

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ  
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-методичний комплекс  
«Інститут післядипломної освіти»

Кафедра системного програмування і спеціалізованих комп'ютерних систем

«До захисту допущено»

Завідувач кафедри

Віталій РОМАНКЕВИЧ

(підпис) (ініціали, прізвище)

“ \_\_\_ ” \_\_\_\_\_ 20\_\_ р.

**Дипломний проєкт**

на здобуття ступеня бакалавра

зі спеціальності

123 «Комп'ютерна інженерія»

(код і назва)

на тему: Цифрові обчислювальні засоби для відеоспостереження за об'єктами

Виконав (-ла): слухач (-ка) IV курсу, групи ЗКІ-зп71

(шифр групи)

Кучер Андрій Петрович

(прізвище, ім'я, по батькові)

(підпис)

Керівник доцент каф. СПіСКС, к.т.н., доцент Клятченко Я.М.

(посада, науковий ступінь, вчене звання, прізвище та ініціали)

(підпис)

Консультант з нормоконтролю Клятченко Ярослав Михайлович.

(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали)

(підпис)

Рецензент \_\_\_\_\_

(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали)

(підпис)

Засвідчую, що у цьому дипломному  
проєкті немає запозичень з праць інших  
авторів без відповідних посилань

Слухач \_\_\_\_\_

(підпис)

Київ – 2020 року

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ  
імені ІГОРЯ СІКОРСЬКОГО»**

**Навчально-методичний комплекс  
«Інститут післядипломної освіти»**

Кафедра системного програмування і спеціалізованих комп'ютерних систем

Рівень вищої освіти – перший (бакалаврський)

Напрямок підготовки 123 «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ  
Завідувач кафедри

\_\_\_\_\_ Віталій РОМАНКЕВИЧ  
(підпис)

“\_\_\_” червня 2020 р.

**ЗАВДАННЯ**

**на дипломний проєкт слухачу**

IV курсу, групи ЗКІ-зп71 Кучер Андрій Петрович \_\_\_\_\_  
(прізвище, ім'я, по батькові)

1. Тема проєкту Цифрові обчислювальні засоби для відеоспостереження за об'єктами

керівник проєкту \_\_\_\_\_ доцент каф. СПіСКС, к.т.н., доцент Клятченко Я.М. \_\_\_\_\_,  
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом НМК „ІПО” КПІ імені Ігоря Сікорського від «\_\_\_» \_\_\_\_\_  
2020 р. №1130-с

2. Термін подання слухачем проєкту \_\_\_\_\_ червня 2020р.

3. Вихідні дані до проєкту див. Технічне завдання

4. Зміст пояснювальної записки \_\_\_\_\_  
аналіз існуючих рішень та обґрунтування теми дипломного проєкту  
розроблення програмного забезпечення

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо) \_\_\_\_\_

Підключення ір камер. Схема структурна \_\_\_\_\_

РоЕ. Схема структурна \_\_\_\_\_

Підключення відеокамер по оптоволокну. Схема структурна \_\_\_\_\_

Алгоритмів термінального наведення. Схема структурна \_\_\_\_\_

#### 6. Консультанти розділів проєкту\*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Клятченко Я.М.		

7. Дата видачі завдання \_\_\_\_\_

#### Календарний план

№ з/п	Назва етапів виконання дипломного проєкту	Термін виконання етапів проєкту	Примітка
1	Вивчення літератури за тематикою проєкту	20.11.19	
2	Розроблення та узгодження технічного завдання	15.01.2020	
3	Аналіз існуючих рішень	25.01.2020	
4	Підготовка матеріалів першого розділу дипломного проєкту	05.02.2020	
5	Розроблення програмного забезпечення	15.02.2020	
6	Відлагодження програмного продукту	26.02.2020	
7	Підготовка матеріалів другого розділу дипломного проєкту	15.03.2020	
8	Розроблення програмної частини	05.04.2020	
9	Підготовка матеріалів третього розділу дипломного проєкту	29.04.2020	
10	Підготовка матеріалів четвертого розділу дипломного проєкту	12.05.2020	
11	Підготовка графічної частини дипломного проєкту	23.05.2020	
12	Оформлення документації дипломного проєкту	05.06.2020	

Слухач \_\_\_\_\_

(підпис)

(Ім'я та ПРІЗВИЩЕ)

Керівник проєкту \_\_\_\_\_

(підпис)

**Ярослав КЛЯТЧЕНКО**

(Ім'я та ПРІЗВИЩЕ)

\* Консультантом не може бути зазначено керівника дипломного проєкту

## АНОТАЦІЯ

Метою даного дипломного проекту є проектування системи відеоспостереження. Розглянути цифрові обчислювальні засоби для відеоспостереження за об'єктами.

Відповідно до мети роботи необхідно вирішити наступні завдання:

1. Розглянути поняття про системи відеоспостереження.
2. Проаналізувати основні цифрові (комп'ютерні) системи відеоконтролю, представлені на ринку.
3. Охарактеризувати інтегровані системи безпеки.
4. Розкрити особливості технології динамічного транскодингу.
5. Окреслити необхідність у відео спостереженні.
6. Дослідити інформаційне обстеження трафіка в локальній мережі.
7. Здійснити проектування системи відеоспостереження.
8. Провести математичні розрахунки системи.
9. Проаналізувати заходи забезпечення безпеки мережі. Об'єкт дослідження - проектування системи відеоспостереження.

## АННОТАЦИЯ

Целью данного дипломного проекта является проектирование системы видеонаблюдения. Рассмотреть цифровые вычислительные средства для видеонаблюдения за объектами.

Согласно цели работы необходимо решить следующие задачи:

1. Рассмотреть понятие о системах видеонаблюдения.
2. Проанализировать основные цифровые (компьютерные) системы видеоконтроля, представленные на рынке.
3. Охарактеризовать интегрированные системы безопасности.
4. Раскрыть особенности технологии динамического транскодинг.
5. Обозначить необходимость в видео наблюдении.
6. Исследовать информационное обследование трафика в локальной сети.
7. Осуществить проектирование системы видеонаблюдения.
8. Провести математические расчеты системы.
9. Проанализировать меры обеспечения безопасности сети.

Объект исследования - проектирование системы видеонаблюдения.

## **ABSTRACT**

The aim of this graduation project is to design a video surveillance system. Consider digital computing tools for video surveillance of objects.

According to the purpose of the work, it is necessary to solve the following tasks:

1. Consider the concept of video surveillance systems.
2. The main digital (computer) video monitoring systems on the market have been analyzed.
3. Describe integrated security systems.
4. To reveal the features of dynamic transcoding technology.
5. Indicate the need for video surveillance.
6. Explore traffic information survey in the local network.
7. Carry out the design of a video surveillance system.
8. Conduct mathematical calculations of the system.
9. Analyze network security measures.

Object of study - designing a video surveillance system.

Поз.	Формат	ПОЗНАЧЕННЯ	НАЙМЕНУВАННЯ	Кільк. акр.	№ примірн.	Прим.
			<u>Документація загальна</u>			
			<u>Новорозроблена</u>			
	A4	ІАЛЦ 466120.002 ТЗ	Цифрові обчислювальні засоби для відеоспостереження за об'єктами.	1		
			Технічне завдання			
	A4	ІАЛЦ 466120.003 ТП	Цифрові обчислювальні засоби для відеоспостереження за об'єктами.	2		
			Відомість технічного проекту			
	A4	ІАЛЦ 466120.004 ПЗ	Цифрові обчислювальні засоби для відеоспостереження за об'єктами.	72		
			Пояснювальна записка			
	A1	ІАЛЦ 466120.005 Д1	Цифрові обчислювальні засоби для відеоспостереження за об'єктами.	1		
			Підключення ір камер.			
			Схема структурна.			
ІАЛЦ 466120.001.ОА						
Змін.	Арк.	№ докум.	Підпис	Дата		
Розробив		Кучер А.П.			Літ.	Аркуш
Перевірив		Клятченко Я.М				Аркушів
Н.контроль		Клятченко Я.М				30
Затвердив		Романкевич В.О				84
Цифрові обчислювальні засоби для відеоспостереження за об'єктами. Опис альбому.					КПІ ім. Ігоря Сікорського НМК «ІПО» Каф. СПіСКС Гр. ЗКІ-зп71	



## ЗМІСТ

1. Розглянути поняття про системи відеоспостереження.
2. Проаналізувати основні цифрові (комп'ютерні) системи відеоконтролю, представлені на ринку.
3. Охарактеризувати інтегровані системи безпеки.
4. Розкрити особливості технології динамічного транскодингу.
5. Окреслити необхідність у відео спостереженні.
6. Дослідити інформаційне обстеження трафіка в локальній мережі.
7. Здійснити проектування системи відеоспостереження.
8. Провести математичні розрахунки системи.
9. Проаналізувати заходи забезпечення безпеки мережі.

					ІАЛЦ 466120.002 ТЗ			
Изм.	Лист.	№ докум.	Підпис	Дата	Цифрові обчислювальні засоби для відеоспостереження за об'єктами. Технічне завдання	Літ.	Лис	Листів
Розроб.		Кучер А.П.						
Перевір.		Клятченко Я.М					32	1
Н. Контр.		Клятченко Я.М				КПІ ім. Ігоря Сікорського НМК «ІПО» Каф. СПіСКС, Гр. ЗКІ-зп71		
Затверд.		Романкевич В.О.						

Поз.	Формат	ПОЗНАЧЕННЯ	НАЙМЕНУВАННЯ	Кільк. акр.	№ примірн.	Прим.
			<u>Документація загальна</u>			
			<u>Новорозроблена</u>			
	A4	ІАЛЦ 466120.002 ТЗ	Цифрові обчислювальні засоби для відеоспостереження за об'єктами.	1		
			Технічне завдання			
	A4	ІАЛЦ 466120.003 ТП	Цифрові обчислювальні засоби для відеоспостереження за об'єктами.	2		
			Відомість технічного проекту			
	A4	ІАЛЦ 466120.004 ПЗ	Цифрові обчислювальні засоби для відеоспостереження за об'єктами.	72		
			Пояснювальна записка			
	A1	ІАЛЦ 466120.005 Д1	Цифрові обчислювальні засоби для відеоспостереження за об'єктами.	1		
			Підключення ір камер.			
			Схема структурна.			
			ІАЛЦ 466120.003.ТП			
Змін.	Арк.	№ докум.	Підпис	Дата		
Розробив		Кучер А.П.			Літ.	Аркуш
Перевірив		Клятченко Я.М				Аркушів
						33
Н.контроль		Клятченко Я.М			84	
Затвердив		Романкевич В.О			КПІ ім. Ігоря Сікорського НМК «ІПО» Каф. СПіСКС Гр. ЗКІ-зп71	
			Цифрові обчислювальні засоби для відеоспостереження за об'єктами			
			Відомість технічного проекту.			

Поз.	Формат	ПОЗНАЧЕННЯ	НАЙМЕНУВАННЯ	Кільк. акр.	№ примірн.	Прим.
A1		ІАЛЦ 466120.006Д2	Цифрові обчислювальні засоби для відеоспостереження за об'єктами. РоЕ. Схема структурна.	1		
A1		ІАЛЦ 466120.007Д3	Цифрові обчислювальні засоби для відеоспостереження за об'єктами. Підключення відеокамер по оптоволокну. Схема структурна.	1		
A4		ІАЛЦ 466120.008Д4	Цифрові обчислювальні засоби для відеоспостереження за об'єктами. Алгоритм термінального наведення. Схема структурна.	1		
		Диск CD-ROM	Текст ПЗ. Тексти програм. Графічний матеріал	1		
ІАЛЦ 466120.003.ТП						
Змін.	Арк.	№ докум.	Підпис	Дата	Арк.	
					34	

# **Пояснювальна записка до дипломного проєкту**

на тему: Цифрові обчислювальні засоби для відеоспостереження за об'єктами

---

---

Київ – 2020 року

## ЗМІСТ

ВСТУП .....	2
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ.....	39
1.1. Поняття про системи відеоспостереження .....	39
1.2. Використання комутаторів для відеоспостереження <b>Error! Bookmark not defined.</b>	
1.3. Технологія PoE і відеокомутатори .....	46
1.4. Популярні моделі PoE відеокомутаторів.....	50
РОЗДІЛ 2. ХАРАКТЕРИСТИКА ПІДПРИЄМСТВА І НЕОБХІДНІСТЬ У ВІДЕОСПОСТЕРЕЖЕННІ.....	53
2.1 Необхідність у відеоспостереженні.....	53
2.2 Інформаційне обстеження трафіка в локальній мережі .....	65
2.3. Проектування системи відеоспостереження .....	82
РОЗДІЛ 3. МАТЕМАТИЧНІ РОЗРАХУНКИ СИСТЕМИ.....	85
РОЗДІЛ 4. ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖІ.....	92
ВИСНОВКИ.....	68
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	69

### ДОДАТОК: Копії графічних матеріалів

ІАЛЦ 466120.005Д1 Підключення ір камер. Схема структурна

ІАЛЦ 466120.006Д2 PoE. Схема структурна

ІАЛЦ 466120.007Д3 Підключення відеокамер по оптоволокну. Схема структурна

ІАЛЦ 466120.008Д4 Алгоритм термінального наведення. Схема структурна

					<b>ІАЛЦ 466120.004 ПЗ</b>			
Изм.	Лист.	№ докум.	Підпис	Дата	Цифрові обчислювальні засоби для відеоспостереження за об'єктами Пояснювальна записка	Літ.	Лис	Листів
Розроб.		Кучер А.П.						
Керівн.		Клятченко Я.М					36	
Консульт.		Клятченко Я.М				КПІ ім. Ігоря Сікорського НМК «ІПО» Каф. СПіСКС, Гр. ЗКІ-зп71		
Н. Контр.		Клятченко Я.М						
Затверд.		Романкевич В.О.						

## ВСТУП

**Актуальність дослідження.** В наші дні системи відеоспостереження виділилися в самостійну область засобів охорони, що мають власні правила і особливості експлуатації. Системи відеоспостереження - найефективніший технічний засіб забезпечення безпеки, що дозволяє оперативно зафіксувати факт скоєння того чи іншого протиправного діяння, а також дає можливість контролювати якість роботи співробітників, загальну ситуацію на об'єкті.

У сучасному світі безпеку об'єкта – будь-то квартира, замський будинок, школа або офіс - неможлива без ведення відеоспостереження. Саме відеоспостереження дозволяє вчасно виявити, попередити або припинити правопорушення. Сьогодні складно знайти об'єкт, де не було б потрібно відеоспостереження.

На сьогоднішній день можна контролювати системою відеоспостереження і системою контролю доступом на віддаленій відстані за допомогою сучасних технологій передачі даних, якими є локальні мережі, Інтернет, WI-FI з'єднання. Можливий контроль над торговим, або виробничим підприємством, не виходячи з офісу.

У більшості випадків система відеоспостереження дозволяє записувати зображення на носії інформації, а також виконувати інші функції. Наприклад, повністю управляти відеокамерами, повертати об'єктив, масштабувати зображення, створювати архіви записів, переглядати і управляти ними. Крім запису відео, сучасні системи відеоспостереження можуть також сприймати аудіо інформацію, реагувати на рух і виконувати охоронні функції.

**Метою нашої роботи** є проектування системи відеоспостереження. Розглянути цифрові обчислювальні засоби для відеоспостереження за об'єктами.

Відповідно до мети роботи необхідно вирішити **наступні завдання:**

1. Розглянути поняття про системи відеоспостереження.

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		37

2. Проаналізувати основні цифрові (комп'ютерні) системи відеоконтролю, представлені на ринку.

3. Охарактеризувати інтегровані системи безпеки.

4. Розкрити особливості технології динамічного транскодингу.

5. Окреслити необхідність у відео спостереженні.

6. Дослідити інформаційне обстеження трафіка в локальній мережі.

7. Здійснити проектування системи відеоспостереження.

8. Провести математичні розрахунки системи.

9. Проаналізувати заходи забезпечення безпеки мережі.

**Об'єкт дослідження** - проектування системи відеоспостереження.

**Предмет дослідження** - цифрові обчислювальні засоби для відеоспостереження за об'єктами.

**Структура роботи.** Складається зі вступу, чотирьох розділів основної частини, висновків та списку використаних джерел.

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		3

# РОЗДІЛ 1

## ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

### 1.1. Поняття про системи відеоспостереження

Системи відеоспостереження за останні роки стали невід'ємною частиною нашого життя, і основною частиною системи безпеки, як приватного житла, офісу, так і території. Відеоспостереження може бути вуличним, внутрішнім і прихованим. Без запису і з записом відеосигналу на відеокасету або на жорсткий диск комп'ютера. Кількість відеокамер і їх різноманітність, найчастіше, обмежена тільки матеріальними можливостями замовника [4].

Залежно від типу використовуваного обладнання системи відеоспостереження діляться на цифрові та аналогові. Камери відеоспостереження бувають вуличного і внутрішнього виконання, кольорові і чорно-білі, прихованої і відкритої установки.

Залежно від того, де встановлюється система відеоспостереження, наприклад, квартира, будинок, офіс або прилегла територія, необхідний різний набір обладнання.

Велику роль відіграє якість зображення. У системах відеоспостереження воно складається з якості зображення, одержуваного на камері, і якості використовуваної відеосистеми. У відеокамері є об'єктив і матриця. Розмір діафрагми в об'єктиві визначає як "широко" або "далеко" може бачити камера. Матриця ж, допомагає перетворити зображення в відеосигнал. Розмір її буває різним: 1,2/3,1/2,1/3,1/4. Чим він більший, тим вище якість зображення. Якість об'єктива залежить від того, яка оптика в ньому встановлена: дешевша - пластикова або дорожча – скляна [11, с .108].

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		4

Існує два способи запису даних - аналоговий і цифровий. Аналоговий спосіб, більш простий, передбачає, що запис буде вестися на звичайний або спеціальний відеомагнітофон. При цьому сигнал обробляється квадратором або мультиплексором. Обидва ці пристрої дозволяють робити запис відеоданих з декількох камер одночасно. При використанні квадратора швидкість запису збільшується, але при цьому істотно втрачається якість запису. При використанні мультиплексора якість запису значно краще, так як записується повний кадр, а не зменшений в 4-9 разів. Але швидкість втрачається в силу того, що кадри посилаються по черзі з кожної камери. Чим більше кількість камер буде в системі, тим менше буде швидкість запису. Накопичувачем при використанні аналогового способу запису є проста або спеціальна відеокасета.

У цифрових відеореєстраторів є ряд додаткових можливостей: моментальний пошук за часом, за датою, по особі, що цікавить або події; перезапис інформації без втрати якості; миттєве перемотування; дистанційне керування і т. д.

Цифрове обладнання системи відеоспостереження в даний час дозволяє не тільки спостерігати і записувати події, що відбуваються, але і програмувати реакцію всієї системи безпеки при виникненні нештатних ситуацій [22, с .56].

У деяких випадках потрібно управляти системою на значній відстані від об'єкта. Наприклад, якщо у вас кілька об'єктів відеоспостереження розташовані в різних місцях, будь-то квартира і заміський будинок. Сучасні пристрої дозволяють робити це за допомогою локальних мереж або Інтернету. Наприклад, можна спостерігати за дітьми, які відпочивають за містом, не виходячи з кабінету офісу або перебуваючи в іншому місті. Застосування віддаленого доступу у відеосистемі безпеки дозволяє отримувати зображення, працювати з архівом, змінювати налаштування.

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		5

Будь-яке зображення можна дивитися і записувати в повній темряві. Для цього поруч з камерою встановлюють прожектор інфрачервоного випромінювання. Та ж можна використовувати спеціалізовані системи, такі як: датчики руху, система ідентифікації осіб по зображенню людини. Система сканує і запам'ятовує обличчя тих, хто знаходиться в зоні дії відеокамери, потім здійснює їх аналіз, порівняння з базою даних і розпізнавання з високим ступенем точності.

Проектування, монтаж і налагодження систем відеоспостереження, звичайно ж, краще довірити професіоналам. Вони не тільки допоможуть підібрати необхідне обладнання, відповідно до ваших цілей і матеріального достатку, але і після монтажу системи, будуть обслуговувати по гарантії.

Відеоспостереження - це вагомий аргумент проти різного роду зловмисників. Але потрібно розуміти, що відеоспостереження – це один з найдорожчих способів захисту житла і його можна віднести більше до допоміжних методів захисту. Тому максимально використовувати можливості відеоспостереження краще спільно з охоронно-пожежними сигналізаціями [26].

До складу системи відеоспостереження обов'язково включаються різні пристрої, що дозволяють транслювати і отримувати відеопотік. Вони монтується всюди: в будинках, офісах, квартирах, розважальних закладах, бізнес-центрах. За рахунок такого обладнання можна спостерігати за подіями, що відбуваються на об'єктах з будь-якого місця в онлайн-режимі. Система відеоспостереження складається з великого числа компонентів, які мають різну функціональність і технічні характеристики.

Захисні системи можна розділити по комплектації на цифрові та аналогові. Аналогова апаратура функціонує за досить простим принципом: кадри записуються на відеореєстратор. Більшою популярністю користуються цифрові прилади спостереження, тому що вони відрізняються безліччю

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		6

функціональних можливостей і можуть інтегруватися з іншими системами безпеки [33].

Цифрові системи відеоспостереження: передають дані з відеокамер, пожежних і охоронних комплексів на прилади відображення відомостей; фіксують і аналізують інформацію; автоматично приймають рішення, що дозволяє забезпечувати безпеку об'єкта. Найчастіше аналогові системи використовуються для приватного користування і монтуються в житлових будівлях. Цифрові механізми застосовуються на великих підприємствах, які складаються з великого числа об'єктів [19, с .76].

Системи відеоспостереження можуть мати різноманітний склад і функціональність. На її комплектацію впливає багато факторів: особливості об'єкта, де монтуються механізми відеоспостереження; завдання, які потрібно вирішити; фінансові можливості людей. Найпростіша система складається з монітора і відеокамери, які взаємодіють один з одним. На думку багатьох, цих пристроїв достатньо, щоб організувати якісне спостереження за об'єктами. Але це помилкова думка. При використанні подібної системи відеоспостереження перед монітором повинен постійно перебувати черговий. Крім того, система забезпечує лише частковий перегляд об'єкта. Для усунення подібних недоліків і розширення функціональності пристрою потрібно користуватися таким компонентним складом системи:

- Комп'ютер;
- Джерела живлення;
- програмне забезпечення;
- відеокамери;
- прилади для обробки відеосигналу, квадратори, мультиплекс ори [12].

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		7

Відеокамери бувають монохромними і кольоровими. Вони поділяються на кілька головних типів:

- Цифрові;
- провідні аналогові;
- суміщені з GSM або Wi-Fi приймачами.

Комплект відеоспостереження включає відеореєстратор. Це прилад, який записує і архівує відомості з камер протягом довгого часу, дозволяючи в подальшому їх переглядати. У відеореєстраторах передбачено кілька записуючих режимів:

- безперервний: використовується, як правило, в касах, банках і т.д.;
- при фіксації руху в огляді камери;
- за розкладом, створеним користувачем;
- за сигналом тривоги [19, с. 54].

Залежно від фінансових можливостей, вимог і бажань замовника, системи відеоспостереження можуть містити додаткові пристрої: матричні комутатори; термопринтери; блоки безперебійного живлення; пульт управління PTZ відеокамерами; модулятори; пристрої підсвічування.

На сучасному ринку представлений величезний асортимент аксесуарів для систем відеоспостереження: захист від грози; термокожухи; подовжувачі та дроти; мікрофони; кріплення і кронштейни для відеокамер; поворотні механізми; ІЧ-прожектори; перехідники. Не потрібно вважати аксесуари зайвою розкішшю, тому що в процесі організації систем відеоспостереження вони мають велике значення, особливо, якщо установка обладнання проектується самостійно.

При виборі компонентів для монтажу системи необхідно брати до уваги якість приладів, марку виробника і наявність ліцензії.

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		8

## 1.2 Використання комутаторів для відео спостереження

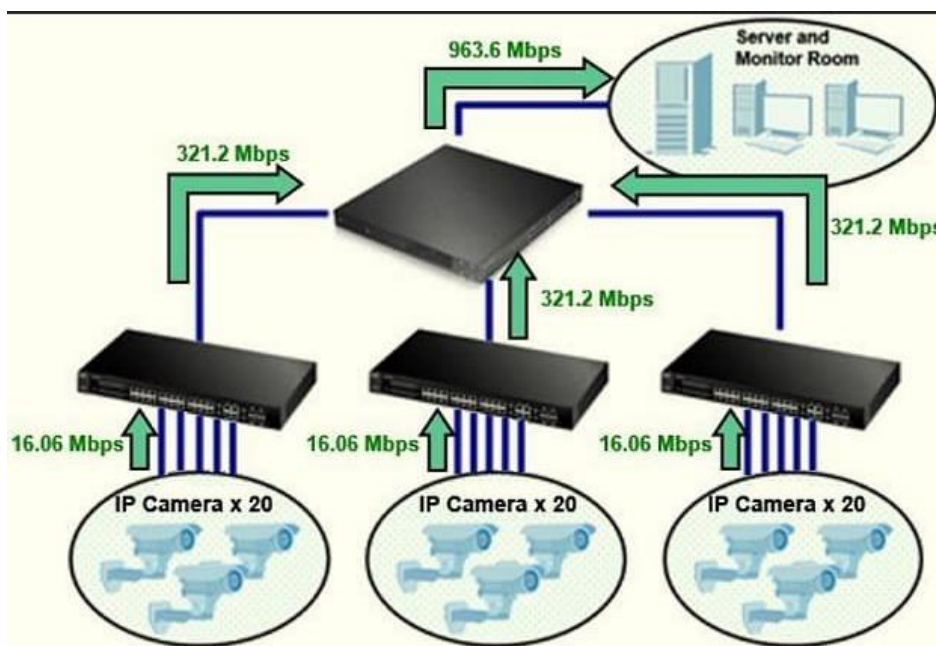
Відеокамери і відеореєстратори, підключені до різних мережевих комутаторів с POE і без, роутерів, міцно влаштувалися на ринку систем відеоспостереження. Про повсюдний перехід на цифрове обладнання говорити поки передчасно. Однак тенденція до послідовного завоювання ринку і витіснення координатно-матричних структур проглядається вже протягом останніх п'яти років. У відповідній галузі торгівлі з'явилися компанії-виробники, які спеціалізуються тільки на пристроях відеоспостереження, що працюють через Інтернет. У свою чергу збільшилася затребуваність в профільному обладнанні для створення стабільності функціонування системи. Нерідко можна зіткнутися з точкою зору, що полягає в тому, що пристрої ір-відеоспостереження, підключені до всесвітньої павутини, можна приєднати до вже функціонуючої мережі організації, що дає гарантію економії витрат на установку. Разом з тим на практиці ефективність роботи подібної системи не відрізняється високою якістю. Типові мережеві пристрої не можуть подужати навантаження, що збільшилося на них. В результаті виникають неполадки не тільки у функціонуванні пристроїв відеоспостереження, але і всієї мережі підприємства. З цієї причини слід загострити увагу на мережевих комутаторах для систем відеоспостереження, так як на ці пристрої, накладається головне навантаження з перенаправлення масиву інформації [24].

У структурах відеослеження з Internet Protocol нерідко застосовують стандартні мережеві перемикачі, більш знамениті як комутатори. Їх також називають світчі (від англ. «switch»). Такі пристрої створюють об'єднання сполучних елементів місцевої мережі. В ході функціонування комутатор проводить аналіз MAC адрес всього приєданого обладнання і створює особливу таблицю відповідності входів, що дає можливість обмежити

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		9

передачу інформації локальною мережею. В ході розробки структури відеоконтролю, підключеного до мережі Інтернет, увага загострюється на поєднанні технічних параметрів світча, пристроїв відеоспостереження і загальних вимог до функціонування системи.

Кожен мережевий комутатор для відеоспостереження наділений певними можливостями по обробці інформації. Іншими словами, це реальна величина відомостей, яку пристрої здатні обробити за той чи інший проміжок часу. Крім того, також береться до уваги здатність обробляти дані кожного роз'єму. Найбільш часто зустрічаються показники 10-100 мегабіт в секунду і один гігабіт в секунду. Необхідно мати на увазі, що нерідко загальна здатність обробки масиву даних комутатора може виявитися меншою, ніж об'єднане значення всіх входів. Якщо такий пристрій встановити в повному обсязі, то структура не здатна функціонувати в належній якості. Зокрема, користувач буде стикатися з гальмуванням відеозйомки. Крім того, час від часу буде пропадати сигнал [28, с .34].



Дана характеристика комутатора відображає граничне число пристроїв відеоспостереження або інших мережевих компонентів. Для домашнього відеоконтролю нерідко застосовують світчі з маленьким числом входів (від 4). Для спеціалізованих структур експлуатується обладнання з вісьмома,

шістнадцятьма або двадцятьма чотирма роз'ємами. Беручи до уваги число входів, необхідно мати на увазі сполучуваність загальної здатності обробляти інформацію за одиницю часу.

Так само як і пристрої відеоспостереження з Internet Protocol, комутатори можуть розроблятися для зовнішніх (вуличних) і внутрішніх мереж відеоконтролю. Свічі для зовнішнього використання повинні давати гарантію функціонування незалежно від погодних умов. З цієї причини пристрої виготовляються в оболонках посиленої стійкості з рівнем захисту не менше IP66.

Для структур, що монтуються всередині будівель, застосовується комутатори для пристроїв відеоспостереження в звичайному виготовленні. Широко поширені портативні пристрої, які можна встановити на DIN рейку. Але для них характерно невелике число роз'ємів.

### **1.3. Технологія POE і відеокмутатори**

Присутність Power over Ethernet значно полегшує установку структури відеоконтролю, оскільки живлення направляється по звичайному мережевому кабелю (кручена пара). Потрібно відзначити, що комутатор з POE застосовується разом з пристроями відеоспостереження, які підтримують дану опцію (це в обов'язковому порядку знаходить своє відображення в технічних параметрах).

Специфіка перемикачів з Power over Ethernet PoE являє собою технологію для організації інформаційного каналу спільно з живленням для ір відеокамер за допомогою звичайного Ethernet з'єднання. Беручи до уваги труднощі установки ір структур відеоконтролю живлення і передача зображення по єдиному проводу - найкращий варіант. З цієї причини нерідко досвідчені користувачі віддають пріоритет пристроїв з Power over Ethernet. Максимальна відстань передачі відеосигналу ір відеокамери по крученій парі

					<b>ІАПЦ 466120.004 ПЗ</b>	Лист
Изм.	Лист	№ докум.	Підпис	Дата		11

без використання додаткових пристроїв 100 метрів. При цьому варто відзначити, що живити камеру на такій відстані необхідно безпосередньо біля відеокамери [4].

РоЕ комутатор дозволяє передавати і сигнал і напругу по одному кабелю на відстань до 150 метрів. РоЕ комутатор - це відмінне рішення в сфері ір відеоспостереження в 99 % випадків, за винятком (той самий 1 %) коли наприклад, нинішні камери з панорамуванням, зумом і PTZ управлінням з потужністю приблизно в 90 ВАТ не здатні функціонувати без прокладки зайвого кабелю живлення, тому що звичайних 25 ВАТ Power over Ethernet комутатора безумовно не вистачить. Але в останні роки фірми-виробники створюють профільні рішення зі збільшеною потужністю, що дає можливість застосовувати досить потужні пристрої відеоконтролю з відеоаналітикою, а також живити додаткові пристрої (такі, як інфрачервоні освітлювачі). Але занадто покладатися на них не слід. У будь-якій ситуації необхідно скрупульозно обчислити споживану структурою потужність, співвідніши її зі здібностями перемикача [5].

Комутатор РоЕ пропонує блок живлення і підключення даних до РоЕ ІР системі відеоспостереження через мережеві кабелі, такі як Cat5, Cat5e і Cat6. РоЕ комутатор 8 є одним з найпопулярніших комутаторів РоЕ для просто ІР - системи відеоспостереження. Використання РоЕ керованого комутатора для ІР-камера спостереження, щоб забезпечити безпеку людей і бізнесу - дуже поширена поведінка. Зазвичай для різних ІР-систем відео спостереження є розгорнуті комутатори РоЕ з різними портами. Коли мова йде про прийняття технології РоЕ, деякі користувачі можуть подумати, що немає необхідності купувати РоЕ комутатор з відносно високою ціною.

Інжектор РоЕ також може постачати електроживлення ІР-камерами і економити більше простору. Однак, що буде, якщо є багато пристроїв, на яких потрібно підключити десять ІР-камер? В цьому випадку, оптимальним

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		12

варіантом є PoE комутатор. Крім того, PoE комутатори пропонують безліч інших переваг для PoE IP системи відео спостереження [3].

В даний час керовані PoE комутатори стають новою тенденцією. Більш передові, керовані PoE комутатори дозволяють дистанційно керувати робочою потужністю кожної камери з будь-якої точки в системах IP-камер. Це дозволяє адміністраторам перезавантажувати будь-яку IP-камеру PoE, не переходячи в місце розташування камери, заощаджуючи витрати і працю.

Підключені до комутатора PoE, IP-камери можуть бути встановлені в будь-якому місці, і навіть у віддаленому місці розташування. З використанням одного кабелю Cat5e, робоча відстань IP-камери PoE може досягати 100 м. Якщо потрібні більш тривалі робочі відстані, можуть знадобитися PoE повторювачі [6].

Зазвичай всі IP-камери живляться від єдиного джерела (PoE комутатор). Тому підключення центрального UPS (джерело безперервного енергопостачання) до PoE комутатора може забезпечити безперервний контроль в разі відключення електрики.

PoE гігабітні комутатори зазвичай входять в конфігурації 5, 8, 10, 16, 24, 28, 48 і 52 порти. Ці порти можуть бути комбінацією слотів SFP / SFP+ для оптичного з'єднання, але частіше вони являють собою мідні порти з роз'ємами RJ45 спереду, що дозволяє досягати відстані до 100 метрів. З оптичними модулями SFP, можна перейти на відстань до 40 кілометрів.

Існують два стандарти для PoE комутатора: IEEE802.3AF і IEEE802.3AT. Таким чином, PoE комутатори з різними стандартами також пропонують різні потужності на кожному порті для IP-камер. Наприклад, IEEE802.3AF стандартний PoE комутатор 8 працює тільки з IP-камерами, які не перевищують 15,4 Вт. І IEEE802.3AT PoE комутатор може підтримувати макс. до 25 Вт PoE пристроїв.

Чим більше загальна потужність PoE комутатора, тим більше камер та інших пристроїв PoE можуть бути підключені. І максимальна споживана

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		13

потужність комутатора часто тісно пов'язана з його ціною. Однак, якщо вибрати уважно, можна знайти деякі економічні PoE комутатори з більше максимальною споживаною потужністю.

Некерований PoE комутатор тільки пропонує базове з'єднання між мережевими пристроями. У той час як керований PoE комутатор дозволяє користувачам контролювати мережу і брати на себе відповідальність за будь-які конфігурації, які викликають час простою. У довгостроковій перспективі, керований PoE комутатор 8 портів може бути кращим вибором.

IP система відеоспостереження часто складається з PoE комутатора, IP-камери, мережевого відеомагнітофона (NVR) і кабельних систем Cat5e або Cat6. Серед них, PoE комутатор може передавати дані і пропонувати живлення для інших пристроїв [23, с .48].

PoE комутатор часто має 8 портів Gigabit Ethernet RJ45 і 2 порти SFP. Порти RJ45 використовуються для підключення до IP-камер і NVR, а порти SFP підключені до мережі LAN / WAN.



Рис. 1.1. PoE комутатор

На наступному малюнку показано загальне застосування PoE комутатора 8:



Рис. 1.2 Загальне застосування PoE комутатора 8

1. Підключіть маршрутизатор до порту LAN на PoE комутаторі 8 з використанням кабелю Ethernet (cat5e або cat6).

2. Підключіть кабель живлення до комутатора PoE і штепсельної розетки або пристрою захисту від перенапруги.

3. Підключіть IP-камери до порту 1 ~ 8 на PoE комутаторі з використанням подовжувальних кабелів Ethernet.

4. Додайте камери в NVR для перегляду камер і дозволу запису. Якщо потрібні великі відстані, підключіть маршрутизатор до Інтернету.

PoE гігабітний комутатор робить установку спостереження більш безпечним і дешевим. Якщо вирішили створити IP систему відеоспостереження, варто переконатися, що вибрали правильний PoE комутатор для надійної IP системи відеоспостереження. Як правило, PoE комутатор 8 може майже задовольнити всі вимоги до малих IP-спостережень.

#### 1.4. Популярні моделі POE відеокмутаторів

Завдання живлення відеокамер одне зі стандартних в використанні комутаторів PoE. Обладнання застосовують різні ритейлери, в тому числі група компаній X5 RETAIL GROUP.

### *TP-Link T1500-28pct*

Дана модель призначена для монтажу в телекомунікаційну стійку, має 24 порти Fast Ethernet, чотири роз'єми Gigabit Ethernet і два комбінованих гігабітних SFP-слота. До сильних сторін комутатора можна також віднести вбудовані функції захисту і пріоритезації трафіку.

T1500-28pct: 180-ватний енергетичний бюджет ідеально підійшов під їх вимоги. Типові внутрішні камери для відеоспостереження відносяться до другого класу пристроїв з точки зору стандарту IEEE 802.3 af і вписуються в діапазон споживаної потужності від 3,8 до 6,5 ВАТ. В їх системі відеоспостереження використовувалися внутрішні неповоротні моделі камер (без сервоприводів і підігрівачів) [27, с .49].

T2600G-28mps - для 24 гігабітних портів PoE відводиться потужність до 384 Вт. На базі даного комутатора (спільно з TRASSIR) була розгорнута система відеоспостереження в мережі сімейних гіпермаркетів (всього для побудови широкомасштабної системи відеоспостереження замовнику знадобилося близько 750 комутаторів з підтримкою PoE+).

### *Sigrand'a*

Компанія виробляє продукцію для систем відеоспостереження: IP-камери, комутатори (у тому числі з PoE), прожектори PoE і пр. В серії SG-1 моделі мають 6 Ethernet портів, дають потужність до 60 Ст. Цікавість обладнання Sigrand'a в тому, що обладнання можна приєднувати послідовно в одну лінію. Це економить кошти і зменшує витрати на витратні матеріали. Максимальна довжина ланцюга 500м

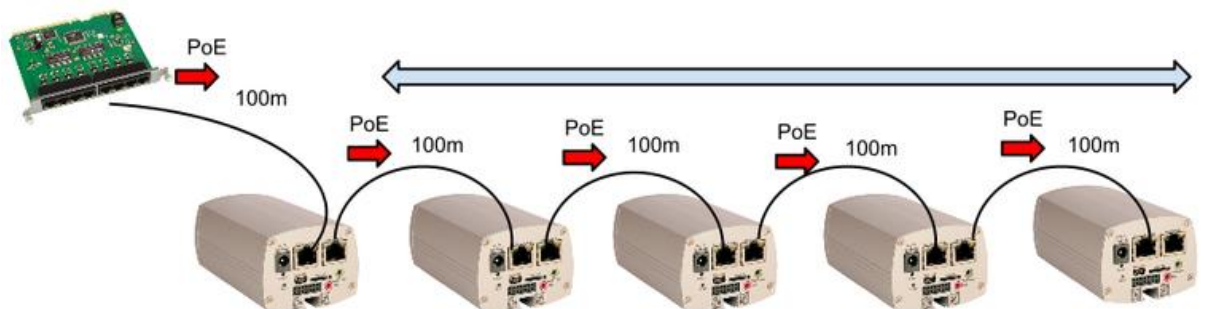


Рис. 1.3. Схематика побудови мережі на базі обладнання Sigrand

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		16

Зовнішній вигляд комутатора представлений на рис. 1.4.



Рис. 1.4. Зовнішній вид Sigrand POE switch

*Raisecom*

Бренд надає широкий вибір різного устаткування і комутаторів, які можна використовувати в системах відеоспостереження. Комутатори серії ISCOM відрізняються великою кількістю портів і можливістю віддаленого управління.



Рис. 1.5. Обладнання RAISCOM

*Cisco*

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		17

Компанія має великий вибір комутаторів, які можуть застосовувати в промисловості. Пристрої відрізняються компактними розмірами, енергоефективні, програмовані. Для програмування використовується продуманий API. Cisco досить поширений бренд, в каталозі якого є високоякісне обладнання для промислового застосування. У компанії сильно завищена якість, а ціна завжди залежить від цього показника.



Рис. 1.6. POE світч Cisco SG100D-08P на 8 портів

Є багато різних інших брендів, які нічим не гірше і не краще (хоча, як подивитися). Вибір краще робити за технічними характеристиками, зовнішнього вигляду, способу монтажу і місця розташування, а також за ціною.

## РОЗДІЛ 2

### ХАРАКТЕРИСТИКА ПІДПРИЄМСТВА І НЕОБХІДНІСТЬ У ВІДЕОСПОСТЕРЕЖЕННІ

#### 2.1 Необхідність у відеоспостереженні

Компанія "Кур'єр сервіс" почала свою діяльність на ринку кур'єрських послуг в 1997 році.

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		18

В даний час «Кур'єр сервіс» є надійним партнером для тисяч компаній, які зробили свій вибір на користь надійних і сучасних послуг з доставки вантажів і кореспонденції по Україні, ближньому і далекому зарубіжжю [28].

Широкий спектр транспортних можливостей, а також власна філіальна мережа "Кур'єр сервіс" дозволяють компанії забезпечити доставку документів і вантажів згідно вступників заявок.

Власна філіальна мережа «Кур'єр сервіс» включає 76 філій і більше 50 представництв.

З 2006 року «Кур'єр сервіс» є офіційним членом Всесвітнього дистриб'юторського Альянсу GDA, а в 2007 році компанія стала офіційним партнером Всесвітньої кур'єрської служби AramexInternationalCouriers. Компанія здійснює термінову доставку поштових відправлень і вантажів в 218 країн світу, включаючи країни Африки, всі арабські держави.

Клієнтами "Кур'єр сервіс" є більше двох тисяч підприємств малого, середнього і великого бізнесу, що працюють в Україні і за кордоном. Кожному клієнту компанія забезпечує гнучкий підхід в обслуговуванні і максимально враховує його інтереси в експрес-доставці по Україні і за кордоном.

Під організаційною структурою підприємства розуміються склад, співвідпорядкованість, взаємодія і розподіл робіт по підрозділах і органам управління, між якими встановлюються певні відносини з приводу реалізації владних повноважень, потоків команд та інформації.

У ТОВ "Кур'єр сервіс" застосовується лінійна структура. Характеризується тим, що на чолі кожного підрозділу стоїть керівник, який зосередив у своїх руках всі функції управління і здійснює одноосібне керівництво підлеглими йому працівниками. Його рішення, що передаються по ланцюжку "зверху вниз", обов'язкові для виконання нижчестоящими ланками. Він, у свою чергу, підпорядкований вищестоящому керівнику.

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		19

Структура організації - це фіксовані взаємозв'язки, які існують між підрозділами і працівниками організації. Її можна розуміти як встановлену схему взаємодії і координації технологічних елементів і персоналу.

На ефективність діяльності організації впливають:

- реальні взаємозв'язки між людьми і їх роботою, що відображаються в схемах організаційних структур і посадових обов'язків;
- політика керівництва і методи, що впливають на поведінку персоналу;
- повноваження і функції працівників організації на різних рівнях управління (нижчому, середньому і вищому).

Структура управління визначається складовими її ланками та ієрархічними ступенями управління.

Структура повинна забезпечувати єдність стійких зв'язків між її складовими і надійне функціонування системи в цілому.

В даний час в «Кур'єр сервіс Брянськ» працює 18 осіб. Прийом і відбір персоналу на роботу йде на підставі рекомендацій співробітників підприємства, а також за результатами запитів в Центри зайнятості та кадрові агентства. Основним критерієм оцінки працівників є їх трудова діяльність, освіта [28].

Форми, системи та розміри оплати праці працівників, у тому числі додаткові виплати стимулюючого та компенсуючого характеру, встановлюються на підставі колективного договору, угоди та трудового договору. Працівники отримують доплати та надбавки:

- професійна майстерність;
- суміщення професій, розширення зони обслуговування;
- класність, ненормований робочий день;
- роботу у вечірній і нічний час;
- роботу зі шкідливими умовами праці;
- стаж роботи;
- високі досягнення в праці, виконання особливо важливої роботи.

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		20

Заробітна плата нараховується в залежності від кількості та якості праці. З цією метою проводиться контроль діючих норм виробітку. Діючі Положення про преміювання охоплюють всі категорії працюючих. Преміювання працівників «Кур'єр сервіс» проводиться відповідно до "Положень про преміювання за результати виробничої діяльності", затверджених директором підприємства:

- виконання плану реалізації послуг;
- забезпечення необхідного рівня якості обслуговування клієнтів.
- преміювання керівників проводиться за основними показниками:
- зростання реалізації послуг у порівнянних цінах до відповідного періоду минулого року (від 10 до 50%);
- зростання реалізованих робіт, послуг у фактичних цінах порівняно з відповідним періодом попереднього року (від 10 до 50%).

Розмір премії працівникам зменшується за невиконання показників виробничої діяльності [28].

У ТОВ "Кур'єр сервіс" на роботі використовують ряд програмних продуктів, які автоматизують основні бізнес-процеси. Розглянемо можливість використання програмного забезпечення та технічної підтримки.

В основному, заходи, що вживаються для поліпшення матеріально-технічного забезпечення підприємства, пов'язані з модернізацією комп'ютерної техніки та комунікаційного обладнання.

Існує доступ до Інтернету та електронної пошти. У всіх офісах компанії була створена спеціальна програма електронної пошти, яка забезпечує дуже високу швидкість доставки пошти в загальній системі. Для роботи в мережі на підприємстві використовується топологія "зірка", в неї входить 11 робочих місць. Пропускаючи здатність мережі 1г / біт.

Всі робочі станції оснащені програмними продуктами, в залежності від їх функцій, таких як системне програмне забезпечення "1С: Підприємство"; антивірус; офісні програми.

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		21

Всі відділи мають по одному ПК, крім бухгалтерії та кабінету операторів, в яких встановлюється по 2 ПК.

Зірка - це топологія мережі, де кожна робоча станція з'єднана з центральним пристроєм (комутатором або маршрутизатором). Центральний блок регулює трафік пакетів в мережі. Кожен комп'ютер через мережеву карту підключений до комутатора, використовуючи окремий кабель.

При необхідності, можна об'єднати кілька мереж з топологією "зірка" - в результаті отримаємо конфігурацію мережі з топологією дерева. Топологія дерева поширена у великих компаніях [26].

Топологія "зірка" є однією з ключових у побудові локальних мереж. Це відбувається через численні переваги:

- відмова однієї робочої станції або пошкодження кабелю не впливає на продуктивність всієї мережі в цілому;
- відмінна масштабованість: для підключення нової робочої станції достатньо, щоб лежати на окремому вимикачі кабелю;
- полегшує пошук несправностей і обривів в мережі;
- високу продуктивність;
- простота налаштування і управління;
- додаткове обладнання може бути легко інтегроване в мережу.

На всіх робочих станціях встановлені персональні комп'ютери на базі процесора 530 IntelCore i3 2.9 GHz, що дозволяє прискорити процес обробки даних. Ці ПК встановлені в офісах: логістичного оператора, бухгалтерії та охорони. Його характеристики: материнська плата Socket-1156 h55, процесор IntelCore i3 530 2.9 GHz, пам'ят4Gb DDR III, NVIDIA GTX 550Ti 10124mb відеокарта, звукова карта HD Audio, мережа плата10 \ 100, жорсткий диск 750GB.V встановлені інші шафи, інша система, вузли: корпус ATX1 450W материнська плата MSI iG31 2ddr2 / 800 DulaCh / SATA II ап, Vga, mAtx, процесор IntelCore 2 Duo E7500 (BX80571E7200) C-2,93 / 3/1066 Socket 775

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		22

BOX, пам'ять DIMM PC - 6400 DDR II 2Gb, HDD SATA II 250.0 GB wd 7200rpm 16MB, NVIDIA GTX 550Ti 1024MB карта.

Робочі місця оснащені моніторами-CD. Вони набагато більш компактні в порівнянні зі звичайними моніторами, що забезпечує більш раціональне використання області робочого столу. Монітори у всіх офісах однакові. Характеристика ViewSonic VA903B: діагональ 19 дюймів, макс. 1280x1024, час відгуку 8 м / с, співвідношення сторін 4 : 3, яскравість 300 кд / м<sup>2</sup>.

МФУ встановлені лазерні, щоб забезпечити високий рівень друку різних документів, а також прайс-листи і рахунків-фактур, призначених для клієнтів «Кур'єр сервіс».

Своєчасна заміна обладнання в зразках обладнання нового покоління забезпечується за рахунок регулярних візитів представників науково-технічних виставок компанії, щоб ознайомити їх з останніми моделями цього типу продукту, а також подальше придбання нового обладнання для «Кур'єр сервіс».

На всіх робочих станціях встановлено антивірусне Avast Endpoint Protection. Утиліта є безкоштовною.

У процесі роботи, користувачі можуть встановити оновлення. Коли нова версія Avast на екрані з'явиться відповідне повідомлення негайно. Користувач приймає або ігнорує його. Оновлення антивірусних баз відбувається автоматично. Це дає можливість постійно контролювати процес появи нових загроз.

Основні характеристики Avast:

- гнучкість конфігурації;
- зручність експлуатації;
- інтуїтивно зрозумілий інтерфейс;
- висока продуктивність;
- гарантована конфіденційність та безпека.

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		23

Додаток сканує окремі диски, файли, папки і навіть знімні носії. Утиліта дозволяє розрахувати параметри вірусної активності. Якщо загроза ідентифікується, то відразу визначається його місцем розташування і подальшим блокуванням.

Програма добре працює з іншими антивірусами, не викликаючи конфліктів. Служба видаляє вірус повністю, не залишаючи ніяких файлів на пристрої. Якщо ви не можете вилікувати шкідливий файл, Avast видаляє його з системи назавжди [24].

Також на комп'ютери встановлені текстовий процесор MicrosoftWord і табличний процесор MicrosoftExcel для редагування текстових документів і електронних таблиць. Дані програмні продукти є частиною офісного пакету MicrosoftOffice.

Microsoftoffice - офісний пакет додатків, створених корпорацією Microsoft для операційних систем MicrosoftWindows і AppleMac OS X. До складу цього пакету входить програмне забезпечення для роботи з різними типами документів: текстами, електронними таблицями, базами даних та ін. MicrosoftOffice є сервером і його функції можуть використовуватися іншими додатками, а також самими додатками MicrosoftOffice. Підтримує скрипти і макроси.

MicrosoftWord – текстовий процесор. Доступний під Windows і AppleMac OS X. Дозволяє готувати документи різної складності. Підтримує OE, модулі сторонніх розробників, шаблони та багато іншого. Основним форматом в останній версії є позиціонування як відкритий MicrosoftOfficeOpen XML, який являє собою ZIP-архів, що містить текст у вигляді XML, а також всю необхідну графіку. Найбільш поширеним залишається двійковий формат файлів MicrosoftWord 97-2003 з розширенням DOC. Продукт займає провідне положення на ринку текстових процесорів, і його формати використовуються як стандарт де-факто в

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		24

документообігу більшості підприємств. Word також доступний у деяких редакціях MicrosoftWorks.

MicrosoftExcel - табличний процесор. Підтримує всі необхідні функції для створення електронних таблиць будь-якої складності. Займає провідне положення на ринку. Остання версія використовує формат ООХМ з розширенням ".xlsx", більш ранні версії використовували двійковий формат з розширенням «.xls». Доступний під Windows і AppleMac OS X.

"Кур'єр сервіс" застосовує в роботі програмний продукт КАРГОЗ, який призначений для кур'єрських компаній, операторів експрес-доставки, транспортно-експедиторських компаній та інтернет-магазинів. Програма дозволяє автоматизувати основні виробничі логістичні процеси.

Система реалізує оперативні підрозділи, адміністративний та фінансовий облік:

- підсистема управління відносинами з контрагентами;
- управління тарифної підсистеми та розрахунок вартості послуг;
- підсистема управління замовленнями клієнтів;
- підсистема контролю доставки (маршрутизації);
- контроль підсистеми вантажних власних або взятих напрокат транспортних засобів;
- перевезення повними траками (FT) у внутрішньоміському, міжміському або міжнародному сполученні;
- залізничні та авіаперевезення;
- експрес-доставки та поштові розсилки;
- управління розподілом підсистеми товарів;
- управління підсистемою складу;
- підсистема управління грошовими коштами;
- підсистема управління бюджетного аналізу;
- електронний архів договорів перевезення та бухгалтерських документів;

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		25

- Call-центр;
- веб-портал, що забезпечує відстеження вантажів, редагування замовлень, калькулятор для розрахунку вартості послуг для клієнтів;
- управління продуктивністю підсистеми віддалених офісів і філіальної мережі;
- Web-служба, яка надає систему інтеграції даних на корпоративному веб-сайті;
- підсистема роботи з електронними картами;
- вбудований поштовий клієнт.

В офісі бухгалтерського програмного забезпечення встановлено "1С: Бухгалтерія 8", щоб відобразити облікові операції [25].

"1С: Бухгалтерія" - інтегрований програмний продукт, призначений для оптимізації та автоматизації обліку, управління бізнесом всіх форм власності, з різними типами оподаткування.

Програма має гнучку конфігурацію, яка дозволяє адаптувати його до потреб і особливостей практично будь-якого бізнесу, від індивідуальних підприємців і до забезпечення великого холдингу, з багатьма дочірніми компаніями і великою кількістю співробітників.

"1С: Бухгалтерія" дозволяє вести бухгалтерський і податковий облік діяльності декількох організацій, які можуть бути проведені в окремих базах даних. Можливе використання загальних списків товарів, підрядників, співробітників, а також обов'язковий облік поведінки окремо.

Програма також підтримує різні системи оподаткування для комерційних організацій та індивідуальних підприємців:

- загальна система оподаткування;
- спрощена система оподаткування;
- податкова система для окремих видів діяльності.

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		26

Автоматизована система обліку торгових операцій, реєстрація вступників товарів і послуг. Програма підтримує агентський договір (комісія), здійснює облік продажів через агента.

Облік грошових коштів і безготівкових розрахунків: при реєстрації всіх валютних операцій. Програма дозволяє вводити і роздруковувати платіжні доручення; автоматизована робота провайдерів платіжних послуг, виведення грошових коштів на банківські рахунки (виплати заробітної плати персоналу і т.д.). Платежі можуть бути розділені на передоплати та оплати.

Робота з підрядниками, теж, може бути автоматизована через "1С: Бухгалтерія", відображається аналітичний облік в контексті підрядників і контрактів.

Крім того, "1С: Бухгалтерія" дозволяє вести:

- облік основних засобів і нематеріальних активів;
- рахунки виробництва (основні та допоміжні);
- бухгалтерський облік;
- ПДВ;
- виплата заробітної плати працівникам, персоналу та особистих записів;
- розрахунок податку на прибуток для податкового обліку;
- розрахунок спрощеної системи оподаткування в автоматичному режимі;
- розрахунок доходів і витрат індивідуальних підприємців-платників податків;
- підтримувати Книгу доходів на спеціальному бланку для патентної системи оподаткування;
- робити експрес-перевірку рахунку.

На складі встановлено "1С: Торгівля і склад", необхідна для автоматизації роботи з великою кількістю вантажу [28].

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		27

"ІС Торгівля і склад" дозволяє виконувати всі функції обліку - від ведення довідкових даних і введення первинних документів в системі для отримання різних звітів і аналітичних звітів. Основний напрямок програми «ІС Торгівля і склад» - запис, наявність і рух матеріальних і грошових коштів.

"ІС Торгівля і склад" дозволяє:

- вести роздільний управлінський і фінансовий облік;
- вести облік від імені декількох осіб;
- контроль за станом запасів з вибором методу витрат лінії (FIFO, IFO, в середньому);
- вести роздільний облік власних товарів і товарів, прийнятих на реалізацію;
- оформити купівлю та продаж товарів;
- виконати автоматичне початкове заповнення документів на основі раніше введених даних;
- вести облік розрахунків з клієнтами і постачальниками, в якому детально взаємне за окремими договорами;
- формувати необхідні первинні документи;
- виписувати рахунки автоматично будувати книгу продажів і купити книгу, вести кількісний облік в контексті ГТЕ кімнат;
- резервне копіювання своїх товарів і контроль оплати;
- вести облік грошових коштів на поточних рахунках і в готівковій формі;
- вести облік товарних кредитів і контроль їх погашення;
- вести облік переданих на продаж товарів, їх повернення та оплати.

Програма "платник податків" дає можливість формувати велику кількість документів для різних видів податкової та бухгалтерської звітності. Всі форми створюваних документів підтримуються в актуальному стані.

Основні можливості програми:

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		28

- підтримується робота "майстра документів" - з його допомогою створити необхідні форми звітності може навіть непрофесіонал;
- у програму вбудований актуальний Календар бухгалтера на поточний рік;
- можна вести одночасно кілька платників податків (юридичних осіб та / або індивідуальних підприємців);
- є функція резервного копіювання і вивантаження даних (можна перенести введену інформацію на інший комп'ютер);
- підтримується робота в операційних системах linux;
- грамотно складена система довідки, діючий форум підтримки і новинна розсилка по e-mail;
- довідники: КБК (Класифікатор доходів бюджетів Російської Федерації), Класифікатор податкових пільг, коди послуг по ОКУН, Довідник пільг з податку на майно, довідник видів доходів, КВЕД (види економічної діяльності) і багато інших [28].

У кабінеті операторів і логістики встановлені програми "1С Бухгалтерія" і КАРГОЗ.

Впровадження автоматизованих систем обробки інформації підвищує ефективність роботи підприємства; збільшує якість послуг, що надаються. Використання систем автоматизації основних процесів діяльності дозволяє прийняти оптимальні рішення; підвищиться працездатність співробітників, отже, збільшити обсяг надаваних кур'єрських послуг, що дозволить розширити коло клієнтів, підвищити доходи.

Керівництво ТОВ "Кур'єр сервіс" прийняло рішення посилити систему безпеки на підприємстві. Виникла необхідність розробки системи відеоспостереження зовні і всередині приміщення.

Система відеоспостереження дозволить:

- зменшити ризик розкрадань цінностей на підприємстві;
- контролювати і враховувати робочий час;

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		29

- попереджати протиправні дії третіх осіб;
- детально розібратися в конфліктній ситуації, що сталася в офісі, переглянувши архів;
- також застосування звукозапису спільно з відеозаписом актуально в місцях, де здійснюються грошові операції, приймаються замовлення та ін.

Впровадження автоматизованих систем обробки інформації та відеоспостереження підвищить ефективність роботи підприємства; збільшиться якість надаваних послуг, так як будуть знаходитися найбільш оптимальні рішення; підвищиться працездатність співробітників, отже, збільшиться обсяг послуг, що дозволить розширити коло клієнтів, підвищити доходи.

## **2.2 Інформаційне обстеження трафіка в локальній мережі**

Розглянемо як здійснюється процес розробки системи відеоспостереження. Для початку необхідно побудувати модель. Модель повинна бути адекватна предметній області, отже, вона повинна відповідати предметній області, і повинна містити в собі знання всіх учасників, задіяних в розробці. Найбільш зручною методологією моделювання бізнес-процесів є методологія IDEF0.

В рамках методології IDEF0 бізнес-процес представляється у вигляді набору елементів-робіт, які взаємодіють між собою, а також показується інформаційні, людські та виробничі ресурси, споживані кожною роботою.

Найбільш популярним програмним продуктом для розробки моделей бізнес-процесів є програмний продукт "AllFusionProcessModeer".

"AllFusionProcessModeer" - це потужний інструмент для створення моделей, що дозволяє аналізувати, документувати і планувати зміни складних бізнес-процесів. Програма дозволяє перевіряти створювані моделі з

					<b>ІАПЦ 466120.004 ПЗ</b>	Лист
Изм.	Лист	№ докум.	Підпис	Дата		30

точки зору синтаксису обраної методології, перевіряє посилальну цілісність між діаграмами, а також виконує ряд інших перевірок [22].

Методологія IDEF0 може бути використана для моделювання широкого класу систем. Для нових систем застосування IDEF0 має своєю метою визначення вимог і вказівку функцій для подальшої розробки системи, що відповідає поставленим вимогам і реалізує виділені функції. Стосовно до вже існуючих систем IDEF0 може бути використана для аналізу функцій, виконуваних системою і відображення механізмів, за допомогою яких ці функції виконуються. Результатом застосування IDEF0 до певної системи є модель цієї системи, що складається з ієрархічно впорядкованого набору діаграм, тексту документації і словників, пов'язаних один з одним за допомогою L перехресних посилань.

Двома найбільш важливими компонентами, з яких будуються діаграми IDEF0, є бізнес-функції або роботи (представлені на діаграмах у вигляді прямокутників) і дані і об'єкти (зображувані у вигляді стрілок), що зв'язують між собою роботи. При цьому стрілки, в залежності від того, в яку грань прямокутника роботи вони входять або з якої грані виходять, діляться на кілька видів:

- стрілки входу (входять в ліву грань роботи) - зображують дані або об'єкти, що змінюються в ході виконання роботи;
- стрілки управління (входять у верхню грань роботи) - зображують правила і обмеження, згідно з якими виконується робота;
- стрілки виходу (виходять з правої грані роботи) - зображують дані або об'єкти, що з'являються в результаті виконання роботи;
- стрілки механізму (входять в нижню грань роботи) - зображують ресурси, потрібні для виконання роботи, але не змінюються в процесі роботи (наприклад, обладнання, людські ресурси і т.п.).

Всі роботи і стрілки повинні бути іменовані. Перша діаграма в ієрархії діаграм IDEF0 завжди зображує функціонування системи в цілому. Такі

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		31

діаграми називаються контекстними. У контекст входить опис мети модельованої області (опису того, що буде розглядатися як компонент системи, а що як зовнішній вплив) і точки зору (позиції, з якої буде будуватися модель). Зазвичай в якості точки зору вибирається точка зору особи або об'єкта, відповідального за роботу модельованої системи в цілому [19].

Апаратне забезпечення відеоспостереження етоелектронні і механічні частини обчислювального пристрою, що входять до складу системи або мережі, виключаючи програмне забезпечення і дані (інформацію, яку обчислювальна система зберігає і обробляє). Апаратне забезпечення включає: комп'ютери та логічні пристрої, зовнішні пристрої та діагностичну апаратуру, енергетичне обладнання, батареї та акумулятори.

Розглянемо тип систем відео спостереження - спеціалізований комплект обладнання (СК). Необхідно відзначити, що відносно дешеві системи відеоспостереження спеціалізованого комплекту в усіх відношеннях гірше аналогічних на базі типового комп'ютера. Системи на базі спеціалізованого комплекту є дорогими. Придбати таку систему і утримувати - досить витратна стаття для підприємства [21]. Системи відеоспостереження (СК) володіють наступними перевагами:

- спеціалізація та компактність;
- розвинені функції охоронної та пожежної сигналізацій, контроль доступу;
- одночасне обслуговування десятків камер стеження;
- відповідність спеціальним вимогам з безпеки, сертифікат відповідності.

Система відеоспостереження (СК) включає обов'язкові компоненти:

- відеокамера;
- Відеомонітори;
- квадратори (якщо використовується чотири відеокамери)

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		32

- відеомультіплексори (якщо використовується від 4-х до 32-х відеокамер);
- матричні комутатори відеосигналу (якщо число камер більше 32)
- спеціальні відеомагнітофони тривалого запису;
- відеомонітори спеціалізованого комплексу (не на базі комп'ютера).

Відеомонітор - це пристрій відображення картинки, переданої відеокамерою або збереженої в архіві.

При виборі відеомонітора враховується ряд характеристик.

Розмір екрану - для охоронного відеоспостереження застосовуються відеомонітори з розміром екрану від 5 до 21 " (дюйма) по діагоналі (один дюйм дорівнює 2,54 см); - дозвіл (кількість горизонтальних рядків, що відображаються відеомонітором). Вимірюється в ТВ-лініях. Залежно від типу монітора цей параметр може становити від 300 до 1000 ТВ-ліній.

Кількість відеовходів (число підключених джерел відеозображення, наприклад, відеокамер) - як правило, відеомонітори містять один, два або чотири відеовходи, перемикання між якими може проводитися в ручному або автоматичному режимі (через заданий час).

Наявність сервісних функцій (вбудований квадратор, аудіоканал, "тривожні" входи і т.д.).

Недоліки системи відеоспостереження спеціалізованого комплексу (СК):

- відеозапис у багатьох системах СК ведеться на магнітофонну стрічку. Тому пошук потрібного відеофрагменту в таких системах вкрай утруднений;
- касети зі стрічкою, на якій записана відеоінформація, уразливі для розмагнічування;
- ремонт обладнання систем відеоспостереження можливий тільки в спеціалізованих майстернях [21].

Останнім часом відбулося деяке зотоварювання продукції систем відеоспостереження СК. Причина з одного боку та, що дуже швидко

вдосконалюються системи на базі КК - потужна конкуренція. З іншого боку, в комплект переважної більшості систем СК входять застарілі монітори з електронно-променевими трубками, що виділяють багато тепла, споживають багато електроенергії, випромінюють при роботі шкідливі для здоров'я важкі іони. Причому, замінити такий монітор на комп'ютерний рідкокристалічний, неможливо.

Розглянемо другий тип систем відеоспостереження - комп'ютерна система відеоспостереження (КК). Система відеоспостереження на базі типового комп'ютера включає наступні компоненти: комп'ютер; плата системи відеоспостереження (плата відеозахоплення); програмний супровід плати відеоспостереження; відеокамери. Недоліком відеосистем КК є неможливість одночасного обслуговування (безпосередньо, без плати розширення) понад восьми камер стеження [22].

Ще один недолік системи відеоспостереження КК є складність прийняттого вибору з величезної кількості варіантів і виробників. Для відеоконтролю в невеликих офісах і на складах, для зовнішнього і внутрішнього відеоспостереження в квартирах і на дачах буває цілком достатньо установки від однієї до восьми камер стеження, сигнали від яких здатний обробити будь-який сучасний комп'ютер. Навіть якщо для відеоспостереження потрібно більше восьми відеокамер, то як варіант можна застосувати другий точно такий же комплект системи відеоспостереження на базі комп'ютера. Вартість двох комп'ютерних комплектів все одно виявиться набагато дешевшою однієї аналогічної системи на базі спеціалізованого комплекту.

Виходячи з проведеного аналізу оптимальний вибір - система відеоспостереження на базі комп'ютера (КК).

Мінімальний склад основного комплекту для обладнання системи відео спостереження:

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		34

- типовий комп'ютерний комплект (системний блок, монітор, безперебійне живлення, модем);
- плата відеозахоплення системи відеоспостереження (адаптер системи відеоспостереження КК);
- комплект програмного забезпечення системи відеоспостереження (до плати відеозахоплення);
- відеокамери відео спостереження - джерело (адаптер) живлення 220/12 вольт на струм 1 або 2 ампера;
- кабельна розводка від адаптера живлення до відеокамер і від відеокамер до комп'ютера.

Вимоги до плати системи відеоспостереження:

- робота з програмним забезпеченням, сумісним з операційною системою Windows XP / Vista / 7;
- апаратно в реальному часі кодування відеосигналу від камер стеження в архівному інформаційному форматі.

Цілодобово працює система відеоспостереження навіть в самому повільному режимі від декількох камер, обробляє дуже багато відеоінформації. При необхідності (або в плановому порядку) її перегляд і пошук потрібного фрагмента може займати дуже багато сил і часу.

Відеозапис в цьому випадку здійснюється тільки в той час, коли на цій ділянці об'єкта (екрану) є рух. Як вже говорилося, система відеоспостереження складається з камер стеження і засобів запису - відображення відеоінформації. Завдання відеокамер охопити якомога більш детально контрольований простір [21].

Іноді для розширення зони огляду застосовують поворотні пристрої відеокамер, при цьому слід врахувати що:

- вартість поворотного пристрою в кілька разів більше, ніж вартість відеокамери;

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		35

- при повороті змінюється фокусна відстань до об'єкта, тому доводиться застосовувати дорогі камери з функцією регулювання фокусної відстані;

- поворотний пристрій має обмежений температурний діапазон, в той час для відеокамери в термозахисті такого обмеження не існує;

- управління поворотним пристроєм вимагає додаткової проводки і спеціального програмного супроводу;

- механізм повороту споживає додаткову електроенергію;

- важлива подія може статися саме в тому секторі, від якого тільки що "відвернулась" камера;

- програмний "детектор руху" системи не працює з рухається камерою;

- складний механізм пристрою повороту знижує надійність всього вузла в цілому.

З урахуванням вищесказаного, для розширення зони відеоспостереження доцільніше збільшувати число відеокамер, а поворотні пристрої застосовувати лише у виняткових випадках.

Плати відео нагляду характеризуються:

- кількістю каналів (максимальне число камер стеження), оброблюваних однією платою;

- наявністю і кількістю аудіо (звукових) входів;

- можливістю апаратного кодування відеосигналу в стандартні відеоформату;

- розвиненістю функціональних можливостей програмного забезпечення. Комп'ютерна система відеоспостереження включає наступні компоненти:

- комп'ютер;

- плата системи відеоспостереження;

- програмний супровід плати відеоспостереження;

- відеокамера;

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		36

- матричні комутатори відеосигналу (якщо число відеокамер перевищує 8).

Провівши аналіз апаратного забезпечення, прийшли до висновку, що для ТОВ «Кур'єр сервіс» для зовнішнього відеоспостереження найбільш оптимально буде використання системи відеоспостереження на базі комп'ютера (КК).

Мінімальні вимоги до конфігурації ПК:

- процесор: Pentium 4 2.8 ГГц (або аналог AMD);
- Оперативна пам'ять: 2 Гб;
- жорсткий диск: 60 Гб;
- звукова карта: необхідна при використанні мікрофона (зворотного зв'язку) або звукової сигналізації;
- відеокарта: не нижче Nvidia Geforce FX5200 або ATI RADEON 7000 (9000), 256 Мб ОЗУ.

Програмне забезпечення:

- Microsoft.NET Framework 2.0 або вище;
- DirectX 9.0 сот серпня 2008 року або вище;
- Кодеки для відтворення MPEG - 4 (рекомендується K-ite 470f або новіші).

Розглянемо можливості, пропоновані на ринку інформаційних технологій, вуличних і внутрішніх відеокамер, з яких необхідно вибрати для ТОВ оптимальний варіант для «Кур'єр сервіс».

Розглянемо різновиди і функціонал вуличних відеокамер.

Камера AXIS 11225-Н. 264 має високу роздільну здатність до 1 мегапікселя, що задовольняє завдання, які вона повинна виконувати. Можлива настройка кількості переданих кадрів в секунду з кроком в 5 кадрів. Температурний діапазон від мінус 10°C до плюс 60°C, можлива установка термокожуха. Також можливо віддалене управління об'єктивом, що сильно спрощує налаштування камери. Так само AXIS 12125-Н. 264 підтримує

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		37

специфікації ONVIF, що гарантує сумісність з програмними комплексами сторонніх виробників. Так само дана камера підтримує технологію PoE. Основним недоліком є дальність вбудованого інфрачервоного підсвічування, яке становить тільки 50 метрів.

Камера Smartec 1926-2MP має високу роздільну здатність до 2 мегапікселів, що задовольняє завданням, які вона повинна виконувати. Так само можлива настройка кількості переданих кадрів в секунду з кроком в 5 кадрів. Температурний діапазон від мінус 20°C до плюс 60°C, можлива установка термокожуха. Неможливо віддалене управління об'єктивом, що сильно ускладнює настройку камери. Так само Smartec 1926-2MP не підтримує специфікації ONVIF. Так само дана камера підтримує технологію PoE. Основним недоліком є дальність вбудованого інфрачервоного підсвічування, яке становить тільки 50 метрів.

Камера ArecontMisionH.264-HDI-356b має високу роздільну здатність до 2 мегапікселів, що задовольняє завданням, які вона повинна виконувати. Так само можлива настройка кількості переданих кадрів в секунду. Температурний діапазон від мінус 20°C до плюс 70°C, можлива установка термокожуха. ArecontMisionH.264-HDI-356b не підтримує специфікації ONVIF. Основними недоліками є відсутність підтримки специфікації ONVIF і неможливість віддаленого управління об'єктивом.

Камера A-TW105 має високу роздільну здатність до 1.5 мегапікселів, що задовольняє завданням, які вона повинна виконувати. Так само можлива настройка кількості переданих кадрів в секунду. Температурний діапазон від мінус 20°C до плюс 60°C, можлива установка термокожуха. Так само можливо віддалене управління об'єктивом, що сильно спрощує настройку камери. A-TW105 не підтримує специфікації ONVIF. Дана камера підтримує технологію PoE. Дальність вбудованого інфрачервоного підсвічування становить тільки 100 метрів.

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		38

Камера PoivisionH.264-3MP-2B має високу роздільну здатність до 3 мегапікселів, що задовольняє завданням, які вона повинна виконувати. Так само можлива настройка кількості переданих кадрів в секунду. Температурний діапазон від мінус 10°C до плюс 60°C, можлива установка термокожуха. Так само можливо віддалене управління об'єктивом, що сильно спрощує настройку камери. PoivisionH.264-3MP-2B підтримує специфікації ONVIF. Дана камера підтримує технологію PoE. Дальність вбудованого інфрачервоного підсвічування становить тільки 100 метрів.

Камера Sony 3MP-O-N. 264-HD має високу роздільну здатність до 3 мегапікселів, що задовольняє завданням, які вона повинна виконувати. Так само можлива настройка кількості переданих кадрів в секунду. Температурний діапазон від мінус 20°C до плюс 60°C, можлива установка термокожуха. Так само можливо віддалене управління об'єктивом, що сильно спрощує настройку камери.

Sony 3MP-O-N. 264-HD підтримує специфікації ONVIF. Дана камера підтримує технологію PoE. Дальність вбудованого інфрачервоного підсвічування становить тільки 100 метрів.

Камера Avigilon 2.0 MP-HD-H264-B має високу роздільну здатність до 2 мегапікселів, що задовольняє завданням, які вона повинна виконувати. Так само можлива настройка кількості переданих кадрів в секунду. Температурний діапазон від мінус 20°C до плюс 60°C, можлива установка термокожуха. Так само можливо віддалене управління об'єктивом, що сильно спрощує настройку камери.

Avigilon 2.0 MP-HD-H264-B підтримує специфікації ONVIF. Дана камера підтримує технологію PoE. Дальність вбудованого інфрачервоного підсвічування становить тільки 100 метрів. Системи контролю доступу Avigilon повністю працює на основі браузеру і не вимагає установки програмного забезпечення, що робить її готовою до розгортання і економить час.

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		39

Побудуємо зведену таблицю, в яку внесемо основні параметри розглянутих камер зовнішнього спостереження (табл. 2.1)

Таблиця 2.1

Зведена таблиця основних параметрів камер зовнішнього спостереження

Марка камери	Роздільна здатність Мпiкс.	Настройка кількості кадрів в секунду	Температурн. діапазон, °С	Термок.	Управління об'єктивом	ONV IF	Ціна, тис. грн.
AX IS 1225-H.264	1	так	від -10 до+60	так	так	так	18000
Sm artec 1926-2MP	2	так	від -20 до+60	так	ні	ні	19000
Ar econt Mision H.264-HD-356B	2	так	від -20 до+70	так	ні	ні	13000
A-TW105	1.5	так	від -20 до+60	так	так	ні	16000
Poivision H.264-3MP-2B	3	так	від -10 до+60	так	так	так	10000
Sony 3MP-O-H.264-HD	3	так	від -20 до+60	так	так	так	12000
Avigilon 2.0MP-HD-H264-B	2	так	від -20 до+60	так	так	так	11000

На основі проведеного аналізу, можна зробити висновок, що оптимальним рішенням для ТОВ "Кур'єр сервіс" буде вибір камери Avigilon 2.0 MP-HD-H264-B.

Камера Avigilon 2.0 MP-HD-H264-B є оптимальною, так як вона повністю задовольняє вимогам викладеним у завданні, не має явних

недоліків. Габарити відеокамери Avigilon 2.0 MP-HD-H264-B представимо на малюнку 2.1.

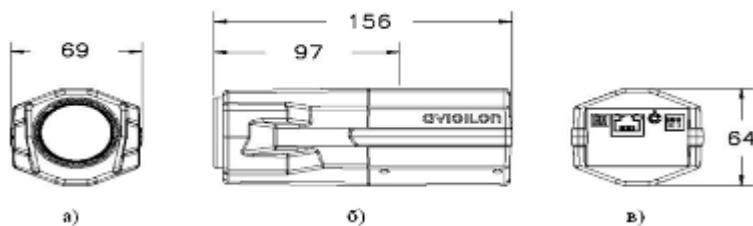


Рис.2.1. Габарити відеокамери Avigillon 2.0 MP-HD-H264-B

У програмного забезпечення Avigilon для управління системами відеоспостереження і контролю доступу легкий у використанні і інтуїтивно зрозумілий інтерфейс. Програмне забезпечення Avigilon Control Center (ACC) має простий інтерфейс для управління відео. Крім того, ACC дозволяє керувати системою, надаючи повний контроль над відтворенням відео.

Розглянемо огляд камер, які оптимально підходять для внутрішнього відеоспостереження ТОВ «Кур'єр сервіс».

Купольні відеокамери, найчастіше мають форму обтічної півсфери, завдяки своєму форм-фактору вони зручно монтуються на стіни і стелі без використання кронштейнів, зручні при юстируванні об'єтивів.

Мініатюрні відеокамери, зазвичай мають циліндричну або кубічну форму, головний показник даних камер, це компактність, циліндричні мініатюрні відеокамери часто мають вологозахисений корпус, що дозволяє їх застосовувати у вологих середовищах, тому при установці відеоспостереження на автомийках, в бокси ставлять саме їх. Так само даний тип відеокамер з об'єктивами використовують в системах прихованого відеоспостереження.

Модульні відеокамери (безкорпусні) це, як правило, одноплатні відеокамери з мініатюрним об'єктивом, міні-об'єктив в таких камерах встановлюється безпосередньо на друковану плату. Застосовуються в основному для вбудовування в різні предмети інтер'єру або меблів, а так

само для установки в окремі корпуси пристроїв і приладів. Особливо часте використання даних телекамер відзначено в домофонних системах зв'язку і системах прихованого відеоспостереження [31].

Корпусні відеокамери, це камери стандартного дизайну, основна особливість даних телекамер полягає в тому, що поставляються вони окремо без об'єктива і кронштейна. Це дозволяє їх використовувати для різноманітних цілей, легко компонуючи потрібний набір під конкретний об'єкт і завдання. Варто відзначити високу якість зображення і надійність даного виду камер. Дані камери добре зарекомендували себе в відеоспостереженні для банків, різних установ, на підприємствах.

На підставі проведеного аналізу характеристик, пропонованих IP-камери внутрішнього спостереження, при співвідношенні ціна-якість, розглянемо наступні моделі відеокамер.

Однією з поширених моделей відеокамер є IP-камери INFINITY.

Проведемо огляд асортименту камер INFINITY з серією мініатюрних захищених купольних камер SRD, яка поставляється в двох модифікаціях: моделі SRD-2000EX і SRD-3000at, з роздільною здатністю 2 і 3 мегапікселя відповідно.

Камера SRD являє собою мініатюрний купол з діаметром 100мм і висотою 53мм (рис. 2.2). Корпус камери виконаний з металу і відповідає класу захищеності ІК10. Камера повністю герметична: всі з'єднання, включаючи кабельний ввід, мають еластичний гумовий ущільнювач, тому можна не боятися повністю занурити її в воду. Камера живиться від джерела 12VDC або по PoE. Крім мережевого RJ - 45 і клем для підключення живлення присутній аудіовхід для підключення зовнішнього активного мікрофона, аудіовихід, а також роз'єм для підключення тестового аналогового монітора.

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		42



Рис. 2.2. Камера SRD для внутрішнього відеоспостереження

Серія SRD оснащена ширококутним об'єктивом 3.6 мм (80°) з ІЧ-корекцією. Також для додаткового підсвічування ближньої зони в передній частині камери є ІЧ-світлодіод.

До камери додається CD з докладними інструкціями на весь модельний ряд, а також утиліта для пошуку камер. Особливістю Web-інтерфейсу камер є те, що для відображення відео використовується технологія FASH.

Двомегапиксельна модель SRD-2000EX побудована на матриці 1/2.8" Sony Exmor IMX 122.

Трьохмегапиксельна модель SRD - 3000at використовує сенсор 1/3" ARTINA AR0331. Матриці обох моделей є хорошим і сучасним рішенням.

При порівнянні цих камер можна виділити наступні особливості:

- SRD-2000EX більш світлочутлива ніж SRD-3000at. При цьому, щоб отримати хорошу картинку при недостатній освітленості необхідно провести додаткову настройку посилення, різкості і шумозаглушення через веб-інтерфейс;

- SRD-3000AT менш "чутлива", проте не вимагає додаткових налаштувань, практично ніколи не "шумить" і формує різку картинку;

- SRD - 3000at добре обробляє зустрічне засвічення. Навіть при наявності яскравого джерела світла в кадрі і темні, і світлі ділянки відображаються однаково якісно [29].

Моделі SRD оснащені процесором Texas Instruments. На основі даного процесора успішно реалізований ряд алгоритмів, що поліпшують зображення: підвищення різкості зображення, динамічне шумозаглушення, кольорокорекція. У web-інтерфейсі камери можна вручну змінювати параметри даних функцій, однак цього не довелося робити, тому що обидві моделі і при стандартних налаштуваннях давали чітке насичене зображення.

Для ТОВ "Кур'єр сервіс" для внутрішнього відеоспостереження найбільш оптимально буде використання мініатюрної відеокамери моделі SRD-3000at, так як не вимагає додаткових налаштувань, практично ніколи не «шумить» і формує різку картинку. У меню цієї камери є окремий розділ WDR, з деякими настройками відеообробки.

Кут огляду є одним з основних критеріїв при виборі камери відеоспостереження оскільки визначає контрольовану нею зону спостереження. Залежить цей кут від фокусної відстані об'єктива камери і формату її матриці.

При виборі кута огляду камери відеоспостереження, слід враховувати, що об'єктив забезпечує різкість зображення в певних межах, званих глибиною різкості, що також накладає обмеження на розмір зони відеоспостереження в напрямку осі відеокамери.

Необхідно враховувати особливості, які в підсумку впливають на відмовостійкість і надійність системи. Деякі продукти дозволяють додати відеоспостереження до системи безпеки, інші - виступають в якості ядра, з яким інтегруються інші системи, що розширюють і доповнюють базовий функціонал.

При створенні комплексних систем безпеки, що включають в себе крім систем відеоспостереження також і системи контролю і управління доступом

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		44

можливо інтеграція обох систем в єдине ціле, причому в залежності від ступеня інтеграції конкретної системи в конкретне програмне забезпечення інтеграція відбувається або на рівні контролерів (вони підключаються до сервера відеоспостереження) або на рівні серверів (сервер СКУД підключається до системи відеоспостереження).

Вибір програмного забезпечення в даному випадку в першу чергу залежить від обраної СКУД і її підтримки системою відеоспостереження. Як правило, програмні модулі інтеграції з СКУД ліцензуються і купуються додатково [22].

Далі розглянемо програмне забезпечення для побудови системи відеоспостереження. При огляді програм для побудови системи відеоспостереження вибір був зроблений на користь програмного забезпечення «лінія» ([www.devine.ru](http://www.devine.ru)), так як ПО «лінія» володіє широкими функціональними можливостями і прийнятною вартістю.

Система відеоспостереження «лінія», розроблена компанією «ДевЛайн». Торгова марка «лінія» включає в себе три варіанти поставки: відеосервери с однойменною назвою, плати відеозахоплення «лінія Hybrid IP», софт «лінія IP», призначений тільки для роботи з IP-камерами.

Програмне забезпечення "лінія" поставляється з усіма продуктами компанії, не має мережевих, адміністративних і функціональних обмежень.

Програмне забезпечення системи "лінія" складається з двох частин — оболонки і ядра. Ядро системи призначене для захоплення і обробки відео і аудіоданих відповідно до призначених для користувача налаштувань і працює непомітно для користувача. Запускається ядро автоматично перед авторизацією Windows і працює, записуючи дані і передаючи їх при необхідності в мережу, навіть якщо оболонка закрита.

Оболонка ПЗ "лінія" призначена для взаємодії з ядром системи, здійснення призначених для користувача налаштувань і перегляду відео та аудіоданих. Оболонка складається з трьох розділів.

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		45

"Спостережний пост" - призначений для перегляду зображення з відеокамер і прослуховування звуку в режимі реального часу. Спостереження може здійснюватися як на локальному, так і на віддаленому комп'ютері. Інтерфейс системи відеоспостереження "лінія" представлений на рис.2.3.

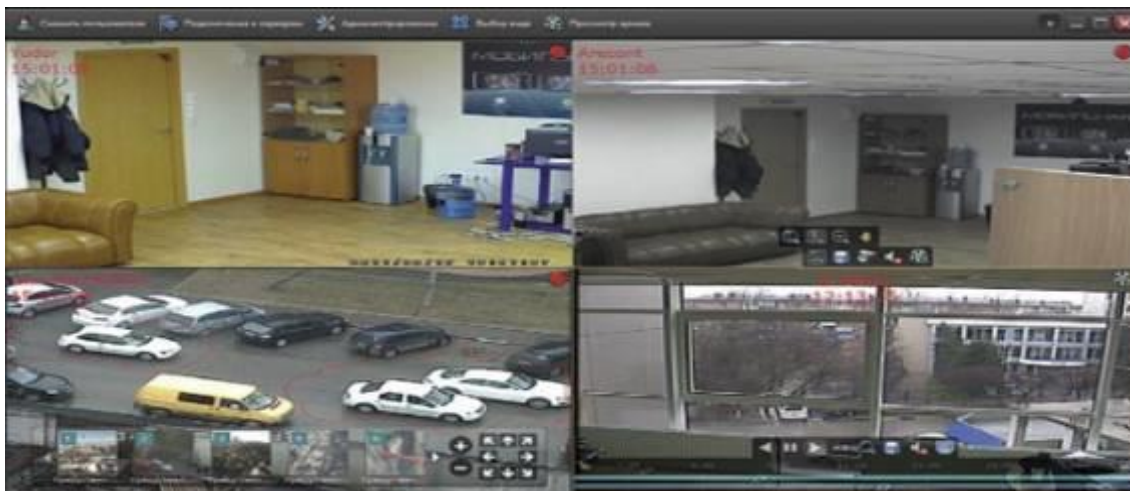


Рис. 2.3. Інтерфейс системи відеоспостереження «лінія»

«Адміністрування» - частина оболонки, призначена для налаштування роботи всієї системи «лінія».

"Перегляд архіву" - призначений для перегляду архіву та експорту в зручний формат вже записаної інформації.

ПЗ "лінія" дозволяє об'єднувати в одному сервері як аналогові, так і IP-відеокамери, поєднуючи переваги перших і других.

На території ТОВ "Кур'єр сервіс" необхідно організувати охоронне відеоспостереження по периметру зовні і всередині приміщення.

Охоронне відеоспостереження працюватиме цілодобово. Елементи системи розташовані поза приміщенням матимуть всепогодне виконання (працювати в штатному режимі при температурі навколишнього середовища -40..+ 40 С, мати захист від пилу і вологи не нижче 6б), роззахист.

У разі перебоїв з електроенергією система охоронного відеоспостереження переходить на роботу від резервованого джерела живлення (ДЖ) і працює період, протягом якого обслуговуючий персонал відреагує на аварію і прийме відповідні заходи.

### 2.3. Проектування системи відеоспостереження

Сервер відеоспостереження і центральний комутатор потрібно розташувати в кабінеті охорони. Сервер веде контроль за роботою відеокамер і обробляє відеоінформацію, що надходить.

Підключатися камери будуть за допомогою технології PoE.

PoE або PoweroverEthernet - технологія дозволяє передавати віддаленому пристрою разом з даними електричну енергію через стандартну виту пару в мережі Ethernet. PoweroverEthernet стандартизована за стандартом IEEE 802.3 af-2003. Відповідно до даного стандарту забезпечується постійний струм з номінальною напругою 48 В. Через дві пари провідників в чотирьохпарному кабелі, з максимальним струмом 400 мА для забезпечення максимальної потужності 12,95 Вт [25].

Для підключення використовується комутатор. В даному випадку буде присутній спеціальний мережевий комутатор (маршрутизатор з великою кількістю портів), до якого є можливість підключити до 20-30 (а то і більше) камер відеоспостереження. В даному випадку 11 камер.

Застосування комутатора дає тільки вигоду - не потрібні блоки живлення для камер, немає необхідності прокладати додаткові дроти для живлення камер. Комутатор має вбудований грозозахист по живленню 220В і по Ethernet портам.

Комутація всіх пристроїв здійснюється за допомогою «прямого» патч-корду, а настройка відповідно керівництву конкретного виробника (рис.2.4)

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		47



Рис. 2.4 Схема підключення пристроїв

В табл. 2.2 зробимо розрахунок вартості необхідного обладнання Системи відеоспостереження, на основі розглянутих раніше характеристик камер відеоспостереження.

Таблиця 2.2

Розрахунок вартості обладнання системи відеоспостереження

Категорія обладнання	Виробник і модель	Ціна, грн.	Кількість, шт./м.	Вартість, грн
Персональний комп'ютер	DNS	20000	1	20000
IP-камера відеоспостереження (зовн.)	Avigilon 2.0MP-HD-H264-B	11000	5	55000
IP-камера відеоспостереження (внутр.)	SRD-3000AT	6000	6	36000
Комутатор	D-link DES-1210-28P	12400	1	12400
Кабель «Кручена пара»	UTP	5	305	1525
Кабель-канал (короб)	ECO 40X16	26,73	80	2139
Конектор	8P8C	2	20	40
ПО «Лінія»	Лінія А Hybrid IP	16128	1	16128
Інші витратні матеріали	ECO	300	-	300
Всього				143532

Складемо схему установки системи відеоспостереження виходячи з характеристик відеокамер і технічного плану будівлі. Схема об'єкта відеоспостереження представлена на рис. 2.4.

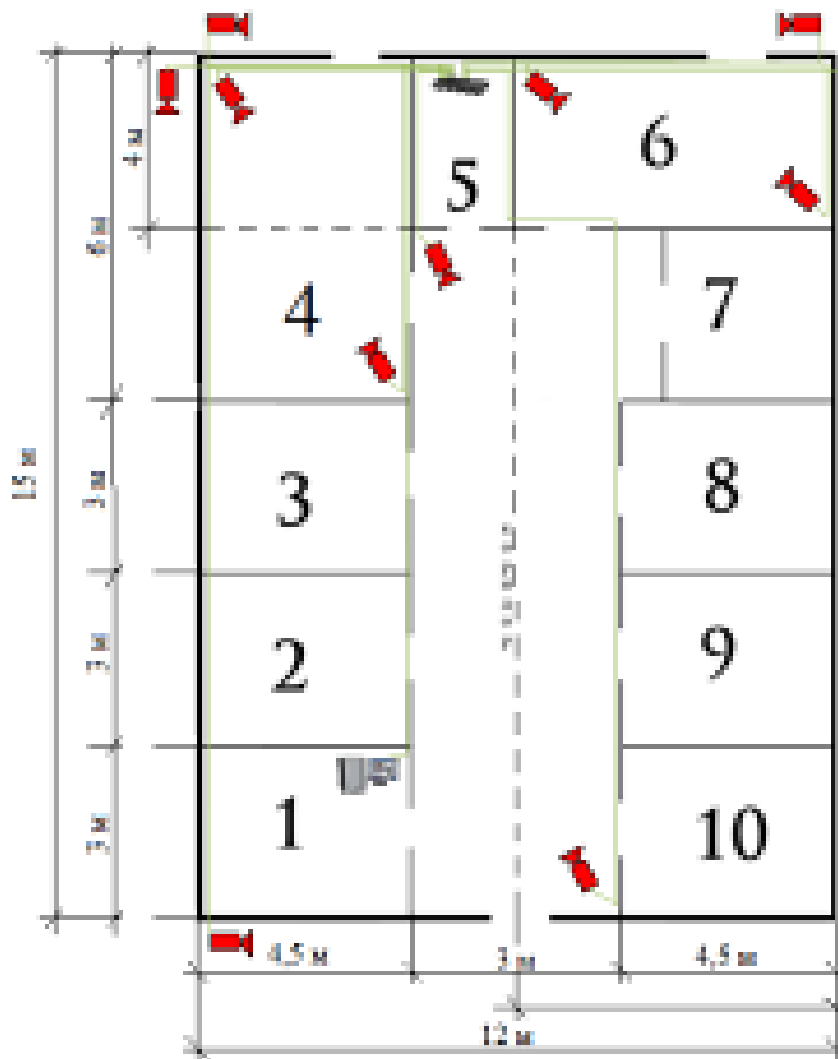


Рис. 2.4. Схема об'єкта відеоспостереження

Для комутації знадобиться спеціальний кабель і роз'єми. В якості з'єднувального кабелю застосовується "кручена пара", а в якості роз'ємів використовуються RG-45.

Для підключення всіх пристроїв знадобиться 100 м «крученої пари».

З'єднання роз'єму і кабелю здійснюється за допомогою спеціального обтискного пристрою, що нагадує пасатижі.

Коли кабель готовий, відеокамеру необхідно з'єднати з мережевою картою комп'ютера і відповідно до керівництва користувача призначити їй IP-адресу.

Изм.	Лист	№ докум.	Підпис	Дата

Для доступу до камери через Інтернет набирають IP-адресу провайдера і доданий до нього номер порту. Часто обов'язковою умовою є статична адреса інтернет-провайдера. В іншому випадку він буде постійно змінюватися і камери будуть недоступні. Якщо немає можливості використання статичної адреси, то можна скористатися динамічним "білим" (тобто з можливістю зовнішнього підключення) з прив'язкою адреси до доменного імені або спеціальним сервісом відеоспостереження провайдера.

Розроблена система відеоспостереження дозволяє: спостерігати за периметром навколо офісу, а також всередині приміщення; стежити за робочим процесом в офісі; здійснювати відеозапис у форматі AVI на жорсткий диск персонального комп'ютера.

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		50

## РОЗДІЛ 3

### МАТЕМАТИЧНІ РОЗРАХУНКИ СИСТЕМИ

Витрати - спожиті, витрачені або втрачені матеріальні, трудові та фінансові ресурси для отримання прибутку в процесі господарської діяльності підприємства.

Витрати можна розділити на дві великі групи, це первинні і вторинні витрати.

Первинні види витрат або виручки – це позиції, що відносяться до витрат або виручки в плані рахунків, для яких у фінансовій бухгалтерії існує відповідний основний рахунок (витрати на матеріали, витрати по утриманню персоналу, витрати на електроенергію).

Вторинні види витрат можуть бути створені і оброблятися тільки в обліку витрат. Вони відображають внутрішні потоки сум, які існують у внутрішньовиробничому перерахунку робіт, розрахунках непрямих витрат і розрахункових угодах (види витрат для внутрішньовиробничого перерахунку робіт, види витрат для внутрішніх/зовнішніх позамовних розрахунків витрат).

В даному розділі викладена методика і специфіка розрахунку матеріальних витрат на розробку системи відеоспостереження, а також вказані всі необхідні для висновків показники і формули для розрахунків.

Для розрахунку економічної ефективності використовуються наступні показники: трудові, вартісні.

Визначимо вагові показники дійових осіб. Всі дійові особи системи діляться на три типи: прості; середні; складні.

«Прості» - представляють зовнішню систему з чітко визначеним програмним інтерфейсом.

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		51

"Середні" - представляють або зовнішню систему, яка взаємодіє з даною системою за допомогою протоколу на зразок ТСР/ІР, або особистість, що користується текстовим інтерфейсом.

"Складні" - представляє особистість, що користується графічним призначеним для користувача інтерфейсом [23].

Типи дійових осіб та їх вагові коефіцієнти представлені в таблиці 3.1.

Таблиця 3.1

Вагові коефіцієнти дійових осіб

Тип дійової особи	Ваговий коефіцієнт
Простий	1
Середній	2
Складний	3

Загальна кількість дійових осіб множиться на відповідний ваговий коефіцієнт, потім обчислюється загальний ваговий показник.

У розробці системи відеоспостереження бере участь одна дійова особа "Розробник", контролює процес Керівник. Розробник в даному проекті являє собою складний тип дійових осіб, Керівник - складний тип дійових осіб. В такому випадку ваговий коефіцієнт дійових осіб буде обчислюватися як:  $A = 1*3+1*3 = 6.1$

Визначимо вагові показники варіантів використання. Всі варіанти використання в залежності від кількості транзакцій в потоках подій діляться на три типи (табл. 3.2): прості; середні; складні.

Таблиця 3.2

## Вагові коефіцієнти варіантів використання

Тип варіанта використання	Опис	Ваговий коефіцієнт
Простий	3 або менше транзакцій	5
Середній	від 4 до 7 транзакцій	10
Складний	Більше 7 транзакцій	15

При розрахунку витрат загальна кількість варіантів використання кожного типу множиться на відповідний ваговий коефіцієнт, виходячи з цього обчислюється загальний ваговий показник. Складність варіантів використання для даної розробки представлена в таблиці 3.3

Таблиця 3.3

## Складність варіантів використання

Варіант використання	Тип
Збір та обробка необхідної документації для розробки систем відеоспостереження	Простий (5)
Підбір необхідного апаратного забезпечення	Простий (5)
Підбір програмного забезпечення	Простий (5)

У розроблюваній системі відеоспостереження був задіяний простий варіант використання.

Таким чином, загальний ваговий показник дорівнює:

$$UC = 15.$$

В результаті отримуємо показник UUCP (UnadjustedUseCasePoints):

$$UUCP = A + UC = 6 + 15 = 21$$

Визначимо технічну складність розробки TCF (TCF – TechnicalComplexityFactor). Вона розраховується з урахуванням показників технічної складності за такою формулою:

$$TCF = 0,6 + (0,01 * (\sum Ti * Vi)) \quad (3.1)$$

де  $T_i$  – показник складності компонента;

$B_i$  – вага цього компонента.

Далі необхідно розставити значення перерахованих показників. Всі дані повинні бути об'єктивними і відповідати реальності. Вага визначає значимість показників для розроблюваної системи. Тому одним з основних показників визначення витрат на розробку системи є «значення з урахуванням ваги». Кожен з показників отримує значення в діапазоні від 0 до 5 і показує значимість для даної розробки (так, наприклад, значення 0 – відсутність значущості). Характеристики даної розробки представлені в табл. 3.4.

Таблиця 3.4

Показники технічної складності розробки

Показник	Опис	Вага	Значення	Значення з огляду на вагу
T1	Розподілена система	2	4	8
T2	Висока продуктивність (пропускна здатність)	1	3	3
T3	Робота кінцевих користувачів в режимі on-line	1	5	5
T4	Складність обробки даних	1	1	1
T5	Повторне використання коду	1	0	0
T6	Простота установки	0,5	5	2,5
T7	Простота використання	0,5	5	2,5
T8	Переносимість	2	0	0
T9	Простота внесення зміни	1	4	4
T10	Паралелізм роботи	1	5	5
T11	Спеціальні вимоги до безпеки	1	3	3
T12	Безпосередній доступ до системи з боку зовнішніх користувачів	1	5	5
T13	Спеціальні вимоги до навчання користувачів	1	1	1
$\Sigma$		–	–	40

Розрахуємо показник TCF:

$$TCF = 0,6 + (0,01 * 40) = 1$$

Визначимо рівень кваліфікації розробників (EF-EnvironmentalFactor). Він обчислюється за допомогою показників рівня кваліфікації F1-F8 за формулою.

Кожному показнику присвоюється значення в діапазоні від 0 до 5. Для показників F1-F4 0-означає відсутність, 3-середній рівень, 5-високий рівень. Для показника F5 0-означає відсутність мотивації, 3 - середній рівень, 5-високий рівень. Для F6 0-означає високу нестабільність вимог, 3-середню, 5-стабільні вимоги. Для F7 0-означає відсутність фахівців з частковою зайнятістю. Для показника F8 0-означає простої мови програмування, 3 – середню складність, 5-високу складність.

Рівень кваліфікації розробників обчислюється за допомогою показників рівня кваліфікації за формулою:

$$EF = 1,4 + (-0,03 * (\sum Fi * Vi)) \quad (3.2)$$

Показники рівня кваліфікації розробників системи представлені в табл.

3.5

Таблиця 3.5

Показники рівня кваліфікації розробників

Показник	Опис	Вага	Значення	Значення з огляду на вагу
F1	Знайомство з технологією	1,5	2	3
F2	Досвід розробки додатків	0,5	2	1
F3	Досвід використання об'єктно-орієнтованого підходу	1	1	1
F4	Наявність провідного програміста	0,5	2	1
F5	Мотивація	1	3	3
F6	Стабільність вимог	2	3	6
F7	Часткова зайнятість програміста	-1	1	-1
F8	Складні мови програмування	-1	0	0
$\Sigma$		-	-	14

Таким чином, рівень кваліфікації розробників матиме таке значення:  
 $EF = 1,4 + (-0,03 * 14) = 0,98$ .

Остаточне значення UCP (UseCasePoints):

$$UCP = UUCP * TCF * EF = 21 * 1 * 0,98 = 20,58$$

Останнім етапом стане обчислення оцінки трудомісткості. Розглянемо показники F1-F8 і визначимо, скільки показників F1-F6 мають значення менше 3, і скільки показників F7-F18 мають значення більше 3L.

Загальна кількість F1-F6, що мають значення менше 3 - 3, відповідно, необхідно використовувати 20 люд.- год. на одну UCP. Одержуємо, що загальна кількість людино-годин на весь проект дорівнює  $20,58 * 20 = 411,60$  1 люд.-год, що становить 10,29 тижні при 40-годинному робочому тижні або 2,6 місяці. З метою попередження різних непередбачених ситуацій термін розробки був збільшений до 3 місяців.

Розрахунок вартості витрат на електроенергію на період розробки системи представлений в табл. 3.6

Таблиця 3.6

Розрахунок електроенергії для восьмигодинного робочого дня

Назва	Кі-сть	кВт/год	кВт в робочий день	кВт в місяць
Комп'ютер	1	0,35	2,80	61,60
Освітлення	1	0,24	1,92	42,24
всього	—	—	—	103,84

## РОЗДІЛ 4

### ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖІ

В процесі експлуатації системи відеоспостереження несправність може виникнути в будь-якому місці, однак, ймовірність виходу з ладу певних складових частин і обладнання системи різні. Розглянемо несправності, що найбільш часто зустрічаються, варіанти їх зовнішніх проявів і способи виявлення [28]. Одним із слабких місць будь-якої системи відеоспостереження є з'єднувальна лінія. Зникнення зображення однієї з камер або наявність на ньому різного роду перешкод може бути викликано:

1. Обривом сигнальних ланцюгів або лінії живлення.
2. Частковим пошкодженням проводів, в тому числі мікроскопічним, як наслідок зміною їх характеристик (опір, ємність).

3. Несправністю використовуваних конекторів (роз'ємів).

Несправність блоку живлення.

Це визначається вимірюванням вихідної напруги. При значеннях нижче норми можна говорити:

- про несправність блоку,
- або можливий варіант несправності однієї з камер відеоспостереження.

Другий випадок досить ймовірний, тому перед тим як остаточно приймати рішення про заміну блоку живлення цей варіант слід виключити. Справа в тому, що несправна відеокамера може "садити" напругу.

Несправність відеореєстратора.

Крім таких "дрібниць" як порушення контактів в роз'ємах, більшість несправностей реєстратора діагностується і усувається в спеціалізованих майстернях. Однак, можливі випадки, коли сам відеореєстратор не при чому.

Наприклад:

- несправність HDD ( жорсткого диска) - начебто все працює, а записи ні,

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		57

- вихід з ладу внутрішньої батареї - при відключенні живлення, особливо надовго, скидаються всі налаштування.

Крім того, якщо не працює один канал, швидше за все, причина відноситься до категорії, описаних вище.

Несправність камери відеоспостереження.

Даний пункт більшою мірою відноситься до вуличного відеоспостереження, однак, на обладнання, встановлене всередині приміщення, також може наводитися електромагнітна перешкода.

Грозозахист систем відеоспостереження є частиною комплексу технічних заходів, спрямованих на захист обладнання від наведених небезпечних напруг. Їх причиною можуть бути [29]:

- високовольтні лінії електропередач, контактні мережі електротранспорту,

- потужні радіотехнічні передавальні (випромінюючі) установки,

- потужне електротехнічне обладнання, наприклад зварювальне,

- вже згадана атмосферна електрика, до речі, по потужності наведення здатне перевершити всі перераховані фактори разом узяті.

Електроживлення, виконане за технологією РoЕ винятком не є. Готових захисних пристроїв сьогодні існує безліч.

Крім того, деякі типи обладнання відеоспостереження, наприклад, приймачі сигналу по кручений парі, можуть мати вбудований захист.

Тому досить буде розглянути основні принципи дії і типові конфігурації захисту.

Основними характеристиками наведеної ЕРС перешкоди є швидкість наростання і значення напруги. Збільшення напруги, наведеної, наприклад, від розряду блискавки до значень порядку декількох кіловольт відбувається за проміжок часу, вимірюваний декількома десятками мікросекунд.

Безпека мережі — заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу

мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу [13].

Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів.

Найбільш поширений і простий спосіб захисту мережевих ресурсів є присвоєння їм унікального імені та відповідного паролю. [13]

Мережева безпека починається з аутентифікації, що зазвичай включає в себе ім'я користувача і пароль. Коли для цього потрібно тільки одна деталь аутентифікації (ім'я користувача), то це називають однофакторною аутентифікацією. При двофакторній аутентифікації, користувач ще повинен використати маркер безпеки або ключ, кредитну картку або мобільний телефон, при трьох факторній аутентифікації, користувач повинен застосувати відбитки пальців або пройти сканування сітківки ока.

Після перевірки дійсності, брандмауер забезпечує доступ до послуг користувачам мережі. Для виявлення і пригнічування дії шкідливих програм використовується антивірусне програмне забезпечення або системи запобігання вторгнень (IPS) [10].

Зв'язок між двома комп'ютерами з використанням мережі може бути зашифрований, щоб зберегти конфіденційність.

Для кращого захисту мережі від несанкціонованого доступу, використовується технологія під назвою брандмауера Internet (Internet Connection Firewall, скорочено ICF) зараз перейменована в брандмауер Windows. Вона дає можливість захистити мережу і комп'ютери від небажаного трафіку Internet. Брандмауер Internet (як і будь-який брандмауер), повинен запобігати можливій загрозі зараження вірусами через Internet,

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		59

комп'ютерів мережі. Тому брандмауер розміщується між мережею та Інтернетом.

Якщо є декілька з'єднань з Інтернетом, брандмауер потрібно встановити на кожному з них, і всі брандмауери виставити так, щоб забезпечити виконання правил встановленого захисту. Крім цього, захистити потрібно і сам брандмауер. Таким чином, концепція використання брандмауера має на увазі наступне:

- Весь трафік, що отримують користувачі, повинен проходити через брандмауер;
- Весь трафік, що відправляють користувачі, повинен проходити через брандмауер;
- Брандмауер забезпечує виконання правил захисту і відкидає весь трафік, що не задовольняє вимогам захисту;
- Сам же брандмауер не чутливий до спроб злому;

Основний механізм, що використовується при створенні брандмауерів, відомий як, фільтрація пакетів. Фільтр пакетів взаємодіючи з програмним забезпеченням, практично запобігає проходження сторонніх пакетів через проксі-сервер шляху від однієї мережі до іншої. Фільтр пакетів перевіряє поля в назві кожного пакета. Адміністратор повинен налаштувати фільтр і встановити, які пакети будуть проходити через сервер, а які будуть заблоковані.

Крім використання IP-адрес пакетів, фільтр може забезпечити перевірку протоколу, який використовується для передачі пакета, або служби високого рівня, якій відповідає пакет.

Як приклад адміністратор може настроїти фільтр на блокування всіх пакетів, які забезпечують зв'язок за протоколами WWW (Word Wide Web) і дозволити тільки проходження трафіку електронної пошти.

Брандмауер Internet складається з трьох систем (фільтрів): один фільтр визначає які пакети користувачі мають право отримувати з Інтернету, другий

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		60

визначає які пакети можуть виходити з мережі або комп'ютера, третій фільтр забезпечує експлуатацію прикладного програмного забезпечення.

Захищений хост знаходиться в окремій мережі. Фактично захищений хост перебувати між двома фільтрами пакетів; фільтри налаштовані на перенаправлення пакетів до цього хосту. Перший фільтр (пакети що приходять) налаштований на знищення всіх пакетів крім тих, які приходять від спеціальних програм з захищеного хоста. Аналогічно першому, другий фільтр (пакети що виходять) налаштований на знищення всіх пакетів, крім тих, що спрямовані до спеціальних додатків захищеного хоста. Тому всі дані якими обмінюються комп'ютери організації та комп'ютери з доступом до Internet, проходять через захищений хост.

На захищеному хості працює спеціальне програмне забезпечення, яке відоме під назвою шлюзу прикладного рівня, або проху-сервера.

Наприклад, користувач бажає використовувати протокол FTP для скачування файлу. Після подачі користувачем запиту, клієнтське програмне забезпечення, встановлене на комп'ютері користувача, вступає у взаємодію з проху-сервером FTP на захищеному хості. Після відправлення клієнтом запиту на отримання файлу, проху-сервер перевіряє, дозволений чи запит за правилами захисту організації, отримує копію з сервера Internet, перевіряє її на відсутність вірусів, а потім передає її на комп'ютер користувача. Програмне забезпечення шлюзу прикладного рівня може вести журнал всіх запитів для перевірки в автономному режимі.

Перша задача, яка виникає перед адміністратором проксі-сервера - авторизація та ідентифікація користувачів для виходу в Інтернет через нього. Підтримка проксі таких схем авторизації як NTLM, MSNT, SMB, LDAP, істотно полегшує вирішення поставленого завдання. Ідентифікація особливо важлива, коли необхідно вирішити питання аудиту та фільтрації трафіку.

Для вирішення даної задачі каналотворюючим протоколом вибрано протокол Internet Protocol Security (IPSec). Він описує усі стандартні методи

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		61

VPN та визначає методи ідентифікації при ініціалізації тунелю, методи шифрування між цими вузлами. Цей протокол орієнтований тільки на IP-протокол. IPSec вирішує наступні основні задачі встановлення та підтримання захищеного з'єднання:

- аутентифікацію користувачів або комп'ютерів при ініціалізації захищеного з'єднання;
- шифрування та аутентифікацію передаваних даних між кінцевими точками з'єднання;
- автоматичний обмін кінцевих точок секретними ключами, які необхідні для роботи протоколів аутентифікації та шифрування даних.

Для вирішення цих задач система IPSec використовує протоколи трьох типів:

- протокол обміну ключами Internet IKE (Internet Key Exchange), що використовується для першого етапу установки з'єднання та визначення способу ініціалізації захищеного каналу, а також процедури обміну та керування секретними ключами в рамках захищеного з'єднання;
- протокол АН (Authentication Header ), який забезпечує цілісність та аутентифікацію джерела даних, а також захист від помилкового відтворення пакетів;
- протокол ESP (Encapsulation Security Payload), що забезпечує шифрування, аутентифікацію та цілісність передаваних даних.

Для шифрування даних в IPSec може бути використаний будь-який симетричний алгоритм шифрування, що використовує секретні ключі. Перевірка цілісності та аутентифікація даних виконується з допомогою визначення хеш-коду даних.

Взаємодіють протоколи IKE, АН та ESP наступним чином. Спочатку за допомогою протоколу IKE між двома точками встановлюється SA. При установці каналу виконується аутентифікація його кінцевих точок, вибираються параметри захисту даних. Потім починають працювати

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		62

протоколи АН або ESP, за допомогою яких виконується захист даних з використанням вибраних параметрів. В рамках однієї асоціації може працювати тільки один з протоколів – АН або ESP. Для роботи протоколів АН та ESP по захисту даних між двома кінцевими точками повинна існувати безпечна асоціація SA. Параметри SA визначають, який з протоколів використовується для захисту даних, та режим роботи протоколу – транспортний або тунельний. Система IPSec дозволяє використовувати два способи встановлення асоціації – ручний або автоматичний. У IPSec пакети аутентифікуються з використанням хеш-функції MD5 або за допомогою хеш-функції SHA-1, а шифруються за допомогою алгоритму DES, 3DES, AES. Протоколи IPSec можуть захищати дані в двох режимах: транспортному та тунельному. В транспортному режимі передача пакету виконується за допомогою оригінального заголовку цього пакету. В тунельному режимі початковий пакет розміщується у новому пакеті і передача відбувається за допомогою заголовку нового пакету.

Для шифрування даних пропонується алгоритм шифрування 3DES. 3DES - симетричний блоковий криптографічний алгоритм, створений на основі алгоритму DES, з метою усунення головного недоліку останнього - малої довжини ключа (56-бітний), який може бути зламаний методом перебору ключа. У 3DES був вибраний простий шлях збільшення довжини ключа, без необхідності переходити на новий алгоритм – в ньому над 64 бітовим блоком даних кілька разів проводиться шифрування алгоритмом DES (звичайно з різним ключем), в простому варіанті це виглядає як:  $DES(k_3; DES(k_2; DES(k_1; M)))$ , де M – блок початкових даних,  $k_1$ ,  $k_2$ , і  $k_3$  - ключі DES, цей варіант відомий як EEE - оскільки три операції DES є шифруванням, поширеніший варіант EDE, в якому в середині шифрування DES з ключем  $k_2$ , замінюється операцією дешифровки з тим же ключем ( $k_2$ ):  $DES(k_3; DES^{-1}(k_2; DES(k_1; M)))$ . Довжина ключа алгоритму 3DES дорівнює 168 бітам (3х ключ DES).

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		63

Підписання пакетів кодами HMAC забезпечує перевірку точного збігу отриманих і відправлених даних. Це називається перевіркою цілісності і має критичну важливість при обміні даними через небезпечні середовища.

Коди HMAC забезпечують цілісність шляхом створення хеша з ключем, математично обробляючи повідомлення із застосуванням функції хешування у поєднанні із загальним секретним ключем. Хеш зазвичай описується як підпис на пакеті. Проте хеш відрізняється від цифрового підпису. Хеш використовує секретний загальний ключ, а цифровий підпис - технологію відкритого ключа і закритий ключ відправляючого комп'ютера. Цифровий підпис забезпечує неможливість заперечення авторства, а хеш - ні. Функції хешування також називають односторонніми. За допомогою односторонніх функцій легко отримати хеш з повідомлення, але визначити початкове повідомлення з хеша математично неможливо. Двосторонні функції, навпаки, дозволяють отримати початкове повідомлення з перетвореної форми. Прикладами двосторонніх функцій є схеми шифрування і розшифровки.

Хеш є криптографічною контрольною сумою або кодом цілісності повідомлення, який повинен бути обчислений кожною стороною з'єднання для перевірки повідомлення. Наприклад, відправляючий комп'ютер використовує функцію хешування і загальний ключ для обчислення контрольної суми повідомлення, що додається в пакет. Приймаючий комп'ютер повинен виконати ту ж хеш-функцію над отриманим пакетом і загальним ключем, а потім порівняти результат з результуючим (включеним в отриманий пакет). Якщо повідомлення було змінено на шляху проходження, значення хеша відрізнятяться і пакет відкидається.

Для перевірки цілісності при настройці політики можна вибрати одну з двох хеш-функцій:

- алгоритм MD5 (Message Digest 5) заснований на RFC 1321. Розроблений як відповідь на виявлену ненадійність алгоритму MD4. MD5

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		64

оброблює блоки даних в чотири проходи (MD4 виконував три проходи), кожного разу використовуючи різні числові константи для кожного слова в повідомленні. Число 32-розрядних констант, використовуваних при обчисленнях по алгоритму MD5, рівне 64, що кінець кінцем дає 128-розрядний хеш, який використовується для перевірки цілісності. Алгоритм MD5 забезпечує цілісність надійніше, ніж MD4, хоч і інтенсивніше використовує ресурси.

- SHA1 (Secure Hash Algorithm 1) був розроблений національним інститутом стандартів і технологій США (National Institute of Standards and Technology, NIST), як описано в документі FIPS (Federal Information Processing Standard). Процес SHA багато в чому нагадує MD5. Обчислення SHA1 створюють 160-розрядний хеш, який використовується для перевірки цілісності. Оскільки надійність хешу прямо пропорційна його довжині, SHA надійніше, ніж MD5.

Для використання у мережі пропонується хешування за алгоритмом SHA-1.

Для вирішення задачі обміну ключами між віддаленими пристроями використовується протокол IKE. Протокол IKE автоматизує обмін ключами та встановлює безпечне з'єднання. Крім того, IKE дозволяє змінювати ключ для вже встановленого з'єднання, що підвищує конфіденційність передаваної інформації. IKE представляє собою комбінацію декількох протоколів – ISAKMP, Oakley та SKEME. Розробники протоколу IKE доповнили загальні правила та процедури протоколу ISAKMP процедурами аутентифікації та обміну ключами, взятими з протоколів Oakley та SKEME. Аутентичність сторін в IKE встановлюється двома способами: за протоколом аутентифікації з використанням хеш-функції або з використанням сертифікатів відкритих ключів стандарту X.509. Після перевірки аутентичності сторін протокол IKE використовує алгоритм Діффі-Хеллмана, за допомогою якого сторони визначають ключ, який буде використаний протоколами AH та ESP. [4]

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		65

Алгоритм Діффі-Хеллмана – алгоритм, що дозволяє двом сторонам отримати загальний секретний ключ, використовуючи незахищений канал зв'язку. Цей ключ може бути використаний для шифрування подальшого обміну за допомогою алгоритму симетричного шифрування.

Алгоритм був вперше опублікований Вітфілдом Діффі (Whitfield Diffie) і Мартіном Хеллманом в 1976 році, проте, пізніше з'ясувалося, що цей же метод був придуманий декількома роками раніше Малькольмом Вільямсоном для англійського штабу урядового зв'язку, і був засекречений. У 2002 році Хеллман запропонував називати алгоритм «Діффі - Хеллмана - Меркле», визнаючи внесок Меркле у винахід криптографії з відкритим ключем.

При роботі алгоритму, кожна сторона:

1. Генерує випадкове натуральне число  $a$  - закритий ключ ;
2. Спільно з видаленою стороною встановлює відкриті параметри  $p$  і  $g$  (зазвичай значення  $p$  і  $g$  генеруються на одній стороні, і передаються іншій),  $p$  може бути будь-яким натуральним числом ,  $g$  повинне бути первісним коренем;
3. Обчислює відкритий ключ  $B$  використовуючи необоротне перетворення над закритим ключем, з використанням відкритих параметрів  $B = g^a \bmod p$ , де  $\bmod$  - операція ділення по модулю;
4. Обмінюється відкритими ключами з видаленою стороною ;
5. Обчислює загальний секретний ключ  $K$ , використовуючи відкритий ключ видаленої сторони  $B$  і свій закритий  $K = B^a \bmod p$ .

Ключ виходить рівним з обох сторін, тому що:

$$B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = A^b \bmod p. \quad (6.1)$$

Стійкість алгоритму Діффі - Хеллмана (тобто проблема визначення  $a$ ,  $b$  або  $K$  з відомих  $p$ ,  $g$ ,  $A$  і  $B$ ) заснована на передбачуваній складності завдання дискретного логарифмування. У практичних реалізаціях, для  $a$  і  $b$

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		66

використовуються числа порядку  $10^{100}$  і  $p$  порядку  $10^{300}$ . Число  $g$  не повинне бути великим і зазвичай має значення 2 або 5.

Отже, візуальний огляд приміщень доцільно проводити перед початком або після завершення нарад, а також на початку і після завершення робочого дня. Під час проведення візуального огляду особливу увагу необхідно приділити тим місцям, куди можна таємно і швидко встановити закладний пристрій. Таким чином, можна виявити закладки, які залишені відвідувачами в легкодоступних місцях: за шторами, за меблями, за батареями, під підвіконнями, під сидіннями стільців.

Для захисту мережі електропередачі, потрібно щоб підприємство мало власну підстанцію, на своїй території. Це дозволить закрити цей канал витоку інформації.

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		67

## ВИСНОВКИ

В рамках роботи, метою якої була розробка системи відеоспостереження були вирішені поставлені завдання:  
-Викладено теоретичні та правові основи розробки систем безпеки. Систему безпеки можна розділити на фізичні, технічні та комбіновані системи охорони. Технічні системи охорони можна розділити на механічні та електронні. Складовою частиною електронних систем охорони є системи відеоспостереження.

-Проведено огляд сучасних архітектур систем відеоспостереження.

-Розглянуто програмне та технічне забезпечення типового підприємства.

-Розроблена система відео спостереження.

В результаті аналізу апаратного та програмного забезпечення, пропонуваного на ринку інформаційних технологій, розроблений оптимальний варіант системи відеоспостереження.

Розроблена система включає:

-IP-камери зовнішнього відеоспостереження моделі Avigilon 2.0 MP-HD-H264-B;

-IP-камери внутрішнього відеоспостереження моделі SRD-3000at;

-програмне забезпечення відеоспостереження «лінія», розроблена компанією «ДевЛайн», комутатор, кабель, коннектор та інші витратні матеріали.

В результаті проведеної роботи була розроблена електронна система відеоспостереження, яка дозволяє:

- спостерігати за периметром навколо всього офісу, а також всередині;

- стежити за робочим процесом в офісі;

- здійснювати відеозапис у форматі AVI на жорсткий диск персонального комп'ютера.

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		68

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алтуев М. Перспективы развития цифрового CCTV. Мнения специалистов // Алгоритм Безопасности. – 2003. – № 4. - 56с.
2. Відеокамери (серія Радіомайстер) – Партал О.Н – [Електронний ресурс]. – Режим доступу: URL: [http://www.bookzone.com.ua/Netshop/catalogue/catalogue\\_3271.html](http://www.bookzone.com.ua/Netshop/catalogue/catalogue_3271.html)
3. Відеокамери види та різниця – [Електронний ресурс]. – Режим доступу: URL:<http://www.bezpekacity.com.ua7>
4. Відеоспостереження і охоронні системи.[Електронний ресурс]. – Режим доступу: URL: <http://www.install.in.ua>.
5. Відеоспостереження, спеціалізована відео техніка.- [Електронний ресурс]. – Режим доступу до ресурсу: <http://kaschtan.com.ua/shop>.
6. Все про відеокамери в Україні – [Електронний ресурс]. – Режим доступу: URL: <http://videokamera.in.ua>
7. Гавриш В.А. Практическое пособие по защите коммерческой тайны. — Симферополь: Таврида, 1994. — 112 с
8. Гвоздек М. Справочник по технике для видеонаблюдения. Планирование, проектирование, монтаж: пер. с нем. [Текст] / М. Гвоздек. — Москва: Техносфера, 2010. - 552 с.
9. Гедзберг Ю. М. Охранное телевидение. – М.: Горячая линия – Телеком, 2005.–312 с.
10. Герасименко В. А., Малюк А. А. Основы защиты информации. — М.: МГИФИ,1997. — 538 с
11. Дворкович В. П. Цифровые видеoinформационные системы (теория и практика) [Текст] / В. П. Дворкович, А. В. Дворкович. – Москва: Техносфера, 2012. - 1008 с.
12. Загальний підхід до проектування систем відеоспостереження // Режим доступу: <http://skaz.com.ua/jurnalistika/11745/index.html>

					ІАПЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		69

13. Інтегровані системи безпеки // Режим доступу:  
[https://відеокамери.com.ua/integrovani\\_sustemu\\_bezpeku/](https://відеокамери.com.ua/integrovani_sustemu_bezpeku/)

14. Информационная безопасность современного коммерческого предприятия: Монография. – Старый Оскол: ООО «ТНТ», 2005. – 448.

15. Использование PoE коммутатора для PoE IP системы видеонаблюдения// Режим доступу:  
<https://zen.yandex.ru/media/id/5d2d875b998ed600acf9c37b/ispolzovanie-poe-kommutatora-dlia-poe-ip-sistemy-videonabliudeniia-5ebbc60988866d29dba7c7f3>

16. Кашкаров А. Системы видеонаблюдения. Практикум [Текст] / А. Кашкаров. – М: Феникс, 2014.

17. Коммутатор POE для видеонаблюдения // Режим доступу:  
<https://bezopasnik.info>

18. Кругль Г. Профессиональное видеонаблюдение. Практика и технологии аналогового и цифрового CCTV [Текст] / Г. Кругль. 2010. - 640 с.

19. Лутц Х. Видеоаналитика: Мифы и реальность [Текст] / Х. Лутц, Т. Анштедт, И. Келлер. 2014. - 176 с.

20. Лыткин А. IP-видеонаблюдение: наглядное пособие [Текст] / А. Лыткин. - 2011 . - 200 с.

21. Никулин О.Ю., Петрушин А.Н. Системы телевизионного наблюдения: Учебно-справочное пособие. – М.: Оберег-РБ, 1997. - 125с.

22. Пескин А. Е. Системы видеонаблюдения. Основы построения, проектирования и эксплуатации [Текст] / А. Е. Пескин. – М: Горячая линия-Телеком, 2016. – 256 с

23. Попов А. Моя азбука видеонаблюдения [Текст] / А. Попов. – Санкт-Петербург, 2013. - 248 с.

24. Проект відеоспостереження // Режим доступу:  
[https://www.vostok.dp.ua/ukr/infa1/sistemy\\_vidyeonablyudeniya/psv/](https://www.vostok.dp.ua/ukr/infa1/sistemy_vidyeonablyudeniya/psv/)

25. Проектування системи відео спостереження // Режим доступу:  
[https://відеокамери.com.ua/proektyvannya\\_videosposterejennya/](https://відеокамери.com.ua/proektyvannya_videosposterejennya/)

					ІАПЦ 466120.004 ПЗ	Лист
						70
Изм.	Лист	№ докум.	Підпис	Дата		

26. Проектування системи відеоспостереження - основа забезпечення безпеки об'єкта // Режим доступу: <http://analitic.ub.ua/25246-proektuvannya-sistemi-videosposterejennya--osnova-zabezpechennya-bezpeki-obekta.html>

27. Рассел Дж. Видеонаблюдение [Текст] / Дж. Рассел, 2012.

28. Рыжова В.А. Проектирование и исследование комплексных систем безопасности. СПб: НИУ ИТМО, 2012.-157с.

29. Сердюков В. С., Пономаренко С. В. Инженерно-техническая защита информации: Методические указания по выполнению курсовой работы. – Белгород: Кооперативное образование, 2006. – 88 с.

30. Системи безпеки // Режим доступу: <http://bibliograph.com.ua/spravochnik-105-oborudovanie/34.htm>

31. Система відеоспостереження // Режим доступу: <http://www.elvis.com.ua/ua/cctv-ua.html>

32. Системи відеоспостереження -[Електронний ресурс]. – Режим доступу: URL: <http://www.bastion.kiev.ua/Main/Videonablyudenie>

33. Системи відеоспостереження для чайників - [Електронний ресурс]. – Режим доступу: URL: <http://www.sec4all.net/cameras1.html>

34. Торокин А.А. «Основы инженерно-технической защиты информации». – М.: Издательство «Ось-89» 1998 г. - с. 143

35. Установка відеоконтролю: різновиди систем відео спостереження // Режим доступу: <http://awtceft.com/821-ustanovka-vdeokontrolyu-rznovidi-sistem-videosposterezhennya.html>

36. Халяпин Д. Б., Ярочкин В. И. Основы защиты информации. - М.: ИПКИР,1994

37. Хонович Дж. Руководство по видеонаблюдению [Текст] / Дж. Хонович. – 2010.

38. Шиверский А. А Защита информации: проблемы теории и практика.-М.: Юрист, 1996.

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		71

39. Ярочкин В. И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Фонд "Мир", 2003. - 640с.

					ІАЛЦ 466120.004 ПЗ	Лист
Изм.	Лист	№ докум.	Підпис	Дата		72