб викликати тривогу, але кожна окремо, щоб підтвердити тривогу), більшість систем четвертого покоління вимагали, щоб кожна система виявлення мала власні входи (забезпечуючи тривогу - функцію «або»). Тоді система відображала б стан цих входів на вихідних реле, які потім були б з'єднані між собою для створення функцій «і», а ці з'єднані виходи були б підключені до додаткових входів як тривоги функції «і».

Це може здатися складним завданням, але для систем периметра, що складаються з 50 або більше зон виявлення в кожній системі виявлення, вартість дротових кабелів і проводки часто на тисячі доларів перевищувала вартість системи на базі ПЛК.

Однак деякі експерти галузі зрозуміли, що не існує жодної функції, яку бажає виконати клієнт, і яку не можна виконати за допомогою простішої, а не складнішої архітектури системи. Кожну функцію, яку тільки можна собі уявити, можна виконати за допомогою простої комбінації входів, виходів, пам'яті, логічних елементів, лічильників і таймерів.

Ця структура визначає архітектуру ПЛК. Кілька виробників представили системи сигналізації та контролю доступу на основі ПЛК, особливо ті, хто випускав системи автоматизації будівель (САБ), які вже були засновані на архітектурі ПЛК. Однак ці продукти ніколи не мали значного впливу на ринку,

оскільки виробники продовжували зосереджувати свої маркетингові зусилля на своїх лінійках продуктів САБ, а не на продуктах систем контролю доступу.

Ключовою особливістю систем сигналізації та контролю доступу п'ятого покоління є те, що всі вони базуються на повністю програмних функціях, тоді як попередні системи базувалися на функціях, які були визначені в апаратному забезпеченні. Однак наприкінці 1980-х і 1990-х років галузь була підштовхнута до інтеграції декількох будівель і об'єктів. Галузь боролася з різноманітними невдалими системними архітектурами, поки поступово не перейшла на мережеву інфраструктуру, яка вже існувала в більшості підприємств - локальну мережу (LAN), муніципальну мережу (MAN) та архітектуру Ethernet для глобальних мереж (WAN). Коли виробники почали адаптувати свої системи до архітектури Ethernet, почалася конвергенція систем безпеки, об'єднуючи системи сигналізації, контролю доступу, відеоспостереження та голосового зв'язку в єдину інтегровану систему.

Ця конвергенція триває і сьогодні. На наступному етапі розподілені контролери систем сигналізації та контролю доступу, можливо, повністю зникнуть, оскільки виробники систем відеоспостереження зрозуміють, що вони можуть повністю інтегрувати функції сигналізації, доступу та інтеркому в свою архітектуру Ethernet для систем відеоспостереження. Це призведе до того, що система буде повністю складатися з «периферійних пристроїв» (камер, домофонів, обладнання для доступу до дверей і т.д.) і сервера/робочої станції для користувацького інтерфейсу. Вони об'єднані між собою в локальну мережу.

Сучасні цифрові відеокамери вже мають чіпи цифрової обробки сигналів (DSP) і до 64 мегабайт оперативної пам'яті. Незабаром пристрої доступу до кожної окремої двері будуть обслуговуватися одним крихітним контролером в розподільчій коробці над дверима. Ця крихітна плата матиме входи, виходи, порт для зчитувача карток, вихід для дверного замка та порт для пристрою виходу, і все це обслуговуватиметься мікросхемою DSP та кількома мегабайтами пам'яті. База даних всіх користувачів для цих дверей міститиметься на платі

пам'яті DSP. Один центрально розташований контролер може керувати всіма мікроконтролерами у всій будівлі.

Коли ці периферійні пристрої почнуть підключатися безпосередньо до локальної мережі без проміжного контролера, витрати різко знизяться. Хоча галузь, здається, стурбована таким розвитком подій, насправді це призведе до значно більшого використання систем. Так само, як виробники систем відеоспостереження боялися падіння ціни нижче 1000 доларів за камеру, а потім виявили, що продажі камер різко зросли, так само зростуть продажі систем сигналізації, контролю доступу та домофонів, оскільки поява мікроконтролерів призведе до зниження цін на них. Коли ці пристрої будуть поєднані з програмованим ПЛК, що дозволить використовувати їх у безмежному розмаїтті застосувань без нескінченного запасу апаратного забезпечення. Протягом наступних кількох років галузь, швидше за все, буде обслуговуватися лише периферійними пристроями та програмним забезпеченням.

1.2 Системи відеоспостереження

1.2.1 Загальні принципи роботи відеоспостереження

Візуальне спостереження почалося наприкінці дев'ятнадцятого століття, щоб допомогти тюремній адміністрації у виявленні способів втечі ув'язнених. Лише в середині двадцятого століття спостереження розширилося і стало використовуватися для забезпечення безпеки майна та людей. Астрономічна вартість перших систем відеоспостереження, заснованих на традиційних фотокамерах і плівці на основі срібла, обмежувала їх використання урядовими будівлями, банками і казино. Якщо було виявлено сумнівну діяльність, охоронна фірма, що здійснювала моніторинг, проявляла плівки в захищеній приватній фотолабораторії, щоб пізніше проаналізувати їх. Під час спеціальних заходів для спостереження за натовпом іноді використовувалося телебачення в прямому ефірі, але правоохоронні органи зазвичай обмежувалися телевізійною студією для перегляду відеозаписів з численних камер. Теорія візуального спостереження ґрунтувалася на тих самих чотирьох ключових факторах, що й сьогодні.

Рисунок 1.5. Ключові фактори візуального спостереження

Стримування

Якщо потенційні злочинці знають, що за ними спостерігають і записують їхні дії, вони можуть вирішити, що ризик бути викритими значно переважає переваги. Візуальне спостереження як засіб стримування використовується від казино до магазинів і громадського транспорту. Країни по всьому світу використовують відеоспостереження, зосереджуючи його переважно на громадському транспорті (літаках, поїздах, автомобілях) та окремих громадських місцях.

Виявлення

Виявлення - це найбільш важливий фактор успіху, який надає реальні докази того, що відеоспостереження працює. Британія добре відома своєю системою відеоспостереження, яка надає правоохоронцям можливість стежити за будь-ким по всьому Лондону за допомогою понад 200 000 камер (з більш ніж 4 мільйонами камер по всій країні). Ця система допомогла знайти чотирьох терористів, народжених у Лондоні, в тому числі широко відомого терориста-смертника Хасіба Хусейна, знятого камерами відеоспостереження. Крім того, Скотланд-Ярд засудив 500 злочинців, використовуючи базу даних камер відеоспостереження, яка містила дані про 7000 правопорушників за 3 роки.

Ефективність

Перегляд записів відеоспостереження одночасно з переглядом відео в реальному часі надає додаткову інформацію про ситуацію, що дозволяє користувачам приймати кращі рішення щодо розгортання потрібних видів і кількості ресурсів. Залежно від кількості камер спостереження та їхнього розташування, одночасний перегляд відео в реальному часі та архівних записів

може підтвердити спритність рук або будь-яку незаконну діяльність ще до того, як до відвідувача, клієнта або підозрюваного звернеться служба безпеки.

Ефективний охоронець

Сьогодні охоронцю навіть не обов'язково спостерігати, достатньо лише архівувати за допомогою більш розумних технологій. Сучасне відеоспостереження включає в себе складне програмне забезпечення для відеоаналітики з можливістю моніторингу територій для програмованих ситуацій (наприклад, додати в закладки всі червоні автомобілі), таких як покинуті автомобілі або рюкзаки, транспортні засоби, що кружляють, або навіть певні номерні знаки. Відеоаналітика може перетворити пасивну систему безпеки на активну. Це дає змогу створити ефективного охоронця, наділивши пасивну систему спостереження «мозком» і дозволивши їй краще реагувати на потенційні злочинні дії.

Камера відеоспостереження мало чим відрізняється від звичайної відеокамери, хоча цифрові камери відеоспостереження (DVS) призначені для роботи в умовах низької освітленості і мають довший термін служби. Удосконалення камер відеоспостереження відбувалося паралельно з розвитком кінематографічних технологій: від використання плівки до відеокасет, а тепер до цифрових відеофайлів для архівування. Не має значення, наскільки технологічно просунутими стають камери, тому що всі вони все одно повинні слідувати законам оптики: вони все ще потребують об'єктива, налаштування фокусу, діафрагми і витримки, а також повинні дотримуватися всіх оптичних законів глибини різкості. Об'єктиви, по суті, не змінилися, хоча тепер їх проектують на комп'ютері, щоб отримати кращу оптику за меншу ціну. Хоча багато недорогих камер безпеки використовують пластикові лінзи, скляна оптика все ще забезпечує найкращі результати.

1.2.2 Системи відеоспостереження та функції відеоаналітики

Відеоспостереження, більш відоме як CCTV (замкнене телебачення), - це галузь, якій вже понад 30 років, і яка пережила свою частку технологічних змін.

Як і в будь-якій іншій галузі, постійно зростаючі вимоги кінцевих користувачів до продуктів і рішень є рушійною силою змін, а технології, що розвиваються, допомагають їх задовольнити. На ринку відеоспостереження ці вимоги включають в себе наступне:

- Краща якість зображення;
- Спрощене встановлення та обслуговування;
- Більш безпечна та надійна технологія;
- Більш тривале зберігання записаного відео;
- Зниження витрат;
- Розмір і масштабованість;
- Можливість віддаленого моніторингу;
- Інтеграція з іншими системами;
- Більше вбудованого системного інтелекту.

Щоб відповідати цим вимогам, відеоспостереження пережило ряд технологічних змін. Останнім з них є перехід від аналогових систем відеоспостереження до повністю цифрових, мережевих систем відеоспостереження. Системи відеоспостереження починалися як 100-відсотково аналогові системи і поступово стають цифровими. Сучасні системи, що використовують мережеві камери і сервери ПК (персональні комп'ютери) для запису відео в повністю цифровій системі, пройшли довгий шлях від ранніх аналогових лампових камер, які підключалися до відеомагнітофона.

Аналогові системи відеоспостереження на базі відеомагнітофонів.

Традиційна аналогова система відеоспостереження передбачала використання аналогових камер, які підключалися до відеомагнітофона для запису відео (рис. 1.6). Система була повністю аналоговою. Відеомагнітофон використовував той самий тип касет, що й домашні відеомагнітофони. Кожна камера потребувала власного коаксіального кабелю, який йшов від камери до відеомагнітофона. Відео не стискалося, і при записі з повною частотою кадрів однієї касети вистачало максимум на вісім годин.

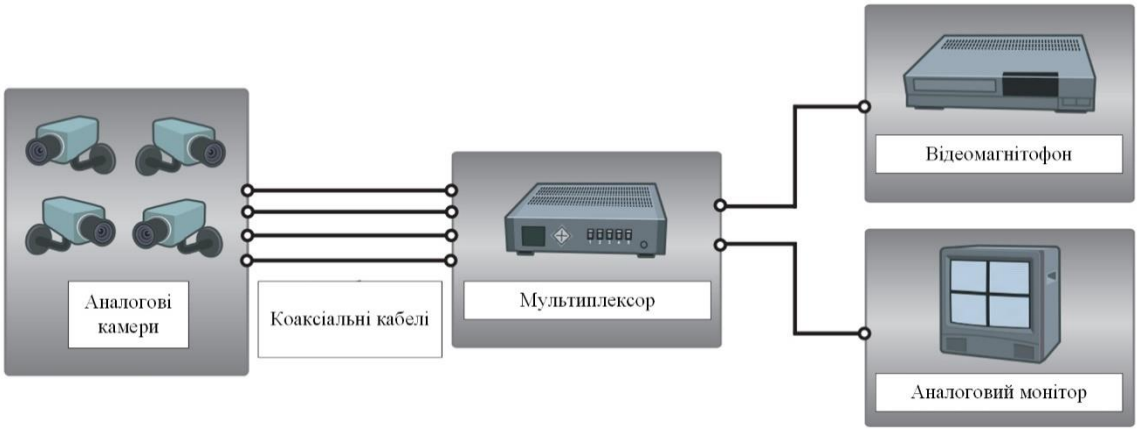


Рисунок 1.6. Структурна схема роботи аналогової системи відеоспостереження з відеомагнітофоном та мультиплексором

Аналогові системи відеоспостереження на основі відеореєстраторів.

До середини 1990-х років індустрія відеоспостереження пережила першу цифрову революцію з появою цифрового відеореєстратора (DVR). Цифрові відеореєстратори з жорсткими дисками замінили відеомагнітофони як носії інформації (Рис. 1.7).

Відео оцифровувалося, а потім стискалося, щоб зберегти якомога більше відео за кілька днів. У ранніх відеомагнітофонах простір на жорсткому диску був обмежений, тому тривалість запису була обмежена або доводилося використовувати меншу частоту кадрів.

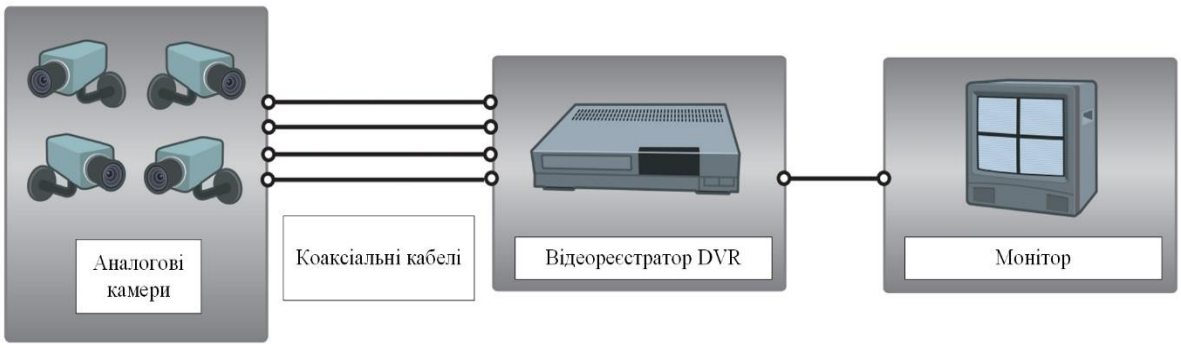


Рисунок 1.7. Структурна схема роботи аналогової системи відеоспостереження з відеореєстратором

Через обмеження місця на жорсткому диску багато виробників розробили власні алгоритми стиснення. Хоча вони могли працювати добре, кінцеві користувачі були прив'язані до інструментів одного виробника, коли справа доходила до відтворення відео. З роками вартість місця на жорсткому диску

різко знизилася, а стандартні алгоритми стиснення, такі як MPEG-4, стали доступними і широко поширеними, більшість виробників відмовилися від власних алгоритмів стиснення на користь стандартів - на користь кінцевих користувачів.

Мережеві аналогові системи відеоспостереження на базі відеореєстраторів.

Згодом відеореєстратори почали оснащувати портом Ethernet для підключення до мережі. Це привело до появи на ринку мережевих відеореєстраторів і дозволило здійснювати віддалений відеомоніторинг за допомогою комп'ютера (Рис. 1.8).

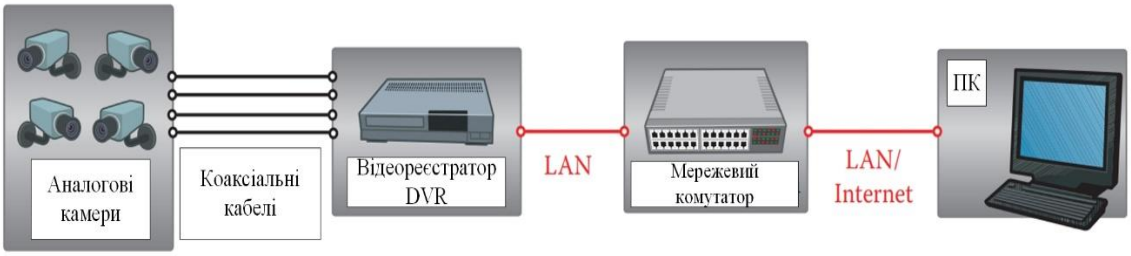


Рисунок 1.8. Структурна схема роботи аналогової системи відеоспостереження на базі мережевого відеореєстратора

Деякі мережеві відеореєстратори, що використовуються сьогодні, дозволяють здійснювати моніторинг як живого, так і записаного відео, тоді як інші лише записаного. Крім того, деякі системи вимагають спеціального Windows-клієнта для моніторингу відео, тоді як інші використовують стандартний веб-браузер; останній робить віддалений моніторинг більш гнучким. більш гнучким.

Мережева система відеоспостереження має наступні переваги:

– Віддалений моніторинг відео через ПК;

– Віддалене управління системою.

Хоча цифрові відеореєстратори мали значні переваги порівняно з відеомагнітофонами, їм також були притаманні певні недоліки. Відеореєстратор був обтяжений багатьма завданнями, такими як оцифрування відео з усіх камер, стиснення відео, запис і підключення до мережі. Крім того, це було рішення «чорного ящика», тобто пропрієтарне обладнання з попередньо завантаженим програмним забезпеченням, що часто змушувало кінцевого користувача шукати

запчастини в одного виробника, що робило обслуговування та модернізацію дорогими.

Мережеві відеосистеми на базі відеокодерів.

Перший крок до мережевої відеосистеми на основі відкритої платформи з'явився з впровадженням відеокодера, який також часто називають відеосервером. Відеокодер підключається до аналогових камер, оцифровує і стискає відео. Потім він надсилає відео по IP-мережі через мережевий комутатор на ПК-сервер, на якому запущено програмне забезпечення для моніторингу та запису (рис. 1.9).

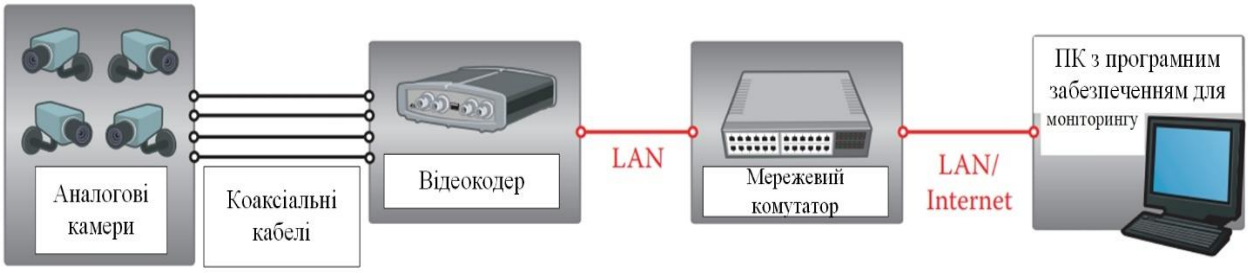


Рисунок 1.9. Структурна схема роботи відеосистеми на базі відеокодерів

Це справжня мережева система відеоспостереження, оскільки відео постійно надсилається через IP-мережу. По суті, завдання, які раніше виконував відеореєстратор, тепер розділені - оцифрування і стиснення здійснюється відеокодером, а запис - сервером ПК, що забезпечує кращу масштабованість.

Мережева відеосистема на базі відеокодера має наступні переваги:

– Використання стандартного мережевого та серверного обладнання для запису та управління відео;

– Масштабованість з кроком в одну камеру за раз;

– Можливість запису за межами об'єкта;

– Перспективність, система легко розширюється за рахунок підключення мережевих камер.

Альтернативи відкритій платформі (на базі ПК зі встановленим програмним забезпеченням для управління відео) також можливі завдяки наявності різних типів NVR (мережевих відеореєстраторів; рис. 1.10) та гібридних відеореєстраторів. NVR або гібридний відеореєстратор - це

спеціальний апаратний блок з попередньо встановленим програмним забезпеченням для керування відео з відеокодерів або мережевих камер.

Рисунок 1.10. Приклад вигляду мережевого відеореєстратора (NVR)

Мережевий відеореєстратор обробляє лише мережеві відеосигнали, тоді як гібридний відеореєстратор може обробляти як мережеві, так і аналогові відеосигнали паралельно. Перевагою використання мережевого або гібридного відеореєстратора є простота оскільки функції запису та керування відео доступні в одному корпусі - подібно до відеореєстратора. Рішення NVR або гібридний відеореєстратор популярний у невеликих системах з 4-16 камерами.

Мережеві відеосистеми на основі мережевих камер.

Мережева камера, яку також часто називають IP-камерою, - це, як випливає з назви, камера з підключенням до IP-мережі. У мережевій відеосистемі на основі мережевої камери відео передається по IP-мережі через мережеві комутатори і записується на ПК-сервер зі встановленим програмним забезпеченням для керування відео (рис. 1.11). Це і є справжня мережева відеосистема. Система є повністю цифровою, оскільки в ній не використовуються аналогові компоненти.

Однією з найбільших переваг мережевої камери є те, що після зйомки зображення оцифровується одразу всередині камери і залишається цифровим у всій системі, що забезпечує високу і стабільну якість зображення. З аналоговими камерами це не так. Хоча більшість аналогових камер сьогодні називають «цифровими», вони мають аналоговий вихід, і це може призвести до певної плутанини. Аналогові камери дійсно оцифровують захоплені зображення, щоб

забезпечити функції покращення зображення. Однак потім ці зображення знову перетворюються в аналогове відео. Важливо знати, що при кожному перетворенні з аналогового в цифровий формат або з цифрового в аналоговий відбувається певна втрата якості відео.

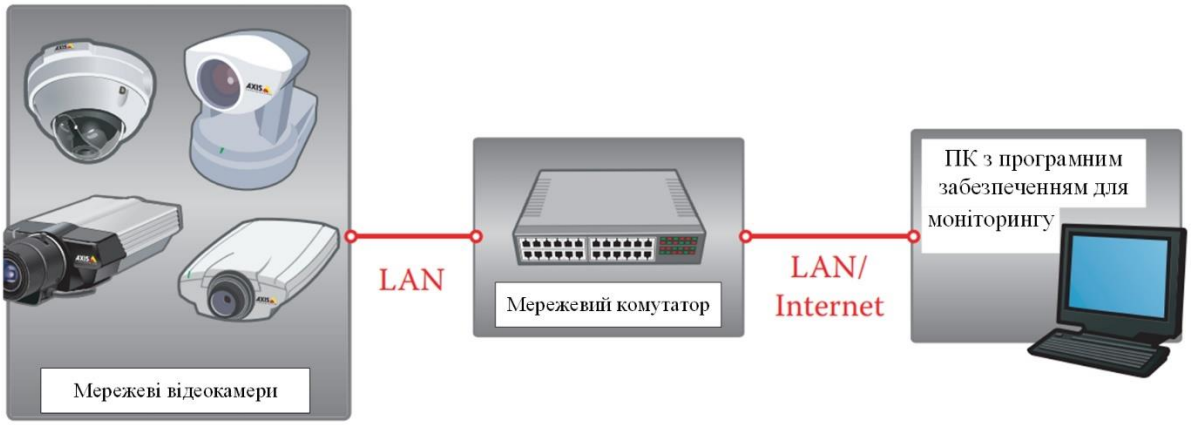


Рисунок 1.11. Структурна схема роботи мережевої відеосистеми з мережевими відеокамерами

Крім того, аналогові сигнали погіршуються при транспортуванні довгими кабелями і з часом, якщо зберігаються на стрічці. Тому відео в ідеалі має бути оцифроване один раз і залишатися цифровим протягом всієї системи. Перевага використання IP-мережі полягає в тому, що її можна використовувати не лише для передачі відео. IP-мережі надають можливість декільком мережевим камерам використовувати один і той самий фізичний кабель. Крім того, мережа може передавати живлення для мережевих камер і інформацію на вихідні та вхідні контакти камер. Вона також може передавати двосторонній звук, а також команди панорамування, нахилу і масштабування, якщо камера має таку функцію. Крім того, IP-мережа дозволяє віддалено налаштовувати мережеві камери, а відео та інші дані, що передаються мережею, досягають практично будь-якого місця без погіршення якості. В цілому, мережа забезпечує надзвичайно гнучке і економічно ефективне середовище для всіх комунікацій в рамках мережевої системи відеоспостереження. Масштабованість мережевого відео дає можливість будувати системи відеоспостереження з сотнями відеоспостереження з сотнями і навіть тисячами камер.

Багато сучасних систем відеоспостереження записують величезні обсяги відео, але величезний обсяг записів і брак часу призводить до того, що значна частина матеріалу ніколи не переглядається і не переробляється. Як наслідок, події та інциденти залишаються поза увагою, а підозріла поведінка не виявляється вчасно, щоб запобігти вчиненню злочинів.

Крім того, хоча стиснення відео пройшло довгий шлях, типова камера з повною частотою кадрів все ще генерує близько 5 ГБ даних на день, що аналогічно потоковому перегляду фільму в Інтернеті. Враховуючи, що по всьому світу встановлені сотні мільйонів камер, а час зберігання відеозаписів часто становить тижні або місяці, все ще існує потреба у зменшенні обсягу даних.

Відеоаналітика, також відома як аналітика, аналіз відеоконтенту (VCA), інтелектуальне відео, інтелектуальний відеоаналіз, а іноді навіть штучний інтелект (ШІ), може заповнити ці прогалини. Аналітика - ширше поняття, яке включає в себе аудіо- і не-відеодатчики, такі як пасивні інфрачервоні (PIR) датчики і радари. Аналітичні програми перетворюють відео, аудіо та інші типи вхідної інформації на дані і аналізують їх, щоб знайти події, що становлять інтерес. Наприклад, деякі програми розпізнають автомобільні номерні знаки, а інші зосереджені на захисті критичної інфраструктури за допомогою віртуальних ліній, які запускають сигнали тривоги в разі вторгнення.

Розробка нових систем відеоаналітики постійно зростає, задовольняючи потреби багатьох видів безпеки та ефективності. Системи на основі аналітики ніколи не простоюють. Вони сканують відео та аудіо в режимі реального часу, цілодобово, шукаючи інформацію, події або загрози і негайно реагуючи на них, починаючи запис або сповіщаючи персонал служби безпеки. Аналітика може значно знизити вимоги до пропускної здатності мережі і місця для зберігання даних, використовувати хмару для зберігання даних і звільнити персонал для виконання інших завдань, крім постійного моніторингу численних камер.

Аналітика також може забезпечити інтелектуальний пошук для швидкого визначення конкретних подій. Системи на основі аналітики також можуть витягувати дані з відеоспостереження та інтегрувати інформацію в інші

програми, такі як управління роздрібною торгівлею або системи контролю доступу, створюючи нові переваги і відкриваючи широкий спектр бізнес-можливостей.

Відеоаналітика - це процес аналізу відеоданих з метою перетворення їх на корисну інформацію. Аналітичні системи використовують складні алгоритми для аналізу відео та перетворення його на дані. Зазвичай вони виділяють рухомі об'єкти або інші розпізнавані форми, відфільтровуючи нерелевантні рухи.

Отримані дані зберігаються в базах даних, в яких можна здійснювати пошук за певними правилами, наприклад, об'єкт, що перетинає віртуальну лінію на відео, або більше десяти автомобілів, що стоять в черзі на проїзд. Правила можуть бути запрограмовані таким чином, щоб допомогти визначити, чи є події, які спостерігаються на відео, нормальними, чи вони повинні бути позначені як тривожні сигнали для співробітників служби безпеки. Відеоаналітика є життєво важливим компонентом критично важливих систем безпеки, підтримуючи своєчасне прийняття рішень у критичних ситуаціях. Такі програми, як підрахунок людей або трафіку, також відкривають нові ефективні способи управління бізнесом.

У 1997 році Управління інформаційних систем Агентства передових оборонних дослідницьких проектів (DARPA) у США розпочало трирічну програму з розробки технології відеоспостереження та моніторингу (VSAM). Метою проекту VSAM була розробка автоматизованого відео та надання йому можливості розуміти і оцінювати отриману інформацію для використання в програмах спостереження за полем бою. Технології, розроблені в рамках цього проекту, дозволяють одній людині-оператору контролювати діяльність на великій території за допомогою відеоаналітики, яка була спроектована як автономна і лише сповіщала оператора про виникнення загроз безпеці.

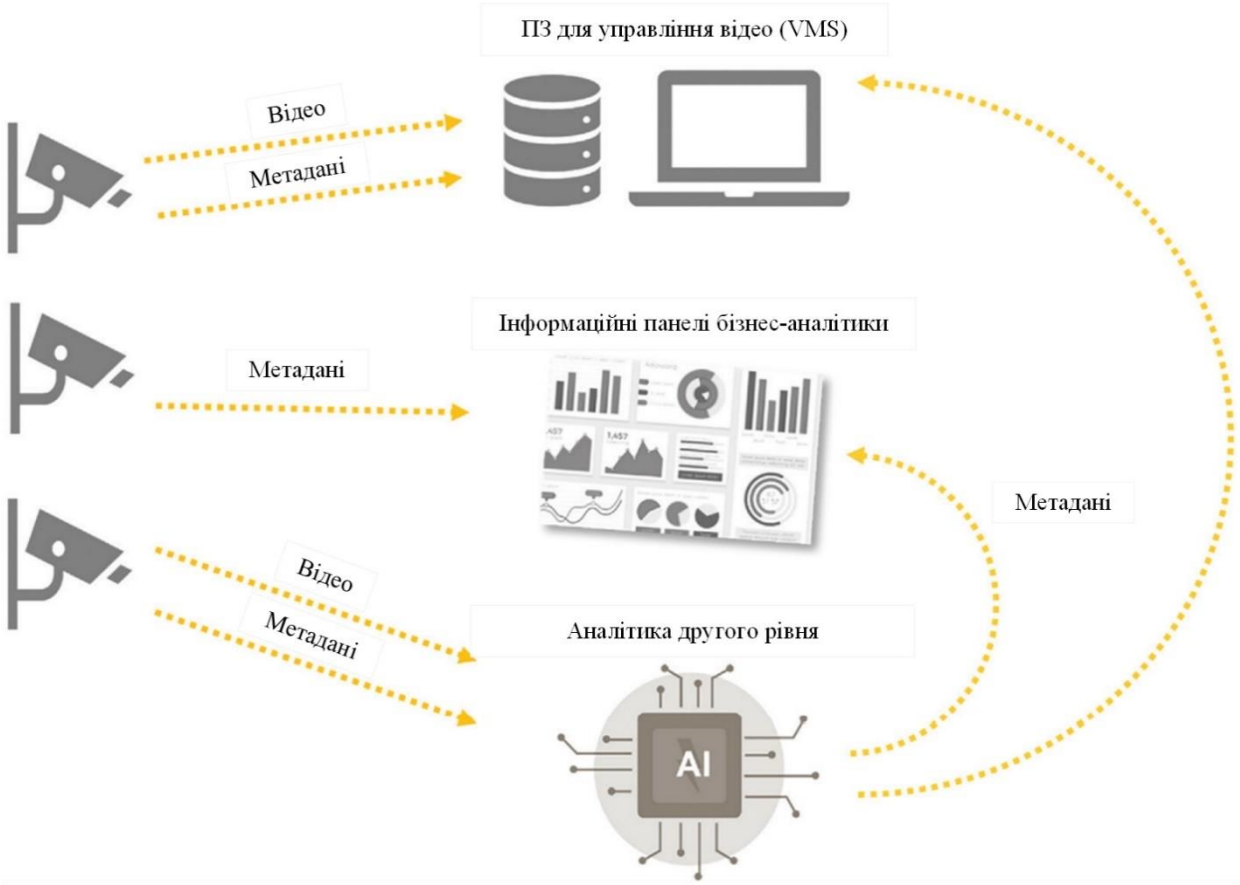


Рисунок 1.12. Логіка роботи відеоаналітики

Багато дослідників з таких університетів, як Університет Карнегі-Меллона (CMU) і Массачусетський технологічний інститут (MIT) були обрані для розробки широкого спектру передових методів спостереження. Вони включають в себе наступне:

– Виявлення та відстеження рухомих об'єктів у реальному часі зі стаціонарних і рухомих платформ камер;

– Розпізнавання загальних класів об'єктів (наприклад, людина, седан, вантажівка) і конкретних типів об'єктів (наприклад, поліцейський автомобіль або кур'єрський фургон);

– Оцінка положення об'єкта по відношенню до геопросторової моделі об'єкта;

– Активне керування камерами та спільне відстеження з декількома камерами;

– Аналіз ходи людини;

– Розпізнавання простих багатоагентних дій;
– Поширення даних у реальному часі;
– Ведення журналу даних;
– Динамічна візуалізація сцени.

Багато ранніх компаній і технологій відеоаналітики були похідними від проекту VSAM. Сьогодні більшість виробників додатків і камер VMS пропонують певні види відеоаналітики, які часто добре інтегровані в їхні пропозиції. Деякі з них також надають платформу, необхідну для підтримки використання сторонніх додатків.

Хоча перші дні відеоаналітики принесли багато нових розробок і додатків, на цю технологію також покладалося багато необґрунтованих очікувань, які часто не виправдовувалися. Останні розробки - загалом у сфері штучного інтелекту і, зокрема, у сфері глибокого навчання - дали нам набагато надійніші рішення.

1.3 Системи контролю та управління доступом (СКУД)

1.3.1 Поняття СКУД

Для початку потрібно розуміти що системи контролю та управління доступом (СКУД) є важливою частиною комплексної системи безпеки, яка спрямована на стримування та зменшення як злочинної діяльності, так і порушень політик безпеки організації. Однак важливо пам’ятати, що це лише один із її компонентів, але не менш важливим ніж всі інші. Завдяки сучасним системам забезпечується автоматизований процес надання дозволу авторизованому персоналу на вхід через точку проходу без необхідності ручної перевірки з боку охоронця. Зазвичай це реалізується за допомогою ідентифікаційного засобу, який користувач пред’являє системі для підтвердження своїх прав доступу.

Точка проходу, або охоронний портал - це двері або прохід, що створює точку входу в межі захищеної зони.

Рисунок 1.13. Приклади ідентифікаторів доступу користувачів СКУД

До поширених видів охоронних порталів належать стандартні двері, турнікети, обертові двері, шлагбауми для в'їзду транспортних засобів та інші. Приклади охоронних порталів показані на рис. 1.2:

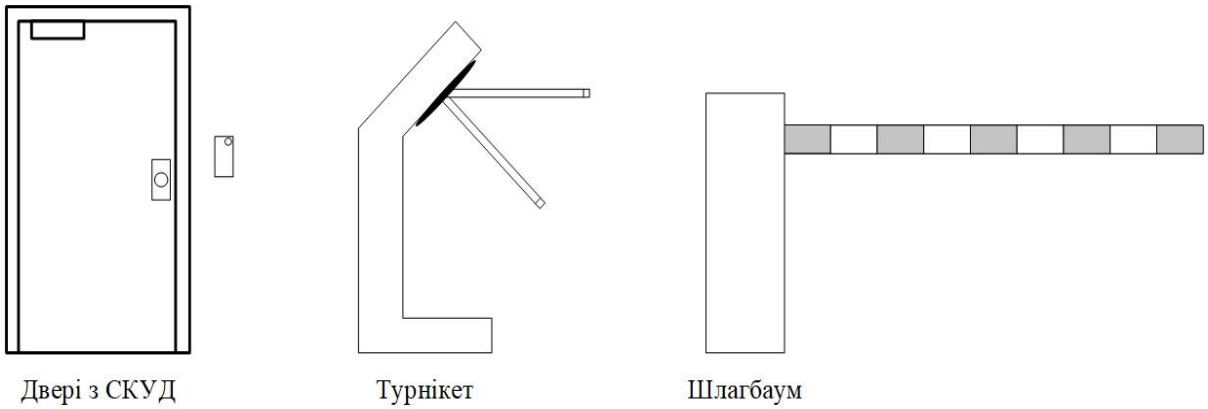


Рисунок 1.14. Приклади охоронних порталів

Загалом контроль доступу не є безпосереднім елементом системи безпеки, а швидше компромісним рішенням, яке впроваджується для забезпечення зручності повсякденної роботи. Ідеальна безпека означає ідеальний контроль доступу, тобто такий, за якого до охоронної зони не може потрапити жодна особа, яка не є безумовно перевіреним і відданим прихильником безпекової політики організації. У реальних умовах досягти такого рівня контролю майже неможливо.

Сучасні системи контролю доступу є автоматизованими механізмами, що дозволяють «припустимо» лояльним особам входити в контрольовані, обмежені та охоронювані зони з мінімальною перевіркою в точці доступу. Фактично, охоронні портали є проходами через захисний периметр, де вхідні особи "припускаються" дружніми на підставі їхнього статусу як працівника, підрядника або попередньо перевіреного відвідувача.

1.3.2 Компонентний склад та типи СКУД

Хоча електронні системи контролю доступу існують лише близько 50 років, потреба в контролі доступу існує набагато довше. Спочатку важливо зрозуміти, як задовольнялися потреби в контролі доступу до використання електронних систем контролю доступу. Хороші програми контролю доступу завжди включали в себе всі перераховані нижче елементи:

Рисунок 1.15. Основні елементи програм контролю доступу

Основні політики контролю доступу:

– Усі сфери, що належать до компетенції організації, будуть логічно організовані в зони доступу (включаючи багато порталів, які логічно пов'язані між собою, наприклад, усі двері у відділі);

– Кожен відділ або підрозділ організації визначить, куди його працівникам потрібен доступ. Всі відділи та підрозділи організації будуть об'єднані в групи доступу (включають зони доступу, до яких працівникам цього відділу або підрозділу потрібен доступ, а також графік, за яким група може мати доступ до зони доступу);

– Окремі працівники організації будуть віднесені до однієї або декількох груп доступу відділів;

– Кожен працівник отримає обліковий запис доступу (унікальний номер для пошуку в списку авторизованих користувачів);

– Кожен працівник може використовувати свій обліковий запис для отримання доступу до порталу в межах авторизованої групи доступу у встановлений для цієї групи доступу час.

Експлуатація:

– Авторизовані користувачі підходять до порталу доступу (двері, ворота тощо) і пред'являють свій обліковий запис пристрою зчитування облікових даних (у минулі часи це був охоронець);

– Зчитувач облікових даних звіряє облікові дані з базою даних (раніше це був щоденний список авторизованих користувачів) авторизованих власників облікових даних;

– Потім зчитувач порівнює власника з фотографією на посвідченні (зазвичай на картці).

Правила для підрядників та відвідувачів:

– Для роботи з підрядниками та відвідувачами будуть розроблені аналогічні правила;

– Зазвичай відділ завчасно повідомляє на рецепції про запланований візит;

– Підрядникам можуть видаватися власні картки або такі картки можуть зберігатися на стійці реєстрації служби безпеки.

Аудит:

– Усі записи про контроль доступу слід регулярно перевіряти, щоб переконатися, що політики застосовуються належним чином.

За часів до появи електронних систем контролю доступу всі ці політики здійснювалися вручну штатом кваліфікованих співробітників служби безпеки. Електронні системи контролю доступу вбудовують всі ці функції (за винятком, можливо, візуального підтвердження фотографії) електронно.

Електронні системи контролю доступу складаються з електронних елементів, фізичних елементів, операційних елементів, елементів інформаційних технологій та логічних елементів для створення цілісної робочої системи, яка забезпечує швидкий та надійний доступ авторизованих користувачів до об'єкта за мінімальних довгострокових витрат для організації.

Елементи контролю доступу включають в себе:

Рисунок 1.16. Елементи контролю доступу

Доступ до порталів контролю доступу надається лише авторизованим користувачам. Авторизація користувачів надається залежно від потреби. Користувачі можуть бути авторизованими, оскільки вони є працівниками, постійними підрядниками або постачальниками, або тимчасовими законними відвідувачами. Кожна система контролю доступу використовує певний тип облікових даних, які авторизовані користувачі можуть пред'являти системі контролю доступу як доказ того, що вони є авторизованими. Система проаналізує обліковий запис і перевірить, чи він дійсний. Після цього система дозволяє користувачеві пройти через портал. Програмування користувачів можна спростити, об'єднавши користувачів спільного типу в групи користувачів. Таким чином, всі працівники можуть бути в групі працівників, прибиральники - в групі прибиральників, а менеджери - в групі менеджерів. У більшості систем група логічно пов'язаних порталів безпеки може бути згруповані разом, щоб сформувати зону доступу.

У більшості випадків користувачі не потребують і не повинні мати доступ до всіх авторизованих дверей у будь-який час. Відповідно, більшість привілеїв доступу користувачів призначаються за розкладом, який може бути: цілодобовим; денна зміна; вечірня зміна; нічна зміна; вихідні; святкові дні; спеціальна подія. Група доступу - це комбінація груп користувачів, зон доступу та розкладів. Таким чином, велика кількість користувачів може бути запрограмована на доступ до логічної групи порталів за певним розкладом або розкладом, наприклад, робочі години плюс вихідні.

Найпоширенішою проблемою безпеки, пов'язаною з порталами електронних систем контролю доступу, є «слідкування». Це коли один або кілька людей слідують за авторизованим користувачем через портал доступу після того, як він був відкритий авторизованим користувачем. Як правило, авторизований користувач пред'являє свій обліковий запис і відчиняє двері. Коли вони проходять, неавторизована особа ловить двері, що зачиняються, і заходить за авторизованим користувачем. Це серйозна проблема електронних систем контролю доступу, і саме її повинні вирішувати менеджери програм безпеки.

Схеми запобігання зворотному використанню призначені для того, щоб один авторизований користувач не дозволив використати свою картку іншій неавторизованій особі. Схеми антипассбеку створюють зону антипассбеку, яка обмежена порталами контролю доступу. Портали контролю доступу включаються в зону захисту від несанкціонованого доступу таким чином, що авторизований користувач повинен увійти в зону і знову вийти з неї (через той самий або інший портал в зоні захисту від несанкціонованого доступу), перш ніж його картка може бути використана для повторного входу. Одна й та сама картка не може бути використана для входу двічі поспіль. Один раз увійти, один раз вийти, а потім знову увійти. Таким чином, авторизований користувач, який передає свою картку назад неавторизованому відвідувачу, виявить, що картка не дозволить йому увійти, оскільки вона не була використана для виходу.

Ідея порталу контролю доступу є центральною для всієї концепції систем контролю доступу. Портал контролю доступу - це прохід, через який людина або транспортний засіб повинні пройти з одного простору в більш контрольований або обмежений простір, і в який допускаються тільки уповноважені особи. Існує два основних типи порталів контролю доступу: для пішоходів і для транспортних засобів. Кожен тип має багато варіацій. Практично кожен портал контролю доступу має наступні п'ять загальних елементів:

- Шлагбаум, що замикається і працює;
- Метод або пристрій для перевірки особи;
- Механізм замикання;

– Пристрій, що реагує на тривогу;

– Датчик запиту на вихід.

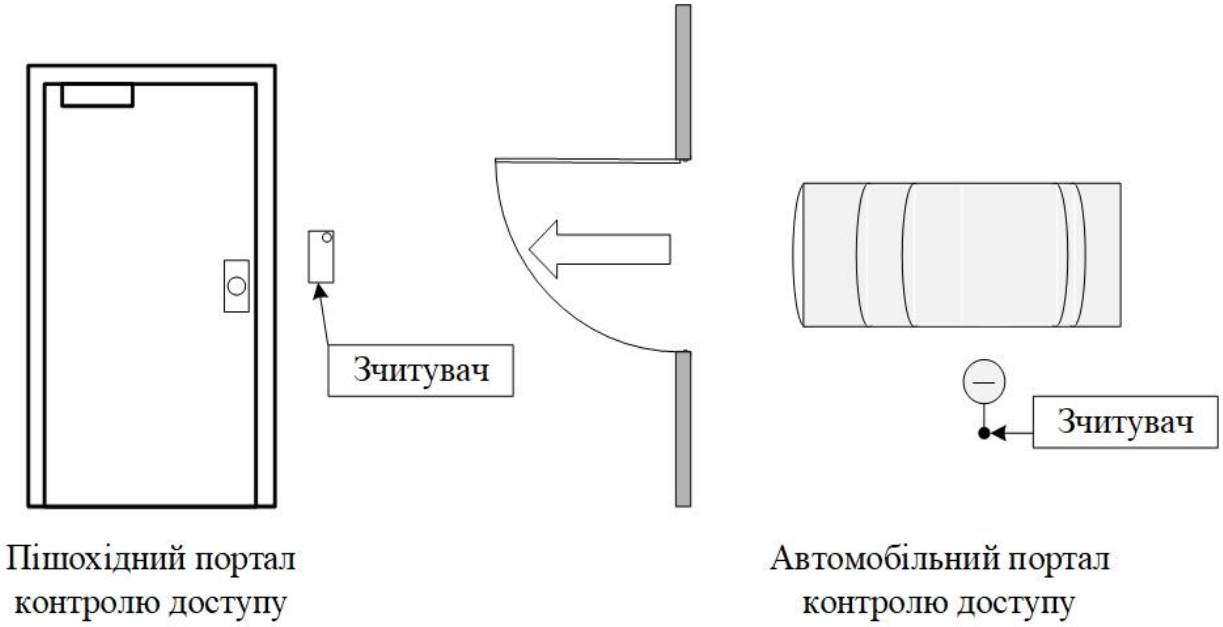


Рисунок 1.17. Типи порталів контролю доступу

Від найпоширеніших звичайних пластикових дверей до найскладнішого контрольно-пропускного пункту для транспортних засобів - усі вони мають спільні елементи.

Робочим бар'єром на вході до кожного порталу контролю доступу є зчитувач облікових даних. Авторизовані користувачі мають дійсний обліковий запис і можуть увійти, а неавторизовані користувачі не мають дійсного облікового запису і, відповідно, не можуть увійти. Існує три типи зчитувачів: зчитувачі карток, клавіатури та біометричні зчитувачі.

Двома основними компонентами дверей з контролем доступу є зчитувач посвідчення особи та електрифікований замок. Один з них дає дозвіл на вхід, а інший дозволяє його здійснити. Існує два основних типи електрифікованих замків з точки зору безпеки: Fail Safe та Fail Secure. Замки Fail Safe можна відчинити для виходу за відсутності живлення, а замки Fail Secure не можна відчинити для виходу за відсутності живлення. Деякі замки за своєю природою є відмовостійкими, наприклад, магнітні замки та електрифіковані аварійні замки. Оскільки магнітний замок потребує електроенергії, щоб утримуватися в безпеці, при втраті живлення замок розблоковується. Електрифікована аварійна

фурнітура використовує принцип «вільного механічного виходу», тобто, незалежно від стану замка, якщо натиснути на аварійну планку, двері відчиняються. В обох типах можна знайти й інші замки, наприклад, електрифіковані врізні замки, електрифіковані циліндрові замки та електрифіковані ригелі з електроприводом.

Електронні системи контролю доступу - це цифрові мережі, які контролюють доступ до порталів безпеки. Портал безпеки - це вхід або вихід за межі кордону безпеки. Більшість електронних систем контролю доступу також функціонують як система охоронної сигналізації. З цього моменту ми будемо вважати, що системи, які ми обговорюємо, мають елемент сигналізації. Електронні системи контролю доступу складаються з польового обладнання (датчиків і керованих пристроїв), модулів прийняття рішень, мережі зв'язку, однієї або декількох баз даних і одного або декількох терміналів людського інтерфейсу (комп'ютерних робочих станцій). Не настільки очевидними є «м'які» елементи системи контролю доступу. До них відносяться користувачі, політики і процедури, структура управління і звітності, а також використання системи для поліпшення постійної оцінки загальної програми безпеки.

1.4 Охоронна сигналізація

Крадіжки зі зломом - це великий бізнес. Більше того, статистика злочинності демонструє приголомшливий темп зростання кількості крадіжок з приватних будинків. Тож не дивно, що багато власників будинків і підприємств серйозно замислюються про захист електронною сигналізацією. Оператори сигналізацій прагнуть заробити швидкі гроші, а необережні клієнти, які купують те, що здається вигідною пропозицією, часто виявляються ошуканими.

Вибір належної системи сигналізації - справа непроста, адже потреби кожного домовласника або власника бізнесу відрізняються, як набір відбитків пальців. Деякі фактори, які визначають вимоги до індивідуальної системи сигналізації та питання, на які необхідно відповісти при виборі системи, включають в себе наступні:

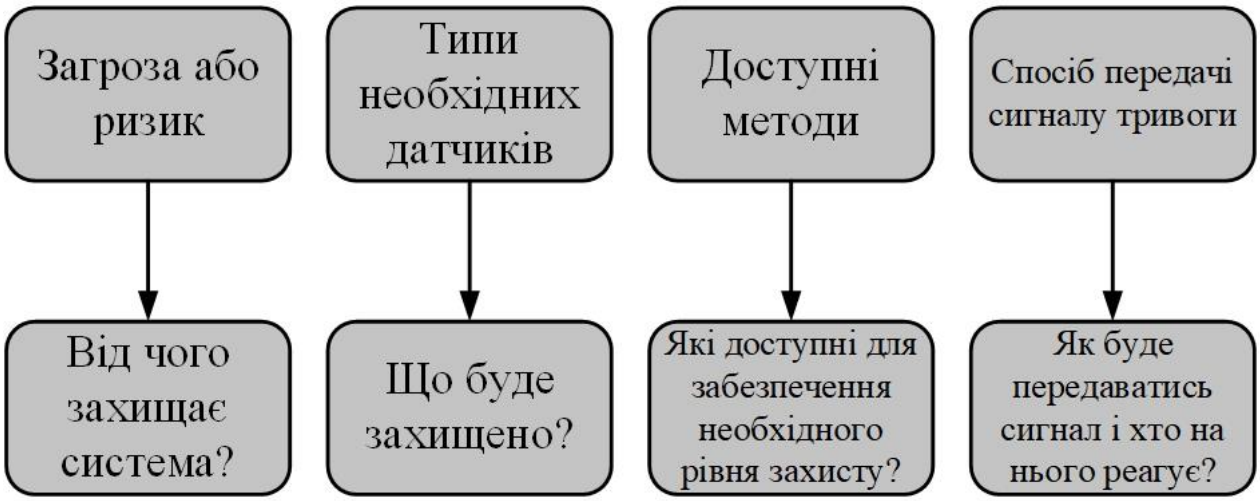


Рисунок 1.17. Вимоги до індивідуальної системи охорони

Більшість плутанини щодо систем виявлення вторгнень є результатом різноманітності методів, доступних для забезпечення необхідного захисту. Комбінації методів виявлення обчислюються тисячами. Система виявлення вторгнень може відлякати потенційного зловмисника. Однак основна функція системи сигналізації - сигналізувати про присутність зловмисника. Система виявлення вторгнень може бути лише частиною загального необхідного захисту. Багато великих підприємств доповнюють ці системи охоронцями та іншим персоналом служби безпеки. Успішна робота будь-якої системи сигналізації залежить від її правильного встановлення та обслуговування компанією, що встановлює сигналізацію і правильного використання системи замовником.

1.4.1 Рубежі захисту

Надійна система безпеки зазвичай поділяється на три лінії захисту.

Рисунок 1.18. Три рубежі охоронної сигналізації

Перша лінія захисту складається із зовнішніх сигналізацій, які мають на меті виявити зловмисника і подати сигнал тривоги до того, як йому вдасться проникнути в приміщення. Ця лінія захисту часто схильна до хибних спрацьовувань через рух птахів, тварин, невинних перехожих тощо. Тривога, яку

піднімає ця система, може лише попередити вас про те, що щось може статися. Вона ніколи не може надати точного попередження про те, що відбувається пограбування.

Зовнішня сигналізація має на меті виявити зловмисника якомога раніше, ще до того, як він потрапить до головної будівлі. Вона покладається на датчики, розташовані в землі або на стіні чи паркані. Оскільки ці датчики часто схильні до помилкових спрацьовувань, за ними зазвичай стежить приватна охорона, і їх можна очікувати лише в надзвичайно багатих районах або на корпоративних чи урядових об'єктах. Для цього часто використовують фотоелементи, які можна розмістити по всьому периметру, щоб захистити весь периметр. Інші поширені датчики, що використовуються для цієї мети, - мікрохвильові огорожі та детектори на основі польового ефекту. У певних об'єктах з підвищеним ризиком також використовуються спеціальні детектори бар'єрів або огорож. Ще один пристроєм, що використовується для зовнішньої сигналізації, є геофон.

Геофони – це чутливі сейсмічні сенсори, які активно застосовуються в геофізичних дослідженнях, зокрема під час проведення каротажу. Їх основна функція полягає у фіксації механічних коливань ґрунту, що виникають унаслідок поширення звукових хвиль, збуджених на поверхні землі та відбитих від геологічних шарів на різній глибині.

Сигналізація периметра - друга лінія захисту. Вона призначена для захисту оболонки будівлі (тобто стін, дверей та вікон). Датчики по периметру виявляють зловмисника, щойно він проникає в будівлю. Це найбільш важлива лінія захисту, оскільки вона показує, що зловмисник дійсно увійшов або, принаймні, намагався увійти в будівлю, що охороняється. Датчики периметральної сигналізації бувають різних типів. Магнітні геркони, фотоелементи, детектори розбиття скла, відеодетектори, детектори вібрації, інерційні датчики, інфразвукові датчики, датчики польового ефекту, плунжерні вимикачі та датчики тиску – це найпоширеніші датчики, які використовуються в периметральній сигналізації. У деяких старих системах також використовується віконна плівка або збірна віконна плівка і дротяні контакти.

Інфрачервоний сенсор

Датчик на основі польового ефекту

Геофонні датчики

Спеціальні бар'єрні датчики

Рисунок 1.19. Охоронні датчики зовнішньої сигналізації

Будь-які охоронці повинні поспішати на місце події - і пам'ятати, що якщо вони знаходяться далеко, то можуть запізнитися і не встигнути зловити зловмисника до того, як він втече. Втім, більшість професійних охоронних компаній все ж вважають за краще вичікувати. З їхньої точки зору, це ефективно, оскільки багато зловмисників навмисно активують периметральну сигналізацію за один або кілька разів до того, як потрапляють у будівлю, лише для того, щоб перевірити реакцію охоронців. Однак, з точки зору власника будинку, тобто вас, це катастрофічно. Коли грабіжник нарешті вирішить увійти, співробітники вашої охоронної компанії сприймуть це як чергову хибну тривогу. Вони не встигнуть дістатися до вашого будинку вчасно, щоб запобігти пограбуванню, не кажучи

вже про те, щоб завадити пограбуванню, не кажучи вже про те, щоб затримати зловмисника.

Датчик тиску

Плунжерний вимикач

Детектор вібрації

Камера з відеодетектором (відеоаналітика руху)

Детектор розбиття скла

Рисунок 1.20 Охоронні датчики периметральної сигналізації

Охоронні компанії виправдовують таку поведінку тим, що вони також встановлюють пастки - третю лінію захисту. Сигналізації-пастки - це пристрої виявлення, встановлені в стратегічних місцях всередині будинку, щоб виявити зловмисника після того, як він уже проник до будівлі. Вони також часто використовуються для захисту окремих предметів, що мають велику цінність або важливість. Теоретично, якщо охоронна компанія відстежила спочатку зовнішній сигнал тривоги, потім сигнал тривоги по периметру і, нарешті, сигнал тривоги пастки, вона знає, що відбувається пограбування. Тільки тоді вона реагує, щоб уникнути поспішного відправлення людей на віддалені об'єкти через хибну тривогу. Знову ж таки, це має сенс з точки зору компанії, але ви - той, хто заплатив за дорогу систему безпеки та охоронців, які можуть лише потім сказати вам, що так, ваш будинок пограбувала невідома особа або особи.

Рисунок 1.21. Охоронні датчики «пастки»

Датчики, що використовуються як пастки, зазвичай включають пасивні інфрачервоні детектори, мікрохвильові детектори руху, ультразвукові детектори руху, фотоелементи, магнітні геркони, напірні килимки, світлові детектори та відеодетектори. Інші датчики (наприклад, датчики з польовим ефектом), а також звукові та теплові детектори (не плутати з інфрачервоними) також належать до цієї категорії сигналізацій. Іонізаційні детектори також належатимуть до цієї групи, якщо і коли вони стануть загальновживаними. Сигналізації-пастки також включають спеціальні сигналізації, що використовуються для охорони цінних картин, комп'ютерів тощо.

1.4.2 Особливості проектування та компоненти охоронної сигналізації

При проектуванні системи безпеки завжди потрібно оцінювати концепцію системи з точки зору зловмисника. Будь-яка система може чудово працювати в лабораторних умовах, але чи витримає вона перший контакт з реальністю в особі досвідченого грабіжника? Можливо, системі доведеться впоратися з навмисним саботажем до злому, і розробник системи неодмінно повинен враховувати зловмисників, які намагатимуться обійти її або будь-яким іншим чином вивести систему безпеки з ладу. Крім того, в деяких місцях система повинна бути здатна витримувати екстремальні кліматичні умови. Холод і вологість можуть вплинути на роботу будь-якої електронної системи. Очевидно, що проектування надійної системи безпеки - справа серйозна. Розглянемо функції правильної сигналізації

поетапно. Базова система охоронної сигналізації складається з наступних елементів:

– Блок управління, зазвичай (але не оптимально) встановлюється в межах легкої досяжності від основних засобів виходу і входу, як правило, від вхідних дверей. Це мозок системи сигналізації;

– Один або кілька пристроїв оповіщення, наприклад, звукові коробки з попереджувальними дзвониками або сиренами, або стробоскопи, часто закріплені на стіні із зовнішнього боку будинку;

– Один або кілька пристроїв виявлення або датчиків.

Рисунок 1.19. Основні елементи охоронної сигналізації

Інші основні компоненти включають пристрої для постановки та зняття системи сигналізації з-під охорони, обладнання для автоматичного набору номера, джерело живлення (наприклад, ДБЖ) та електропроводку між різними компонентами. Блок управління розміщується в захисному ящику, як правило, металевому, і знаходиться в центральному місці на території, що охороняється. Для цього може бути використана шафа в приміщенні. Вкрай важливо, щоб блок управління не був доступним або навіть очевидним для грабіжника. Пристрої такого типу іноді називають сигналізаторами або оповіщувачами, хоча слово «сигналізація» найчастіше використовується для позначення пристроїв звукового оповіщення. Додаткові пристрої можуть бути встановлені всередині будинку, головним чином як психологічний вплив на зловмисника, а також можливі так звані безшумні сигналізації. Тоді буде використовуватися система дистанційної сигналізації. Датчик - це пристрій, який передає інформацію на блок управління. Якщо блок управління - це еквівалент людського мозку, то датчики схожі на органи чуття людського тіла. Датчик, або детектор, - це

пристрій для сканування та відсіювання. Його ефективний діапазон дії називається зоною виявлення.

Датчики бувають різних типів і, як зазначалося вище, зазвичай поділяються на три лінії захисту. Датчики з'єднані з блоком управління, який, отримавши попередження від датчика, передає сигнал тривоги на пристрій оповіщення, таким чином подаючи звуковий сигнал тривоги. Існує три лінії захисту, але насправді існує чотири різні види тривожного захисту:

- Зовнішні тривоги;
- Периметральна сигналізація;
- Тривоги пасток;
- Навмисне спрацьовування тривог.

Основна перевага полягає в тому, що мешканці будівлі можуть вибрати, активувати всі, деякі або жодну з частин системи в будь-який момент часу.

Наприклад, можна виключити спальню, щоб мешканець міг пересуватися по ній, не викликаючи сигналізацію, яка вже активована в холі, біля вхідних дверей. Кожне коло складається з низки контактів, розташованих в одній зоні. Сигнал тривоги спрацьовує, коли будь-який з цих контактів розривається. Зазвичай в кожній охоронній групі встановлюють кілька різних типів датчиків, які мають свій функціонал охорони.

1.5 Порівняння технологічних рішень брендів обладнання для реалізації проекту

1.5.1 Ринок систем безпеки України і ключові виробники

Незважаючи на глобальні виклики, спричинені пандемією COVID-19 та збройною агресією проти України, ринок технічних засобів безпеки, продовжує демонструвати динамічний розвиток. Зростаюча потреба у надійному контролі та захисті інфраструктури стимулює попит на інтелектуальні рішення, зокрема в корпоративному секторі. Все частіше на практиці реалізуються комплексні проєкти, що включають не лише відеоспостереження, але й інтеграцію з системами контролю доступу, сигналізації та іншими підсистемами безпеки.

В умовах стрімкого розвитку цифрових технологій зростає потреба у високофункціональному обладнанні, яке забезпечує не лише зйомку, але й аналітичну обробку відео в режимі реального часу – зокрема розпізнавання облич, номерних знаків, підрахунок відвідувачів тощо. Такі функції найбільш актуальні для великих підприємств, об’єктів критичної інфраструктури, торговельно-розважальних центрів та логістичних хабів.

Через обмеження, запроваджені в період пандемії, темпи розвитку галузі дещо знизилися. Зокрема, у 2020 році очікуваний приріст на рівні 25% було зменшено до 6% у грошовому вираженні та 8% у кількісному. Одночасно відчувався дефіцит електронних компонентів, зокрема мікросхем, що призвело до тимчасових перебоїв у постачанні продукції. Проте, ринок швидко адаптувався, і вже до кінця року показав ознаки відновлення.

У поточних умовах особливу актуальність набувають інтегровані рішення, які включають взаємодію кількох систем безпеки – єдиної платформи безпеки, що забезпечує централізований моніторинг, управління доступом, оповіщення та аналітику. Використання програмного забезпечення з елементами штучного інтелекту, хмарної інфраструктури та засобів кіберзахисту стає стандартною вимогою до сучасних систем.

Водночас спостерігається розподіл ринку за спеціалізацією: окремі компанії орієнтовані на виконання складних корпоративних проєктів, інші – працюють з представниками малого та середнього бізнесу. Таке сегментування сприяє формуванню гнучких рішень, адаптованих до різного бюджету та технічних вимог.

При виборі обладнання для побудови комплексної системи безпеки важливо враховувати не лише вартість пристроїв, але й їхню надійність, функціональні можливості та репутацію виробника. Обладнання преміум-класу, як правило, обирається для державних або великих комерційних об’єктів, тоді як для приватного використання або невеликих підприємств можуть застосовуватися рішення середнього чи бюджетного сегменту. Водночас, занадто дешеві системи часто виявляються менш надійними та потребують додаткових

витрат у процесі експлуатації.

Загалом, попит на комплексні системи безпеки в Україні зберігає позитивну динаміку, особливо на тлі зростання актуальності організації безпеки об’єктів критичної та промислової інфраструктури. Очікується, що у найближчі роки тенденція до інтеграції, інтелектуалізації та автоматизації систем безпеки лише посилюватиметься.

Dahua Technology – один із відомих світових виробників систем відеоспостереження та безпеки, заснований у 2001 році з головним офісом у Ханчжоу, Китай. Компанія активно працює у понад 180 країнах і регіонах через 35 дочірніх компаній.

Рисунок 1.20. – Логотип компанії Dahua Technology

У 2017 році її дохід склав $2,89 млрд, що демонструє швидке зростання та глобальну експансію.

Dahua інвестує близько 10% свого обороту в дослідження й розробки (R&D), маючи понад 6000 інженерів і чотири науково-дослідні інститути. Сфери розробок охоплюють штучний інтелект, великі дані, кібербезпеку, хмарні технології, відеоаналітику та IoT.

Станом на 2016 рік компанія зареєструвала понад 800 патентів. Основна продукція Dahua включає перелік, представлений на рис. 1.21.

Серед інновацій: тепловізійні гібридні камери, Smart Scene Adaptive, підтримка 4K через коаксіал, відеоаналітика на базі глибокого навчання, платформа Dahua Open Platform (DHOP) для встановлення сторонніх додатків. Компанія також активно впроваджує рішення у сфері контролю доступу, відеоконференцій та управління трафіком.

Рисунок 1.21. Основна продукція компанії Dahua

Dahua позиціонує себе як бренд, що здійснює перехід від "Зроблено в Китаї" до "Інновації в Китаї", прагнучи забезпечити безпечніше суспільство та розумніше життя.

Заснована у 1984 році, шведська компанія Axis Communications є світовим лідером у розробці інтелектуальних мережевих пристроїв, зокрема серверів друку, сховищ даних, сканерів і мережевих камер відеоспостереження. Axis першою в світі представила IP-камеру, PTZ-камеру, камеру з підтримкою HDTV і тепловізійну мережеву камеру.

Рисунок 1.22. Логотип компанії Axis Communications

Свою діяльність компанія починала з ринку серверів друку й досі входить до трійки лідерів у цій галузі. Продукція Axis використовується як у малому бізнесі, так і у великих корпораціях, таких як Microsoft, Ford і Alcatel. Штаб-квартира знаходиться в Лунді, Швеція, а офіси – по всьому світу. Компанія має партнерства з Ricoh, Canon, Epson, Ericsson та іншими, а її рішення продаються у понад 60 країнах через дистриб'юторів та OEM-виробників. Особливу увагу Axis приділяє дослідженням та розробкам: понад 800 інженерів у Лунді займаються

створенням інноваційної продукції. Компанія працює за моделлю непрямих продажів, яка довела свою ефективність у глобальному масштабі.

Рисунок 1.23. Логотип компанії Hikvision

Hikvision – провідна китайська компанія у сфері відеоспостереження, заснована у 2001 році. Вона входить до списку Forbes 2000 і частково належить уряду КНР. Завдяки активному зростанню, компанія має представництва у понад 20 країнах, а її продукти використовуються у сферах освіти, роздрібної торгівлі, транспорту, фінансів та промисловості.

Асортимент включає IP-камери, DVR/NVR-регістраційні системи, програмне забезпечення, системи доступу та сигналізації. Hikvision впроваджує інновації, такі як 4K-камери з функціями розпізнавання облич і номерів, відеоаналітика, теплове картографування та біометрія. Завдяки відкритій платформі HEOP, клієнти можуть використовувати сторонні додатки, що робить обладнання гнучким для інтеграції.

1.5.2 Порівняння ключових характеристик обладнання

З метою обґрунтування вибору технічного забезпечення для побудови комплексної системи безпеки на підприємстві було здійснено зіставлення продукції трьох провідних брендів у галузі відеоспостереження – Hikvision, Dahua та Axis Communications. Інформаційна база для аналізу формувалася на основі вивчення технічної документації, специфікацій обладнання, а також узагальнення оцінок і коментарів користувачів та фахівців, оприлюднених у відкритих джерелах – профільних форумах, оглядових сайтах, маркетплейсах і професійних оглядах.

Таблиця 1.1. Основні характеристики обладнання

Параметр або характеристика	**Hikvision**	**Dahua**	**Axis Communications**
Якість зображення відеокамер	Висока (до 4К, технологія DarkFighter)	Висока, але дещо програє конкурентам в нічному режимі	Висока, особливо вдень (кольорова передача)
Асортимент технологічних рішень	Найширший (велика екосистема бренду)	Великий	Вузько сегментований, фокус на відеоспостереження
Простота програмного забезпечення для роботи	iVMS-4200, HikCentral: інтуїтивно зрозуміле	SmartPSS: більш складне в налаштуваннях	AXIS Camera Station: складне, вимагає професійного досвіду
Інтеграція з іншими системами	Широкі можливості (ONVIF, API, SDK)	Аналогічні з Hikvision, але менше SDK	Є інтеграція, але обмежено пропрієтарністю
Інтелектуальні функції (AI)	Багато, доволі точні за тестами	Багато, менш точні за тестами	Багато, є спеціалізовані
Технічна підтримка	Широка, з сервісними центрами та актуальною документацією	Широка	Сервісне обслуговування та ТП через партнерів
Надійність та стабільність роботи	Висока	Висока, бувають скарги на прошивку	Висока
Впізнаваність бренду	Популярний бренд	Популярний бренд	Популярний серед великих підприємств
Цінова характеристика	Оптимальне співвідношення «ціна/якість»	Середній бюджет	Преміум сегмент ринку, відносно аналогів конкурентів

|За результатами порівняння можна виділити основні ключові особливості бренду Hikvision:

Рисунок 1.24. Ключові переваги Hikvision

Hikvision вирізняється раціональним поєднанням вартості та функціоналу, що робить його особливо ефективним для проєктів середнього і великого рівня складності. Компанія пропонує широкий модельний ряд – від базових пристроїв до високотехнологічних комплексних систем.

У сфері аналітики відео та застосування елементів штучного інтелекту Hikvision демонструє лідерські позиції завдяки стабільній реалізації функцій розпізнавання облич, аналізу динаміки переміщень, підрахунку об’єктів тощо. Аналогічні функції доступні в Dahua, однак реалізовані на менш надійному рівні. Axis також має відповідні можливості, але вони представлені переважно в преміальному ціновому сегменті, що обмежує їх застосування в більшості типових проєктів.

У контексті сумісності та інтеграції з іншими підсистемами безпеки, Hikvision підтримує відкриті стандарти (зокрема ONVIF), а також забезпечує можливість роботи з SDK та API, що значно розширює сценарії інтеграції з іншими технічними засобами.

Продукція Axis Communications, хоча і характеризується високою якістю та довговічністю, має суттєво вищу вартість порівняно з конкурентами. Крім того, її обмежена доступність на внутрішньому ринку України та недостатній рівень технічного супроводу знижують привабливість у контексті реалізації стандартних корпоративних рішень.

Dahua є прямим конкурентом Hikvision у сегменті середнього цінового рівня, однак дещо поступається в аспектах користувацького інтерфейсу, стабільності програмного забезпечення та рівня сервісної підтримки.

Загалом, з урахуванням комплексної оцінки технічних характеристик, експлуатаційної зручності, доступності сервісу та економічної ефективності, обладнання торгової марки Hikvision є найбільш доцільним вибором для впровадження у системі безпеки підприємства. Такий вибір дозволяє реалізувати на практиці збалансовану та масштабовану систему з оптимальним співвідношенням ціни, якості та функціональності – що особливо важливо в сучасних умовах зростаючих вимог до безпеки об’єктів.

1.6 Технічне завдання на проектування комплексної системи безпеки підприємства

Діяльність обраного мною підприємства буде виконувати продаж та обслуговування систем фізичного захисту об’єктів. Спроектована система повинна вирішувати питання контролю за певними приміщеннями підприємства, його та персоналу, від дій зловмисників та вирішення конфліктних ситуацій, шляхом впровадження охоронної сигналізації, системи відеоспостереження, та системи контролю та управління доступом. Система повинна працювати в одній екосистемі Hikvision.

Мета системи полягає в підвищенні рівня фізичної безпеки підприємства, унеможливлення несанкціонованого доступу до критично важливих зон об’єкту, забезпечення фіксації певних подій в журналі, для їх подальшого аудиту.

Підсистема відеоспостереження повинна виконувати наступні функції:

– Відеомоніторинг внутрішніх приміщень та зон;

– Зберігання відеоархіву не менше ніж 30 діб;

– Наявність інтелектуальних функцій та відеоаналітики;

– Можливість віддаленого перегляду відео через ПК/та мобільний додаток.

Задачі підсистеми охоронної сигналізації:

– Контроль проникнення до всіх зон підприємства;

– Наявність сповіщувачів розбиття скла в ключових зонах підприєвства;

– Можливість підключення системи до центрального пульта спостереження;

– Функції постановки/зняття з охорони за допомогою клавіатури та або мобільного додатку.

Система контролю та управління доступом повинна:

– Обмежувати доступ до важливих зон об’єкту (кабінет керівництва, фінансового відділу, складського приміщення, тощо);

– Формувати журнал подій;

– Мати авторизацію за біометричними даними та або RFID-картками;

– Інтегруватись з системою відеоспостереження (фіксувати зображення при спробах ідентифікації).

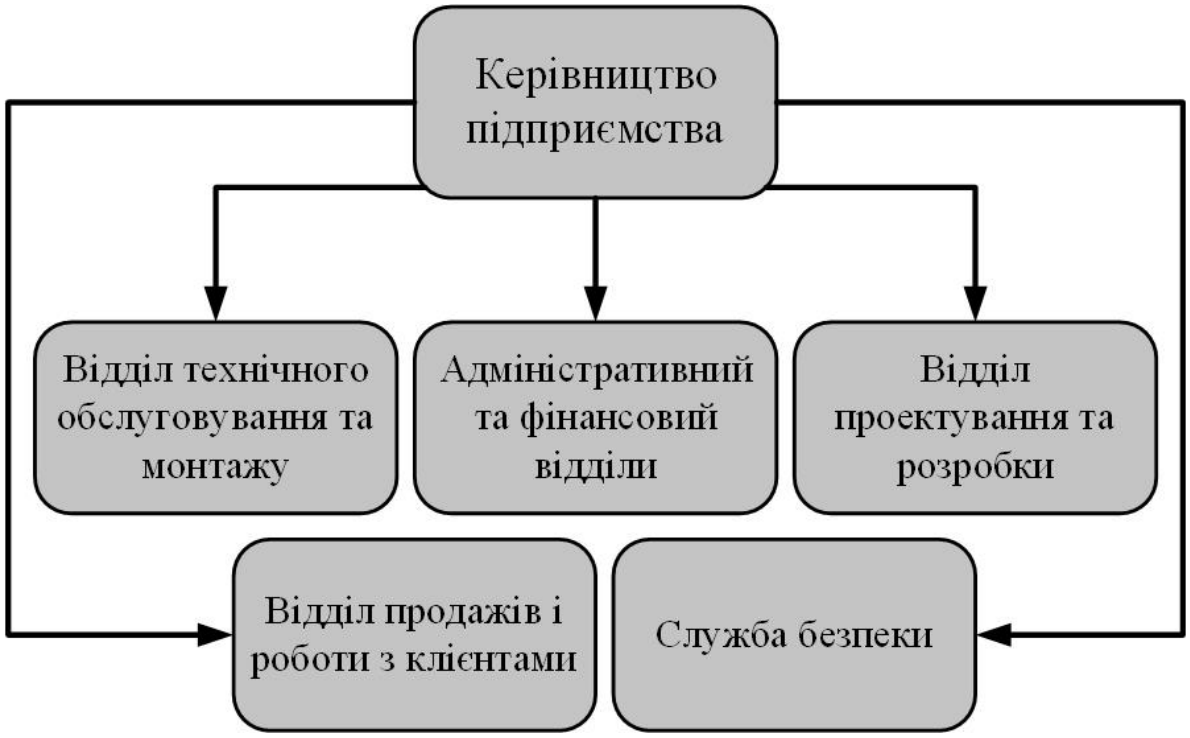


Рисунок 1.25. Організаційно-штатна структура підприємства

Приміщення підприємства можна розділити на наступні зони:

– Адміністративна зона (кабінети керівництва, бухгалтерії, продажів);

– Технічний відділ (майстерня для обслуговування та тестування обладнання);

– Складське приміщення (зберігання запчастин, камер, контролерів, кабелів тощо);

– Переговорна кімната (для зустрічей з клієнтами);

– Серверна (за необхідності);

– Зона відпочинку для персоналу.

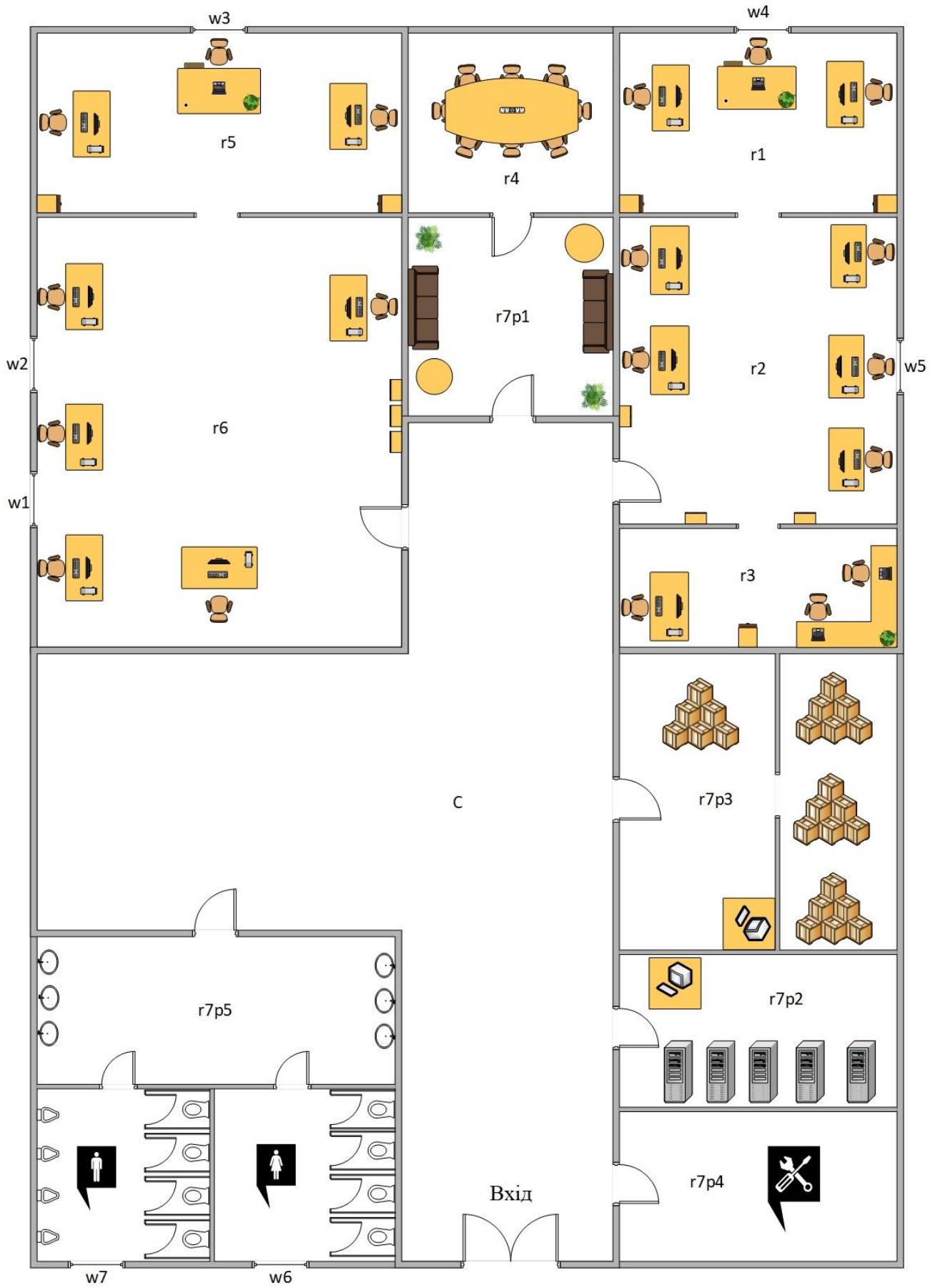


Рисунок 1.26. План приміщення підприємства

Таблиця 1.2. Призначення приміщень на рисунку 1.26

Позначення в кімнатах	Призначення кімнати	Площа приміщення S, м^2
C	Коридор	23,5
r1	Кабінет керівництва	8
r2	Відділ проектування та розробки	13
r3	Адміністративний та фінансовий відділ	6
r4	Кімната переговорів	7
r5	Кабінет служби безпеки	9
r6	Відділ продажів і роботи з клієнтами	20
r7p1	Зона відпочинку для персоналу	8
r7p2	Серверна кімната	15
r7p3	Сладське приміщення	10
r7p4	Відділ технічного обслуговування (майстерня)	10
r7p5	Вбиральня	13
w1, w2, w3, w4, w5, w6, w7	Вікна	
Загальна площа		142,5 м^2

1.7 Проектування комплексної системи безпеки підприємства

1.7.1 Обладнання проекту

Знаючи особливості підприємства, його організаційно-штатну структуру можна починати підбір обладнання для реалізації проекту.

Система охоронної сигналізації:

- Централь – Hikvision DS-PWA64-L-WE;
- Бездротовий датчик відкриття – Hikvision DS-PDMC-EG2-WE;
- Бездротовий сповіщувач руху – Hikvision DS-PDP15P-EG2-WE;
- Бездротовий датчик розбиття скла – Hikvision DS-PDBG8-EG2-WE;
- Бездротова клавіатура – Hikvision DS-PK1-E-WE.

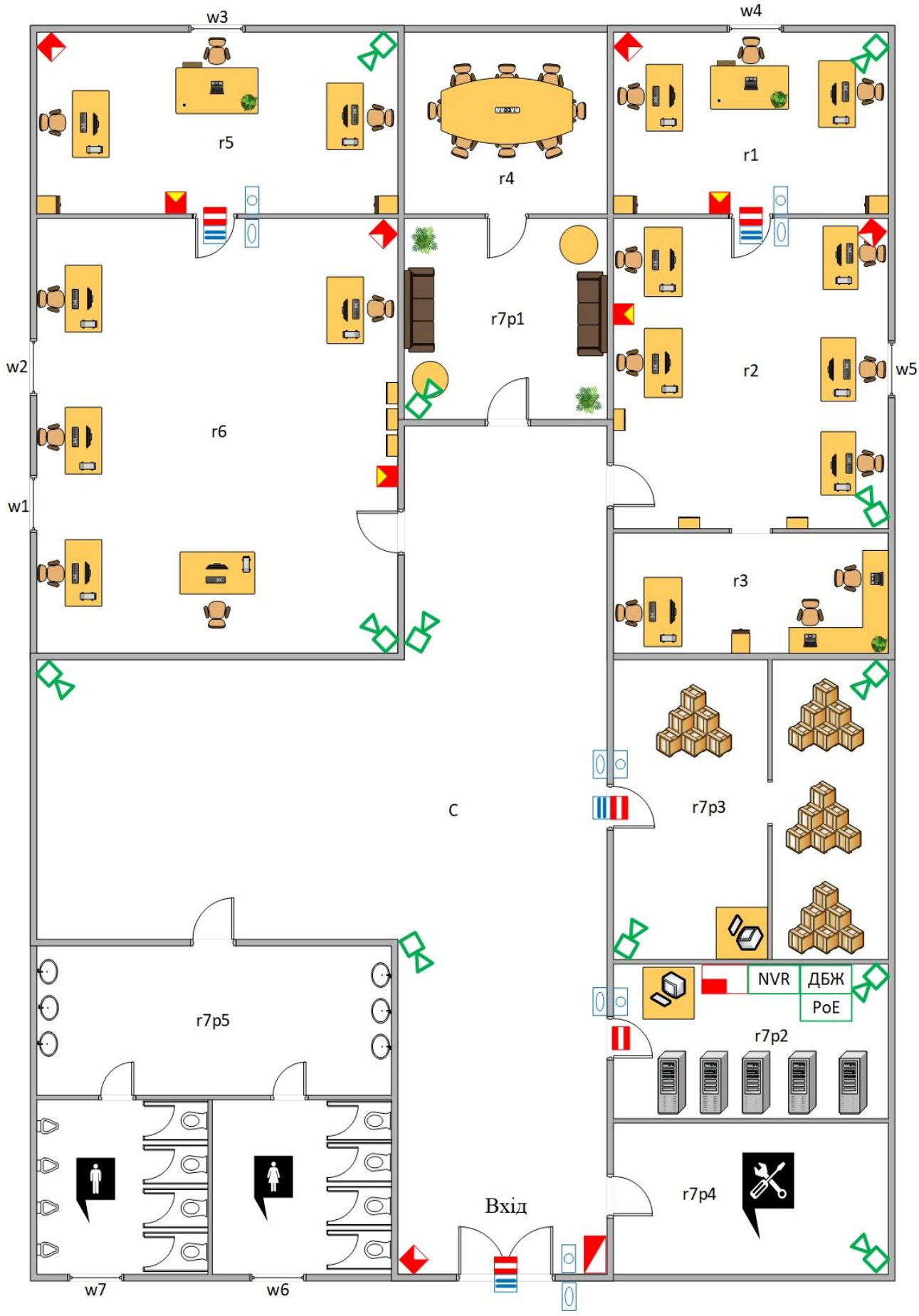


Рисунок 1.27. Комплексна система безпеки підприємства

Система відеоспостереження:

– Купольна відеокамера 4 МП – Hikvision DS-2CD1341G0-I;

– Відеореєстратор – Hikvision DS-7716NXI-K4 16-канальний;

– PoE комутатор – Hikvision DS-3E1318P-EI 16 портовий;

– Джерело безперебійного живлення на АКБ;

– Кабельна продукція.

Система контролю та управління доступом:

– Контролер доступу на 4 двері – Hikvision DS-K2604T;

– Контролер доступу на 1 двері – Hikvision DS-K2801;

– Зчитувач відбитків пальців та RFID карток – Hikvision DS-K1201AMF Mifare;

– Прилад додавання відбитків пальців – Hikvision DS-K1F820-F;

– Електромагнітні замки;

– Кнопки виходу;

– Кабельна продукція.

Таблиця 1.3. Умовні позначення СКУД

Позначення елементу	Опис елементу
	Контролери доступу
	Зчитувач відбитків пальців та карток
	Кнопка виходу
	Електромагнітний замок

Таблиця 1.4. Умовні позначення системи відеоспостереження

Позначення елементу	Опис елементу
	Відеореєстратор

Продовження таблиці 1.4

	Відеокамера
	Джерело безперебійного живлення та АКБ
	PoE комутатор

Таблиця 1.5. Умовні позначення системи охоронної сигналізації

Позначення елементу	Опис елементу
	Сповіщувач відкриття
	Сповіщувач руху
	Датчик розбиття скла
	Клавіатура
	Централь системи охорони

1.7.2 Розрахунок глибини відеоархіву за кодеком H.265

Розрахунок інформаційної ємності відеоархіву в системі відеоспостереження є дуже важливим аспектом при проектуванні таких систем. При підборі обладнання необхідно враховувати популярні нині стандарти відеокодування, наприклад H.265.

H.265, також відомий як HEVC (High Efficiency Video Coding) – це сучасний стандарт відеокодування, який став наступником широко використовуваного H.264/AVC, його офіційно затверджено у 2013 році. Головною метою створення H.265 стало зменшення обсягу даних, необхідного для передачі або зберігання відео, без втрати якості.

Цей кодек особливо ефективний для відео з високою роздільною здатністю, таких як 4K та 8K, що робить його популярним у потокових сервісах,

цифровому телебаченні, відеоспостереженні та мобільних застосунках. Попри свою ефективність, H.265 вимагає більшої обчислювальної потужності для кодування та декодування, що може бути викликом для старішого або малопотужного обладнання. Проте завдяки високій якості та ефективності H.265 залишається одним із провідних стандартів у сфері відеокодування і широко використовується в сучасних системах відеоспостереження. Розраховувати глибину відеоархіву будемо з урахуванням цього стандарту:

Таблиця 1.6. Розрахунок обсягу відеоархіву для однієї камери 4 МП

Параметри налаштування IP камери							
Розширення	Швидкість (кадрів/с)	Потік	1 день/Гб	7 днів/Гб	14 днів/Гб	30 днів/Гб	60 днів/Гб
4 МП	25	6,42	71,04	497,30	994,59	2131,27	4262,54
	15	3,85	42,63	298,38	596,76	1278,76	2557,53
	8	2,06	22,73	159,13	318,27	682,01	1364,01
	5	1,28	14,21	99,46	198,92	426,25	852,51
	1	0,26	2,84	19,89	39,78	85,25	170,50

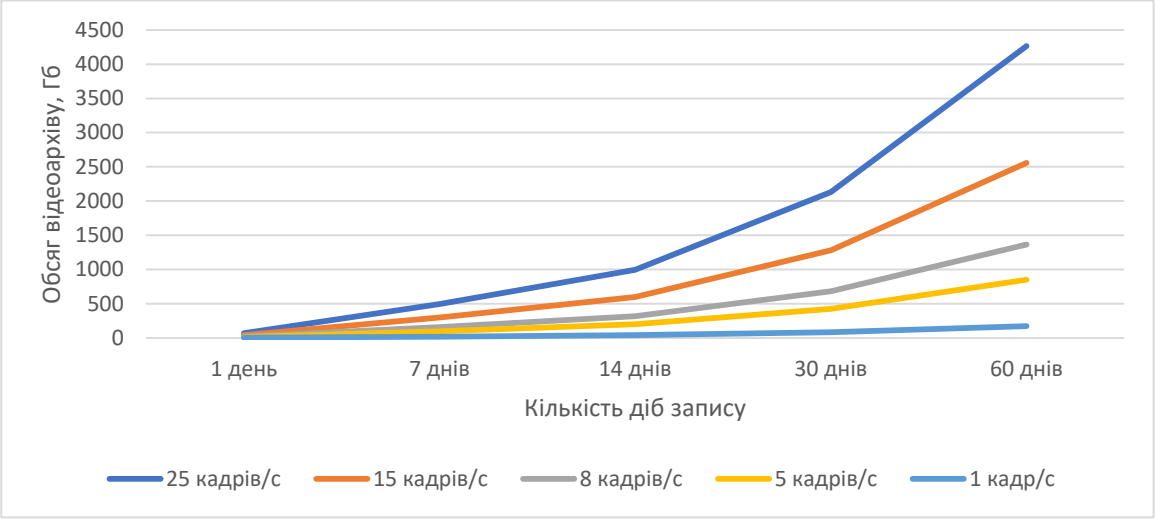


Рисунок 1.28. Графічне зображення залежності 4 МП камери кількості кадрів на секунду до глибину відеоархіву

Проаналізувавши таблицю та діаграму можна зробити висновок, що оптимальним буде використання швидкості запису 15 кадрів/с. При такій швидкості запису важливі деталі на зображені не загубляться, а обсяг пам'яті, який необхідний для зберігання відео буде сягати 18 ТБ. При такій конфігурації запису і кількості камер – необхідно встановити до відеореєстратора 2 жорстких диска, по 10 ТБ кожен. Це дасть змогу зберігати архів 30 діб.

2 ЕКОНОМІЧНИЙ РОЗДІЛ

Цей проект є науково-дослідною розробкою. що має на меті розрахувати вартість створення комплексної системи безпеки підприємства на базі обладнання Hikvision**.** У дипломній роботі ми знайдемо структурований та обґрунтований підхід до впровадження сучасної системи безпеки, що базується на перевірених рішеннях і технологіях. Це дозволить забезпечити високий рівень захисту персоналу, ресурсів та інфраструктури підприємства**.** Для оцінки якості цього науково-дослідного проекту ми детально визначаємо трудомісткість і вартість його розробки**.** Повний перелік усіх етапів і робіт, що виконуються в рамках цього дослідження, наведено в Таблиці 2.1.

Таблиця 2.1 Розподіл робіт по етапах і видах виконавців.

Етап проведення НДР	Вигляд робіт	Посада виконавця
Розробка технічного завдання (ТЗ)	1.Складання і затвердження ТЗ для НДР по розробці «Проектування комплексної системи безпеки підприємства на основі обладнання Hikvision»	Дипломник, керівник
Вибір напряму дослідження	1. Збір і вивчення науково-технічної літератури. 2. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняння. 3. Розробка плану проведення досліджень для подальшої розробки.	Дипломник керівник

Продовження таблиці 2.1. Розподіл робіт по етапах і видах виконавців

Етап проведення НДР	Вигляд робіт	Посада виконавця
Теоретичні і експериментальні дослідження	1. Історичні передумови та еволюція комплексних систем безпеки 2. Дослідження напряму систем відеоспостереження 3. Системи контролю та управління доступом 4.Алгоритми отримання інформації в сучасних системах відеоспостереження. 5.Порівняння технологічних рішень різних брендів обладнання для реалізації проекту 6. Розробка технічного завдання на проектування комплексної системи безпеки підприємства 7.Проектування комплексної системи безпеки підприємства	Дипломник керівник консультанти
Узагальнення і оцінка результатів досліджень	1.. Оцінка повноти вирішення завдань. 2.. Складання і оформлення звіту. 3. Розгляд результатів проведеною НДР і прийняття рішення.	Дипломник керівник консультанти

За відсутності належної нормативної бази, тривалість виконання окремих робіт визначається на основі ймовірнісних оцінок, наданих самими виконавцями. Очікувана трудомісткість робіт (визначена як витрат певної кількості днів на конкретний етап роботи) представлена в табл.. 2.2. Як видно, життєвий цикл щодо системи відеоспостереження починається із складання технічного завдання та завершується безпосередньо проектуванням комплексної системи безпеки (стадія проекту узгоджується).

Таблиця 2.2.Очікувана трудомісткість робіт

Вигляд роботи	Очікуваний час виконання (дні)
1. Складання і затвердження ТЗ для НДР по розробці ««Проектування комплексної системи безпеки підприємства на основі обладнання Hikvision»	1
2. Збір і вивчення науково – технічної літератури, технічної документації і інших матеріалів.	2
3. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка.	2
4. Розробка плану проведення досліджень для подальшої розробки.	2
5. Дослідження напряму систем відеоспостереження	3
6. Системи контролю та управління доступом	5
7. Алгоритми отримання інформації в сучасних системах відеоспостереження	5
8. Порівняння технологічних рішень різних брендів обладнання для реалізації проекту	3
9 Розробка технічного завдання на проектування комплексної системи безпеки підприємства.	2
10. Проектування комплексної системи безпеки підприємства	2
Всього:	27

Через значну роль інтелектуальної праці у створенні науково-технічної продукції, собівартість та ціна виконання науково-дослідних робіт (НДР) формуються з таких основних статей витрат:

1. Витрати на матеріали –380 грн.

2.До витрат «Основна заробітна плата» відносяться оплата праці виконавців, безпосередньо притягнених до її виконання. Розмір основної заробітної плати

для науково-дослідних робіт (НДР) розраховується з урахуванням кількості залучених фахівців різних категорій, обсягу роботи, яку вони виконують, а також їхньої середньоденної заробітної плати.Згідно зі статтею 8 Закону України «Про Державний бюджет України на 2025 рік», встановлено такі показники:

- Мінімальна місячна заробітна плата з 1 січня 2025 року становить 8000 гривень.
- Мінімальна погодинна тарифна ставка — 48 гривень.

. Середня зарплата за один робочий день для кожного виконавця визначена по формулі:

Зден= п.т.с. * 8;

де п.т.с – погодинна тарифна ставка, грн..;

8 – тривалість робочого дня,год.

Витрати на основну заробітну плату, НДР, що включаються в собівартість, приведені в таблиці 2.3.

Таблиця 2.3 Витрати на основну заробітну плату.

Виконавець	Погодинна тарифна ставка, грн	Денна ставка, грн	Трудомісткість робочих днів	Сума основної зарплати,грн
Дипломник	48,00	364	27	9828,00
Керівник	80,50	644	1	644,00
Консультант по економіч. част.	70,50	564	0,25	141,00
Консультант по охороні праці	70,50	564	0,25	141,00
Нормоконтроль	70,50	564	0,25	141,00
Всього (Зо)				10895,00

3. Додаткова заробітна плата розраховується як відсоток від основної заробітної плати**.** У наукових установах цей показник зазвичай становить 10-12% від суми основної заробітної плати.

Зд=10%Зо= 10895,00*0,1 = 1089,50 грн

4. До собівартості науково-дослідних робіт (НДР) включаються відрахування до єдиного соціального внеску (ЄСВ)**,** які для більшості роботодавців в Україні становлять 22% від бази нарахування

Зєсв=0,22*(Зо+Зд)=0,22*(10895,00 +1089,50) = 2636,59 грн.

5. Накладні витрати — це кошти, що йдуть на управління та господарське обслуговування всіх науково-дослідних робіт (НДР), які виконує організація. У наукових установах їхня частка зазвичай коливається від 40% до 120% від загальної суми основної та додаткової заробітної плати**.**

Рнакл= (З0+Зд)*0,5= (10895,00 +1089,50) * 0,6 = 7190,70 грн.

На основі даних, отриманих по кожній статті витрат, ми сформували калькуляцію планової собівартості всієї науково-дослідної роботи (НДР)**.**

Таблиця 2.4. Калькуляція планової собівартості

Статті витрат	Сума, грн.
1. Матеріали	380,00
2. Основна заробітна плата	10895,00
3. Додаткова заробітна плата	1089,50
4. Відрахування до єдиного соціального внеску	2636,59
5. Накладні витрати	7190,70
Планова собівартість (Спл)	22221,79

Плановий прибуток визначений по формулі:

Ппл = 0,1*Спл= 0,1*22221,79= 2222,18 грн

Де 0,1 – норматив, який враховує граничний рівень рентабельності, встановлений чинним законодавством для науково-технічної продукції..

Договірна ціна визначається по формулі:

Цндр = Спл + Ппл = 22221,79+ 2222,18= 24443,97 грн.

Звідси ціна реалізації НДР становить:

Цр = Цнір + ПДВ = 24443,97 + 24443,97 *0,2= 29332,77 грн.

3 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

Охорона праці спрямована на забезпечення безпечних і нешкідливих умов для робітників. На сучасному етапі технічного розвитку вона набуває дедалі більшого значення.

Забезпечення безпеки на робочому місці ґрунтується на досягненнях науки про організацію праці, ергономіки, гігієни та фізіології людини, а також психофізіологічних факторів. Крім того, рівень охорони праці залежить від швидкості впровадження новітніх технологій, рівня механізації та автоматизації виробничих процесів.

Тема мого проекту: «Проектування комплексної системи безпеки підприємства на основі обладнання Hikvision». Запровадження систем безпеки на підприємствах вимагає ретельного врахування норм охорони праці та промислової безпеки. Монтаж та експлуатація обладнання Hikvision потребують дотримання правил роботи з електричними пристроями, захисту даних та уникнення кібератак. Особливу увагу слід приділити роботі з мережевими інфраструктурами, розташуванню відеокамер та забезпеченню правомірного використання зібраної інформації.

Забезпечення безпеки праці можливо лише за умови суворого дотримання вимог трудового законодавства, державних стандартів України та нормативних актів, що регламентують збереження здоров’я працівників.

3.1 Аналіз небезпечних та шкідливих чинників, що впливають на працівника

Під час роботи за комп’ютером на людину можуть впливати такі негативні фактори:

Випромінювання електромагнітного поля;

Коливання яскравості екрану;

Тривале перебування в статичному положенні.

Сукупний ефект цих факторів може зменшувати енергетичний потенціал організму, погіршувати імунітет, викликати м’язову втому та інші негативні наслідки.

3.2 Розробка заходів з охорони праці

Зменшити вплив перерахованих факторів ризику і зберегти здоров'я людині, яка постійно використовує в роботі ПК, дозволяє дотримання всіх заходів і засобів, передбачених охороною праці.

Мікроклімат робочої зони працівників, вентиляція

Освітлення робочого місця має бути рівномірним, а рівень шуму в межах допустимих значень, щоб запобігти перевтомі.

Рівні позитивних і негативних іонів в повітрі приміщень з ВДТ повинні задовольняти санітарно-гігієнічним нормам № 2152-80.

Освітлення робочого місця, шум, вібрація

Штучне освітлення в приміщеннях з робочими місцями, обладнаними ЕОМ і ПЕОМ, має здійснюватись системою загального рівномірного освітлення. Значення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300 - 500 лк.

Як джерело світла при штучному освітленні застосовуються переважно люмінесцентні лампи.

Значення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300 - 500 лк.

Система загального освітлення має становити суцільні або переривчасті лінії світильників, розташовані збоку від робочих місць (переважно зліва), паралельно лінії зору працюючих Застосування світильників без розсіювачів та екрануючих грат заборонено.

Рівні звукового тиску в октавних смугах частот мають відповідати вимогам СН 3223-85, ГОСТ 12.1.003-83, ГР 2411-81.

Організація робочого місця користувача ПК

– Важливо, щоб офісний працівник сидячи за комп'ютером знаходився за добре освітленим робочим столом. Найчастіше саме погане освітлення робочого місця надає більш згубний для зору вплив, ніж сам факт перебування за комп'ютером.

– Робочі столи слід розміщувати таким чином, щоб монітори були орієнтовані бічною стороною до світлових прорізів, щоб природне світло падало переважно ліворуч.

– При розміщенні робочих місць відстань між робочими столами повинна бути не менше 2,0 м, а відстань між бічними поверхнями відеомоніторів - не менше 1,2 м.

– Конструкція робочого столу повинна забезпечувати оптимальне розміщення на робочій поверхні використовуваного обладнання.

– Конструкція робочого стільця або крісла повинна забезпечувати підтримку раціональної робочої пози працівника.

– Клавіатуру слід розташовувати на поверхні столу на відстані 100..300 мм від краю, зверненого до користувача, або на спеціальній поверхні, відокремленій від основної стільниці.

– Екран відеомонітора повинен знаходитися від очей користувача на відстані 600-700 мм, але не ближче 500мм.

Рисунок 3.1. Правильне положення оператора ПК на робочому місці

Безпека праці при роботі за комп’ютером передбачає, що тривалість безперервної роботи за комп'ютером без регламентованої перерви не повинна перевищувати 2 години.

Не рекомендується працювати за комп'ютером більше 6 годин за зміну. Рекомендується робити перерви в роботі за ПК тривалістю 10 хвилин через кожні 50 хвилин роботи. Під час регламентованих перерв доцільно виконувати комплекси вправ.

При нерегламентованій роботі підвищеної інтенсивності можливі головні болі, нервові зриви та інше.

3.3 Пожежна безпека

Належна пожежна безпека – це інтегральна складова організації виробничих приміщень, що ґрунтується на дотриманні чинних законодавчих норм. Сфера пожежного захисту регулюється Правилами пожежної безпеки, затвердженими наказом Міністерства внутрішніх справ України, із періодичними доповненнями та уточненнями, що відображають сучасні вимоги.

Навіть при оснащенні будівель різноманітними системами пожежогасіння, сигналізації та внутрішніми пожежними кранами, офісні приміщення повинні бути додатково обладнані основними засобами гасіння пожеж. До них відносяться вогнегасники, кошми (спеціальні негорючі покривала), ящики з піском, бочки з водою, пожежні відра, багри, ломи, сокири та інші пристосування, причому вогнегасники вважаються найбільш зручними у використанні.

За своєчасне та повне забезпечення об’єктів заходами пожежного захисту відповідає роботодавець спільно з керівниками відповідних підрозділів. Вони зобов’язані розробити та впровадити комплекс заходів, що включає створення протипожежного режиму та інструкцій, відповідно до вимог чинних нормативних актів.

Режим пожежного захисту повинен містити детальний опис зон спеціального призначення та встановлювати правила їх експлуатації та обслуговування, зокрема:

- шляхи евакуації;
- спеціально відведені зони для куріння (так звані «курилки»);
- приміщення для зберігання продукції та сировини;
- території для стоянки автомобілів.

Рисунок 3.2. Засоби пожежогасіння

Ключовим елементом протипожежного режиму є розробка алгоритму дій на випадок пожежі. Обов’язковим є створення чіткого плану евакуації, в якому буде описано порядок відключення електроустановок та визначено послідовність дій співробітників у надзвичайній ситуації.

Основні складові алгоритму дій:

Оповіщення про пожежу – використання системи сигналізації та негайний виклик рятувальних служб.

Організація евакуації – дотримання встановлених маршрутів виходу та контроль безпечного переміщення людей.

Застосування засобів пожежогасіння – правильне використання вогнегасників та інших протипожежних систем.

Взаємодія з екстреними службами – оперативне надання інформації щодо загоряння та потенційних ризиків.

ВИСНОВКИ

У результаті виконання дипломного проєкту було здійснено всебічне дослідження сучасних підходів до побудови комплексних систем безпеки, що поєднують підсистеми відеоспостереження, охоронної сигналізації та контролю доступу. Робота охопила як історичний розвиток відповідних технологій, так і практичний аналіз актуальних технічних рішень, що застосовуються на підприємствах із підвищеними вимогами до фізичного захисту.

На основі аналізу технічної інформації, користувацьких відгуків, стандартів та практик проєктування було сформовано технічне завдання на побудову інтегрованої системи безпеки, адаптованої до потреб підприємства, що обслуговує засоби фізичного захисту. Здійснено порівняльний огляд обладнання провідних виробників у сфері безпеки (Hikvision, Dahua, Axis), що дозволило обґрунтовано визначити перевагу рішень на базі продукції Hikvision як найбільш збалансованих у співвідношенні функціональності, надійності та вартості.

Визначено, що впровадження сучасної комплексної системи безпеки дозволяє не лише підвищити рівень охорони об’єкта, а й створити передумови для автоматизованого управління доступом, централізованого моніторингу та відеоаналітики. Такий підхід сприяє підвищенню ефективності роботи персоналу, зниженню ризиків людського фактору та оперативному реагуванню на інциденти.

Таким чином, поставлену в дипломній роботі мету досягнуто повністю. Запропонована система безпеки відповідає сучасним технічним вимогам, є масштабованою, інтегрованою та має практичну цінність для підприємств, діяльність яких пов’язана з технічним обслуговуванням об’єктів критичної інфраструктури. Результати дослідження можуть бути використані як основа для впровадження або модернізації систем безпеки на аналогічних об’єктах

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1 Гребенніков В. Комплексні системи захисту інформації. Проектування, впровадження, супровід. – Litres, 2018..

2 Безсонова А. О., Василенко О. Д. Застосування систем контролю доступу для різних типів підприємств. – 2023.

3 Гульков О. М. ОГЛЯД ПРОГРАМНИХ ЗАСОБІВ ОХОРОННИХ СИСТЕМ. – 2015.

4 Катеринчук І., Бабарика А., Табенський С. Аналіз сучасного стану побудови систем відеоспостереження. – 2018.

5 Benson A. Arduino Home Security & Environment Monitoring System. Medium.com. 01.12.2018. URL: https://medium.com.

6 Bissessar D., Gorodnichy D. O. Integrating LPR with CCTV systems: problems and solutions //Automatic Target Recognition XXI. – SPIE, 2011. – Т. 8049. – С. 188-200..

7 Norman T. L. Electronic access control. – Elsevier, 2011.

8 Arduino Create. [Електроний ресурс]. – Режим доступу: https://www.arduino.cc/en/main/create.

9 Христич В. В. и др. Системи пожежної та охоронної сигналізації //Академія пожежної безпеки України. – 2001.

10 McTague D., Doug Smith D. The Alarm Book A Guide to Burglar and Fire Alarms.

11 Семеренська В. В. Дослідження методів виявлення аномалій за допомогою відеоаналітики на основі штучного інтелекту у комплексних системах безпеки. – 2023.

12 Пересада М. Д., Кисіль Т. М. Відеокамери з функціями штучного інтелекту //III всеукраїнська науково-практична конференція «Сучасні інтелектуальні інформаційні технології в науці та освіті». – С. 153.

ДОДАТОК А. Слайди мультимедійної презентації

ПРОЕКТУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ БЕЗПЕКИ НА ОСНОВІ ОБЛАДНАННЯ HIKVISION

ДИПЛОМНА РОБОТА

Керівник:
к.ф.н., доцент каф. КБ та ТЗІ ДУІТЗ Стайкуца С.В.

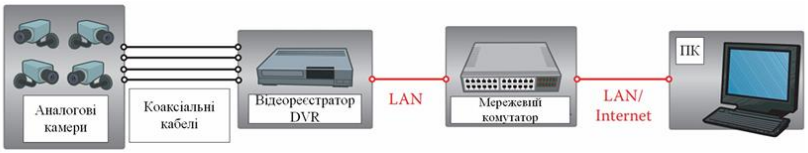
Виконав:
студент групи 4КБ-02 Кондратюк Д.В.

2025

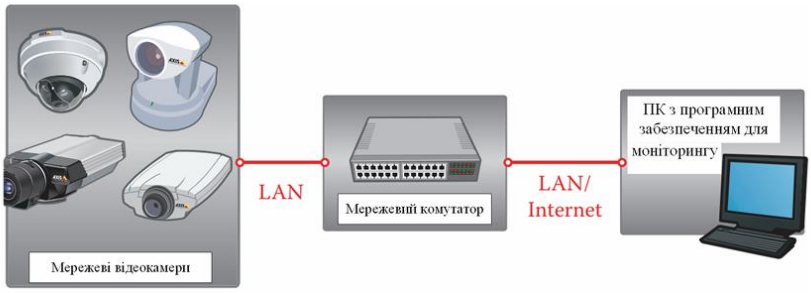
Теорія візуального спостереження

Стримування	*Якщо потенційні злочинці знають, що за ними спостерігають і записують їхні дії, вони можуть вирішити, що ризик бути викритими значно переважає можливість "заробити".*
Ефективність	*Залежно від кількості камер спостереження та їхнього розташування, одночасний перегляд відео в реальному часі та архівних записів може підтвердити будь-яку незаконну діяльність ще до того, як до відвідувача, клієнта або підозрюваного звернеться служба безпеки.*
Виявлення	*Виявлення злочинців - це найбільш важливий фактор успіху, який надає реальні докази того, що відеоспостереження працює.*
Ефективний охоронець	*Сьогодні охоронцю навіть не обов'язково спостерігати, достатньо лише архівувати за допомогою більш розумних технологій. Це дає змогу створити ефективного охоронця, наділивши пасивну систему спостереження «мозком» і дозволивши їй краще реагувати на потенційні злочинні дії.*

Види систем відеоспостереження та їх компоненти

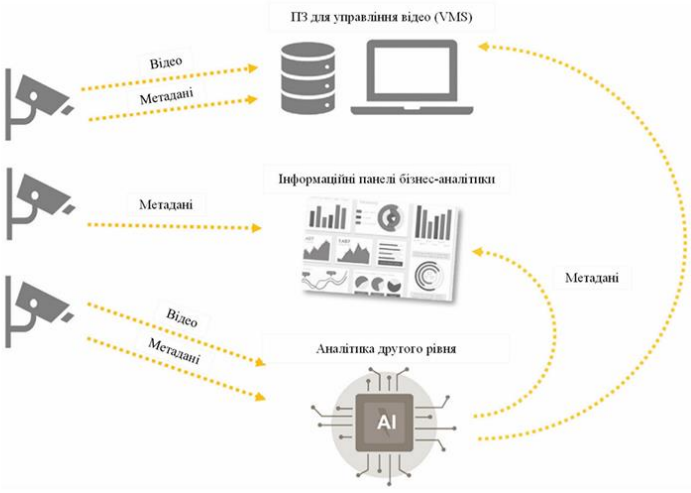


Структурна схема роботи аналогової системи відеоспостереження на базі мережевого відеореєстратора



Структурна схема роботи мережевої відеосистеми з мережевими відеокамерами

Відеоаналітика



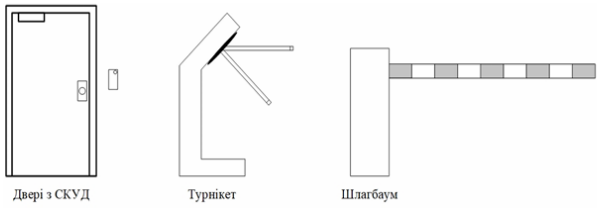
Логіка роботи відеоаналітики

Відеоаналітика - це процес аналізу відеоданих з метою перетворення їх на корисну інформацію. Аналітичні системи використовують складні алгоритми для аналізу відео та перетворення його на дані.

Системи контролю та управління доступом

Ідентифікатори доступу користувачів СКУД

Точка проходу, або охоронний портал - це двері або прохід, що створює точку входу в межі захищеної зони. До поширених видів охоронних порталів належать стандартні двері, турнікети, обертові двері, шлагбауми для в'їзду транспортних засобів та інші.

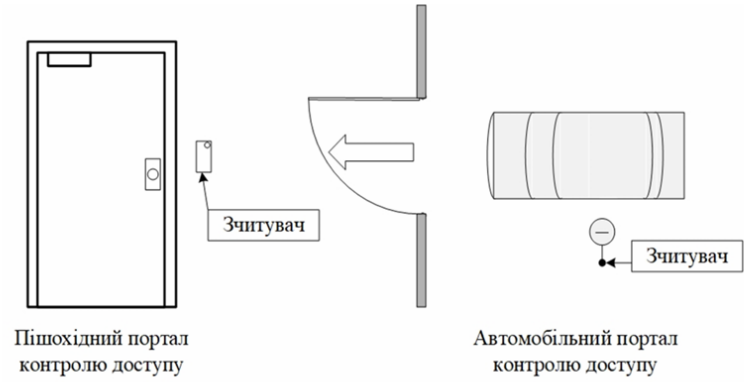


Приклади охоронних порталів

Типи порталів контролю доступу

Практично кожен портал контролю доступу має наступні п'ять загальних елементів:

- Метод або пристрій перевірки особи;
- Механізм замикання;
- Пристрій, що реагує на тривогу;
- Датчик запиту на вихід



Пішохідний портал контролю доступу

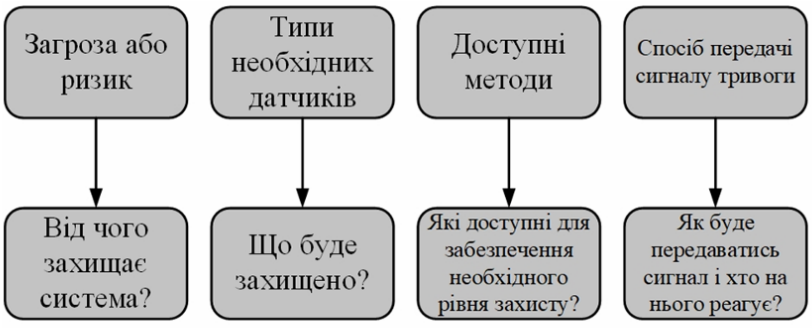
Автомобільний портал контролю доступу

Елементи контролю доступу

Електронні системи контролю доступу складаються з електронних елементів, фізичних елементів, операційних елементів, елементів інформаційних технологій та логічних елементів для створення цілісної робочої системи, яка забезпечує швидкий та надійний доступ авторизованих користувачів до об'єкта за мінімальних довгострокових витрат для організації.

Охоронна сигналізація

Вибір належної системи сигналізації - справа непроста, адже потреби кожного домовласника або власника бізнесу відрізняються, як набір відбитків пальців. Деякі фактори, які визначають вимоги до індивідуальної системи сигналізації та питання, на які необхідно відповісти, включають в себе:

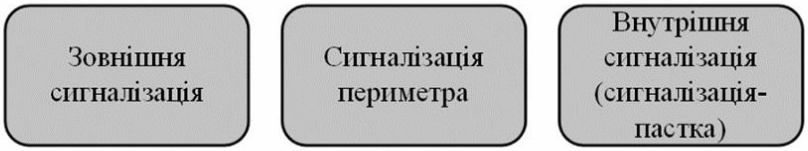


Вимоги до індивідуальної системи охорони

Компонентний склад системи охорони

Базова система охоронної сигналізації складається з наступних елементів:

Інші основні компоненти включають пристрої для постановки та зняття системи сигналізації з-під охорони, обладнання для автоматичного набору номера, джерело живлення (наприклад, ДБЖ) та електропроводку між різними компонентами. Та має три рубежі захисту:



Загальний стан ринку безпеки України

При виборі обладнання для побудови комплексної системи безпеки важливо враховувати не лише вартість пристроїв, але й їхню надійність, функціональні можливості та репутацію виробника.

Порівняння ключових характеристик обладнання

Параметр або характеристика	Hikvision	Dahua	Axis Communications
Якість зображення відеокамер	Висока (до 4K, технологія DarkFighter)	Висока, але дещо програє конкурентам в нічному режимі	Висока, особливо вдень (кольорова передача)
Асортимент технологічних рішень	Найширший (велика екосистема бренду)	Великий	Вузько сегментований, фокус на відеоспостереження
Простота програмного забезпечення для роботи	iVMS-4200, HikCentral: інтуїтивно зрозуміле	SmartPSS: більш складне в налаштуваннях	AXIS Camera Station: складне, вимагає професійного досвіду
Інтеграція з іншими системами	Широкі можливості (ONVIF, API, SDK)	Аналогічні з Hikvision, але менше SDK	Є інтеграція, але обмежено пропрієтарністю
Інтелектуальні функції (AI)	Багато, доволі точні за тестами	Багато, менш точні за тестами	Багато, є спеціалізовані
Технічна підтримка	Широка, з сервісними центрами та актуальною документацією	Широка	Сервісне обслуговування та ТП через партнерів
Надійність та стабільність роботи	Висока	Висока, бувають скарги на прошивку	Висока
Впізнаваність бренду	Популярний бренд	Популярний бренд	Популярний серед великих підприємств
Цінова характеристика	Оптимальне співвідношення «ціна/якість»	Середній бюджет	Преміум сегмент ринку, відносно аналогів конкурентів

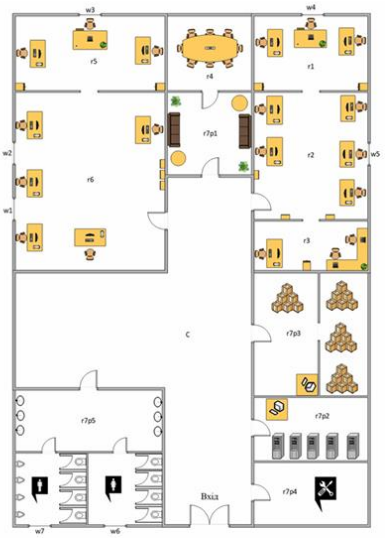
Інформаційна база для аналізу формувалася на основі вивчення технічної документації, специфікацій обладнання, а також узагальнення оцінок і коментарів користувачів та фахівців, оприлюднених у відкритих джерелах – профільних форумах, оглядових сайтах, маркетплейсах і професійних оглядах.

Висновки порівняльного аналізу

Загалом, з урахуванням комплексної оцінки технічних характеристик, експлуатаційної зручності, доступності сервісу та економічної ефективності, обладнання торгової марки Hikvision є найбільш доцільним вибором для впровадження у системі безпеки підприємства.

Ключові переваги бренду Hikvision серед конкурентів

Технічне завдання на проектування комплексної системи безпеки



Розроблений план приміщення підприємства

ОБ'ЄКТ ЗАХИСТУ:

Підприємство з продажу та обслуговування систем фізичного захисту об'єктів

ЗАВДАННЯ СИСТЕМИ:

Спроектована система повинна вирішувати питання контролю за певними приміщеннями підприємства, його та персоналу, від дій зловмисників та вирішення конфліктних ситуацій, шляхом впровадження охоронної сигналізації, системи відеоспостереження, та системи контролю та управління доступом. Система повинна працювати в одній екосистемі Hikvision.

МЕТА ВПРОВАДЖЕННЯ:

Підвищення рівня фізичної безпеки підприємства, унеможливлення несанкціонованого доступу до критично важливих зон об'єкту, забезпечення фіксації певних подій, для їх подальшого аудиту

Вимоги до конкретних підсистем

Підсистема відеоспостереження повинна виконувати наступні функції:
- *Відеомоніторинг внутрішніх приміщень та зон;*
- *Зберігання відеоархіву не менше ніж 30 діб;*
- *Наявність інтелектуальних функцій та відеоаналітики;*
- *Можливість віддаленого перегляду відео через ПК/та мобільний додаток.*

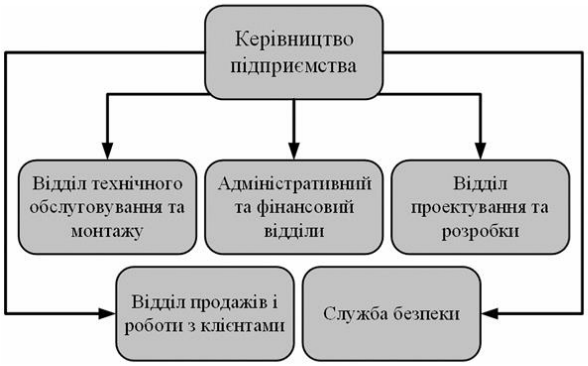
Задачі підсистеми охоронної сигналізації:
-Контроль проникнення до всіх зон підприємства;
-Наявність сповіщувачів розбиття скла в ключових зонах підприєвства;
-Можливість підключення системи до центрального пульта спостереження;
-Функції постановки/зняття з охорони за допомогою клавіатури та або мобільного додатку.

Система контролю та управління доступом повинна:
-Обмежувати доступ до важливих зон об'єкту (кабінет керівництва, фінансового відділу, складського приміщення, тощо);
-Формувати журнал подій;
-Мати авторизацію за біометричними даними та або RFID-картками;
-Інтегруватись з системою відеоспостереження (фіксувати зображення при спробах ідентифікації).

Опис приміщень та складу персоналу підприємства

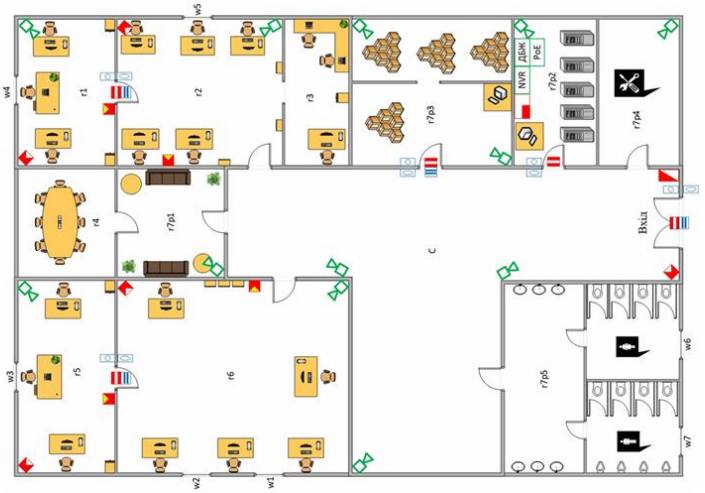
Позначення в кімнатах	Призначення кімнати	Площа приміщення S, м²
C	Коридор	23,5
r1	Кабінет керівництва	8
r2	Відділ проектування та розробки	13
r3	Адміністративний та фінансовий відділ	6
r4	Кімната переговорів	7
r5	Кабінет служби безпеки	9
r6	Відділ продажів і роботи з клієнтами	20
r7p1	Зона відпочинку для персоналу	8
r7p2	Серверна кімната	15
r7p3	Складське приміщення	10
r7p4	Відділ технічного обслуговування (майстерня)	10
r7p5	Вбиральня	13
w1, w2, w3, w4, w5, w6, w7	Вікна	
Загальна площа		142,5 м²

Призначення приміщень підприємства



Організаційно-штатна структура підприємства

Спроектована комплексна система безпеки на основі Hikvision

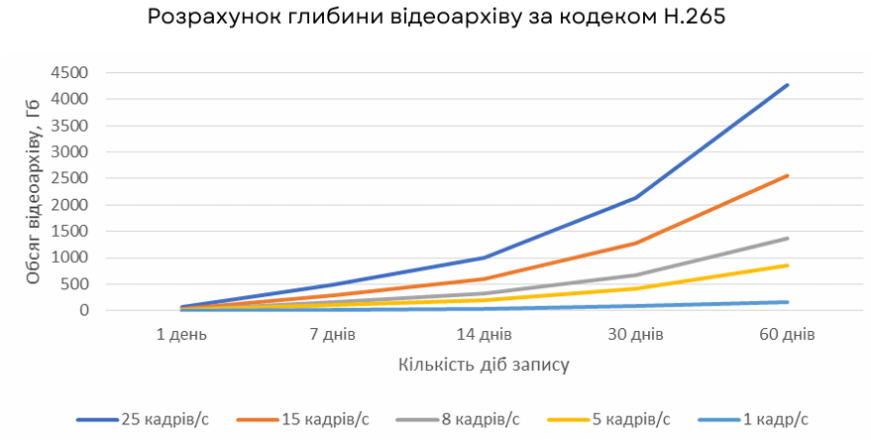


Позначення елементу	Опис елементу
NVR	Відеореєстратор
	Відеокамера
ДБЖ	Джерело безперебійного живлення та АКБ
PoE	PoE комутатор

Система відеоспостереження

Позначення елементу	Опис елементу
	Сповіщувач відкриття
	Сповіщувач руху
	Датчик розбиття скла
	Клавіатура
	Централь системи охорони

Система охоронної сигналізації



Залежність кількості кадрів на секунду до глибину відеоархіву при розподільній якості камери в 4 МП

Проаналізувавши таблицю та діаграму можна зробити висновок, що оптимальним буде використання швидкості запису 15 кадрів/с. При такій швидкості запису важливі деталі на зображені не загубляться, а обсяг пам'яті, який необхідний для зберігання відео буде сягати 18 ТБ.
При такій конфігурації запису і кількості камер – необхідно встановити до відеореєстратора 2 жорстких диска, по 10 ТБ кожен. Це дасть змогу зберігати архів 30 діб.

Висновки

Ході роботи було здійснено:

- Дослідження сучасних підходів до побудови комплексних систем безпеки, які поєднують в собі підсистеми відеоспостереження, охоронної сигналізації та контролю доступу;
- Було сформовано технічне завдання на побудову інтегрованої системи безпеки, адаптованої до потреб підприємства.
- Проаналізовано и порівняно, за ключовими характеристиками, обладнання провідних брендів на ринку України. Це дозволило обґрунтовано визначити перевагу одного із них і будувати систему на базі цієї продукції;
- Визначено, що впровадження сучасної комплексної системи безпеки дозволяє не лише підвищити рівень охорони об'єкта, а й створити передумови для автоматизованого управління доступом, централізованого моніторингу та відеоаналітики

Результати роботи та досліджень можуть бути використані як основа для впровадження або модернізації систем безпеки на аналогічних об'єктах

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Кондратюка Дениса Вячеславовича

(прізвище, ім`я та по батькові)

Спеціальність *123 «Комп'ютерна інженерія»*

Освітня програма *«Безпека комп'ютерних систем і мереж»*

Керівник дипломного проекту (роботи) *Стайкуца Сергій Володимирович*

(прізвище, ім`я та по батькові)

Тема дипломного проекту (роботи) *Проектування комплексної системи безпеки підприємства на основі обладнання Hikvision*

Обсяг розрахунково-пояснювальної записки *77* сторінок

Обсяг графічної (презентаційної) частини *18* аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту завданню

Представлений на рецензію дипломний проект відповідає затвердженій темі та виконаний відповідно технічному завданню. Дипломний проект присвячений темі проектування комплексної системи безпеки та складається з пояснювальної записки та мультимедійної презентації, що містить логіку роботи та отримані при виконанні рішення.

б) характеристика виконання кожного розділу дипломного проекту

Пояснювальна записка складається з основного розділу (базова інформація, виявлення проблематики, розробка технічного завдання, розрахунки технологічних параметрів), економічного розділу, розділу охорони праці та додатків. Перелічені розділи поетапно охоплюють розробку, виконані докладно та обґрунтовано. Розділ охорони праці містить загальну інформацію та аналіз небезпечних факторів. Економічний розділ проекту містить обчислення вартості науково-дослідної розробки.

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту

Графічна частина складається з 18 слайдів мультимедійної презентації, виконаної у програмному продукті MS PowerPoint, які містять ілюстративні схеми, алгоритми, рішення та розрахунки, передбачені технічним завданням. Пояснювальна записка виконана акуратно та у відповідності до норм. Якість виконання графічної частини проекту та пояснювальної записки добра, розробку виконано у повному обсязі.

г) перелік позитивних якостей дипломного проекту *Комплексно розглянуто екосистему бренду Hikvision – технології, компонентний склад, можливості.*

Проектування системи безпеки розглянуто на прикладі конкретного об'єкту інформаційної діяльності.

д) основні недоліки дипломного проекту *Було б доцільним при проектування впровадити додаткові підсистеми захисту. При розрахунках глибини архіву додали б об'єктивності додаткові завдання, наприклад, порівняння при різній якості зображення, при використанні детектора руху, застосування при різних кодеках тощо. Слабка деталізація мережевої архітектури: немає розгорнутої схеми розміщення комутаторів, VLAN, резервування каналів.*

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Добре*

Загальна оцінка *Добре*

Прізвище, ім'я, по батькові рецензента *к.т.н. Шибаєва Наталя Олегівна*

Місце роботи і посада рецензента *Національний університет «Одеська політехніка», доцент кафедри інформаційних технологій*

Підпис: _____

«27» 06 2025 р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Кондратюка Дениса Вячеславовича

(прізвище, ім`я та по батькові)

Спеціальність: *123 "Комп'ютерна інженерія"*

Освітня програма: *«Безпека комп'ютерних систем і мереж»*

Тема дипломного проекту: *Проектування комплексної системи безпеки підприємства на основі обладнання Hikvision*

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проекту (графічного матеріалу і розрахунково-пояснювальної записки) *Дипломний проект виконано відповідно технічному завданню. Пояснювальна записка містить __ сторінки. У пояснювальній записці розглянуто проблематику проектування комплексної системи безпеки на основі обладнання з напряму ТЗО бренду Hikvision. Графічна частина складається з слайдів мультимедійної презентації, які також містять креслення, передбачені технічним завданням. Якість виконання пояснювальної записки та графічної частини добра, розробку виконано в повному обсязі.*

б) самостійність роботи над проектом: *Протягом всього строку дипломного проектування та переддипломної практики здобувач освіти Кондратюк Д.В. виконував всі етапи розробки проекту, без порушення термінів. Роботу студент виконував в більшій мірі самостійно, з оглядом на рекомендації керівника та отримуючи зворотній зв'язок.*

в) теоретична підготовка випускника (випускниці): *Здобувач освіти Кондратюк Д.В. під час роботи над дипломним проектом проаналізував достатню кількість літературних джерел та матеріалів за даною тематикою.*

Вважаю, що теоретична підготовка дипломника якісна і він готовий до захисту дипломного проекту.

г) вміння розв'язувати виробничі та конструкторські питання

Під час дипломного проектування здобувач освіти Кондратюк Д.В. приймав рішення щодо вибору обладнання, аналізував вимоги на етапах проектування, розробляв проектні рішення, обґрунтовував вибір платформи розробки, мови програмування та алгоритмів реалізації розробленого проекту.

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Добре*

Прізвище, ім'я, по батькові керівника дипломного проекту

Стайкуца Сергій Володимирович

Місце роботи і посада керівника дипломного проекту

"Державний університет інтелектуальних технологій і зв'язку", доцент кафедри кібербезпеки та технічного захисту інформації, помічник декана факультету інформаційних технологій та кібербезпеки

Підпис

«18» 06 2025 р.

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
(ДИПЛОМНОГО ПРОЕКТУ)
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Кондратюк Денис Вячеславович
здобувач освіти гр. 4КБ-02, та

Стайкуца Сергій Володимирович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до дипломного проекту фахового молодшого бакалавра на тему:

«Проектування комплексної системи безпеки підприємства на основі обладнання Hikvision» (автор роботи – Кондратюк Д.В., керівник роботи – Стайкуца С.В.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2025 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи і даємо згоду на обробку персональних даних.

Виконавець _____ / Кондратюк Д.В. /

Керівник _____ / Стайкуца С.В. /

«18» червня 2025 р.

ДОВІДКА

циклової комісії КТ та ПІ
про допуск до захисту дипломного проєкту
здобувача (здобувачки) освіти IV курсу
відділення комп'ютерних систем групи 4КБ-02

Кондратюка Дениса Вячеславовича

на тему *Проектування комплексної системи безпеки підприємства на основі обладнання Hikvision*

Висновок відповідальної особи за проведення нормоконтролю:
пояснювальна записка до дипломного проєкту виконана з некритичними порушеннями ДСТУ та оформлена відповідно до вимог Положення про дипломне проєктування

(підпис) *18.06.2025* (дата) *Петрашова В.І.* (П.І.Б.)

Висновок відповідальної особи за перевірку роботи на наявність академічного плагіату *згідно звіту про перевірку від 18.06.2025 р. значення коефіцієнту подібності в роботі становить 11,13%, коефіцієнт цитування – 0,91%.*

(підпис) *18.06.2025* (дата) *Краснокутська К.Г.* (П.І.Б.)

Попередня експертиза (малий захист) дипломного проєкту

здобувача (здобувачки) освіти *Кондратюка Д.В.* (П.І.Б.)

проведена «*18*» *червня* 20*25* р.

Висновки *Пояснювальна записка до дипломного проєкту виконана у повному обсязі. Випускна кваліфікаційна робота (дипломний проєкт) відповідає вимогам Положення про дипломне проєктування та рекомендована до захисту.*

Голова ЦК КТ та ПІ (підпис) *Кривченко Ю.В.* (П.І.Б.)

Звіт подібності

метадані

Назва організації
Odesa Technical Professional College of Odesa National University of Technology
Заголовок
Проєктування комплексної системи безпеки підприємства на основі обладнання Hikvision

Автор
Кондратюк Денис Вячеславович
Науковий керівник / Експерт
Стайкуца Сергій Володимирович

підрозділ
Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету"

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

25	13393	109175
Довжина фрази для коефіцієнта подібності 2	Кількість слів	Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		1
Інтервали	A→	0
Мікропробіли		46
Білі знаки		1
Парафрази (SmartMarks)	a	52

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download	51 0.38 %
2	https://conferences.vntu.edu.ua/public/files/itpf/conf_itpf-2016_all.pdf	46 0.34 %
3	https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download	43 0.32 %
4	https://card-file.ontu.edu.ua/bitstreams/c1f3e592-1123-419d-b14a-4c28662f0f1e/download	42 0.31 %
5	https://revolution.allbest.ru/management/00769018_0.html	39 0.29 %

6	https://card-file.ontu.edu.ua/server/api/core/bitstreams/8da72e29-656f-4ee4-9b22-716dedf53ff5/content	37 0.28 %
7	https://card-file.ontu.edu.ua/bitstreams/53ed22ad-8700-4162-b97a-082a1ad472d6/download	34 0.25 %
8	https://card-file.ontu.edu.ua/server/api/core/bitstreams/a05c07c5-bf65-4cb0-bdfa-e28694707551/content	34 0.25 %
9	https://card-file.ontu.edu.ua/server/api/core/bitstreams/4bb7255e-46d4-4349-9726-9698476da02d/content	31 0.23 %
10	https://card-file.ontu.edu.ua/bitstreams/c1f3e592-1123-419d-b14a-4c28662f0f1e/download	30 0.22 %

з домашньої бази даних (0.29 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Розробка 3D-гри у жанрі survival-horror з налаштуваннями рівнів складності [redacted] 6/12/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	39 (6) 0.29 %

з програми обміну базами даних (0.80 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	2018_6050903_Kolodii_Mykhailo_Bohdanovych_42985 [redacted] 10/26/2024 **National University "Lviv Politechnika" (National University Lviv Politechnika)**	**54 (4) 0.40 %**
2	Долготер_Р-4.1 [redacted] 6/13/2025 State University of Intellectual Technologies and Communications (Кафедра радіоелектронних систем і технологій)	24 (3) 0.18 %
3	2017_6050903_Vitrovyi_Iurii_Iuriiovych_3405 [redacted] 10/26/2024 National University "Lviv Politechnika" (National University Lviv Politechnika)	22 (1) 0.16 %
4	Постоленко_Максим_БК-713м [redacted] 12/20/2024 National University "Zaporizhzhia Polytechnic" (Кафедра "Інформаційна безпека та наноелектроніка")	7 (1) 0.05 %

з Інтернету (10.04 %)

ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	**https://card-file.ontu.edu.ua/bitstreams/53ed22ad-8700-4162-b97a-082a1ad472d6/download**	**183 (14) 1.37 %**
2	**https://conferences.vntu.edu.ua/public/files/itpf/conf_itpf-2016_all.pdf**	**117 (6) 0.87 %**
3	**https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download**	**94 (2) 0.70 %**
4	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/a05c07c5-bf65-4cb0-bdfa-e28694707551/content**	**89 (6) 0.66 %**
5	**https://card-file.ontu.edu.ua/bitstreams/c1f3e592-1123-419d-b14a-4c28662f0f1e/download**	**79 (3) 0.59 %**
6	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/6eb6bf1c-5813-45e6-93c5-25539b4709d3/content**	**76 (4) 0.57 %**
7	https://card-file.ontu.edu.ua/server/api/core/bitstreams/44c16132-5f53-48e2-b6c0-61e9a2f0fd75/content	71 (7) 0.53 %

8	https://card-file.ontu.edu.ua/bitstreams/62baa43e-b968-4993-bb54-8cf8761a89b2/download	62 (4) 0.46 %
9	https://studopedia.org/6-120929.html	60 (5) 0.45 %
10	https://card-file.ontu.edu.ua/bitstreams/549ee9fe-7574-4ae5-b500-9fe2711f33e6/download	59 (5) 0.44 %
11	**https://revolution.allbest.ru/management/00769018_0.html**	**50 (2) 0.37 %**
12	https://card-file.ontu.edu.ua/bitstreams/8999d5af-6274-44f4-ae78-d23e08048d38/download	40 (2) 0.30 %
13	https://card-file.ontu.edu.ua/bitstreams/82a6d375-2b69-4233-b80f-fbfd149b7747/download	39 (5) 0.29 %
14	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/8da72e29-656f-4ee4-9b22-716dedf53ff5/content**	**37 (1) 0.28 %**
15	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/4bb7255e-46d4-4349-9726-9698476da02d/content**	**36 (2) 0.27 %**
16	https://card-file.ontu.edu.ua/server/api/core/bitstreams/ead3fa83-2e3d-4cd7-bfbd-1d5ed04c1ce4/content	31 (2) 0.23 %
17	https://card-file.ontu.edu.ua/bitstreams/29489599-0581-4ce6-8890-c3b13d9f2e0e/download	26 (2) 0.19 %
18	https://card-file.ontu.edu.ua/bitstreams/bbaf3f38-16a8-4070-bead-5562769b7c71/download	23 (1) 0.17 %
19	https://card-file.ontu.edu.ua/bitstreams/aed610a6-43ef-47e0-9066-e85c89456f3e/download	21 (2) 0.16 %
20	https://www.manualslib.com/manual/2228673/Hikvision-Ds-Pdmc-Eg2-Wb.html	21 (3) 0.16 %
21	https://card-file.ontu.edu.ua/bitstreams/2b75599e-e1ac-412d-bf09-10d2eb49022f/download	21 (1) 0.16 %
22	https://card-file.ontu.edu.ua/server/api/core/bitstreams/76e3c1ec-4240-49ea-88c2-457a2c955630/content	19 (2) 0.14 %
23	https://card-file.ontu.edu.ua/bitstreams/1dff552d-7200-49b8-ae1d-ba76a1335685/download	16 (2) 0.12 %
24	https://card-file.ontu.edu.ua/server/api/core/bitstreams/fc8a1853-39fc-4671-8807-2fd27ddb0779/content	15 (1) 0.11 %
25	https://card-file.ontu.edu.ua/server/api/core/bitstreams/21ac499a-a9e9-4137-810c-5f21a0318048/content	12 (1) 0.09 %
26	https://card-file.ontu.edu.ua/bitstreams/63ee88cb-a3d0-4005-9cf2-0cff89f28c0d/download	12 (1) 0.09 %
27	https://card-file.ontu.edu.ua/bitstreams/3eefb1c3-f20f-4e1f-84b4-f7ccdc6077af/download	11 (1) 0.08 %
28	https://books.google.com/books/about/The_Alarm_Book.html?id=ivdBSipclV8C	10 (1) 0.07 %
29	http://elcat.pnpu.edu.ua/docs/%D0%91%D0%96%D0%942020.pdf	10 (1) 0.07 %
30	https://studopedia.org/11-67047.html	5 (1) 0.04 %

Список прийнятих фрагментів (немає прийнятих фрагментів)

ПОРЯДКОВИЙ НОМЕР	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»
Освітньо-професійна програма: **«Безпека комп'ютерних систем і мереж» Група:** 4КБ- 02

Дипломний **проект здобувача освіти денної форми навчання КБ.** 02.09.000.ДП

КОНДРАТЮКА
ДЕНИСА В'ЯЧЕСЛАВОВИЧА