МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ

ЗАТВЕРДЖУЮ
Зав. кафедри КСУ
_____ П. Леонтьєв
_____2022р.

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему:

«*Автоматизація системи охоронної сигналізації підприємства*»

Дипломний проект

Виконав:
студент групи СУдн-84п О. С. Шаповал

Керівник проекту:
доцент, к.т.н. В. Д. Черв'яков

СУМИ 2022

№ строчки	Формат	Позначення	Найменування	Кількість листів	№ екз.	Примітка
1			Документація загальна			
2			Знову розроблена			
3						
4	А4		Реферат	2		
5	А4		Технічне завдання	3		
6	А4	СУдн-84П.151.10.ПЗ	Пояснювальна записка	119		
7						
8			Примінена			
9						
10	А4		Завдання	2		
11						
12			Документація конструкторська			
13			Знову розроблена			
14						
15	А4	СУдн-84П.151.10.А1	Типова схема побудови системи охоронної сигналізації на базі обладнання Рубіж-08	1		
16	А4	СУдн-84П.151.10.А2	Схема підключення обладнання «Рубіж -08»	1		
17	А4	СУдн-84П.151.10.А3	Структурна схема централізованої системи охоронної -пожежної сигналізації	1		
18						
19						
20						
21						
22						
23			Документація по плакатам			
24			Знову розроблена			
25						

Зм.	Лист	№ документа	Підпис	Дата	СУдн-84П.151.10.ДП		
Розробив		Шаповал О. С.			Автоматизація системи охоронної сигналізації підприємства. Відомість проекту	Літ.	Лист 2 / Листів 1
Керівник		Черв'яков В. Д.					
Рецензент						Гр.СУдн-84П	
Н.контроль							

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра: " Комп'ютеризованих систем управління "
Спеціальність: 151-«Автоматизація та комп'ютерно-інтегровані технології»

ЗАТВЕРДЖУЮ
Зав. кафедри КСУ
_____ П. Леонтьєв

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра (дипломний проект) студенту

Шаповал Олексію Сергійовичу

1.Тема проекту:
Автоматизація системи охоронної сигналізації підприємства

затверджена наказом по університету від "_10_" _червня 2022_р. №0433-VI

2. Термін здачі студентом закінченого проекту *15.06.2022 р*

3. Початкові дані до проекту: *Завдання кафедри, технічне завдання на проектування, матеріали переддипломної практики.*

4. Зміст записки пояснення

1. ЗАГАЛЬНІ ПРИНЦИПИ ЗАХИСТУ ОБЕКТІВ ІНЖЕНЕРНО-ТЕХНІЧНИХ ЗАСОБІВ ОХОРОНИ;
2. ЗАГАЛЬНІ ВІДОМОСТІ ПРО ІНТЕГРОВАНІ СИСТЕМИ І КОМПЛЕКСИ;
3. АНАЛІЗ ОБ'ЄКТУ ПРОЕКТУВАННЯ;
4. ЕКОНОМІЧНА ЧАСТИНА;
5. ОХОРОНА ПРАЦІ.

5.Перелік графічного матеріалу

1. Типова схема побудови системи охоронної сигналізації на базі обладнання Рубіж-08

2. Схема підключення обладнання «Рубіж -08».

3. Структурна схема централізованої системи охоронної -пожежної сигналізації

6.Дата видачі завдання 16.05.22 р

Керівник проекту _____В. Д. Черв'яков
Прийняв до виконання _____О. С. Шаповал

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів дипломного проекту	Терміни виконання етапів проекту	Приміт.
1	*РОЗРОБКА ТЕХНІЧНОГО ЗАВДАННЯ*	*26.05.22–27.05.22*	
2	*ЗАГАЛЬНІ ПРИНЦИПИ ЗАХИСТУ ОБЕКТІВ ІНЖЕНЕРНО-ТЕХНІЧНИХ ЗАСОБІВ ОХОРОНИ*	*27.05.22–31.05.22*	
3	*ЗАГАЛЬНІ ВІДОМОСТІ ПРО ІНТЕГРОВАНІ СИСТЕМИ І КОМПЛЕКСИ*	*31.06.22-02.06.22*	
4	*АНАЛІЗ ОБ'ЄКТУ ПРОЕКТУВАННЯ*	*02.06.22–03.06.22*	
5	*РОЗРОБКА ГРАФІЧНОЇ КОНСТРУКТОРСЬКОЇ ДОКУМЕНТАЦІЇ ПРОЕКТУ*	*03.06.22–08.06.22*	
6	*ОФОРМЛЕННЯ ЕКОНОМІЧНОЇ ЧАСТИНИ І ОХОРОНИ ПРАЦІ ТА БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ*	*08.06.22-12.06.22*	
7	*ОФОРМЛЕННЯ ПЗ, ГРАФІЧНІЙ КОНСТРУКТОРСЬКІЙ ДОКУМЕНТАЦІЇ*	*12.06.22-13.06.22*	
8	*ЗДАЧА ДИПЛОМНОГО ПРОЕКТУ КЕРІВНИКОВІ*	*13.06.22-14.06.22*	
9	*ЗДАЧА ДИПЛОМНОГО ПРОЕКТУ НА РЕЦЕНЗІЮ*	*14.06.22-15.06.22*	

Студент-дипломник _____ О. С. Шаповал
Керівник проекту _____ В. Д. Черв'яков

ТЕХНІЧНЕ ЗАВДАННЯ

на проектування

автоматизації системи охоронної сигналізації підприємства

Розробник:

студент групи
СУдн-84п О. С. Шаповал

Погоджено:
керівник проекту:
доцент, к.т.н. В. Д. Черв'яков

Суми – 2022

ЗАГАЛЬНИЙ ОПИС

Автоматизація системи охоронної сигналізації підприємства.

Науково-виробнича фірма «Сігма - Інтегровані Системи» є одним з провідних розробників і виробників інтегрованих систем безпеки. Прилади «Рубіж-07-3» і «Рубіж-08» служать основою для організації ІСБ середніх і крупних об'єктів, «Рубіж-060» і «Р-020» для організації ІСБ малих і середніх об'єктів. Названі вище прилади застосовуються для організації систем охоронної, тривожної і пожежної сигналізації, управління виконавчими пристроями контролю доступу, технологічної сигналізації, автоматичного пожежогасіння. Всі вказані системи інтегруються на рівні устаткування і функціонують незалежно від наявності ПЕВМ, що забезпечує високу надійність ІСБ в цілому.

МЕТА І ПРИЗНАЧЕННЯ РОЗРОБКИ

Метою даної роботи є ознайомленням та вибором обладнанням автоматизації системи охоронної сигналізації підприємства.

ДЖЕРЕЛА РОЗРОБКИ

1. Системи технічної безпеки: актуальні реалії (http://www.video-control.ru/surveillance_systems.html)

2. Розподілений апаратний інтелект - наступний ступінь в еволюції систем відеоспостереження (http://www.secnews.ru/articles/7512.htm)

3. SecurityNews (http://www.secnews.ru/)

4. IP-видеонаблюдение: переваги і недоліки (http://www.visionpro.ru/art97)

5. Охоронні системи. Інформаційне видання. Випуск 4, М., «Солон», 2018 р.

6. Гавріш В. Практіческоє посібник із захисту комерційної таємниці. Симфе рополь. «Тавріда». 2018 р.

7. Підприємництво і безпека. М., Універсум. 2018 р.

8. Алексєєнко Ст. Н., Сокольський Б. Е. Системи захисту комерційних объек тов. Технічні засоби захисту. М., 2018 р.

9. Бізнес і безпека. М., КМЦ «Центуріон». 2018 р.

10. Кисельов А. Е. і ін. Комерційна безпека. М., Іноро Арт. 2018 р.

11. Технічні засоби охорони, безпеки і сигналізації. Довідник. BIMI, 2018 р.

12. Никулін О. Ю., Петрушин А. Н. Системи телевізійного спостереження. М., «ОБЕРЕГ-РБ», 2017г.

13. Рейці Ч. Д. 55 електронних схем сигналізації. М., Енергоатоміздат, 2011 р.

14. Андріанов Ст. І., Соколів А. В. Охранниє пристрої для автомобілів. «Лань» Спб. 2018 р.

15. Винограду Ю. А. Електронная охорона (елементи і вузли охоронних систем). М., «СИМВОЛ-Р», 2018г.

16.N. V. P. R. Durga Prasad, T. Lakshminarayana, et al., “Automatic Control and Management of lectrostatic Precipitator”, IEEE Transactions on Industry Applications, pp. 561-567, Vol. 35, No. 3, May/June, 1999.

17.Ralf Joost and Ralf Salomon. “Advantages of fpga-based multiprocessor systems in industrial applications”. In 31st Annual Conference of the IEEE Industrial Electronics Society (IECON 2005). IEEE-I ECON, November 2019.

18.Hyman, Anthony. Charles Babbage, pioneer of the computer. — Oxford University Press, 2019.

19. Randell, Brian. The Origins of Digital Computers: Selected Papers.. — 2003.

Реферат

Шаповал Олексій Сергійович. Автоматизація системи охоронної сигналізації підприємства. Кваліфікаційна робота бакалавра (дипломний проект). Сумський державний університет. Суми, 2022 р.

Кваліфікаційна робота бакалавра (дипломний проект) містить 119 сторінок пояснювальної записки, до складу якої входять 7 рисунків, 3 таблиці, 19 джерел інформації, графічно-конструкторська документація складається з 3 креслень та презинтації.

В даній кваліфікаційній роботі розглянуто питання по автоматизації системи охоронної сигналізації підприємства.

Ключові слова: мікропроцесор, датчик.

Summary

Shapoval Alexey Sergeevich. The automation of the security alarm system of the enterprise. Bachelor's thesis (diploma project). Sumy State University. Sumy, 2022.

Bachelor's thesis (diploma project) contains 119 pages of explanatory note, which includes 7 figures, 3 tables, 19 sources of information, graphic design documentation consists of 3 drawings and presentations.

In this qualification work the issues of automation of the security alarm system of the enterprise are considered.

Keywords: microprocessor, sensor.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ

Пояснювальна записка

до кваліфікаційної роботи бакалавра (дипломного проекту)
на тему:

" Автоматизація системи охоронної сигналізації підприємства"

Виконав:
студент групи СУдн-84п О. С. Шаповал

Керівник проекту:
доцент, к.т.н. В. Д. Черв'яков

СУМИ 2022

Зміст

ПЕРЕЛІК СКОРОЧЕНЬ І УМОВНИХ ПОЗНАЧЕНЬ

АПІ	– адресний пожежний оповіщувач
АППК	– адресний приймально-контрольний прилад
АС	– апаратні засоби
АСПС	– адресна система пожежної сигналізації
АЦП	– аналого-цифровий перетворювач
ГСА	– графічна схема алгоритму
ГТІ	– генератор тактових імпульсів
ІМС	– інтегральна мікросхема
ЗУ	– пристрій, що запам'ятовує
КД	– конструкторська документація
КОП	– код операції
КП	– контрольний процес
КУВОП	– код управління виконанням операції
КУД	– контроль і управління доступом
МП	– мікропроцесор
МПС	– мікропроцесорна система
О	– операційний блок
ОЗУ	– оперативний пристрій, що запам'ятовує
ОО	– об'єкт, що охороняється
ОПС	– охоронний – пожежна сигналізація
УО	– пристрій крайовий
ПАО	– пункт автономної охорони
ПДП	– прямий доступ в пам'ять
ПЗП	– постійний пристрій, що запам'ятовує

ППКП	– пожежний приймально-контрольний прилад
ПК	– персональний комп'ютер
ПС	– програмні засоби
ПФ	– передній фронт
ПЦН	– пункт централізованого спостереження
ПЦО	– пункт централізованої охорони
Р	– рентранслятор
РП	– робочий процес
СВН	– система відеоспостереження
СТІЛЬНИК	– система охоронна телевізійна
СПИ	– система передачі сповіщень
ТЗ	– технічне завдання
УА	– автомат, що управляє
УБ	– блок, що управляє
УВВ	– пристрої введення/виводу
ЦАП	– цифро-аналоговий перетворювач
ЕОМ	– електронна обчислювальна машина

ВСТУП

Нормальне, планове функціонування підприємства, компанії, банку, магазина і інших організацій (далі - фірм, об'єктів) - одна з головних турбот їх керівників.

Стійка робота будь-якої фірми неможлива без забезпечення належного рівня її безпеки - здатності функціонувати без збитку і при цьому постійно протистояти всіляким погрозам.

У сучасних умовах проблема забезпечення безпеки будь-якого об'єкту виходить в розряд пріоритетних, що обумовлене рядом причин:

•зростання злочинності в країні;

•активізація терористичної і диверсійної діяльності націоналістичних і підривних організацій;

•збільшення кількості нещасних випадків, стихійних лих і техногенних аварій;

•насущна необхідність реструктуризації бізнесу на базі новітніх інформаційних технологій, сприяючих появі устаткування інформаційно-обчислювального і телекомунікаційного призначення, яке вимагає особливого захисту;

•необхідність підвищення конкурентоспроможності фірми.

Засоби захисту людини і його майна розвивалися протягом тривалого періоду від простих засобів фізичного захисту житла людини до сучасних систем безпеки.

У останні десятиліття багато керівників все більше усвідомлюють необхідність забезпечення безпеки, про що свідчить збільшення витрат фірм на ці цілі. Разом з тим зростання "невиробничих" витрат, до яких найчастіше відносять витрати на безпеку, служить також приводом для неспокою тих керівників, які будують свою політику безпеки в основному на традиційному використанні "живої сили". Тому в даний час як ніколи актуальне питання про підвищення рівня захисту і оптимізації системи безпеки фірми.

Поняття безпеки включає безліч різних аспектів. Зупинимося докладніше на таких як технічна укрепленность об'єкту, технічна система охорони, пожежна безпека, режим об'єкту, інформаційна безпека.

Під технічною системою охорони (ТСО) в даному випадку розуміється система раннього виявлення погроз фірмі від стихійних лих, несанкціонованого проникнення порушників і помилкових або неправомірних дій обслуговуючого персоналу або клієнтів фірми. При цьому виявлення, а часто нейтралізація і навіть ліквідація погроз, здійснюється за допомогою різних технічних засобів (ТС) і методів.

Для того, щоб не було болісне боляче за безцільно витрачені гроші, необхідно вибирати правильні, оптимальні напрями побудови такої системи. При цьому вибір повинен

грунтуватися на концептуальному підході до аналізу особливостей об'єкту і можливостей сучасних технологій, на ретельному маркетинговому опрацьовуванні.

Найбільшого поширення набули системи охоронно-пожежної сигналізації, застосування яких достатнє ефективно вирішує проблеми забезпечення безпеки за допомогою технічних засобів.

Проте найбільш ефективним є комплексне рішення задачі забезпечення безпеки з використанням інтегрованих систем. Як правило, в їх склад окрім систем охоронної і пожежної сигналізації входять системи контролю і управління доступом і охоронного телебачення. У інтегрованих системах контроль і управління всіма технічними засобами здійснюється за допомогою передових комп'ютерних технологій з використанням сучасних аппаратнопрограммных засобів.

Широке застосування сучасних систем безпеки для захисту об'єктів вимагає і відповідного підходу до підготовки кадрів, здатних професійно і грамотно не тільки проектувати, але і здійснювати монтажні і пуско-налагоджувальні роботи, експлуатувати, оперативно усувати виникаючі неполадки.

Монтаж сучасних інженерно-технічних засобів забезпечення безпеки об'єктів є одним з найбільш технічно складних розділів монтажних робіт. Від кваліфікації монтажників, знання ними сучасної технології монтажу, прийомів роботи, уміння користуватися технічно здійсненими інструментами і механізмами багато в чому залежать якість і надійність багаторічної роботи систем безпеки об'єктів, функціонування яких направлене на забезпечення захисту майна і безпеки людей від злочинних посягань і пожежі.

В умовах ринкової економіки монтажники винні не тільки добре знати сучасні технології електромонтажних робіт, уміло ними користуватися, але і поглиблено вивчати технічні і конструктивні особливості технічних засобів систем безпеки, їх принципи побудови і дії, методи їх перевірок і безпечні прийоми монтажу.

Велике значення для забезпечення належної якості підготовки відповідних фахівців, безумовно, мають сучасні засоби навчання: підручники і навчальні посібники, що відображають сучасний рівень розвитку систем безпеки.

Проте більшість з них є описом технічних характеристик конкретних типів устаткування. Відчувається явний недолік підручників і навчальних посібників, в яких розглянуті загальні принципи побудови, дії, проектування, монтажу і експлуатації сучасних систем безпеки.

Метою даного курсового проекту є проектування комплексної системи охорони, дослідження доцільності застосування тих або інших засобів, а також огляд ринку систем охорони з метою вибору системи і устаткування, найбільш відповідних для заданого об'єкту

1. ЗАГАЛЬНІ ПРИНЦИПИ ЗАХИСТУ ОБ'ЄКТІВ ІНЖЕНЕРНО-ТЕХНІЧНИХ ЗАСОБІВ ОХОРОНИ

1.1 Концептуальні питання забезпечення безпеки фірми

Для створення оптимальної ефективної системи безпеки об'єкту необхідно перш за все розробити обгрунтовану концепцію, що визначає цілі захисту, характер можливих погроз і вірогідність їх появи, основні напрями вирішення завдань захисту тих або інших цінностей від аварій, стихійних лих і неправомірних дій потенційних порушників.

Предмет захисту - конкретні цінності фірми, які підлягають захисту за допомогою тієї або іншої системи. До таких цінностей відносяться:

•люди - персонал об'єкту, відвідувачі і клієнти фірми;

•матеріальні і фінансові цінності (гроші, цінні папери, документи, устаткування);

•інформація конфіденційного характеру.

Пріоритети вказаних цінностей у великій мірі обумовлені характером діяльності фірми.

Об'єкт захисту - фізичний простір, де зосереджені ті або інші цінності, багато в чому визначає можливі дії порушника безпеки і у відповідь заходи із запобігання погрозам безпеці фірми.

Шляхи формування технічної системи охорони в значній мірі залежать від характеристик конструкцій приміщень і інженерно-технічних систем об'єкту, що захищають, їх відповідності вимогам нормативно-технічної документації по будівництву, забезпеченню безпеки, протипожежним правилам. Великий вплив на характеристики ТСО надає також стан, в якому знаходиться об'єкт - стадія розробки проекту, будівництва, реконструкції або постійної експлуатації.

У кожній фірмі існують приміщення, що вимагають особливого підходу до забезпечення їх охорони. До таких приміщень насамперед відносяться:

•кабінети керівництва фірми;

•переговорні кімнати;

•касові приміщення;

•центр обчислювальної і телекомунікаційної мережі - "серверна";

•приміщення АТС і комутаційного устаткування телефонної мережі;

•приміщення з комутаційно-розподільною апаратурою інформаційно-телекомунікаційних систем (ІТКС) і систем безпеки;

•базові приміщення систем інженерного забезпечення (СИО) - вентиляційна камера, електрощитова кімната, приміщення резервного електроживлення і диспетчерської служби;

•приміщення служби безпеці фірми - центральний пост охорони, пост пожежної охорони;

•архів паперових і електронних копій;

•найбільш важливі технологічні приміщення, виходячи з характеру бізнес-процеса у фірмі.

Погрози безпеці фірми можна класифікувати таким чином: за природою

виникнення - погрози випадкового характеру і викликані навмисними діями порушників; по відношенню до об'єкту, що захищається: зовнішні і внутрішні.

До погроз випадкового характеру (зовнішнім і внутрішнім) відносяться стихійні лиха і катастрофи природного і техногенного характеру, аварії або порушення в роботі систем життєзабезпечення об'єкту, а також помилкові дії персоналу і відмови устаткування. У число зовнішніх погроз входять також криміногенні погрози, недобросовісна конкуренція, промислове шпигунство зловмисників, що навмисно діють. Погрози, викликані навмисними діями порушників безпеки об'єкту (як зовнішніх, так і внутрішніх), виявляються у вигляді розкрадань матеріальних цінностей, вандалізму вредительства, саботажу, диверсій і терору. Основними мотивами таких погроз можуть бути незадоволеність конкретним керівником, бажання самоствердж уватися, пихатість, корислива прагнення отримати матеріальну або іншу вигоду, а також намір реалізувати свої політичні, релігійні і ідеологічні устремління.

Внутрішні погрози - це зловмисні дії персоналу (зазвичай з соціально-психологічними і моральними проблемами). Ініціаторами такого виду погроз виступають, як правило, самі співробітники або зовнішні структури, що діють шляхом підкупу персоналу.

Оцінка погроз, аналіз риски їх реалізації і прогнозування можливого збитку по кожному виду погроз - найважливіший напрям забезпечення безпеці фірми.(1)

1.1.1 Принципи побудови і оптимізації ТСО об'єкту:

•універсальність, що припускає, що всі рішення мають бути відпрацьовані і уніфіковані;

•комплексність, що припускає, що використовувані прийоми роботи і вживані ТС взаємопов'язані між собою, доповнюють один одного за функціональними і технічними показниками;

•**розумна достатність**, що означає, що заходи щодо забезпечення безпеки об'єкту мають бути адекватні можливим погрозам з боку вірогідного порушника по фінансових, матеріально-технічних і кадрових ресурсах;

•**оперативність**, що припускає пріоритет методів і засобів захисту, що забезпечують швидке виявлення і подальшу нейтралізацію можливих погроз;

•**адаптивність**, що передбачає, що методи і засоби захисту можуть бути достатньо гнучко пристосовані до змін організаційних і технічних умов функціонування об'єкту;

•**безперервність**, систематичність, що означають, що вибрані рішення забезпечать достатньо ефективний цілодобовий захист об'єкту;

•**цілеспрямованість** - зосередження зусиль на захист найбільш цінних ресурсів фірми або найуразливіших ділянок об'єкту;

•**многорубежность**, що припускає використання додаткових просторових рубежів безпеки або методів захисту для найбільш відповідальних, з погляду безпеки, приміщень і зон об'єкту;

•**равнопрочность** створюваних меж безпеки;

•**послідовність** у використанні відповідних методів і засобів при виявленні, віддзеркаленні і ліквідації погроз безпеці об'єкту (так звана эшелонированность безпеці);

•**сумісність** з існуючими системами;

•**простота, екологічна чистота і непомітність** ("дружність"), що припускають, що розгортана система не створить додаткових перешкод для нормального функціонування фірми, не зажадає дуже високої кваліфікації і тривалої підготовки обслуговуючого персоналу, не заподіє шкоди цінностям об'єкту, що захищаються;

•**неуязвимость** - здатність протистояти спробам виведення системи, що робляться, з ладу;

•**документоване, що припускає реєстрацію** подій, що цікавлять, пов'язаних з об'єктом, що захищається, що необхідне для подальшого аналізу тривожних і нештатних ситуацій і досягнутого рівня захищеності об'єкту;

• **правомірність**, що означає, що всі вживані заходи організаційного і технічного характеру легальні і юридично обоснованны.

1.1.2 Основні напрями побудови ТСО

Оптимальна політика при створенні ТСО полягає в тому, щоб, виходячи з виділених ресурсів і намічених пріоритетів, проводити необхідні заходи, що передбачають поступове підвищення ефективності всієї системи забезпечення безпеки. Іншими словами, при наявних

ресурсах необхідно прагнути до того, щоб забезпечити максимально досяжний на даний момент часу рівень захисту об'єкту.

При проведенні конкретних заходів по розгортанню ТСО необхідно дотримуватися концептуальних положень забезпечення безпеки, враховувати і особливості об'єкту, що захищається, і оперативну обстановку на даний момент часу, що дозволить досягти достатньо високого рівня безпеки.

При проведенні конкретних заходів по розгортанню ТСО необхідно дотримуватися концептуальних положень забезпечення безпеки, враховувати і особливості об'єкту, що захищається, і оперативну обстановку на даний момент часу, що дозволить досягти достатньо високого рівня безпеки.

1.1.3 Необхідність інтегрованих рішень

Певний рівень безпеки об'єкту може бути досягнутий різними способами, наприклад, шляхом використання численного штату співробітників охоронних структур або установки декількох автономних технічних систем безпеки (ТСБ) різного типу.

В цілях охорони застосовуються зазвичай такі традиційні ТСБ, як:

система контролю і управління доступом (СКУД); система пожежної сигналізації (включаючи аварійне сповіщення і управління евакуацією персоналу і відвідувачів) (СПС); система охоронної сигналізації (включаючи захист периметра об'єкту і тривожне сповіщення) (СОС); система відеоконтроля (СВК).

Розгортання якою-небудь окремою автономною ТСБ вимагає, як правило, порівняно невеликих фінансових витрат за рахунок використання традиційної апаратної бази і випробуваних технічних рішень.

Застосування тих або інших систем продиктоване часто певним консерватизмом в області забезпечення безпеки і перевагами замовника і виконавця, що склалися. Крім того, підрядчик, що виконує проектування і монтаж ТСБ, схильний пропонувати відомі йому, забезпечені ресурсами і випробувані (але часто не найоптимальніші) технічні рішення і апаратні засоби.

Установка всіх необхідних для забезпечення ефективного захисту об'єкту систем вимагає, як правило, значних витрат і приводить як до непотрібного дублювання функцій і високих експлуатаційних витрат, так і до нестиковок (відсутності взаємодії між окремими системами). В результаті створюється комплекс складних в управлінні, дорогих систем безпеки, але з обмеженими можливостями.

При побудові дійсно ефективної комплексної технічної системи охорони її, як і всяку іншу систему, необхідно розглядати в цілому, як єдність організаційно-технічних мерів, направлених на захист об'єкту.

Відзначимо, що глибока інтеграція ТСБ можлива тільки при підтримці на об'єкті основних, базових рівнів інтеграції, що спираються на організаційно-адміністративні способи захисту об'єкту, а також засоби і методи інженерно-технічного захисту. Ці методи і засоби носять універсальний характер. Вони забезпечують захист всіх видів цінностей об'єкту при залученні, як правило, мінімально можливих ресурсів. Базові рівні особливо ефективні завдяки тому, що сприяють запобіганню погрозам за рахунок створення тих або інших перешкод (фізичного або психологічного характеру) для потенційного порушника.

Якщо виходити з цільового завдання, (а не з традиційних уявлень про існуючі технічні рішення і способи їх реалізації), то найбільш доцільним рішенням при побудові ТСО є використання принципів системної інтеграції і створення комплексної багатофункціональної технічної системи, що суміщає в собі функції всіх традиційних автономних систем. Інтегрована технічна система охорони (ІТСО) припускає об'єднання на базі сучасних інформаційних технологій і програмно-апаратної інтеграції декількох підсистем, функціонально і інформаційно зв'язаних один з одним, і їх роботу по єдиному алгоритму.

Навіть при мінімальному рівні інтеграції взаємодія підсистем здійснюється таким чином, що події в одній з підсистем можуть впливати на інших і викликати певну реакцію. Так, ІТСО, створена на базі традиційних підсистем СКУД, СПС, СОС і СВК, забезпечує, наприклад, наступні види взаємодії між підсистемами:

•розблокування дверей і проходів (СКУД), використовуваних при евакуації, в зонах можливої пожежі або по всьому об'єкту при отриманні сигналу пожежної тривоги (від СПС);

•блокування охоронних зон, тамбурів і шлюзів (СЬКУД) при спрацьовуванні різних охоронних детекторів (у СОС) або детекторів активності від відеокамер (у СВК);

•використання тривожних сигналів (від СПС, СКУД і СОС) для підключення відповідних відеокамер (СВК), що дозволяє уточнити і документувати обстановку в зоні тривоги.

В порівнянні з простий сукупністю окремих систем і засобів захисту застосування інтегрованих систем безпеки забезпечує наступні переваги:

•швидшу і точнішу реакцію на події, що відбуваються;

•оптимальний аналіз поточних ситуацій;

•значне зниження риски, пов'язаної з "людським чинником" - помилками і можливими недобросовісними діями обслуговуючого персоналу і співробітників фірми;

•зменшення витрат на устаткування зважаючи на багатофункціональне використання окремих ТС і повнішого їх завантаження;

•полегшення роботи обслуговуючого персоналу за рахунок автоматизації процесів управління, контролю і ухвалення рішень по забезпеченню безпеки;

•зниження витрат на монтаж і експлуатацію системи безпеки, скорочення обслуговуючого персоналу і витрат на його навчання і зміст.

При побудові і оптимізації ІТСО необхідно враховувати, що сучасним системам безпеки властиві всі характерні ознаки складних людино-машинних систем:

•наявність великого числа взаємозв'язаних елементів;

•неопределенность із-за неповної інформації про потенційного порушника і його дії;
•субъективизм, пов'язаний з необхідністю ухвалення людиною важливих оперативних рішень;

•різноманіття умов функціонування (різні умови експлуатації, наявність природних і промислових перешкод).

1.1.4 Взаємодія ІТСО з іншими системами

При розгляді взаємодії ІТСО і інших систем об'єкту необхідно виходити з наступних положень:

•всяка система є ієрархічною структурою, елементами і зв'язками якої (як внутрішніми, так і зовнішніми) не можна нехтувати;

•накопичення і об'єднання властивостей елементів системи приводить до появи якісно нових властивостей, не характерних для її окремих елементів;

•система працює тим краще і стійкіше, чим менше її окремі частини взаємодіють між собою і з навколишнім середовищем.

Любая система - складова частина що впливає на її структуру і функціонування складнішої системи. До такої системи більш високого рівня можна віднести інтегровану технічну систему безпеки (ІТСБ), яка служить складовою частиною єдиної інтегрованої системи об'єкту, об'єднуючої всі інженерно-технічні системи.

Разом з ІТСО, ІТСБ може охоплювати такі системи, як:

•інформаційно-аналітична система, що забезпечує завдання аналізу рисок, можливих погроз, юридичного захисту;

•система економічної безпеки, що виконує завдання перевірки клієнтів, повернення кредитів, захисту від недобросовісної конкуренції;

•система власної безпеки, що забезпечує виконання завдань перевірки співробітників на лояльність, огляду відвідувачів, персоналу і кореспонденції, контролю систем життєзабезпечення об'єкту, екологічного моніторингу;

•система захисту інформації в інформаційно-обчислювальних і телекомунікаційних мережах;

•система захисту інформації від витоку по технічних каналах;

•система автоматичної пожежогасінні і дымоудаления;

•система фізичної охорони об'єкту;

•система забезпечення безпеки автоперевезень.

Щоб уникнути прикрих помилок при побудові ІТСО необхідно враховувати особливості всіх систем, що сполучаються з нею. Прикладом такої помилки може служити використання в приміщеннях фірми, що вимагають особливої охорони, технічних засобів, що володіють вираженим мікрофонним ефектом (таких, як акустичні охоронні детектори, датчики голосових систем управління, гучномовці систем звукової трансляції). Всі вони можуть бути використані потенційним порушником для несанкціонованого знімання інформації.

Створюючи ІТСО об'єкту, необхідно уявляти собі напрями інтеграції на суміжних ієрархічних рівнях. У нашому випадку буде потрібно сполучення ІТСО на рівні інтегрованої системи будівлі. При цьому найбільш ефективні рішення знаходяться в області концепції "інтелектуальної будівлі" (З), коли на базі новітніх інформаційних технологій інтегруються не тільки системи інженерного забезпечення будівлі, але і телекомунікаційні, обчислювальні системи, а також технічні системи безпеки.

"Інтелектуальну будівлю" забезпечує ефективне використання робочого простору завдяки оптимізації всіх його структур, систем, служб і зв'язків між ними.

Невід'ємна частина З - структурована кабельна мережа (СКС) - ієрархічна базова кабельна система будівлі, що є, по суті, елементом його капітального будівництва. СКС дозволяє об'єднати в єдину систему всі дротяні системи об'єкту.

Структурована мережа вимагає значних первинних витрат, що обумовлене використанням достатньо дорогого устаткування (категорированного високочастотного кабелю, комутаційної апаратури, качественых кабелепроводів). Проте витрати окупаються досить швидко - після декількох перебудов мережі без додаткової прокладки кабелів.

Кабелепроводи СЬКС і розетки різного призначення дозволяють підключати офісну і інформаційно-обчислювальну апаратуру, телекомунікаційну техніку, електропобутові прилади, ТС безпеки, датчики систем життєзабезпечення.

З конфігурується так, щоб функціональні можливості всіх його систем можна було б нарощувати у міру появи додаткових засобів або потреб. При цьому виключається необхідність розтину дротяних комунікацій або повного перепрограмування або заміни систем управління. Важливо також, що З готово до сприйняття нових технологій і послідовної модернізації своїх систем протягом вельми тривалого періоду (15-20 років).

Концепция З припускає інтеграцію найрізноманітніших інженерно-технічних і організаційно-адміністративних систем. Така інтеграція сприяє оптимізації ділових процесів фірми, в які залучені кадрові, матеріальні, фінансові і інформаційні ресурси, і значному підвищенню ефективності роботи фірми за рахунок реинжиниринга бізнесу.

По своїй спрямованості системи З можна класифікувати як "будівельні" (це питання архітектури, реконструкції і будівництва); системи забезпечення життєдіяльності; організаційно-адміністративні і дротяні системи.

Системи інженерного забезпечення включають такі системи забезпечення життєдіяльності, як система водопостачання, газопостачання і каналізації, кондиціонування і вентиляції повітря, а також дротяні енергетичні системи, до них відносяться системи загального електропостачання, гарантованого і безперебійного електроживлення, інтелектуального освітлення (що включає аварійне і чергове освітлення), заземлення і молниезащиты.

Інформаційними системами об'єкту є дротяні слабкострумові системи (можуть бути також системи, що використовують радіо і оптичний канали) не енергетичного призначення, використання, що відрізняються по наступних напрямах:

•зв'язок і передача інформації; •управление експлуатацією будівлі;

•забезпечення безпеки об'єкту;

•забезпечення бізнес-процесів фірми;

•забезпечення відпочинку і комфортних умов роботи.

Інформаційні системи можна умовно розділити на наступні системи:

1.Інформаційно-телекомунікаційна система (ІТКС) в орієнтовному складі: •локальная обчислювальна мережа (ЛВС);

•система учрежденческой автоматичного телефонного зв'язку, що забезпечує комутований і прямий телефонний зв'язок, диспетчерський зв'язок, конференцзв'язок.

2.Система управління експлуатацією (СУЕ) об'єкту - орієнтування в її склад можуть входити наступні системи:

•управління водопостачанням і каналізацією;

•забезпечення кондиціонування і вентиляції повітря;

•управління ліфтовим устаткуванням;

•контролю основних енергетичних показників;

•забезпечення екологічного моніторингу;

•запобігання заледенінню елементів будівельних конструкцій і дренування зливових вод;

•управління автостоянками.

3.Інтегрована технічна система охорони - в її склад орієнтування входять системи: контролю і управління доступом (СЬКУД); пожежній сигналізації (СПС); аварійного сповіщення і управління евакуацією персоналу і відвідувачів (СОУЕ); охоронній сигналізації (включаючи захист периметра і тривожну сигналізацію) (СОС); відеоконтроля (СВК).

4.Технологічні системи об'єкту, наприклад, такі системи, як:

•робототехнічних виробничих ліній для заводів;

•забезпечення дилингпроцессов банків;

•огляду покупців і запобігання крадіжкам магазинів;

•виклику, зв'язку і сигналізації лікарень;

•замкнутого телебачення для учбових закладів.

5.Забезпечуючі системи - орієнтування вони можуть включати системи:

•электрочасофикации і синхронізації;

•дротяній радіотрансляції;

•управління звуком, що забезпечує місцеве гучномовне віщання і сповіщення, озвучування залів засідань і переговорних кімнат;

•колективного прийому телевізійних сигналів.

При підтримці концепції "інтелектуальної будівлі" на об'єкті вдається отримати значну економію засобів за рахунок оптимального використання людських і енергетичних ресурсів при експлуатації будівлі. Більш того, забезпечуються простота експлуатації будівлі і комфортні умови роботи персоналу.

Правильно побудована ІТСО взаємодіє з іншими технічними системами будівлі по наступних позиціях:

•формування необхідної структури і конфігурація системи при використанні кабелепроводів, дротяних каналів і комутаційних можливостей СЬКС об'єкту;

•забезпечення безперебійного і захищеного електроживлення системи при підключенні до промислової мережі електропостачання, систем резервованого живлення, заземлення і молниезащиты;

•створення надійного розподіленого управління системою при підключенні до ЛВС;

•видалений контроль системи при використанні телекомунікаційних ліній і мереж;

•підвищення ефективності візуального контролю, надійності і оперативності виконання евакуаційних заходів при залученні можливостей системи освітлення;

•сповіщення зовнішніх організацій (підрозділів ГУ ГПС, ГУ В МВС РФ, комерційних охоронних підприємств) з метою ліквідації погроз об'єкту при підключенні до міської телефонної мережі;

•запуск систем пожежогасінні і дымоудаления при виявленні спалахів;

•блокування або активація окремих ТС і систем при виявленні погроз (примусовий пуск всіх ліфтів вниз і їх відключення, перемикання вогнестримувальних і герметизуючих заслінок і клапанів на воздуховодах, відключення систем вентиляції);

•активація систем захисту інформації (обмеження доступу до ресурсів інформаційно-обчислювальних мереж, виявлення і придушення засобів несанкціонованого знімання інформації) у відповідних зонах при виявленні тривожних ситуацій.(1)

1.2 Технічне забезпечення об'єкту

1.2.1 Загальні положення

У даному матеріалі даються рекомендації по побудові системи інженерного захисту об'єктів. Під інженерним захистом мають на увазі фізичне зміцнення всіх елементів і будівельних конструкцій об'єкту з метою перешкодити несанкціонованому проникненню зловмисників на територію об'єкту і/або всередину приміщень. Система інженерного захисту повинна протистояти простому подоланню, злому (пролому, тарану), підриву, підпалу. Гарантований час протистояння має бути таким, щоб служби безпеці могли встигнути зафіксувати факт спроби силового проникнення, оцінити ступінь потенційної небезпеки і прийняти адекватні заходи протидії.

До теперішнього часу поки не розроблена єдина нормативна документації по побудові систем інженерного захисту недержавних підприємницьких структур. Існують окремі інструкції по організації захисту банків і інших організацій, що працюють з грошима і цінними паперами, проте всі вони носять достатньо розпливчатий характер, На практиці у кожному конкретному випадку схема побудови системи захисту узгоджується з органом охорони (міліція). Об'єкт приймається під охорону після міліційної інспекції системи захисту. При цьому ті, що найчастіше інспектують керуються вже напрацьованим досвідом, а іноді - і інтуїцією.

Головну роль в забезпеченні комплексної безпеки об'єкту грають технічні засоби охоронно-пожежної сигналізації (ТС ОПС) і засобу технічної укрепленности.

Правильний вибір і застосування ТС ОПС і засобів технічної укрепленности на об'єкті дозволяє забезпечити достатньо високу надійність захисту об'єкту від всіх можливих внутрішніх і зовнішніх видів погроз і небезпечних ситуацій. В той же час відсутність належного підходу до процесу вибору і застосування ТС ОПС і засобів технічної укрепленности знижує рівень (або ефективність) безпеки і приводить до непомірно високих витрат на забезпечення необхідної безпеки.

Вибір варіанту устаткування об'єкту ТС ОПС і засобами технічної укрепленности визначається характеристиками значущості приміщень об'єкту, його будівельними і архітектурно-планувальними рішеннями, умовами експлуатації і обслуговування, режимом роботи, перешкодами, що виникають на об'єкті, і багатьма іншими чинниками, які необхідно враховувати при проектуванні комплексної системи безпеки.

Етап проектування системи безпеки - найбільш важливий період, протягом якого закладаються всі основні функції і структури системи безпеки.

На цьому етапі проводиться обстеження об'єкту, цілями якого є:

•изучение на місці характеристик об'єкту, що визначають його стійкість до передбачуваних злочинних посягань і можливих надзвичайних ситуацій;

•визначення комплексу заходів і розробка технічних пропозицій по організації охорони об'єкту з урахуванням сформованих типових рішень, що забезпечують достатню безпеку.

За наслідками обстеження розробляється технічне завдання на проектування комплексу технічних засобів охорони. Обстеження об'єкту проводиться міжвідомчою комісією (МВК) у складі представників адміністрації (або служби безпеці) об'єкту, підрозділу позавідомчої охорони, госпожнадзора і, при необхідності, інших зацікавлених організацій.

Проектування, підготовка і виконання робіт повинні здійснюватися відповідно до нормативно-технічних документів.(2)

1.2.2 Основні поняття

•**Інженерно-технічна укрепленность об'єкту** - сукупність заходів, направлених на посилення конструктивних елементів будівель, приміщень і територій, що охороняються, що забезпечують необхідну протидію несанкціонованому проникненню в зону, що охороняється, злому і іншим злочинним посяганням.

•**Надійність** - властивість об'єкту зберігати в часі у встановлених межах значення всіх параметрів.

•**Вразливе місце** - частина елемент фрагмент периметра об'єкту, будівлі приміщення, через який найбільш вірогідне проникнення.

•**Конструкції, що несуть,** - конструкції (елементи),воспринимающие постійне і тимчасове навантаження, зокрема навантаження від інших частин будівлі.

•**Категорія об'єкту, що охороняється,** - комплексна оцінка об'єкту, що враховує його економічну або іншу (наприклад, культурну) значущість, залежно від характеру і концентрації зосереджених цінностей, наслідків від можливих злочинних посягань на них, складнощі забезпечення необхідної охорони.

•**Порушник** - особа, що намагається проникнути або що проникло в приміщення (на територію), захищене системою охоронної або охоронно-пожежної сигналізації без дозволу відповідальної особи, користувача або мешканця.

•**Особливо важливий об'єкт** - об'єкт, значущість якого визначається органами державної влади або місцевого самоврядування з метою визначення мерів по захисту інтересів держави, юридичних і фізичних осіб від злочинних посягань і запобігання збитку, який може бути нанесений природі і суспільству, а також від виникнення надзвичайної ситуації.

•**Об'єкт життєзабезпечення** - сукупність життєво важливих матеріальних, фінансових засобів і послуг, згрупованих по функціональному призначенню і використовуваних для задоволення життєво необхідних потреб населення (наприклад, у вигляді продуктів харчування, житла, предметів першої необхідності, а також в медичному, санітарно-епідеміологічному, інформаційному, транспортному, комунально-побутовому забезпеченні та інші).

•**Об'єкт підвищеної небезпеки** - об'єкт, на якому використовують, проводять, переробляють, зберігають або транспортують радіоактивні, взрыво-, пожароопасные, небезпечні хімічні і біологічні речовини, що створюють реальну загрозу виникнення джерела надзвичайної ситуації.

•**Об'єкт, що охороняється,** - підприємство, організація, житло, їх частина або комбінація, обладнані системою охорони і безпеки, що діє.

•**Типові проектні рішення** - технічні вирішення устаткування технічними засобами охорони і елементами інженерно-технічною укрепленности ряду аналогічних за призначенням і конструктивно-будівельним характеристикам об'єктів або їх окремих конструкцій.

•**Збиток від злочинного посягання** - економічні, екологічні або соціальні наслідки (збитки, втрати) від злочинного посягання на об'єкт, що охороняється.

У обгрунтованих випадках, за узгодженням з підрозділом, що здійснює охорону, допускається для захисту окремих конструктивних елементів об'єкту і вразливих місць використовувати тільки системи контролю і управління доступом або охоронного телебачення, за наявності в них пристроїв, що виконують аналогічні функції систем охоронної і тривожної сигналізації (наприклад, контроль відкриття дверей, автоматичне узяття/зняття з охорони по ідентифікатору, застосування обнаружителей руху, передача зображення в пункт централізованої охорони).

1.2.3 Категорювання приміщень

Вибір варіанту устаткування об'єкту ТС ОПС і засобами технічної укрепленности визначається важливістю приміщень об'єкту, виглядом і розміщенням цінностей в цих приміщеннях. Всі приміщення будь-якого об'єкту можна розділити умовно (по вигляду і розміщенню в них цінностей) на чотири категорії:

•**перша категорія** - приміщення, де розміщені товари, предмети і вироби особливої цінності і важливості, втрата яких може привести до особливо крупного або непоправного матеріального і фінансового збитку, створити загрозу здоров'ю і життю великого числа людей, що знаходяться на об'єкті і поза ним, привести до інших тяжких наслідків.

Зазвичай до таких приміщень відносяться: сховища (комори) цінностей, склади зберігання зброї і боєприпасів, приміщення з постійним зберіганням наркотичних і отруйних речовин, а також секретній документації і інших особливо цінних і особливо важливих товарно-матеріальних цінностей;

•**друга категорія** - приміщення, де розміщені цінні і важливі товари, предмети і вироби, втрата яких може привести до значного матеріального і фінансового збитку, створити загрозу здоров'ю і життю людей, що знаходяться на об'єкті.

До таких приміщень можна віднести: спецархіви і спецбібліотеки, сейфовые кімнати

приміщення зберігання табельної вогнепальної зброї, радіоізотопних речовин і препаратів, ювелірних виробів, предметів старизни, мистецтва і культури, грошових коштів, валюти і цінних паперів (головні каси об'єктів);

•**третя категорія** - приміщення, де розміщені товари, предмети і вироби повсякденного попиту і використання.

До таких приміщень відносяться: службові, конторські приміщення, торгові зали і приміщення промислових товарів, побутової техніки, продуктів харчування і т. п.;

•**четверта категорія** - приміщення, де розміщені товари, предмети і вироби технологічного і господарського призначення.

До таких приміщень можна віднести: підсобні і допоміжні приміщення, приміщення з постійним або тимчасовим зберіганням технологічного і господарського устаткування, технічній і конструкторській документації і тому подібне

1.2.4 Категорії об'єктів, що охороняються

1.Об'єкти, що не охороняються, з вільним допуском персоналу і відвідувачів.

2.Об'єкти з простими (пасивними) обмеженнями і огорожами типу загород, що не охороняються (огорожі, стіни, грати і ін.).

3.Об'єкти із загородами, що охороняються, які контролюються охоронцями, з постовими нарядами, патрульними службами і співробітниками пропускної системи.

4.Об'єкти з особливим режимом охорони, допуск на яких забезпечується спеціально підготовленими і розставленими по території і периферії охоронцями. Використовуються складні інтегровані технічні системи санкціонування доступу, теленаблюдения і охоронно-пожежної сигналізації, об'єднані в єдиний комплекс, який управляється компьютером і контролюється на центральному пульті охорони.

За наслідками аналізу української і зарубіжної статистики спроб несанкціонованого проникнення в приміщення комерційних структур (офіси, виробничі і складські приміщення) зроблені наступні виводи про ефективність різних систем безпеки

•на об'єкти першої категорії - до 50% від загального числа спроб проникнення;

•на об'єкти другої категорії - близько 25%;

•на об'єкти третьої категорії - близько 20%;

•на об'єкти четвертої категорії - менше 5%.(3)

1.3 Технічна оснащеність об'єкту

1.3.1. Засоби охоронно-пожежної сигналізації

1.3.1.1 Призначення, класифікація і структура сигналізації

Система охоронно-пожежної сигналізації є складним комплексом технічних засобів, службовців для своєчасного виявлення спалаху і несанкціонованого проникнення в зону, що охороняється. Як правило, охоронно-пожежна сигналізація інтегрується в комплекс, об'єднуючий системи безпеки і інженерні системи будівлі, забезпечуючи достовірною

адресною інформацією системи сповіщення, пожежогасінні, дымоудаления, контролю доступу і ін.

Залежно від масштабу завдань, які вирішує охоронно-пожежна сигналізація, в її склад входить устаткування трьох основних категорій:

•Устаткування централізованого управління охоронно-пожежною сигналізацією (наприклад, центральний комп'ютер зі встановленим на нім ПО для управління охоронно-пожежною сигналізацією; у невеликих системах охоронно-пожежної сигналізації завдання централізованого управління виконує охоронно-пожежна панель);

•Устаткування збору і обробки інформації з датчиків охоронно-пожежної сигналізації: прилади приймально-контрольні охоронно-пожежні (панелі);

•Сенсорні пристрої - датчики і извещатели охоронно-пожежної сигналізації. Інтеграція охоронної і пожежної сигналізації у складі єдиної системи охоронно-пожежної сигналізації здійснюється на рівні централізованого моніторингу і управління. При цьому системи охоронної і пожежної сигналізації адмініструються незалежними один від одного постами управління, що зберігають автономність у складі системи охоронно-пожежної сигналізації. На невеликих об'єктах охоронно-пожежна сигналізація управляється при-емно-контрольными приладами.

Приймально-контрольний прилад здійснює живлення охоронних і пожежних извещателей по шлейфах охоронно-пожежної сигналізації, прийом тривожних сповіщень від извещателей, формує тривожні повідомлення, а також передає їх на станцію централізованого спостереження і формує сигнали тривоги на спрацьовування інших систем.

Система охоронної сигналізації у складі охоронно-пожежної сигналізації виконує завдання своєчасного сповіщення служби охорони про факт несанкціонованого проникнення або спробу проникнення людей в будівлю або його окремі приміщення з фіксацією дати, місця і часу порушення рубежу охорони.

Система пожежної сигналізації призначена для своєчасного виявлення місця спалаху і формування сигналів, що управляють, для систем сповіщення про пожежу і автоматичної пожежогасінні.

Вітчизняні нормативні документи по пожежній безпеці строго регламентують перелік будівель і споруд, що підлягають оснащенню автоматичною пожежною сигналізацією. В даний час весь перелік організаційно-технічних заходів на об'єкті під час пожежі має одну головну мету - врятування життя людей. Тому на перше місце виходять завдання раннього виявлення спалаху і сповіщення персоналу. Вирішення цих завдань покладене на пожежну сигналізацію, основні функції якої сформульовані в наступному визначенні.

Пожежна сигнализация- отримання, обробка, передача і уявлення в заданому вигляді споживачам за допомогою технічних засобів інформації про пожежу на об'єктах, що охороняються.

Основні функції пожежної сигналізації забезпечуються різними технічними засобами. Для виявлення пожежі служать извещатели, для обробки і протоколювання інформації і формування сигналів тривоги, що управляють, - приймально-контрольна апаратура і периферійні пристрої.

Окрім цих функцій, пожежна сигналізація повинна формувати команди на включення автоматичних установок пожежогасінні і дымоудаления, систем сповіщення про пожежу, технологічного, електротехнічного і іншого інженерного устаткування об'єктів. Сучасна апаратура охоронно-пожежної сигналізації має власну розвинену функцію сповіщення. Не дивлячись на те, що системи сповіщення про пожежу виділені в самостійний клас устаткування, на базі технічних засобів пожежної сигналізації достатньо багатьох виробників можна реалізовувати системи сповіщення 1 і 2 категорії.

1.3.1.2 Оповіщувачі охоронно-пожежної сигналізації

Для отримання інформації про тривожну ситуацію на об'єкті до складу охоронно-пожежної сигналізації входять извещатели, що відрізняються один від одного типом контрольованого фізичного параметра, принципом дії чутливого елементу, способом передачі інформації на центральний пульт управління сигналізацією.

За принципом формування інформаційного сигналу про проникнення на об'єкт або пожежу извещатели охоронно-пожежної сигналізації діляться на активних і пасивних.

Активні оповіщувачі охоронно-пожежної сигналізації генерують в зоні, що охороняється, сигнал і реагують на зміну його параметрів.

Пасивні оповіщувачі реагують на зміну параметрів навколишнього середовища, викликану вторгненням порушника або спалахом.

Кожна охоронно-пожежна сигналізація використовує охоронні і пожежні извещатели, контролюючі різні фізичні параметри. Широко використовуються такі типи охоронних извещателей, як інфрачервоні пасивні, магнитоконтактные, извещатели розбиття скла, периметральные активні извещатели, комбіновані активні извещатели. У системах пожежної сигналізації застосовуються теплові, димові, світлові, іонізаційні, комбіновані і ручні извещатели.

Залежно від способів виявлення тривог і формування сигналів, извещатели і системи охоронно-пожежної сигналізації діляться на неадресні, адресні і адресно-аналогові.

У неадресних системах извещатели мають фіксований поріг чутливості, при цьому група извещателей включається в загальний шлейф охоронно-пожежної сигналізації, в якому у разі спрацьовування одного з приладів охоронно-пожежної сигналізації формується узагальнений сигнал тривоги.

Адресні системи відрізняються наявністю в сповіщенні інформації про адресу приладу охоронно-пожежної сигналізації, що дозволяє визначити зону пожежі з точністю до місця розташування извещателя.

Адресно-аналогова охоронно-пожежна сигналізація є найбільш інформативною і розвиненою. У такій системі застосовуються "інтелектуальні" извещатели охоронно-пожежної сигналізації, в яких поточні значення контрольованого параметра разом з адресою передаються приладом по шлейфу охоронно-пожежної сигналізації. Такий спосіб моніторингу використовується для раннього виявлення тривожної ситуації, отримання даних про необхідність технічного обслуговування приладів унаслідок забруднення або інших чинників. Окрім цього, адресно-аналогові системи дозволяють, не перериваючи роботу охоронно-пожежної сигналізації, програмно змінювати фіксований поріг чутливості извещателей при необхідності їх адаптації до умов експлуатації на об'єкті.

Кожен тип извещателя має свій перелік основних технічних характеристик, визначуваних відповідними стандартами. В той же час, навіть однотипні извещатели мають відмінності в конструктивних особливостях складових частин, зручності експлуатації, надійності, рівні дизайну, що враховується при виборі того або іншого приладу або фірми-виробника.(3)

1.3.1.3 Приймально-контрольна апаратура охоронно-пожежної сигналізації

Для отримання і обробки сповіщень охоронно-пожежна сигналізація використовує різні типи приймально-контрольної апаратури: центральні станції, контрольні панелі, прилади приймально-контрольні (назва визначається стандартами країни-виробника, далі по тексту приймемо термін "контрольна панель"). Дана апаратура відрізняється інформаційною ємкістю - кількістю контрольованих шлейфів сигналізації і ступенем розвитку функцій управління і сповіщення. Розрізняють контрольні панелі охоронно-пожежної сигналізації для малих, середніх і великих об'єктів. Як правило, невеликі об'єкти обладналися неадресними системами, контролюючими декілька шлейфів охоронно-пожежної сигналізації, а на середніх і великих об'єктах використовуються адресні і адресно-аналогові системи.

Відмітною конструктивною особливістю адресної і адресно-аналогової охоронно-пожежної сигналізації є застосування кільцевого шлейфу сигналізації, що має підвищений

захист від порушення ліній зв'язку з извещателями. Як правило, кільцевий шлейф контрольних панелей різних фірм-виробників апаратний сумісний з извещателями, розробленими цими ж фірмами. Деякі контрольні панелі підтримують декілька варіантів топології кільцевих шлейфів, що полегшує проектування сигналізації на об'єкті.

Для сумісності адресної або адресно-аналогової охоронно-пожежної сигналізації з неадресними извещателями (зокрема інших фірм-виробників), контрольні панелі додатково можуть підтримувати контроль неадресних шлейфів охоронно-пожежної сигналізації.

Функції управління і сповіщення реалізуються в контрольних панелях за допомогою спеціалізованих вхідних і вихідних інтерфейсів. Для відображення інформації охоронно-пожежна сигналізація широко використовує вбудовані світлові і буквено-цифрові індикатори, звукові сигналізатори. Вихідний інтерфейс в контрольних панелях охоронно-пожежної сигналізації для невеликих об'єктів - це, як правило, набір релейних виходів.

На великих об'єктах системи охоронно-пожежної сигналізації будуються по мережевих технологіях, тому пожежні контрольні панелі оснащуються зовнішніми інтерфейсами RS422 або RS48, а також здатні взаємодіяти по мережі Ethernet або за допомогою модемного зв'язку по комутованому телефонному каналу. Конструктивно інтерфейсні вузли можуть включатися до складу контрольної панелі (розташовуватися на загальній друкарській платі). Переважніший варіант їх реалізації у вигляді окремих друкарських плат, що вмонтовуються при необхідності усередині корпусу контрольної панелі.

1.3.1.4 Периферійні пристрої охоронно-пожежної сигналізації

За периферійні вважаються всі пристрої охоронно-пожежної сигналізації (окрім извещателей), що мають самостійного конструктивного виконання і що підключаються до контроль-ной панелі охоронно-пожежної сигналізації через зовнішні лінії зв'язку. Найчастіше використовуються наступні типи периферійних пристроїв охоронно-пожежної сигналізації:

•пульт управління - застосовується для управління пристроями охоронно-пожежної сигналізації з локальної точки об'єкту;

•модуль ізоляції коротких замикань - використовується в кільцевих шлейфах охоронно-пожежної сигналізації для забезпечення їх працездатності у разі короткого замикання;

•модуль підключення неадресної лінії - для контролю неадресних извещателей охоронно-пожежної сигналізації;

•релейний модуль - для розширення функції сповіщення і управління контрольної панелі;

•модуль входу/виходу - для контролю і управління зовнішніми пристроями (наприклад, автоматичними установками пожежогасінні і дымоудаления, технологічним, електротехнічним і іншим інженерним устаткуванням);

•звуковий оповісник - для сповіщення про пожежу або тривогу в необхідній точці об'єкту за допомогою звукової сигналізації;

•світловий оповісник - для сповіщення про пожежу або тривогу в необхідній точці об'єкту за допомогою світлової сигналізації;

•принтер повідомлень - для друку тривожних і службових системних повідомлень.

1.3.1.5 Інтеграція охоронно-пожежної сигналізації з комплексними системами безпеки будівлі

При установці на крупних об'єктах для забезпечення необхідного рівня безпеки будівлі охоронно-пожежна сигналізація інтегрується з іншими системами безпеки і життєзабезпечення об'єкту. Це необхідно для швидкої реакції на повідомлення про пожежу або тривогу, що поступив від датчиків охоронно-пожежної сигналізації, і забезпечення оптимальних умов для ліквідації виниклої аварійної ситуації. Наприклад, у відповідь на повідомлення про пожежу, яке генерує охоронно-пожежна сигналізація, в тривожній зоні виконуються наступні дії:

•Відключення вентиляції;

•Включення системи дымоудаления;

•Відключення електропостачання (за винятком спецобладнання);

•Вивід з тривожної зони ліфтів;

•Включення аварійного освітлення і світлової індикації шляхів і виходів для евакуації людей;

•Розблокування аварійних виходів на шляхах евакуації;

•Включення системи сповіщення з інформацією для тривожної зони.

Таким чином, охоронно-пожежна сигналізація стає частиною загальної системи безпеки, при цьому вирішуються питання не тільки загального моніторингу з основного поста охраны, але і взаємодія всіх підсистем. У останньому випадку повинно виконуватися

одне їх найважливіших вимог до системи охоронно-пожежної сигналізації - можливість її інтеграції в загальну систему безпеки. Інтеграція може бути потрібною як на простому (релейному) рівні, так і на програмному рівні, коли необхідна сумісність протоколів обміну даними в інформаційних шинах і лініях зв'язку різних підсистем. Велику роль при цьому грає підтримка з боку апаратури охоронно-пожежної сигналізації однієї або декількох мережевих технологій: Ethernet, Arcnet, Lonwork, Internet і ін.

1.3.1.6 Живлення пристроїв охоронно-пожежної сигналізації

Всі пристрої охоронно-пожежної сигналізації повинні забезпечуватися безперебійним електроживленням. Як основний, як правило, використовується мережеве електроживлення контрольних панелей охоронно-пожежної сигналізації, решта пристроїв харчується від низьковольтних вторинних джерел постійного струму або від шлейфу охоронно-пожежної сигналізації. Відповідно до вітчизняних норм пожежної безпеки, охоронно-пожежна сигналізація повинна безперебійно функціонувати у разі пропажі мережевого електроживлення на об'єкті в перебігу 24 годин в режимі очікування і 3 годин в режимі тривоги(без виносних світлових і звукових сигналізаторів). Для виконання цієї вимоги охоронно-пожежна сигналізація повинна використовувати систему резервного електроживлення - додаткові джерела або вбудовані акумуляторні батареї.

1.3.2 Вимоги до технічного оснащення об'єктів засобами охоронної сигналізації

Вимоги до технічного оснащення об'єктів засобами охоронної сигналізації викладені у ВБН В.2.5-78.11.01-2003 (Інженерне устаткування будов і споруд. Системи сигналізації охоронного призначення.) і є обов'язковими для виконання всіма підприємствами, організаціями будь-яких форм власності і приватними особами, що здійснюють проектування, монтажні і пуско-налагоджувальні роботи і сигналізації охоронного призначення, що приймають в експлуатацію системи, на підохоронних об'єктах Державної служби охорони (ГСО) при МВС України.

ВБН В.2.5-78.11.01-2003 (Інженерне устаткування будов і споруд. Системи сигналізації охоронного призначення.) висуває жорсткі вимоги до: проектній документації на системи сигналізації і їх электопитание, устаткуванню робочого місця оператора, блокуванню об'єктів приміщень і будівельних конструкцій, монтажу електричних проводок, монтажу охоронних извещателей різних типів, монтажу приймально-контрольних приладів, акумуляторних установок, пуско-налагоджувальних робіт, прийому в експлуатацію і так далі

Вимоги до технічного оснащення об'єктів засобами охоронно-пожежної сигналізації обумовлені багаторічним досвідом роботи підрозділів Державної служби охорони (ГСО) по охороні об'єктів різних форм власності і важливості, а також тактико-технічними характеристиками технічних засобів охорони, що існують на сьогоднішній день (ТСО).

Технічні укрепленность (інженерний захист) і засоби сигналізації є складовими частинами системи безпеки об'єкту, функції яких доповнюють і компенсують один одного, тому розглядати питання технічного захисту об'єкту необхідно в комплексі.

Одній з особливостей, що характеризують надійність охорони об'єкту, є структура встановленої охоронної сигналізації, яка визначається кількістю рубежів охорони, зон, що охороняються, а також шлейфів сигналізації в кожному рубежі. Об'єкт, що охороняється або спостережуваний підрозділом ГСО, обладнався одним або декількома рубежами охорони. Як правило система багаторубежу охорони об'єкту складається з 2-3 шлейфів сигналізації, які за допомогою приемо-контрольных приладів, телефонних ліній або радіоканалу підключаються на пульти централізованої охорони або спостереження (ПЦО).

Першим рубежем

блокуються будівельні конструкції периметрів об'єктів (віконні і дверні отвори, люки, вентиляційні канали, теплові введення, некапітальні стіни і інші елементи будівель, доступні для несанкціонованого проникнення).

Другим рубежем блокуються внутрішні об'єми і площі приміщень.

Третім рубежем

захищаються локальні об'єкти і матеріальні цінності. За бажанням замовника додатково на об'єкті можуть встановлюватися засоби, так званій, тривожній і пожежній сигналізації.

Приемо-контрольные прилади (ПКП) і концентратори малої ємкості (КМЕ) в системах охоронно-пожежної сигналізації є проміжною ланкою між первинними засобами виявлення проникнення або пожежі (датчиками) і системами передачі сповіщень (СПИ) встановленими на ПЦО.

Одна з основних вимог, що пред'являються до ПКП і КМЕ, це незалежність. При відключенні електроенергії необхідно зберегти контроль за шлейфами сигналізації з боку СПИ, тому ПКП і КМЕ повинні мати джерело резервного електроживлення.

Технічні укрепленность і блокування засобами ОПС вразливих місць об'єктів повинні максимально забезпечити їх захист від несанкціонованого проникнення. Зламати можна будь-які двері і розкрити будь-який сейф, питання тільки в часі, тому дуже важливо, щоб засоби сигналізації спрацьовували на початковому етапі проникнення.

У зв'язку з цим, охоронні датчики при блокуванні вразливих місць в більшості випадків встановлюються перед рубежем механічного захисту.

Найуразливішими будівельними елементами об'єктів є зовнішні двері, вікна і вітрини. На сьогоднішній день є широкий асортимент датчиків за допомогою яких можна надійно заблокувати будь-які конструкції на відкриття, руйнування і пролом.

Стіни, що не проглядаються і некапітальні, на об'єктах, що охороняються, як правило посилюються металевими гратами. Особлива увага приділяється тим стінам, які граничать з підвалами, бойлерними, вентиляційними приміщеннями і тому подібне Некапітальні стелі і пів також блокуються на руйнування і при необхідності зміцнюються. Для їх блокування використовують омічні, інфрачервоні і сейсмічні датчики.

Другим рубежем захищаються підходи до матеріальних цінностей - це внутрішні об'єми і площі приміщень, крім того, до другого рубежу підключають шлейфи блокування куди входять перехідні двері і електромеханічні пастки. Вимоги до другого рубежу охорони в основному зводяться до незалежності електронних извещателей і до правильного вибору місця їх установки, юстирування і налаштування. Метою цих дій є ефективне блокування об'єму і площі приміщення, що охороняється. Для охорони других рубежів використовують інфрачервоні, радіохвильові, ультразвукові, оптико-електронні і комбіновані електронні извещатели. На особливо важливих об'єктах (сховища в банках, комори цінностей, кімнатах зберігання зброї і т. п.) для блокування об'єму і площі приміщення використовуються декілька електронних извещателей, різних за фізичним принципом дії.

Третім рубежем блокуються сейфи, металеві шафи де зберігаються матеріальні цінності або безпосередньо предмети і експонати. Сейфи і металеві шафи блокуються ємкісними извещателями і іншими датчиками на відкриття, перекидання і теплову дію. Для локального блокування матеріальних цінностей використовуються точкові або омічні датчики, установка яких проводиться приховано.

Вибір типу точкових датчиків і електронних извещателей, використовуваних для всіх рубежів охорони, проводиться з урахуванням безлічі чинників: кліматичних умов, конструктивних особливостей об'єкту, що охороняється, вірогідних шляхів проникнення, режиму и тактики охорони. Основні вимоги, що пред'являються до точкових датчиків, - це приховані установки, захист від саботажу і дотримання правил установки. До електромеханічних - незалежність, максимальний захист простору, що охороняється, або площі, захист від дій, що викликають помилкові сигнали "Тривога".Для екстреного виклику нарядів міліції охорони на об'єктах встановлюються кнопки тривожної сигналізації. На їх спрацьовування озброєні мобільні групи підрозділів ГСО реагують насамперед. Кнопки тривожної сигналізації встановлюються приховано, при їх установці має бути виключений

чинник випадкового натиснення. Передача тривожного повідомлення проводиться по індивідуальних телефонних лініях, лініях безпосереднього зв'язку, через апаратуру ущільнення по задіяних телефонних лініях або за допомогою радіоканалу.

Системи теленаблюдения і контролю доступу встановлюються на об'єктах як додаткові рубежі захисту, як правило, за бажанням замовників.

Для особливо важливих об'єктів виконання вимог по технічній укрепленности і оснащенню їх засобами охоронно-пожежної сигналізації є обов'язковим. Для всіх останніх ці вимоги носять рекомендаційний характер.

Залежно від кількості виконаних "Замовником" заходів щодо технічного оснащення його об'єкту передбачаються різні види охорони або спостереження за станом встановлених на об'єкті технічних засобів. Спостереження може здійснюватися не тільки за станом технічних засобів сигналізації, але і за окремими вразливими місцями або предметами об'єкту. На сьогоднішній день спектр охоронних послуг, ГСО, що надаються, дуже широкий.

Проте слід відмітити якщо у Вас власна СБ, або Ви працюєте з комерційним ПЦО, які на сьогоднішній день немало, на всі вимоги м'яко кажучи можна закрити очі.

1.4 Охоронна сигналізація

Охоронна сигналізація має більш ніж вікову історію. Прототипи сучасних систем з'явилися чи не відразу після винаходу електричного дзвінка в першій половині 19 століть. Досить довгий час принцип дії всіх сигналізаторів полягав в замиканні або розмиканні дротяного шлейфу або контактів при спробі проникнути в приміщення, що охоронялося, або викрасти який-небудь предмет.

Вже на початку цього століття всі солідні банки застосовували електричні засоби сигналізації для захисту сховищ і сейфів. Застосування електронних ламп дозволило різко підняти ефективність охоронних систем. Винахід фотоелемента викликала поява светолучевых сигналізаторів, переривання світивши яких приводило до спрацьовування звукового сигналу тривоги.

В кінці 40-х років системи сигналізацій почали широко упроваджуватися для охорони межі СРСР, а також незліченних "спецоб'єктів" - таборів, закритих міст і так далі Тисячі кілометрів периметрів були обладнані простою контактною системою, основою якої була огорожа з колючого дроту.

Різкий стрибок в розвитку радіоелектроніки на рубежі 50-60 років, винахід напівпровідників і досягнення в суміжних областях фізики викликали поява принципово

нових засобів сигналізації. У 1957 році був запатентований перший об'ємний ультразвуковий датчик, що дав життя цілої серії подібних пристроїв.

Слідом за ними послідували мікрохвильові (СВЧ) об'ємні датчики, а з 70-х років, після промислового освоєння піроелектричного кристалічного приймача, був створений пасивний інфрачервоний датчик.

С початки 90-х років різко зросла потреба в системах сигналізації для захисту об'єктів нової форми власності - комерційних банків, фінансових компаній, приватних магазинів і так далі Вітчизняні підприємства-виготівники, орієнтовані в основному на випуск даної продукції для військово-промислового комплексу, перший час не мали дозволу на постачання цих засобів на споживчий ринок. Достатньо малий обсяг випуску даної

продукції не міг забезпечити всіх охочих. Окрім цього вартість систем сигналізації, а також дизайн приладів явно програвали зарубіжним аналогам. У зв'язку з цим на вітчизняний ринок хлинув потік імпортної апаратури.

Зарубіжні компанії відрізняє широта номенклатури пропонованої техніки - від простих датчиків електроконтактів до універсальних систем і комплексів безпеки. Підсистема охоронної сигналізації здійснює функцію охорони об'єкту в будь-якому з передбачених режимів і видає сигнал на виконавчий пристрій у разі порушення режиму охорони.

Чим великою цінністю є те, що знаходиться за закритими дверима, тим більше вірогідність злому цих дверей. Пограбування житлових будинків, підприємств, магазинів і офісів стало явищем щоденного характеру, і, за статистикою, умови для більшості крадіжок створює сама людина. Залишити без нагляду заміський будинок, поставити одного охоронця для контролю багатоповерхової будівлі, розташувати складські приміщення, що не охороняються, на великій території - ці і багато інших дій часто стають причиною розкрадання майна, а іноді і загрозою для життя людини. Своєчасно інформувати про проникнення сторонніх осіб на територію, що охороняється, і сприяти їх упійманню - це завдання систем охоронної сигналізації. Охоронні системи дають можливість вести постійний контроль над обстановкою в житлових, офісних, виробничих приміщеннях, зовнішнього і внутрішнього периметра, незалежно від площі об'єкту, що охороняється, часу доби і присутності охоронного персоналу або господарів приміщення.

Вхідні до складу системи елементи (охоронні датчики, контрольна панель, сигнальні пристрої і пристрої управління сигналізацією) дозволяють встановлювати найбільш ефективні для кожного конкретного об'єкту параметри сигналу тривоги і реакції системи. Різні види датчиків дозволяють враховувати такі чинники, як несанкціонований рух, звук розбиваного скла, руйнування. Сигнальні пристрої, у свою чергу, можуть задіювати слухові

(звукові сирени) і/або зорові канали (строб-вспышки), а також передавати заздалегідь записаний сигнал тривоги на телефонні номери довірених осіб, посилати SMS-сообщения. Для постановки і зняття охоронної сигналізації також можуть використовуватися різні пристрої: сенсорна клавіатура, зручний ношений радіо-брелок, електронні ключі (пластикові проксимити-карточки або ключі Touch Memory).

Залежно від того, куди поступає сигнал тривоги, охоронні системи підрозділяються на автономних і пультових. У першому випадку сигнал тривоги подається безпосередньо на сигнальні пристрої, розташовані на території об'єкту, що охороняється, а в другому - на пульт станції моніторингу і потім в спеціалізовані служби реагування - силові, пожежники, медичні та інші.

Розробка ефективної схеми охоронної сигналізації, як і будь-якої іншої системи безпеки, здійснюється з урахуванням поставлених цілей і особливостей кожного конкретного об'єкту. Сучасні технічні охоронні засоби дозволяють забезпечувати мінімальність помилкових спрацьовувань, вибирати найбільш зручні схеми постановки/зняття на охорону і отримання сигналу тривоги, можливість інтеграції з системами контролю доступу і відеоспостереження.

1.5 Класифікація об'єктів, що охороняються

(Коментарі до ДСТУ 78.11.001-98 Укрепленность об'єктів, які охороняються за допомогою пультів централізованого спостереження Державної служби охорони).

Залежно від значущості, виду і концентрації матеріальних, історичних, культурних і інших цінностей, які зберігаються на об'єктах і в приміщеннях ці об'єкти і приміщення розподіляються на три категорії (А, Би, В).

1.Об'єкти категорії "А":

а)объекты життєзабезпечення населених пунктів;

би)фабрики і центральні сховища дензнаков і цінних паперів;

у)объекты Державного комітету з телебачення і радіомовлення;

грам)государственные центральні статистичні управління;

д)хранилища державних архівів;

же)особенно важливі приміщення, де зберігаються:

•грошові кошти, незалежно від дозволеного залишку зберігання (поштові відділення і вузли зв'язку, виплатні каси підприємств, організацій, установ, головні об'єднані каси торгових підприємств, обмінні пункти валюти і ін.);

•зброя, боєприпаси (стрілецькі тири, кімнати зберігання зброї підприємств і учереждений, стрілецькі стенди, магазини по реалізації мисливської і спортивної зброї, майстерні по ремонту зброї і ін.);

•наркотичні і психотропні речовини, прекурсори, отрути (бази аптекоуправлений, аптеки, склади мобрезерва, наукові, медичні і інші установи, в практиці яких використовуються ці речовини);

•дорогоцінні метали і камені, ювелірні вироби з них (ювелірні заводи і майстерні, магазини, ломбарди, бази, склади, сховища підприємств, установ і організацій, які використовують в своїй діяльності дорогоцінні метали і камені, пункти закупівлі дорогоцінних металів і каменів і ін.);

•історичні і культурні цінності державного значення (музеї, картинні галереї, фондохранилища музеїв, наукові бібліотеки і ін.);

•вибухові і радіоактивні речовини і матеріали;

•бази і склади із зберіганням цінностей на суму понад 100 тисяч мінімальних зарплат;

е)другие об'єкти державного значення.

2. Об'єкти і приміщення категорії "Б" (підприємства, магазини, бази, сховища і ін.), де зберігаються:

а)компьютерная техніка;

би)малогабаритная і дефіцитна оргтехніка;

у)видео- і аудіотехніка, яка має попит;

грам)кино-, фототехніка;

грам)меха натуральні і штучні і вироби з них;

д)кожа натуральна і вироби з неї;

е)автомобили і запасні частини до них;

е)промышленные і продовольчі товари повсякденного попиту;

же)технологическое і господарське устаткування;

з)техническая і конструкторська документація; й) інвентар, напівфабрикати і др.;

і) інші цінні товари.

3. Об'єкту і приміщення категорії "В":

- особисте майно громадян (квартири, садиби громадян, гаражі, дачі, автомобільні стоянки і ін.)

1.6 Склад системи охоронної сигналізації

Будь-яка система охоронної сигналізації складається з датчиків (извещателей), які безпосередньо контролюють зону, що охороняється, а у разі тривоги видають електричний сигнал, приймально-контрольних приладів (пультів-концентраторів), які обробляють цей сигнал за допомогою вбудованих мікропроцесорів і визначають всі подальші дії (включення сирени або автодозвона і тому подібне), а також виконавчих пристроїв, до яких відносяться звукові або світлові оповісники, блоки індикації, принтери для роздруку протоколу подій і тому подібне Зазвичай всі датчики об'єднуються в зони, коли який-небудь об'єкт або частину об'єкту контролює група датчиків.(4)

1.6.1 Охоронні оповіщувачі

Оповіщувачі, вживані в системах охоронних сигналізацій розрізняються за типом тривожних подій, що виявляються:

•на рух (інфрачервоні активні і пасивні, радіохвильові лінійні і об'ємні, ультразвуковий);

•на відкриття (магнитоконтактные);

•на розбиття скла (акустичні, ударно-контактные);

•на наближенні або дотик (ємкісні);

•на трясіння (вібраційні);

•на злочинний напад (тривожні кнопки і педалі, "лялька");

•а також бувають суміщеними або комбінованими.

За способом передачі даних на прилад датчики діляться на дротяних або безпровідних (радіоканальні) В дротяних системах використовуються 2-х дротяні або 4-і дротяні извещатели (для монтажу извещателя необхідно підвести до місця установки извещателя лінію живлячої напруги від блоку живлення і лінію сигналізації).

Пасивні інфрачервоні оповіщувачі

Один з найпоширеніших типів охоронних извещателей. Принцип дії заснований на реєстрації змін потоку теплового випромінювання, що виникають при перетині людиною чутливих зон, перетворенні І До випромінювання в електричний сигнал і проведенні аналізу сигналу по амплітуді і часу. У простих СПИСІВ извещателях обробка сигналу проводиться аналоговими методами, в складніших - цифровими за допомогою вбудованого процесора. Форма зони виявлення формується лінзою Френеля; розрізняють об'ємну, лінійну або поверхневу зони виявлення.

ПІК извещатели бувають як настенными, так і стельовими. Настінний, найпоширеніший тип установки. У комплект деяких извещателей вже входять кронштейни, які дозволяють орієнтувати датчик в потрібному напрямі. У більшості є можливість здійснення монтажу в кутку приміщення без кронштейна.

Не рекомендується встановлювати інфрачервоні извещатели в безпосередній близькості від вентиляційних отворів, вікон і дверей, у яких створюються повітряні потоки, а також радіаторів центрального опалювання, інших опалювальних приладів і джерел теплових перешкод. Також небажане пряме попадання на вхідне вікно извещателя світлового випромінювання від ламп розжарювання, автомобільних фар, сонця. Для постановки під охорону приміщення з тими, що знаходяться усередині кішкою або собакою існують извещатели із спеціальними лінзами із захистом від домашніх тварин.

Активні інфрачервоні оповіщувачі

Є оптичною системою з ІК-ІЗЛУЧАТЕЛЯ і ІК-ПРІЄМНИКА, яка дозволяє сформувати невидимий оком рубіж охорони протяжністю до 100 метрів. Призначений для охорони зовнішніх рубежів і протяжних периметрів об'єктів, що охороняються. Принцип дії активного І До датчика извещателя снован на формуванні випромінювачем імпульсного І До випромінювання, яке уловлюється приймачем.

В момент перетину рубежу, що охороняється, порушником, І До випромінювання перестає потрапляти на приймач і датчик формує сигнал тривоги.

Бувають як однолучевыми, так і багатопроменевими. При кількості променів більше двох зменшується можливість появи помилкового спрацьовування, оскільки формування сигналу тривоги відбувається тільки при одночасному перетині всіх променів

Радіохвильові об'ємні обовіщувачі

Призначені для виявлення проникнення в зону, що охороняється, і допускають маскування матеріалами, проникними радіохвилі (тканини, деревні плити) .Электромагнитное поле СВЧ діапазону, створюване извещателем, не надає шкідливої дії на організм людини на відстані більше 50 мм. У извещателе реалізований принцип виявлення людини по реєстрації доплеровского зрушення частоти відбитого надвисокочастотного сигналу, що виникає при русі людини в електромагнітному полі, створюваним модулем СВЧ

Призначений для виявлення проникнення в приміщення, що охороняється, і формування тривожного сповіщення шляхом розмикання контактів вихідного реле

Лінійні радіохвильові оповіщувачі

Забезпечують виявлення людини, що перетинає зону виявлення. Ізвещатель складається з передавального і приймального блоку, які розміщуються на протилежних кінцях ділянки, що охороняється. Передавальний блок випромінює електромагнітні

коливання у напрямі приймального блоку. Приймальний блок приймає ці коливання, аналізує амплітудні і тимчасові характеристики прийнятого сигналу і у разі їх відповідності закладеній в алгоритмі обробки моделі "порушника" формує тривожне сповіщення

Лінійні радіохвильові извещатели на відміну від об'ємних, виявляючих рух порушника усередині зони виявлення, формує тривожне сповіщення при перетині зони. Тому для таких извещателей важлива не ширина зони виявлення, а ширина зони відчуження для руху людини і транспортних засобів, за межами якої извещатель не видає тривожного сповіщення.

Об'ємні ультразвукові оповіщувачі

Призначені для виявлення проникнення (спроби проникнення) в об'єм, що охороняється, переміщення предметів в об'ємі, що охороняється. До складу извещателя входять блок обробки сигналу, акустичний випромінювач, акустичний приймач. Випромінюючий елемент извещателя, розміщений в блоці випромінювача є п'єзоелектричний ультразвуковий перетворювач, що працює в режимі ультразвука і перетворює електричну напругу з частотою 40 Гц, що виробляється генератором БОСИЙ в акустичні коливання повітря в об'ємі, що охороняється. Чутливий елемент извещателя, розташований в приймачі є п'єзоелектричний ультразвуковий приймальний перетворювач акустичних коливань в змінний електричний сигнал. З виходу приймача сигнал поступає в схему БОСИЙ, яка залежно від закладеного в неї алгоритм, формує те або інше сповіщення.

Ультразвукові датчики у складі охоронної сигналізації випромінюють і приймають відбитий сигнал ультразвукового поля. Їх відрізняє: мала чутливість; високий рівень помилкових спрацьовувань; залежність налаштувань від перепадів температури, протягу, акустичних шумів, коливань вологості. Тому цей тип датчиків знайшов застосування, в основному, в недорогих системах для захисту малих замкнутих ізольованих об'ємів, наприклад, салону автомобіля.

Магнітоконтактні датчики

Магнітні датчики у складі охоронної сигналізації відносяться до найпростіших і встановлюються на вікна, двері і люки. Випускаються двох видів: для зовнішньої і прихованої установки. Зазвичай розміщуються у верхній частині дверей або вікна. З метою підвищення надійності встановлюється по два датчики, сполучених послідовно. При установці на вікнах кожна фрамуга вікна захищається парою "геркон + магніт". Магнітні датчики сигналізації є парою геркон плюс магніт і спрацьовують при відкритті/закритті дверей або вікна. Геркон — це герметично запаяний в скляну трубку контакт.

Он замикається або розмикається при тому, що піднесло до нього магніта. Зазвичай магніт кріпитися до рухомої частини дверей або вікна, а геркон до нерухомої.

Магнітоконтактниє извещатели відрізняються друг від другу за типом установки, матеріалу з якого вони виготовлені, а також величині робочого зазору, при якому извещатель знаходиться в черговому режимі.

Акустичні охоронні оповіщувачі

Призначені для виявлення руйнування листових стекол різних марок: звичайного, загартованого, армованого, тришарового "триплекс". Чутливим елементом таких извещателей є конденсаторний електретний мікрофон з вбудованим передпідсилювачем на польовому транзисторі. Мікрофон перетворить звукові коливання повітряного середовища в електричні сигнали. Електричний сигнал з мікрофону поступає на смугові підсилювачі і далі на мікроконтролер. Мікроконтролер відповідно до заданого алгоритму роботи проводить контроль акустичних сигналів, контроль працездатності електронної схеми извещателя, контроль напруги живлення і формування відповідних сповіщень. При установці извещателя всі ділянки скла, що охороняється, мають бути в межах його прямої видимості.

Ударно-контактниє оповіщувачі

Забезпечують реєстрацію руйнування скляного полотна різної товщини і стійкі до неруйнуючих дій на скло у вигляді низькочастотних коливань від роботи автотранспорту, гуркотів грому і тому подібне Принцип дії ударно-контактных извещателей заснований на реєстрації розмикань рухомих контактів датчика вібрації, що виникають при руйнуванні скла. Ізвещатель фіксує поява двох подовжніх і поперечних високочастотних коливань скляного полотна, що становлять, при його руйнуванні.

Вібраційні оповіщувачі

Служать для захисту від проникнення шляхом руйнування різних будівельних конструкцій: бетонних стенів і перекриттів, цегляних стенів, дерев'яних (рами і двері) і стельових покриттів, а також сейфів, металевих шаф і банкоматів. Принцип дії вібраційних датчиків заснований на п'єзоелектричному ефекті, який полягає в зміні електричного сигналу при вібрації пьезоэлемента. Електричний сигнал, пропорційний рівню вібрації, посилюється і обробляється схемою извещателя по спеціальному алгоритму, щоб відокремити руйнівну дію від помехового сигналу. Основними характеристиками таких извещателей є чутливість до вібрації.

Ємкісні охоронні оповіщувачі

Принцип дії заснований на реєстрації значення, швидкості і тривалості зміни ємкості чутливого елементу, як який використовується підключені до извеща-телю предмети або дріт, розміщений на конструктиві отвору, що охороняється.

Ізвещатель видає сигнал тривоги при зміні електричній ємкості металевого предмету, що охороняється, по відношенню до землі, викликаними наближенням людини до цього предмету.

Цей тип извещателя можна використовувати і як для контролю периметра будівлі через натягнуті дроти (при торканні або наближенні порушника ємкість схеми збільшиться і извещатель сигналізує "тривога)" так і, наприклад, для охорони сейфів, металевих шаф.

Суміщені і комбіновані опопвіщувачі

Дозволяють одночасно контролювати 2 різних зони. Існує декілька варіантів виконання даних извещателей як і із загальним, так і з двома незалежними виконавчими реле, відповідними кожному з каналів виявлення. При появі людини в зоні виявлення спрацьовують обидва канали виявлення (у будь-якій послідовності), при цьому видається сповіщення про тривогу шляхом розмикання контактів вихідного реле.

Тревожные кнопки і педалі

Частіше зазвичай використовують на об'єктах, що знаходяться під охороною міліції і служать для передачі сигналу тривоги на пульт центрального спостереження. Такі кнопки або педалі встановлюють в непомітних місцях, наприклад під столом в касі. Додатково для захисту від розбійного нападу часто застосовують так звані "ляльки". Це по суті імітація грошової упаковки, усередині якої встановлені капсули сльозоточивої і забарвлюючої дії. Спрацьовування відбувається при натягненні нитки із зусиллям 50-100 грама, забезпечуючи одночасний викид спеціальної композиції дратівливої дії і розпилювання рідкого фарбувального складу, що не змивається з шкірного покриву протягом 2-4 діб.

1.6.2. Прилади приймально-контрольні і критерії їх вибору

Останнім часом на ринку охоронних послуг помітно розширилася номенклатура ППК охоронної, охоронно-пожежної і пожежної сигналізації. Проте різноманіття приладів разныхклассов приводить не тільки до поліпшення їх тактико-технічних характеристик. Деякі виробники всіляко намагаються утвердить свої погляди на технічні засоби охорони (ТСО), не зважаючи на багаторічну практику, що існує в цій області. У такій ситуації, щоб уникнути нерозуміння, необхідно детальніше зупинитися на загальних характеристиках ППК, критеріях їх вибору і применения Необходимо, напевно, почати з визначення самих ППК, розглянути їх основні функцій і дати загальну класифікацію, щоб потім детальніше охарактеризувати деякі види цих приладів.

Взагалі кажучи, ППК є основним вузлом в системах охоронної і пожежної сигналізації. Вони призначені для контролю стану параметрів шлейфів сигналізації (ШС) і

можуть працювати як в автономному режимі (з включенням пристроїв сповіщення), так і/або з передачею службових і тривожних сповіщень на пульт централізованого спостереження (ПЦН). У останньому випадку ППК в системах охоронно-пожежної сигналізації є проміжною ланкою між об'єктовими первинними засобами виявлення проникнення (охоронними извещателями) або пожежними извещателями і системами передачі сповіщень (СПИ).

Основні функції ППК:

•прийом і обробка сигналів від извещателей;

•живлення извещателей (по ШС або по окремій лінії);

•контроль стану ШС;

•передача сигналів на ПЦН;

•управління звуковими і світловими оповісниками;

•забезпечення процедур узяття об'єкту під охорону і зняття з охорони. Існує наступна класифікація ППК:

1.За призначенням: охоронні (охоронно-пожежні), пожежники і прилади управління.

2.По інформативності:

•малій інформативності - до 2 видів сповіщень;

•середній інформативності - від 3 до 5 видів сповіщень;

•великій інформативності - більше 5 видів сповіщень.

3.За способом організації зв'язку з извещателями: дротяні і безпровідні (радіоканальні).

4.За типом ШС, що підключаються: безадресні (радіальні) і адресні.

5.За способом постановки на охорону: з роздільною постановкою кожного ШС, з груповою постановкою (по розділах) і змішаною.

6.По резервуванню живлення: з вбудованим джерелом резервного живлення і без нього.

7.По кліматичного виконання: для опалювальних і неопалювальних приміщень.

Для окремих видів об'єктів існують також спеціальні типи ППК, наприклад для охорони пожаро-и вибухонебезпечних приміщень.

ППК охоронний (охоронно-пожежний) - це технічний засіб охоронної або охоронно-пожежної сигналізації для прийому сповіщення від ШС або інших ППК, перетворення сигналів, видачі сповіщень, що безпосередньо сприймаються людиною, подальшої передачі сповіщень і включення оповісників. Додатково прилад може забезпечувати електроживлення извещателей, формування командного імпульсу для управління інженерним (технологічним)

устаткуванням, процес узяття об'єкту під охорону і зняття з охорони за допомогою засобів контролю і управління доступом.

Пожежник ППК, разом з функціями охоронно-пожежного приладу, повинен обов'язково контролювати справність ШС по всій довжині і автоматично виявляти обрив або коротке замикання в них, забезпечувати світлову і звукову сигналізацію при виниклій несправності, реєструвати і передавати в зовнішні ланцюги сповіщення про пожежу (віддаючи перевагу даним повідомленням по відношенню до інших сигналів, формованим приладом) і захищати органи управління від несанкціонованого доступу сторонніх осіб.

Додаткові функції пожежника ППК можуть бути наступними: посилка в ручний пожежний извещатель зворотного сигналу, підтверджуючого прийом поданого ним сповіщення про пожежу; формування стартового імпульсу запуску пожежних приладів управління засобами автоматичної пожежогасінні; можливість включення в один ШС активних (енергоспоживаючих) і пасивних пожежних извещателей з нормально замкнутими контактами і ін.

ППК пожежник управління призначений для автоматичного або дистанційного пуску засобів пожежогасінні, світловій індикації про пуск засобів пожежогасінні з вказівкою напрямів, по яких подається огнетушащее речовина і світловій індикації про стан джерел живлення приладу. Додатково прилад пожежник управління може контролювати лінії зв'язку світлової і звукової сигналізації, зокрема оповісників, звукову сигналізацію про пуск засобів пожежогасінні і про несправність приладу.

Основними параметрами ППК є:

•інформаційна ємкість - кількість контрольованих ШС;

•інформативність - кількість сповіщень, що відображаються приладом за допомогою світлових і звукових оповісників і передаваних їм в зовнішні ланцюги;

•інерційність шлейфу - показник стійкості приладу до перешкод, викликаних короткочасними порушеннями шлейфу. Задається двома значеннями - мінімальною і максимальною тривалістю порушення, при яких прилад гарантовано не переходить або переходить в режим тривоги. Збільшення часу знижує вірогідність помилкових тривог, що виникають при короткочасних наведеннях на шлейфи, наприклад при грозових розрядах, при роботі близько розташованих могутніх радіопередавальних пристроїв в імпульсному режимі або при розмиканні унаслідок вібрації контактів реле извещателей. Проте потрібно пам'ятати, що, при дуже великому часі інерційності (більше 800 мс), виникає небезпека пропуску порушника;

•опір шлейфу - максимально допустимий опір шлейфу без урахування опору крайового резистора. Складається з опору проводів і перехідних опорів в місцях підключення і стиків; при цьому загальний опір шлейфу може досягати сотень Ом;

•опір витоку шлейфу - граничний допустимий опір витоку між проводами шлейфу або між проводами і "землею";

•напруга на шлейфі - напруга в черговому режимі приладу. Його значення визначається необхідністю забезпечити надійність роботи контактних з'єднань шлейфу і живлення активних (енергоспоживаючих) извещателей. Обмеження верхнього значення напруги обумовлене електробезпекою. У сучасних вітчизняних приладах значення напруги вибирається в межах 10-24 Ст. В імпортних приладах, що не працюють з активними (енергоспоживаючими) извещателями, воно значно нижче (0,5-9 В);

•ток у шлейфі - струм в черговому режимі. Повинен забезпечувати живлення активних (енергоспоживаючих) извещателей. Обмеження його значення обумовлене завданнями енергозбереження. У вітчизняних приладах вибирають струм в шлейфі в діапазоні 1-10 мА;

•струм в шлейфі в режимі короткого замикання - значення струму має бути достатнім для забезпечення індикації извещателей, що спрацювали, в той же час воно обмежується із-за необхідності енергозбереження і захисту вхідних ланцюгів приладу. Зазвичай вибирають значення в діапазоні 20-25 мА.

Зважаючи на все вищеперелічене, необхідно відзначити, що основними параметрами ППК є все ж таки інформаційна ємкість і інформативність.

Прилади малої інформаційної ємкості

Вказані ППК застосовуються, в основному, для організації охорони одного приміщення або невеликого об'єкту (декілька приміщень). Вони достатньо прості в технічному обслуговуванні, їх експлуатація не вимагає особливих знань і навиків від персоналу об'єкту, що охороняється.

При виборі ППК малої інформаційної ємкості, слід звертати увагу на наступні характеристики.

1.Тактика постановки на охорону: "з відкритими дверима", "із закритими дверима" або "з програмованою затримкою". Тактика "з відкритими дверима" передбачає процес узяття об'єкту під охорону при відкритих вхідних дверях. Коли двері закриваються, відбувається переклад ППК в режим узяття об'єкту під охорону. Якщо вибирається тактика "із закритими дверима", то узяття об'єкту під охорону відбувається при закритих вхідних дверях. При використанні тактики "з програмованою затримкою", об'єкт береться під охорону через деякий час після перекладу ППК в режим охорони.

2.Універсальність ШС по своєму призначенню (охоронний, пожежник, тривожний) і можливість їх зміни. Для тривожних і пожежних ШС, як правило, використовується цілодобовий режим роботи ППК.

3.Кількість виходів на ПЦН. Ця характеристика важлива при необхідності організації на об'єкті декількох рубежів охорони або при підключенні до ППК разных за призначенням ШС.

4.Тип крайового елементу ШС (резистор, конденсатор, діод). Указує на спосіб контролю ШС, на можливість використання різних типів извещателей в ШС і змінах їх кількості.

5.Наявність виносної світлової і/або звукової сигналізації. Дозволяє вивести сигнали тривоги виносні оповісники і контролювати з їх допомогою стан об'єкту.

6.Споживаний струм в черговому і тривожному режимах. Чим менше дана величина, тим ефективніше робота ППК.

7.Наявність вбудованого джерела резервного живлення і час роботи ППК з ним при відключенні основного електроживлення.

Дана характеристика дуже істотна. Це пов'язано з тим, що, якщо як резервне джерело живлення використовується акумуляторна батарея, повинна забезпечуватися робота ППК протягом часу, вибраного з ряду 4, 8, 12, 24, 36, 48, 72 години згодне ГОСТ 26342. Крім того, застосування ППК з вбудованим акумулятором унеможливлює виникнення помилкових спрацьовувань, викликаних якими-небудь проблемами в мережі напруги змінного струму

Прилади середньої і великої інформаційної ємкості

Дані ППК використовуються для охорони великих об'єктів, для організації охорони багаторубежу, а також як пульти для автономних систем охорони. Ці прилади знаходять широке застосування, оскільки дозволяють одночасно контролювати охоронні ШС "з правом відключення" і шлейфи пожежною і /или тривожної сигналізації в режимі "без права відключення", тобто що працюють цілодобово. При цьому, залежно від вимог, що пред'являються, значення шлейфів і алгоритм роботи приладу можуть змінюватися за допомогою набору перемичок або програмним шляхом. Сучасні умови охорони об'єктів вимагають використання декількох шлейфів навіть для охорони одного житлового приміщення.

Как правило, шлейфів повинно бути не менше чотири: перший шлейф контролює вхідні двері (працює по тактиці "із затримкою виходу"), другий - охоронні извещатели по периметру приміщення, третій - порушення об'єму приміщення (може відключатися для забезпечення "самоохорони", тобто охорона людей, що знаходяться усередині, від

проникнення через периметр), четвертий шлейф використовується як пожежник або тривожного.

В даний час на ринку у великій кількості представлені прилади, які прості в експлуатації, мають можливість управління по кожному шлейфу окремо, тобто майже у всьому аналогічні ППК малої інформаційної ємкості. Проте основна вимога, що пред'являється до ППК в сучасний період, - це наявність у них можливостей нарощування інформаційної ємкості, локального і централізованого управління процесами узяття/зняття ШС під охорону, ідентифікації користувачів і автоматичної реєстрації подій.При виборі ППК середньої і великої ємкості слід звертати увагу на наступні основні характеристики.

1.Можливість управління по кожному шлейфу окремо або по розділах. Управління по кожному шлейфу необхідне на об'єктах, де є велика кількість матеріально відповідальних осіб, за якими закріплені певні приміщення.

2.Тип ШС і извещателей для ППК. Вони підрозділяються на безадресних (радіальні) і адресних. У адресних системах одній адресі відповідає один адресний пристрій.

3.Тип сполучних ліній для зв'язку блоків ППК на об'єкті між собою. Це важливо для монтажу і експлуатації. Наприклад, в деяких ППК використовується інтерфейс RS-485, що вимагає спеціального екранованого кабелю, а в деяких - просто двопровідна витаючи пара. Як показує досвід різних монтажних організацій, роботу по розгортанню ліній з інтерфейсом RS-485 можуть виконувати тільки добре підготовлені фахівці.

4.Можливість нарощування інформаційної ємкості без істотної зміни апаратних засобів. Зазвичай для цих цілей застосовуються розширювачі, які не тільки здійснюють взаємодію з іншими елементами ППК, але і ведуть електронний "протокол" подій.

5.Можливість локального і централізованого управління процесами узяття ШС під охорону або зняття з охорони. Підвищує оперативність управління процесами постановки ШС на охорону за рахунок перерозподілу цих функцій між централізованим і локальним способами. При цьому управління процесами може вестися як з центрального пульта управління (комп'ютера) ППК, так і з локальних (дистанційних) пультів.

6.Можливість використання центрального пульта управління ППК замість комп'ютера. Ця характеристика має дуже велике значення при виконанні вимог керівних і нормативних документів по можливому резервуванню живлення, у тому числі і комп'ютера. На практиці цю проблему часом вирішити складно.

7.Універсальність входів ШС. Дозволяє легко привласнювати будь-яке призначення ШС (охоронний, тривожний або пожежний).

8.Кількість програмованих виходів. Чим воно більше, тим більшою кількістю різних пристроїв і пристосувань можна управляти. З'являється можливість використання виходів не

тільки для передачі тривожних сповіщень на ПЦН, але і для управління різними слабкострумовими пристроями, наприклад пристроями систем протипожежної автоматики.

9.Цінова характеристика. Її необхідно враховувати при виборі ППК. Часто багато фірм-постачальників указують тільки прямі витрати, і визначити, наскільки ефективний один тип ППК по відношенню до іншого, достатньо важко. Для того, щоб розрахувати вартість всього устаткування, слід узяти за основу вартість одного ШС: чим вона менша, тим більше економічним буде застосування ППК на об'єкті, що охороняється.

Крім того, як і при використанні ППК малої інформаційної ємкості, необхідно враховувати наступні аспекти: споживаний струм в черговому і тривожному режимах, наявність і час роботи резервного джерела живлення, час реакції на порушення ШС, перешкодостійкість і тому подібне

1.7 Пожежна сигналізація

Перші пожежні извещатели, а з'явилися вони без малого двісті років тому, були здатні реагувати тільки на високу температуру. Це були натягнуті під стелею шнури, сполучені з дзвоном пожежної тривоги. При пожежі шнур перегорав і дзвонив дзвін. З винаходом електрики з'явилися теплові контактні датчики, які на випадок пожежі включали електричні дзвінки. Використовувався ефект розширення при нагріванні твердих, рідких і газоподібних речовин, зміна положення біметалічної пластини, контакти, спаяні легкоплавким сплавом і так далі Такі извещатели спрацьовують, коли вогнище відкритого вогню складає вже чималу площу, - в цьому випадку найчастіше вже неможливо справитися з вогнем підручними засобами, та і евакуація людей проблематична із-за сильного задимлення.

В даний час извещатели подібного типу застосовуються мало, в основному вони залишаються в житлових будинках, де до цих пір встановлюються в передпокоях квартир. Цим і пояснюється величезне число пожеж в житловому секторі.

Вимоги до складу, монтажу, пуско-налагоджувальним роботам систем пожежної сигналізації регламентує ДБН В.2.5-13-98 Інженерне устаткування будівель і споруд. Пожежна автоматика будівель.

В більшості випадків першою ознакою спалаху є дим, краще всього про біду, що насувається, здатні попередити саме димові извещатели.

Різні типи димових пожежних извещателей мають і різні функціональні можливості. Прості системи передають сигнал на пожежний прилад, який включає сирену. Але

визначити, в якому з приміщень відбувся спалах буває достатньо складно, до того ж частина приміщень може бути закрита. Адже при ліквідації пожежі дорога кожна секунда.

Значно ефективніше адресні системи, застосування яких дозволяє за адресою пожежного извещателя, що спрацював, визначити місце спалаху.

Ще досконаліші системи - адресно-аналогові. У них пожежний извещатель не фіксує перевищення порогу контрольованого параметра, а сам є вимірником. Він може, наприклад, може вимірювати рівень задимлення і рівень температури, і зміна цих величин в реальному масштабі часу аналізується в приймально-контрольному адресно-аналоговому приладі. Це дозволяє відстежувати динаміку розвитку пожежі на найраніших стадіях, при цьому, вірогідність помилкових тривог надзвичайно мала.

Взагалі в системах пожежної сигналізації працюють різні типи пожежних извещателей: порогові, адресні, адресно-аналогові, димові оптико-електронні, ионизацион-

ные, лінійні, теплові, комбіновані, з радіоканалом, аспіраційні і так далі Ультрачувствітельниє лазерні точкові пожежні извещатели використовуються для захисту дорогого устаткування і музейних цінностей. У звичайному димовому извещателе використовується оптична пара зі світлодіода і фотодіода, розташованих під кутом. Принцип дії заснований на розсіюванні в димовій камері світла від світлодіода при появі диму. З чим це можна порівняти? Всі, напевно, бачили, як промінь прожектора проходить через хмару: поки промінь світла проходить через прозоре середовище - ніяких віддзеркалень не немає і він не видно, як тільки промінь потрапляє в хмару - те на частинках вологи відбувається віддзеркалення і видно структура світивши. Той же самий принцип використовується в оптико-електронному извещателе, але сконцентрувати промінь і реалізувати вищу яскравість від світлодіода достатньо складно, адже одночасно росте і сигнал, відбитий від стінок димової камери. Крім того, є обмеження і в струмі споживання, система повинна пропрацювати принаймні 24 години в черговому режимі і 3 години в режимі "пожежа" при живленні від резервного джерела живлення, тобто від акумулятора.

В лазерному димовому извещателе замість світлодіода використовується мініатюрний лазер, яскравість світивши якого приблизно в 100 разів вище, ніж світлодіода, а фокусування забезпечує практично повну відсутність віддзеркалень від стінок димової камери. За рахунок цього чутливість при використанні лазера збільшується в тих же 100 разів.

Такі пожежні извещатели, звичайно, набагато дорожче звичайних, але в приміщеннях, де потрібний дуже високий ступінь захисту, вони застосовуються достатньо широко.

Розвиток мікроелектроніки, безумовно, позначився на рівні розробок сучасних пожежних извещателей. Судите самі: прості извещатели фіксують перевищення рівня сигналу над порогом декількох імпульсів підряд - це, по суті, проста обробка сигналу, яка не

дає захисту від помилкових спрацьовувань. Крім того, є нюанси в роботі димових извещателей: пил на стінках димової камери сприяє збільшенню фонового сигналу на виході фотодіода, відповідно, збільшується і вірогідність помилкових спрацьовувань. Якщо датчик порогової системи не очищати від пилу, система взагалі може стати непрацездатною по даному шлейфу.

Використання мікропроцесорів дозволило стабілізувати чутливість, уникнути помилкових спрацьовувань, дало можливість навіть в порогових системах міняти чутливість залежно від об'єкту, в якому знаходиться пожежний извещатель.

Крім того, сучасна мікропроцесорна техніка забезпечує малі струми споживання. Датчик з максимальним інтелектом на сьогоднішній день може споживати близько 50 мікроампер, хоча перші димові извещатели споживали близько 300 мікроампер, навіть не маючи якого б то не було складної логічної обробки сигналу.

У мікросхемі має бути незалежна пам'ять, в якій зберігається величина компенсації на випадок відключення живлення. Якщо дозволяє об'єм в неї також можна записати інформацію про тип датчика, рівень чутливості, дату випуску, дату технічного обслуговування і так далі Звичайно, необхідно організувати канал для прочитування і перезапису інформації, це можна робити, наприклад через індикаторний світлодіод извещателя. Є багато інших додаткових функцій, наприклад, можливість зміни режимів індикації чергового режиму, можна також, прочитуючи поточні значення контрольованих параметрів, контролювати наскільки рівні диму і тепла близькі до порогу спрацьовування при дії, наприклад, сигаретного диму, при включенні електричних плит, і вже залежно від результатів скоректувати чутливість в ту або іншу сторону, не виходячи при цьому за межі норм пожежної безпеки.

Сучасні теплові пожежні извещатели окрім максимального порогу, досягши порогової температури видається сигнал "пожежа", зазвичай фіксують пожароопасную ситуацію і швидкості наростання температури. Наприклад, якщо за хвилину температура піднялася на 8 градусів, формується сигнал тривоги.

Комбіновані датчики використовують димовий і тепловий канали. При аналізі мікропроцесор враховує дані по обох каналах. Тобто якщо відбувається збільшення температури, не достатнє для спрацьовування теплового каналу, але є невелике задимлення, яке окремо теж не досягає порогу, недостатньо для формування, то сукупність інформації дозволяє сформувати сигнал "пожежа".

Чим вище інтелектуальний рівень як самого датчика, так і системи в цілому, тим більше можливостей оперативного визначення і усунення несправностей.

Способи подачі сигналу про несправності в порогових неадресних датчиках, наприклад, мигання світлодіода, не дуже ефективні. До того ж підвищується споживання електроенергії по шлейфу. А мигання декількох світлодіодів взагалі може викликати помилкове спрацьовування системи. Досконаліші в цьому відношенні - адресні опитні системи, де кожні 3 - 5 секунд здійснюється опит кожного пожежного извещателя з контрольного приладу, при цьому фіксується його стан (черговий режим/пожежа), наявність, зв'язок, рівень запыления, забруднення. Якщо стан відрізняється від чергового режиму адреса извещателя з відповідним повідомленням виводиться на дисплей приладу.

В адресно-аналогових системах забезпечений максимально високий рівень захисту, повний контроль системи, підключення і функціонування пожежної автоматики будь-якого рівня складності. Причому, в одному шлейфі ставляться і адресно-аналогові извещатели, і адресні ручні извещатели, і адресні оповісники і адресні модулі управління і контролю пожежної автоматики і інженерними системами. У цих системах зазвичай використовуються петлеві шлейфи і ізолятори короткого замикання, за рахунок чого вони набагато стійкіші до відмов. Наприклад, при обриві шлейфу петля перетвориться в два радіальні шлейфи, жоден пристрій не відключається, а на дисплеї у вигляді текстової інформації повідомляється вид несправності і місце, де вона відбулася.

1.7.1 Пожежні датчики

Навіть у ідеальному товаристві майбутнього, описаному великими утопістами, в якому немає ніяких кримінальних погроз, залишиться можливість виникнення неконтрольованого спалаху або просто кажучи пожежі. Єдиний спосіб звести можливі втрати до мінімуму - побудувати ефективну систему виявлення і ліквідації спалаху. На жаль, в даний час далеко не кожен об'єкт оснащений системою ефективної автоматичної пожежогасінні, а якщо будівля стара, її і неможливо побудувати без капітальної його переробки. Тому основна тяжкість по забезпеченню своєчасної ліквідації пожежі лягає на систему його виявлення або, кажучи іншими словами, систему пожежної сигналізації.

А основним елементом цієї системи є пристрій, що виявляє спалах по яких-небудь його ознакам, - пожежний извещатель, від якості роботи якого більшою мірою залежить і ефективність роботи всієї системи в цілому.

Пожежні извещатели класифікуються по параметру активації і фізичному принципу виявлення. Для виявлення спалаху використовуються три параметри активації:

•Концентрація в повітрі частинок диму;

•Температура навколишнього середовища;

•Випромінювання відкритого полум'я.

Під фізичним принципом виявлення розуміється конкретний фізичний процес, використовуваний для виявлення того або іншого параметра активації. Теплові извещатели

Теплові извещатели реагують на зміну температури навколишнього середовища. Вони встановлюються в наступних випадках:

Коли в контрольованому обьеме структура матеріалів, що використовуються, така, що при горінні дає більше жару, чим диму (наприклад, якщо стіни фанеровані дерев'яними панелями).

Контактний максимальний тепловий оповіщувач

Найчастіше використовуються максимальні теплові извещатели - пристрої, що видають сигнал тривоги при перевищенні заздалегідь заданої максимально допустимої температури. Найбільш прості пристрої складаються із спаяного контакту двох провідників. При нагріві електричний ланцюг розривається, за рахунок чого і формується сигнал тривоги. До извещателям цього типу відносяться, в основному, прилади вітчизняного виробництва, такі як ІП-105 і аналогічні їм.

Зазвичай встановлювана в них максимальна температура складає 75°С.

Лінійні оповіщувачі

Провідники упаковані в загальний кожух так, що щільно стикаються своїми оболонками. Дроти з'єднуються в кінці лінії попарно між собою, утворюючи дві петлі, дотичні оболонками.

При збільшенні температури оболонки зменшують свій опір, змінюючи загальний опір між петлями, який і вимірюється спеціальним блоком обробки результатів. По величині цього опору і ухвалюється рішення про наявність спалаху.

Чем більше довжина кабелю, а вона може досягати півтора кілометрів, тим вище чутливість приладу.

Димові оповіщувачі

Димові извещатели реагують на появу в повітрі заданої концентрації частинок диму. Оскільки поняття "дим" є менш елементарним, чим базове поняття "температура", варто розглянути його детальніше. Дим є сукупність аерозольних частинок різної природи, що виділяються при процесі горіння різних матеріалів. Він однозначно описується чотирма параметрами: хімічним складом частинок, їх розміром, концентрацією і швидкістю руху. Склад, розмір і концентрація залежать від хімічної природи речовини, що горить, а концентрація і швидкість руху залежать від розподілу повітряних потоків в контрольованій зоні. Власне димовий извещатель визначає лише один параметр з чотирьох: концентрацію частинок диму до певної максимальної швидкості їх руху (зазвичай не вище 10 м/с). Проте, оскільки склад частинок макет бути дуже різним, існують два види димових извещателей з

різними фізичними принципами виявлення: оптичні і іонізаційні. Хоча для багатьох видів складів аерозоля обидва типи виявлення однаково ефективні, для деяких різновидів ефективнішим є один з них.

Оптічекий димовий оповіщувач

Вимірювальна камера цього пристрою містить ІК-СВЕТОДІОД і фотоприймач, орієнтовані щодо один одного так, щоб випромінювання світлодіода в нормальних умовах не попадало на фотоприймач. Для унеможливлення випадкового попадання випромінювання димовий извещатель (наприклад, відбитого від стінок) на фотоприймач, воно прямує в спеціально сконструйовану оптичну камеру. При появі в повітрі частинок диму вони потрапляють в оптичну камеру і на них відбувається хаотичне розсіяння випромінювання діода, унаслідок чого частина його починає потрапляти на фотоприймач, забезпечуючи отримання електричного сигналу. Рівень цього сигналу тим вище, чим більше концентрація розсіюючих частинок диму в повітрі. При перевищенні сигналом певного порогу ухвалюється рішення про наявність спалаху.

Комбіновані оповіщувачі

На території, що захищається, можуть бути присутніми матеріали з різними характеристиками горіння, що припускає використання різних фізичних принципів виявлення спалаху. Оскільки ніколи не відомо, що зажевріє першим, в цьому випадку необхідно було б поставити два різних извещателя. Проте для вирішення цього завдання випускаються спеціальні комбіновані извещатели, де в одному корпусі зібрано обидва типи извещателей.

Подібна модель димового датчика володіє двома перевагами: по-перше, може виявити вельми широкий спектр різних горючих матеріалів, по-друге, цей датчик макет розрізняти справжні продукти горіння і помехообразующие частинки, такі, як водяні випаровування. Це стало можливим за рахунок використання двохвугільної технології розсіяння світла. Зазвичай димові датчики контролюють світло, розсіяне під єдиним кутом, із-за чого вони можуть надійно ідентифікувати тільки деякі типи диму. Датчики последнегопоколения працюють по двох кутах віддзеркалення світла, що дозволяє вимірювати і аналізувати співвідношення характеристик прямого і зворотного розсіяння світла, визначаючи типи диму і знижуючи кількість помилкових тривог. Річ у тому, що інтенсивність сигналів, зміряних по прямому і зворотному розсіяному світлу, змінюється залежно від типу матеріалу, що згорає. Відношення прямого розсіяного світла до зворотного для темного диму (наприклад, при відкритому згоранні дизельного палива) більше, ніж для світлих типів диму (наприклад, при тліючому вогні), і воно навіть ще вище для сухих речовин, подібних до борошняного пилу.

Датчики, які реєструють світло під єдиним кутом, не можуть обчислювати це відношення і, таким чином, нездібні класифікувати типи диму. Навпаки, в даних датчиках помехообразующие частинки можуть бути точно диференційовані від справжніх продуктів горіння, зводячи число помилкових тривог до мінімуму.

Некоторые виробники випускають і так звані тривимірні комбіновані извещатели, в яких в одному корпусі об'єднані димовий оптичний, димовий іонізаційний і тепловий принцип виявлення. Проте випадки використання подібних пристроїв вельми рідкісні.

Хімічний датчик (датчик чадного газу)

Газовий датчик в основному виявляє чадний газ (З), що утворюється при горінні, а також водень (Н) і моноксид азоту (N0). Принцип вимірювання заснований на окисленні електроду під впливом чадного газу і вимірюванні отримуваного при цьому струму. Значення сигналу датчика пропорційне концентрації газу. Газовий датчик надає додаткову інформацію для ефективного придушення помилкових значень.

Проводиться постійний моніторинг стану датчика чадного газу шляхом вимірювання внутрішньої ємкості. Якщо ємкість знаходиться поза дозволеним діапазоном, на пожежній панелі відображається повідомлення про помилку. В цьому випадку, извещатель продовжує працювати тільки як димовий извещатель, що працює за принципом розсіяного світла.

Датчик забруднення

Рівень забруднення на поверхні датчика постійно вимірюється датчиком забруднення; результат оцінюється і відображається на пожежній панелі в трьох стадіях. Забруднення поверхні датчика приводить до активного коректування порогового значення (компенсація забруднення) і до виведення сигналу про несправність у разі сильного забруднення.

Ізвещателі полум'я

Іноді необхідно зареєструвати наявність пожежі при першій появі полум'я (до горіння навколишніх матеріалів). В цьому випадку необхідно використовувати извещатели полум'я.

Відкритий факел полум'я містить характерне випромінювання як в ультрафіолетовій, так і в інфрачервоній частинах спектру. Відповідно, існує два типи цих пристроїв: ультрафіолетові і інфрачервоні.

Ультрафіолетовий извещатель полум'я за допомогою високовольтного газорозрядного індикатора постійно контролює потужність випромінювання в спектральному діапазоні 220-280 мкм. При появі спалаху різко підвищується інтенсивність розрядів між електродами індикатора, що і фіксується при перевищенні порогу випромінювачем. Один такий извещатель може контролювати до 200 кв. м поверхні при висоті установки до 20 м. Інерційність його спрацьовування не перевищує 5 секунд.

Інфрачервоний извещатель полум'я за допомогою ІК-ЧУВСТВІТЕЛЬНОГО елементу і оптичної фокусуючої системи реєструє характерні сплески Ік-ізлученія при появі відкритого полум'я. Цей прилад дозволяє визначати протягом 3 секунд наявність полум'я розміром від 10 см на відстані до 20 м при вугіллі огляду 90о.

1.7.2 Автоматична пожежна сигналізація

Автоматичні системи пожежної сигналізації призначені для швидкого і надійного виявлення пожежі, що зароджується, за допомогою розпізнавання явищ, супроводжуючих пожежу, таких як виділення тепла, диму, невидимих продуктів згорання, інфрачервоного випромінювання і тому подібне У разі виявлення пожежі центральна станція повинна виконувати наказані дії з управління системами автоматики будівлі (відключення вентиляційної системи, включення дымоудаления, системи сповіщення, світлових і звукових оповісників, запуск системи пожежогасінні, останов ліфтів, розблокування дверей і тому подібне). Це дає можливість людям, що знаходяться в будівлі, а також пожежній частині або локальному посту пожежної охорони об'єкту зробити дії, необхідні для ліквідації пожежі на стадії його зародження, і мінімізувати збитку, що завдається.

Призначення системи пожежної сигналізації визначає її загальну структуру, а саме, наявність три складових системи, що виконують різні функції:

•обнаружение пожежі здійснюється автоматичними пожежними извещателями з різними принципами виявлення і різними методами обробки і обміну інформацією;

•обробка інформації, що поступає з извещателей, і видача результатів операторові виконуються центральною станцією і пультом управління;

•виконання, наказаних дій для сповіщення персоналу і пожежної частини для усунення вогнища пожежі, виконується центральною станцією а також швидке і точне реагування підрозділів пожежної частини і локальних постів пожежної охорони.

Всі три ланки тісно взаємозв'язані між собою, і ефективність роботи системи пожежної сигналізації в цілому залежить від надійності і стабільності роботи кожної її складової. Проте, основоположну роль при створенні професійних систем пожежної безпеки об'єктів грають пожежні извещатели. Саме вони повинні забезпечити швидке і надійне виявлення вогнища пожежі.

Пожежна сигналізація - обов'язковий компонент системи безпеки будівлі для своєчасного попередження, захисту від пожежі і складається з наступних складових частин:

•Пожежні извещатели адресні і неадресні.

•Прилад приймально-контрольний.

•Оповісники - світлові (проблискові лампи) і звукові (сирени), табло і так далі

•Виконавчі пристрої - системи пожежогасінні, пристрої автоматики і так далі Безперебійне живлення.

1.8 Системи відеоспостереження

Найважливішою і невід'ємнішою складовою будь-якої системи безпеки є система охоронного відеоспостереження. Засоби охоронного відеоспостереження оточують нас в повсякденному житті усюди: пильна електронна варта стежить за нами в залах супермаркетів, при відвідинах банків, із стенів житлових під'їздів, домофонных панелей, в метро і просто на вулиці. Вид камери, встановленої в найнесподіванішому місці, вже давно не шокує тих, що оточують, тим більше що застережливі таблички присутні в будь-якій організації, що поважає себе (і закон).

За останні роки відеоспостереження стало невід'ємною частиною комплексної системи безпеки об'єкту, оскільки сучасні системи відеоспостереження дозволяють не тільки спостерігати і записувати відео, але і програмувати реакцію всієї системи безпеки при виникненні тривожних подій або ситуацій.

Охоронні системи відеоспостереження призначені для візуального спостереження за об'єктом, що охороняється, за допомогою відеокамер. Системи відеоспостереження дозволяють стежити одночасно за одним або декількома об'єктами. Камери відеоспостереження можна встановити як усередині приміщення, так і зовні. Завдання охоронної системи відеоспостереження полягає в наочному уявленні відеоінформації про оперативну обстановку на контрольованому об'єкті.

Найпростіша система відеоспостереження включає одну або декілька відеокамер і монітор або телевізор. Камери відеоспостереження можуть встановлюватися на поворотныхустройствах зовні або усередині приміщення і дозволяють здійснювати цілодобове стеження за територією, що охороняється. Спільно з системою відеоспостереження можна використовувати датчики руху (детектори), системи освітлення і інші додаткові пристрої.

Охоронні системи відеоспостереження дозволяють створити гнучку і нарощувану систему безпеки, в яку можуть входити не тільки компоненти систем відеоспостереження, але і охоронно-пожежна сигналізація і системи контролю доступу.

Системи прихованого відеоспостереження використовуються для підвищення ефективності охорони і встановлюються там, де необхідно приховати факт спостереження.

Завдання систем прихованого відеоспостереження - не вивчати відвідувачів, а контролювати ситуацію на території, що охороняється.

Ринок сучасних систем відеоспостереження і охоронного телебачення переживає сьогодні бурхливе зростання, пов'язане з підвищенням інтересу до безпеки бізнесу. В кожному випадку система повинна проектуватися під конкретне завдання із залученням фахівців-інтеграторів. Причому при зіставній ефективності вартість схожих проектів по організації відеоспостереження може відрізнятися у декілька разів: за рахунок різниці в ціні на різне устаткування.

1.9 Системи контролю і управління доступом (СКУД)

1.9.1 Загальні відомості про системи контролю доступу

Будь-яка система контролю і управління доступом (найбільш поширено - система контролю доступу, СКУД або СКД) призначена для того, щоб автоматично пропускати тих, кому це належить, і не пропускати тих, кому це заборонено. Одним з позитивних і найбільш важливих якостей системи контролю доступу (СКД) є її незалежність від персоналу охорони, - сумлінності до виконання обов'язків, рівня професіоналізму, уважності, втомі і так далі

Система контролю доступу (СКД) - неупереджена і позбавлена вказаних вище недоліків. Вона дозволяє у будь-який час забезпечити контроль над ситуацією, порядок, безпека персоналу і відвідувачів, збереження матеріальних цінностей і інформації.

За систему контролю і управління доступом (СКУД) прийнято вважати сукупність програмно-апаратних засобів і організаційно-методичних заходів, за допомогою яких вирішується завдання організації автоматизованого пропускного режиму на підприємстві. Іншою основоположною функцією системи контролю доступу (СКД) є можливість забезпечення документального контролю за переміщенням персоналу в межах контрольованих зон підприємства.

Система контролю доступу (СКД) - це не тільки технічні засоби і програмне забезпечення. Насамперед, це продумана система управління людськими і транспортними потоками на підприємстві.

Чим вигідна підприємству установка системи контролю доступу

Традиційно прийнято вважати, що система контролю доступу - це інструмент забезпечення безпеки.

Дійсно, сьогодні це один з найефективніших способів запобігти проникненню небажаних осіб на територію підприємства. Але це тільки частина функцій системи контролю доступу, і, загалом, не найголовніша. Що ж ще дає установка такої системи?

Коротко перерахуємо тільки найосновніші можливості:

•підвищення трудової і технологічної дисципліни;

•раціональне витрачання фонду заробітної плати (тільки за реально відпрацьований час);

•скорочення трудовитрат на ведення табельного обліку, кадрового обліку і видачу пропусків;

•скорочення кількості розкрадань.

Як показує практика експлуатації, середній термін окупності системи контролю доступу складає від 2 до 4 місяців.

Окрім прямого економічного ефекту, система контролю доступу забезпечує відповідність підприємства сучасним корпоративним стандартам, збільшуючи інвестиційну привабливість підприємства і його конкурентоспроможність в умовах ринкової економіки.

У реальному житті складно добитися, щоб співробітники постійно замикали двері, покидаючи приміщення навіть на короткий час.

Надійно захистити робочі приміщення від небажаних візитерів дозволяє установка системи контролю доступу. Система легко вирішує цю проблему: покидаючи приміщення, співробітник закриває двері, а, повертаючись, простим піднесло карти відкриває замок. Для компаній з численним персоналом досить ефективним рішенням може стати установка турнікета при вході в офіс і організація електронної прохідної. У офісних приміщеннях, як правило, використовуються турникеты-триподы, як найбільш популярний тип турнікетів, обумовлений їх невисокою вартістю, компактністю і елегантним зовнішнім виглядом. Для формування зон проходу можливе використання спеціальних огорож, виконаних в єдиному стилі з турнікетами.

1.9.2 Принцип функціонування системи контролю доступу (СКД)

Кожен співробітник, клієнт, відвідувач фірми отримує ідентифікатор (електронний ключ) - пластикову картку або брелок з індивідуальним кодом, що міститься в ній. "Електронні ключі" видаються в результаті реєстрації перерахованих осіб за допомогою засобів системи контролю доступу (СКД). Паспортні дані, фото (відеозображення) і інші відомості про власника "електронного ключа" заносяться в персональну "електронну

картку". Персональна "електронна картка" власника і код його "електронного ключа" зв'язуються один з одним і заносяться в спеціально організовані комп'ютерні бази даних.

Біля входу в будівлю або в підмет контролю приміщення встановлюються считыватели, що прочитують з електронних карток їх код і інформацію про права доступу власника карти і передавальні цю інформацію в контроллер системи контролю доступу (СКД).

У системі контролю доступу (СКД) кожному коду поставлена у відповідність інформація про право картки власників. На основі зіставлення цієї інформації і ситуації, при якій була пред'явлена картка, система контролю і управління доступом (СКУД) ухвалює рішення: контроллер дає команду на відкриття або блокує пристрої, що перегороджують (старанні), - двері (замки), турнікети, шлагбауми і ін., переводить приміщення в режим охорони, включає сигнал тривоги і так далі

Всі факти пред'явлення карток і пов'язані з ними дії (проходи, тривоги і так далі) фіксуються в контроллері і передаються для довгострокової реєстрації в комп'ютер. Інформація про події в системі контролю доступу (СКД), викликаних пред'явленням карток, може бути використана надалі для отримання звітів по обліку робочого часу, порушенням трудової дисципліни і ін.

На підприємствах можна виділити чотири характерні точки контролю доступу:

•прохідні

•офісні приміщення

•приміщення особливої важливості

•въезды/выезды автотранспорту.

Як працює система контролю доступу

Прохідна, входи в цехи, адміністративні будівлі і приміщення оснащуються пристроями (замками, турнікетами, шлагбаумами), що перегороджують, і считывателями карт доступу або біометричними считывателями. Всі ці пристрої підключаються до контроллерів системи -ее інтелектуальної частини, які об'єднуються в мережу і підключаються до комп'ютера, з його допомогою здійснюється управління і контроль над їх станом. Для ідентифікації людей в системі служать безконтактні пластикові карти з індивідуальним кодом або біометрики індивідуальні для кожної людини. Кожній карті, відбитку пальця або веселковій оболонці ока поставлена у відповідність інформація про власника і рівень доступу. Співробітники проходять на територію, в цехи і інші приміщення, використовуючи ці карти (біометрики) як пропуски або ключі. При тому, що піднесло карти до считывателю, встановленому в точці проходу, система зіставляє інформацію, що зберігається в контроллері з кодом на карті, і визначає, чи дозволений доступ власникові

карти. Якщо доступ дозволений, система автоматично розблоковує турнікет або замок для здійснення проходу у разі використання.

Контроль доступу для малого підприємства або офісу

Часто виникає потреба обмежити доступ співробітників і відвідувачів у внутрішні приміщення: кабінети керівництва, бухгалтерію, склад. Це особливо актуально у тому випадку, коли необхідно відокремити приміщення з вільним доступом відвідувачів від службових приміщень.

Дозволяючи тримати двері постійно закритими, навіть в робочий час, ці системи не утрудняють доступ персоналу в ці приміщення, тоді як при оснащенні дверей звичайними замками вони велику частину часу залишаються відкритими із-за незручності частого користування ключами.

При устаткуванні такими системами декількох приміщень одна і та ж картка може служити ключем до декількох дверей, замінюючи незручну зв'язку ключів.

Така система може функціонувати як автономно, так і під управлінням комп'ютера. При підключенні до комп'ютера можна вести кадровий облік, відстежувати порушення трудової дисципліни.

Контроль доступу для крупного підприємства

Не відрізняється від принципу побудови малих систем контролю доступу. Основу системи складає мережа контроллерів, керівників замками і считывателями. Контроллери підключаються до комп'ютера, який за допомогою спеціального програмного забезпечення здійснює централізоване управління системою і обробку даних. Якщо підприємство розташовується на декількох майданчиках, що знаходяться на значній відстані один від одного, то можлива побудова єдиної системи контролю доступу без прокладки спеціальних кабелів, за наявності між цими об'єктами загальної локальної комп'ютерної мережі.

Контроль доступу із застосуванням біометричних считывателей

Застосовується як в малих, так і великих системах контролю доступу. При устаткуванні такими системами приміщень відпадає необхідність в картках. Проте в деяких випадках доводиться додатково використовувати карти і PIN коди для збільшення кількості користувачів системи. Біометрики людини настільки унікальні (помилка помилкового пропуску складає 1:1200000), що дає практичну можливість виключити проникнення стороннього в приміщення. Система розпізнає тільки людину, а не картку (яку можна передати іншому співробітникові або втратити).

1.9.3 Можливості систем контролю доступу

Розмежування прав доступу

Дана функція дозволяє розділити персонал на ієрархічні групи, залежно від рівня доступу на об'єкти. Система дозволяє вирішити доступ кожному співробітникові тільки в ті приміщення, де він має право знаходитися відповідно до своїх службових обов'язків, наприклад, керівництво підприємства може користуватися "генеральними" пропусками, має рацію яких нічим не обмежені. Рядові співробітники - "стандартними", а відвідувачі "тимчасовими" і "разовими" з обмеженим терміном дії.

Можна заборонити доступ співробітників в приміщення фірми в неробочий час, під час іншої зміни, вихідні або свято.

Інформація про всі проходи персоналу зберігається в пам'яті системи і використовується надалі для обліку, а також може виявитися просто незамінною при проведенні службового розслідування. При необхідності завжди можна встановити, хто останнім йшов з приміщення, хто і коли ставив або знімав приміщення з охорони.

Глобальний захист від передачі пропуску

Функція Antipassback, що забезпечує захист від передачі пропуску іншій особі не дозволить двічі увійти на підприємство по одному пропуску не тільки через той же турнікет (двері), але і через будь-який інший, зокрема через іншу прохідну.

Більш того, якщо працівник все ж таки потрапив на територію, система не пропустить його на внутрішній об'єкт (у цех або інше приміщення).

Функція "Охорона"

Функція "Охорона" дозволяє переводити систему в режим, при якому відкрити двері і потрапити в приміщення зможуть лише певні співробітники. Наприклад, право доступу в бухгалтерію в звичайний час мають багато співробітників фірми, але не у відсутність працівників бухгалтерії. Тому, виходячи з кабінету, працівник бухгалтерії подвійним піднесло своєї карти до считывателю переводить контроллер дверей в режим охорони, який не пустить в кабінет співробітників інших підрозділів, що зазвичай мають право доступу в цей кабінет.

Эффективное управління персоналом

Програмне забезпечення системи дозволяє отримувати звіти про тих, що запізнилися, не вийшли на роботу або пішли з роботи завчасно за будь-який необхідний відрізок часу.

Таким чином, контроль над дисципліною покладається на систему, звільняючи адміністрацію від неприємної ролі цербера.

Програмний модуль "Облік робочого часу" забезпечує автоматизований облік робочого часу з формуванням табеля стандартної форми. Досвід експлуатації показує, що установка системи дозволяє зменшити число запізнень і передчасних відходів з роботи в 3-4 рази.

Оперативне управління устаткуванням

ПО системи дозволяє створювати графічні плани приміщень і указувати на них реальну установку устаткування. Система дозволяє підключати датчики і шлейфи охоронно-пожежної сигналізації і аналізувати інформацію, що поступає від них (зломах замків, порушеннях режиму контролю доступу і так далі).

При виникненні тривожної події оператор системи в режимі реального часу отримає сповіщення про подію з вказівкою місця на плані, а також інструкцію про дії в конкретній ситуації. Можливе програмування реакції системи на тривожні ситуації. Наприклад, відкриття дверей аварійного виходу при спрацьовуванні охоронно-пожежної сигналізації.

Комфортні умови праці

Програмне забезпечення системи дозволяє вести автоматизований кадровий облік. Вся інформація про співробітників зберігається в електронному вигляді у формі особистих облікових карток. Можливість оформлення карт доступу (фотографія, ФІО, посада, логотип) дозволяє використовувати їх не тільки як ключі, але і як бэджей або пропусків, біометричних считывателей досить подивитися в камеру прочитуючу веселкову оболонку ока або прикласти палець на считыватель відбитку пальців.

1.10 Системи сповіщення про пожежу

Загальновідомо, що основною причиною загибелі людей на пожежах є супутня паніка. Трохи більше спокій, і люди б неквапливо покинули небезпечну зону, при цьому цілком успішно евакуював і основні матеріальні цінності Більшість нормальних людей почувши слово "пожежа" втрачають здатність міркувати розсудливо. Єдине, що при цьому може допомогти - керівні вказівки з боку професіоналів, що зберегли витримку в екстреній ситуації. Технічна основа для зв'язку нечисленних професіоналів з переляканою публікою - системи мовного сповіщення.

Основне призначення системи сповіщення - це попередження людей, що знаходяться в будівлі, про пожежу або іншу аварійну ситуацію і управління евакуацією. Проте в

штатному режимі системи сповіщення можуть використовуватися також для передачі фонової музики або мовних оголошень, наприклад, по приміщеннях компанії.

Більшість систем сповіщення про пожежу будуються за модульним принципом, тому залежно від архітектурних особливостей будівлі і його призначення система сповіщення може включати пристрої, призначені для екстреної трансляції, або ж доповнюватися модулями, службовцями для підвищення якості звуку.

У торгових центрах і офісних будівлях система сповіщення про пожежу може створювати затишну обстановку, транслюючи приємну фонову музику, або передавати оголошення службового або рекламного характеру. У разі надходження з датчиків сигналу тривоги, трансляція загального призначення уривається, і система сповіщення про пожежу починає передавати екстрене повідомлення, записане в блок пам'яті або зачитуване диспетчером. Така розстановка пріоритетів при трансляції є обов'язковою вимогою для системи сповіщення про пожежу.

Состав системи сповіщення про пожежу

В даний час на українському ринку представлені системи сповіщення про пожежу, призначені для роботи в різних умовах і виконуючі різні функції, - від трансляції по зонах фонової музики або екстрених повідомлень до відсилання тривожного повідомлення на стільниковий телефон. Залежно від ступеня взаємодії з іншими системами безпеки будівлі, система сповіщення про пожежу може бути автономним комплексом або бути частиною складнішої системи. Крім того, системи сповіщення про пожежу розрізняються по максимальній кількості зон сповіщення, по гнучкості програмування логіки подій, по можливості комп'ютерного управління системою сповіщення і ін.

Проте, можна виділити декілька блоків, загальних для всіх систем сповіщення про пожежу.

•Управління цифровою системою сповіщення про пожежу, як правило, реалізується за допомогою комп'ютера.

Управління роботою блоків аналогової системи сповіщення про пожежу здійснюється через матричний блок управління, що входить до складу системи.

•Блок комутації сигналів.

•Підсилювальне устаткування (попередні підсилювачі і підсилювачі потужності) для посилення звукових сигналів, що поступають від джерела звуку (мікрофон, магнітофон і так далі).

•Виносні мікрофонні консолі для організації видаленого робочого місця диспетчера.

•Джерела сигналу - мікрофон, встановлений на пульті диспетчера або на блоці тривожного сповіщення, генератор тонального сигналу, радіоприймач, CD-проигрыватель або магнітофон.

•Гучномовці (рупорні, настенные і стельові)

По складу і принципу роботи системи сповіщення про пожежу підрозділяються на централізованих і локальних.

Локальні системи сповіщення про пожежу є сукупністю модулів, які під час вступу сигналу тривоги від якого-небудь зовнішнього пристрою (наприклад, датчиків пожежної сигналізації) транслюють в обмеженому числі приміщень записане раніше текстове повідомлення. Зазвичай такі системи сповіщення включають мовний процесор, підсилювач і гучномовець і не мають централізованого управління.

Одним з недоліків локальної системи сповіщення про пожежу є те, що за допомогою такої системи неможливо оперативно управляти евакуацією, наприклад, з мікрофонної консолі. Таке управління буває необхідно при виникненні нестандартної ситуації або у разі подій, що динамічно змінюються.

Централізовані системи сповіщення про пожежу мають центральний блок управління і можуть працювати як в автоматичному, так і в напівавтоматичному режимі. У автоматичному режимі система сповіщення про пожежу, у разі надходження сигналу тривоги, транслює по зонах записане екстрене повідомлення. При необхідності диспетчер може сам передавати

екстрені повідомлення з мікрофонної консолі або з мікрофону блоку тривожного сповіщення (напівавтоматичний режим трансляції).

Розподіл сигналу по зонах сповіщення забезпечується шляхом комутації джерел сигналу і зон сповіщення. Залежно від виконуваних завдань, система сповіщення про пожежу може містити декілька джерел сигналу. Розбиття будівлі на зони здійснюється виходячи з його архітектурних і функціональних особливостей.

Звуковий сигнал можна комутувати по зонах сповіщення до або після посилення. У разі комутації сигналу після посилення система сповіщення про пожежу повинна містити по одному підсилювачу на кожну зону. В більшості випадків системи сповіщення про пожежу використовують другий варіант комутації: декілька джерел сигналу підключаються до входу підсилювача, а потім посилений звуковий сигнал розподіляється по зонах сповіщення. При цьому система сповіщення не може одночасно транслювати в різних зонах сигнали з різних джерел звуку.

Джерела перемикаються відповідно до пріоритетності входів підсилювача. Найвищим пріоритетом володіє сигнал, що поступає з мікрофону диспетчера. Найнижчий пріоритет у трансляції загального призначення.

Основні вимоги до системи сповіщення

Сучасна система сповіщення повинна задовольняти вимогам, викладеним у ряді нормативних документів, серед яких основоположним є: ДБН Ст. 1.1-7-2002 Пожежна безпека об'єктів будівництва, Розділ 7. Основні інженерно-технічні засоби захисту від пожежі.

Нормами пожежної безпеки визначені системи сповіщення 5 типів залежно від поверховості будівлі, його площі і кількості людей, що одночасно знаходяться в нім. Згідно ДБН, практично в будь-якій громадській будівлі площею від 500 м2 обов'язково має бути встановлена мовна система сповіщення про пожежу, тобто система сповіщення, через яку можна попереджати людей, що знаходяться в будівлі, про екстрену ситуацію не сиреною, а за допомогою мовного повідомлення, що транслюється в автоматичному або

напівавтоматичному режимі.

ДБН Ст. 1.1-7-2002 визначає способи і порядок управління евакуацією за допомогою системи сповіщення. Основна функція, яку виконують системи сповіщення в аварійній ситуації, - це трансляція по зонах мовних повідомлень, направлених на запобігання паніці і скупченню людей у вузьких місцях (у проходах, на сходах і так далі), а також що містять інформацію про необхідний напрям руху. Такі повідомлення система сповіщення може передавати з носія інформації (наприклад, магнітної плівки) або з пульта диспетчера, якщо сповіщення здійснюється в напівавтоматичному режимі.

Мовна система сповіщення може доповнюватися світловими покажчиками напряму евакуації. Також система сповіщення може апаратний або програмно інтегруватися з системою контролю доступу, і при отриманні тривожного імпульсу з датчиків система сповіщення видаватиме команду на відкриття дверей додаткових евакуаційних виходів (наприклад, обладнаних електромагнітним замком).

Однією з основних вимог для системи сповіщення є принцип зональності багатоповерхових будівель і попереднє сповіщення персоналу будівлі. Зоною сповіщення називається частина будівлі або споруди, де проводиться одночасне і однакове за способом сповіщення людей про пожежу. Розбиття будівлі на зони проводиться для того, щоб легко було організувати евакуацію людей із зон сповіщення. Для кожного типу системи сповіщення обмовляється черговість сповіщення, зв'язок з диспетчерською і способи сповіщення. Як правило, система сповіщення насамперед попереджає про пожежу персонал будівлі, щоб службовці могли спланувати свої дії з евакуації людей.

1.10.1 Світлові системи сповіщення про пожежу

Загальний порядок проектування систем сповіщення (З) про пожежу в будівлях і спорудах, вибір типу системи сповіщення залежно від вигляду і призначення будівель і споруд визначений ДБН Ст. 1.1-7-2002. У приміщеннях, що захищаються, де люди знаходяться в шумозащитном спорядженні, або свысоким рівнем шуму звукові оповісники можуть комбінуватися зі світловими, допускається використання світлових миготливих оповісників.

Також в будівлях, де знаходяться (працюють, проживають, проводять дозвілля) глухі і слабослышащие люди, потрібне використання світлових або світлових миготливих оповісників.

2. ЗАГАЛЬНІ ВІДОМОСТІ ПРО ІНТЕГРОВАНІ СИСТЕМИ І КОМПЛЕКСИ

2.1. Принципи організації інтегрованих систем і комплексів охорони

Проблема безпеки будь-якого об'єкту вимагає для свого вирішення певного підходу. Так, для забезпечення безпеки невеликих об'єктів, як правило, достатньо використання технічних засобів охоронної сигналізації. В той же час очевидний, що вирішити проблему безпеки об'єктів, несанкціоноване проникнення на яких може привести до особливо крупного або непоправного збитку, загрози здоров'ю або життю великої кількості людей, за допомогою одних лише технічних засобів сигналізації неможливо. Тому у нас в країні і за кордоном в охороні таких об'єктів почали широко застосовуватися охоронні системи і комплекси, що включають окрім технічних засобів охоронної сигналізації засобу телевізійного спостереження, контролю і управління доступом, пожежної сигналізації, а також інших технічних засобів безпеки.

Перші комплекси були, як правило, симбіозом з декількох незалежних, не зв'язаних між собою підсистем і не могли вирішити поставлену задачу, оскільки збільшений об'єм продубльованою кожною підсистемою інформації практично не піддавався обробці і не дозволяв операторові ухвалити правильне рішення.

Останнім часом загальновизнаним став комплексний підхід до забезпечення безпеки важливих об'єктів, одним з основних напрямів якого є створення інтегрованих систем охорони.

Цілями інтеграції є отримання ІСО нових функцій при збереженні в повному об'ємі можливостей її окремих складових частин, економія необхідних для реалізації цих функцій засобів, максимальна автоматизація дій зі всіх напрямів захисту об'єкту. Інформація операторові видається після її аналізу і обробки в самій системі, що дозволяє підвищити її достовірність і оперативно ухвалити рішення

відповідності з виниклою ситуацією.

Ланкою будь-якої ІСО, що управляє і обов'язковим, є система збору і обробки інформації (ССОЇ). Залежно від значущості об'єкту і що пред'являються до рівня його безпеки вимог окремі підсистеми можуть входити або не входити до складу ІСО такого об'єкту. До складу ІСО при необхідності можуть входити і інші підсистеми, що забезпечують, наприклад, нормальне функціонування систем життєзабезпечення об'єкту, його інформаційну безпеку і тому подібне що Входять до складу ІСО технічні засоби, окремі підсистеми, складові частини, елементи в тому або іншому ступені функціонально перетинаються між собою і мають окрім загального і своє локальне управління.

Формалізоване визначення ІСО ще не цілком склалося, проте можна вважати, що інтегрована система охорони — сукупність об'єднаних загальним управлінням систем і технічних засобів безпеки, що володіють технічною, інформаційною, програмною і експлуатаційною сумісністю і призначених для вирішення завдань охорони об'єкту.

Більшість ІСО будуються за принципом дворівневої інтеграції.

Перший рівень — системний. ССОЇ або центральний процесор (сервер) об'єднує всі підсистеми ІСО і забезпечує їх взаємодію. Кожна з підсистем автоматично виконує які-небудь дії під час вступу певного сигналу від будь-якої іншої.

Другий рівень — модульний. Контроллери «місцевого» значення управляють невеликою групою извешателей, телевізійних камер, считывателей, виконавчих пристроїв і тому подібне

Такое побудова ІСО має ряд переваг. Завдяки гнучкій архітектурі система легко конструюється з певного набору модулів і блоків практично для будь-яких об'єктів.

В процесі експлуатації досить просто нарощувати і удосконалювати функції системи шляхом підключення різних типів реєструючих і старанних пристроїв.

ІСО будуються на базі комп'ютерних технологій, структурно вони можуть вони бути розбиті на наступні складові частини:

• пристрої прийому, передачі і обробки сигналів, що дозволяють отримувати максимально повну інформацію і відтворювати на центральному пульті управління всесторонню і об'єктивну картину стану приміщень і території об'єкту

працездатності апаратури і устаткування;

• виконавчі пристрої, здатні при необхідності діяти автоматично або по команді оператора;

• пункт (або пункти) контролю і управління системою відображення інформації, через яких операторів можуть стежити за роботою всієї ІСО;

• центральний процесор, що наочно представляє і накопичує інформацію для її подальшої обробки;

• комунікації, за допомогою яких здійснюється обмін інформацією між елементами ІСО і операторами.

Така структура побудови ІСО забезпечує ним наступні функціональні можливості:

• контроль за великою кількістю приміщень і територій

з організацією декількох рубежів охорони;

• багаторівневий доступ співробітників і відвідувачів з чітким розмежуванням повноважень по праву доступу в певні зони, що охороняються, за часом доби і дням тижня;

• ідентифікацію об'єкту, що перетинає певний рубіж;

• розпізнавання порушника, що дозволяє персоналу охорони приймати найбільш раціональні заходи протидії;

• взаємодія постів охорони і органів правопорядку при несенні охорони і у випадках локалізації подій;

• накопичення документальних матеріалів для використання їх при розслідуванні і аналізі подій.

Можливість гнучкого програмування ІСО і окремих підсистем дозволяє активно протидіяти таким несанкціонованим діям, як переривання каналів передачі

тривожній інформації, часткова нейтралізація системи особами, що мають доступ до окремих її елементів і підсистем, знищення інформації про подію, порушення

персоналом охорони встановленого порядку несення служби і тому подібне

2.2. Класифікація і склад інтегрованих систем і комплексів

У загальному випадку система безпеки будь-якого об'єкту є сукупністю інженерно-технічних засобів охорони, обслуговуючого персоналу (служби реагування) і

організаційних заходів. Далі, кажучи про систему безпеки об'єкту, ми матимемо на увазі тільки одну її складову — інженерно-технічні засоби охорони (ІТСО).

У свою чергу, інженерно-технічні засоби охорони підрозділяються на технічні засоби охорони і засобу технічної укрепленности і інженерні споруди.

До технічних засобів охорона відноситься:

• механічні замикаючі пристрої — ригелі, засуви, накладки і т.д.;

• різні замкові пристрої.

Центральный пульт управління КИТСО (ІТСО) включає:

• автоматизовані робочі місця операторів, адміністраторів систем (комплексу), постів охорони і служби безпеці;

• засоби збору і обробки інформації ІСО — комп'ютери, ППК, контрольні панелі, сервери, пульти, консолі управління і іншу апаратуру.

Система охоронної і тривожної сигналізації включає:

• засоби виявлення — извещатели, датчики;

• засоби тривожної сигналізації — кнопки, педалі, извещатели;

• засоби збору, обробки і відображення інформації — ППК, контрольні панелі, концентратори, комп'ютери, розширювачі, адресні і релейні модулі, світлові і звукові

оповісники і тому подібне

Система пожежної сигналізації включає:

• засоби виявлення — пожежні извещатели (теплові, димові, світлові (полум'ю), газові, ручні і тому подібне);

• засоби збору, обробки і відображення інформації — ППК, контрольні панелі, пульти, комп'ютери, панелі і консолі управління, адресні модулі, розширювачі, світлові і звукові оповісники, що погоджують пристрої і тому подібне

Система охоронного телебачення включає:

• телевізійні камери;

• пульти управління;

• пристрої узгодження і посилення;

• пристрої обробки і запам'ятовування відеоінформації;

• відеоконтрольні пристрої — монітори;

• відеозаписуючі пристрої — відеомагнітофони, пристрої цифрового запису і т. п.;

• засоби збору і обробки інформації — мультиплексори, матричні комутатори, ПК і тому подібне

Система контролю і управління доступом включає:

• приймальні пристрої доступу — ідентифікатори особи, считыватели, кодонаборные пристрої, пульти, панелі і консолі управління і т. п.;

• виконавчі пристрої доступу — електромеханічні, електромагнітні і механічні кодові замки, доводчики, автоматичні турнікети і шлагбауми, автоматичні і напівавтоматичні шлюзи (кабіни) і т.д.;

• засоби виявлення різних матеріалів — металлодетекторы, обнаружители вибухових речовин і радіаційних матеріалів і т.д.;

• засоби збору і обробки інформації — ПК, контроллери, панелі і консолі управлінні, що погоджують пристрої і так далі

Система безперебійного і резервного електроживлення включає:

• джерела безперебійного електроживлення — АВР, ІБП, UPS;

• генератори бензинові, дизельні;

• випрямлячі і блоки живлення;

• акумулятори.

Система оперативного і постового зв'язку включає:

• засоби дротяного службового зв'язку;

• засоби гучномовного службового зв'язку;

• засоби реєстрації службових переговорів;

• засоби радіозв'язку охорони.

Система сповіщення про пожежу і управління евакуацією людей

включає:

• засоби сповіщення — сирени, гучномовці, світлові

табло і покажчики і т. п.;

• засоби контролю і управління зонами сповіщення і аварійною автоматикою — підсилювачі, комутатори, магнітофони, релейні блоки, мікрофони і тому подібне

2.3. Засоби і системи охоронною, тривожною і пожежній сигналізації

Системи охоронної, тривожної, пожежної і охоронно-пожежної сигналізації в тому або іншому вигляді використовуються в даний час практично на всіх об'єктах. Це пов'язано з тим, що використання електроніки завжди вигідніше, ніж використання охоронців.

Системи ОПС призначені для визначення факту несанкціонованого проникнення на об'єкт, що охороняється, або появи ознак пожежі, видачі сигналу тривоги і включення виконавчих пристроїв (світлових і звукових оповісників, реле і тому подібне). Системи охоронною, тривожною і пожежною сигнали)ации по ідеології побудови дуже близькі один одному і на невеликих об'єктах, як правило, бувають суміщені на базі

єдиного контрольного блоку — приладу приймально-контрольного або контрольної панелі. Ці системи включають:

• технічні засоби виявлення — извещатели;

• технічні засоби збору і обробки інформації — прилади приймально-контрольні, контрольні панелі, системи передачі сповіщень і т.п.;

• технічні засоби сповіщення — звукові і світлові оповісники, модеми і тому подібне

Технічні засоби виявлення — це извещатели, побудовані на різних фізичних принципах дії. **Оповіщувач** — це пристрій, що формує певний сигнал при

зміні того або іншого контрольованого параметра навколишнього середовища. По сфері застосування извещатели підрозділяються на охоронні, охоронно-пожежні і пожежні. В даний час охоронно-пожежні извещатели практично не випускаються і не застосовуються. Охоронні извещатели по вигляду контрольованої зони підрозділяються на точкові, лінійні, поверхневі і об'ємні. За принципом дії вони підрозділяються на електроконтакти, магнитоконтактные, ударноконтактные, п'єзоелектричні, оптико-електронні, ємкісні, звукові, ультразвукові, радіохвильові, комбіновані, суміщені і ін.

Пожежні извещатели підрозділяються на извещатели ручної і автоматичної дії. Автоматичні пожежні извещатели підрозділяються на теплові, реагуючі на підвищення

температури; димові, реагуючі на появу диму; полум'ю, що реагують на оптичне випромінювання відкритого полум'я, і ін.

2.3.1 Технічні засоби збору і обробки інформації

До технічних засобів збору і обробки інформації відносяться прилади приймально-контрольні, контрольні панелі, сигнально-пускові пристрої, системи передачі сповіщень і тому подібне Вони призначені для безперервного збору інформації від технічних засобів виявлення (извещателей), включених в шлейфи сигналізації, аналізу тривожної ситуації на об'єкті і її відображення, управління місцевими світловими і звуковими

оповісниками, індикаторами і іншими пристроями (реле, модем, передавач і тому подібне), а також формування і передачі сповіщень про стан об'єкту на центральний пост або пульт централізованого спостереження. Вони ж забезпечують здачу під охорону і зняття об'єкту (приміщення) з охорони по прийнятій тактиці, а також у ряді випадків електроживлення извещателей.

Прилади приймально-контрольні класифікуються по інформаційній ємкості (кількості контрольованих шлейфом сигналізації) на прилади малої (до 5 ШС), середньої (від 6 до 50 ШС) і великої (понад 50 ШС) інформаційної ємкості. По інформативності прилади можуть бути малій (до 2 видів сповіщень), середній (3...5 видів) і великій (понад 5 видів) інформативності.

Системи передачі сповіщень класифікуються по інформаційній ємкості (кількості об'єктів, що охороняються) на системи з постійною інформаційною ємкістю і можливістю

нарощування інформаційної ємкості.

По інформативності системи підрозділяються на системи малої (до 2 видів сповіщень), середньої (3...5 видів) і великої (понад 5 видів) інформативності.

За типом використовуваних ліній (каналів) зв'язку системи підрозділяються на системи, що використовують лінії телефонної мережі (зокрема перемикані), спеціальні лінії зв'язку, радіоканали, комбіновані лінії зв'язку і ін.

По кількості напрямів передачі інформації вони підрозділяються на системи з одно- і двонаправленою передачею інформації (з наявністю зворотного каналу).

По алгоритму обслуговування об'єктів, системи передачі сповіщень підрозділяються на:

неавтоматизовані системи з ручною тактикою узяття (зняття) об'єктів під охорону (з охорони) після ведення телефонних переговорів з черговим пульта управління і

автоматизовані з автоматичним узяттям і зняттям (без ведення телефонних переговорів).

За способом відображення поступає на пульт централізованого спостереження інформації системи передачі сповіщень підрозділяються на системи з індивідуальним або груповим відображенням інформації у вигляді світлових і звукових сигналів, з відображенням інформації на дисплеї із застосуванням пристроїв обробки і накопичення бази даних.

Контрольні панелі по основних вирішуваних завданнях відповідають вітчизняним приладам приймально-контрольним. Уточнимо також поняття «Зона охорони» (термін, вживаний в іноземній літературі) і «шлейф сигналізації» (термін, використовуваний у вітчизняній літературі). Відразу ж відзначимо, що ці поняття разные.

Шлейф сигналізації — це електричний ланцюг, що сполучає вихідні ланцюги извещателей, включає допоміжні елементи (діоди, резистори і тому подібне), сполучні

дроти і коробки і призначена для видачі сповіщень про проникнення, спробу проникнення, пожежу, несправність, а в деяких випадках і для подачі електроживлення на

извещатели.

Таким чином, шлейф сигналізації призначений для контролю стану деякої зони, що охороняється.

Зона охорони — це частина об'єкту, що охороняється, контрольована

одним або декількома шлейфами сигналізації. Тому термін «зона охорони», використовуваний в описах зарубіжної апаратури, є в даному випадку синонімом терміну «шлейф сигналізації».

Сучасні багатофункціональні КП володіють широкими можливостями по організації систем охоронної, пожежної і охоронно-пожежної сигналізації. Знання цих можливостей дозволить зробити правильний вибір КП, характеристики і параметри якої якнайповніше задовольняють вирішенню поставлених завдань по охороні конкретного об'єкту.

Структура системи сигналізації, організовуваної на базі КП, в значній мірі визначатиметься способом підключення шлейфів сигналізації, що впливає на функціональні характеристики організовуваної системи охорони і багато в чому визначає вартість монтажних робіт. За способом підключення шлейфів можна виділити наступні типи КП:

• з шлейфами радіальної структури;

• деревовидною структурою;

• адресні.

У КП з шлейфами радіальної структури кожен шлейф підключається безпосередньо до самої панелі. Така структура виправдовує себе при невеликій кількості шлейфів (зазвичай

до 16) і на об'єктах, що не вимагають організації видалених шлейфів. Застосовуються зазвичай для невеликих і середніх об'єктів.

КП з деревовидною структурою мають спеціальну інформаційну шину з декількох проводів (зазвичай 4). На цю шину підключаються розширювачі. У свою чергу, до розширювачів підключаються радіальні шлейфи. До самої КП можуть також підключатися декілька базових радіальних шлейфів. Загальна кількість шлейфів знаходиться зазвичай в межах 24... 128.

Расширители контролюють стан підключених до них шлейфів, кодують інформацію про їх стан і передають по інформаційній шині на КП, що має індикацію стану всіх шлейфів.Такі КП використовуються для побудови систем

охорона середніх і великих об'єктів.

Адресні КП, що використовують шлейфи з адресними извещателями, стоять декілька відособлено від останніх і зазвичай використовуються для створення достатньо складних інтегрованих систем безпеки для великих і відповідальних об'єктів.

Очевидно, що адресні извещатели складніше звичайних і дорожчих; їх застосування і переваги повною мірою виявляються на складних і великих об'єктах.

Існують адресні КП, що мають різну побудову своїх шлейфів:

• променеве;

• кільце;

• кільце з променевими відгалуженнями.

Кільцевий шлейф має серйозна перевага. При його пошкодженні (обриві) він зберігає свою працездатність, оскільки зберігається лінія обміну інформацією. При замиканні шлейфу спеціальні пристрої, роздільники шлейфу, відключають закорочену ділянку, а решта частини шлейфу продовжує функціонувати.

Прилади приймально-контрольні і контрольні панелі є основними елементами, що формують на об'єкті інформаційно-аналітичну систему охоронної, пожежної або охоронно-пожежної сигналізації. Такі системи можуть бути автономними або централізованими. У першому випадку ППК або КП встановлюють в приміщенні (пункті) охорони, що розміщується на об'єкті, що охороняється. При централізованій охороні об'єктовий комплекс технічних засобів, що формується одним або декількома ППК (КП), утворює об'єктову підсистему охоронно-пожежної сигналізації, яка за допомогою системи

передачі сповіщень передає в заданому вигляді інформацію про перебування об'єкту на ПЦН, що розміщується в центрі прийому сповіщень про тривогу, — ПЦО.

Інтегровані системи безпеки

Традиційно в набір засобів забезпечення безпеки входили два розрізнені компоненти — системи відеоспостереження і засобу охоронно-пожежної сигналізації. Приблизно до середини 90-х запити споживачів стали ширшими, і прості системи перестали вирішувати завдання, що ускладнилися. Крім того, як і раніше ІСБ не дозволяли з мінімальними витратами забезпечити весь комплекс безпеки

Інтеграція — якісно новий стрибок в побудові систем безпеки об'єктів. Об'єднання систем безпеки на програмно-апаратному рівні дозволяє: мінімізувати капітальні витрати на оснащення об'єкту, за рахунок зменшення апаратної і програмної частини; понизити кількість інформації, що поступає операторові і зробити її наочнішою; автоматизувати ухвалення рішень для типових ситуацій; істотно зменшити вірогідність помилкових дій оператора; підвищити захищеність системи від зовнішньої дії, стійкість до руйнування;

Інтегрована система безпеки є комплексним інженерно-технічним рішенням, в яке за принципом «одного вікна» включені всі системи безпеки підприємства:

система контролю і управління доступом

система відеоспостереження

системи охоронно-пожежної і охоронно-тривожної сигналізації

система захисту периметра і інші інженерні системи

Принцип «одного вікна» означає, що робота з системою централізована і здійснюється через єдиний спеціалізований інтерфейс – програмний комплекс ССОЇ (система збору і обробки інформації). ССОЇ як центр систем безпеки забезпечує адміністрування, моніторинг і управління комплексом на основі єдиної бази даних і крізних алгоритмів взаємодії підсистем.

Объединение підсистем в єдиний комплекс з централізованим управлінням дозволяє вирішувати задачу забезпечення безпеки підприємства комплексно, використовуючи всі можливості сучасних систем безпеки для мінімізації, попередження і управління ризиками.

2.4 **Огляд ринку інтегрованих систем безпеки**

На ринку широко представлені інтегровані системи різного масштабу, забезпечення безпеки, що дозволяють вирішувати комплексні завдання, на об'єктах від малих офісів до крупних розподілених виробничих підприємств. Розглянемо деякі з них:

«LyriX-Server» від ААМ Системз [1]

"Рубіж" від СИГМА-ІС [2]

«Оріон» від Болід [3]

«ГРІФОС» від група компаній «Охорона» [4]

SECUROS від IIS [5]

Building Integration System (BIS) Bosch Security Systems [6]

Інтелект від ITV [7]

В цілому дані системи можна класифікувати по декількох критеріях, на основі яких можна зробити вивід про придатність конкретної системи для використання на заданому об'єкті.

Залежно від цільового масштабу підприємства (крупне виробництво, малий офіс і так далі) можна розділити ІСБ по категорії масштабу підприємства, для якого ця ІСБ використовуватиметься:

Малі

Середні

Великі

Змішаний тип

ІСБ можуть бути побудовані як на модульній архітектурі, так і на монолітній. Залежно від цього по рівню масштабованості вони можуть ділитися на:

Масштабовані

Немасштабовані

Більшість таких систем масштабовані.

Однією з ключових характеристик ІБС є інтеграція з устаткуванням інших виробників, оскільки саме на його основі будується все апаратна частина системи. Так само виробники устаткування можуть пропонувати комплекси забезпечення безпеки, що використовують виключно продукцію самій цій компанії. До таких ІБС відносяться, наприклад, фірми «Рубіж», «Оріон» і «Болід». Таким чином за типом інтеграції ІСБ діляться на:

Високоінтегированниє

Слабоінтегрірованне

Що використовують свою продукцію

Основним критерієм вибору системи буде якнайкраща економічна ефективність впровадження ІСБ за умови забезпечення всіх необхідних функцій.

Останнім критерієм виберемо легкість розгортання ІСБ і простоту обслуговування.

При класифікації були опущені такі критерії вибору ІСБ, як надійність, інтелектуальність, комплексність, оскільки само поняття інтегрованої системи безпеки несе в собі набір цих понять.

2.4.1 Опис ІСБ:

2.4.1.1 Інтегрована система охорони «LyriX-Server»

Могутня розподілена система безпеки крупного об'єкту, що володіє підвищеною програмною і апаратною стійкістю, гнучкістю і високим ступенем захисту. Може працювати на самих різних програмно-апаратних платформах. Не має обмежень по підтримуваному устаткуванню і можливостям інтеграції вже встановлених на об'єкті систем безпеки в єдиний комплекс. Оптимальна для середнього і крупного підприємства будь-якої сфери діяльності, може бути інтегрована з будь-яким корпоративним ПО.

Об'єднання устаткування різного призначення від різних виробників в єдину систему. Програмний комплекс LYRIX організовує взаємодія між підсистемами безпеки: системою контролю доступу, охоронній і пожежній сигналізації, системою аналогового і цифрового теленаблюдения. При цьому вбудований апарат реакцій дозволяє автоматизувати дії системи у разі потреби - при отриманні відповідних сигналів від однієї або декількох підсистем

Масштабованість - ефективна робота на об'єктах різного масштабу. Використовувані технології і архітектурні рішення в ПК LYRIX забезпечують його роботу на малих, середніх і крупних системах

Висока надійність і живучість забезпечується тим, що працездатність системи в цілому не залежить від окремих модулів. При виході з ладу окремих робочих станцій і серверів, навантаження динамічно перерозподіляється між справними комп'ютерами

Зручне управління і адміністрування системи за рахунок універсального застосування консоль, що "управляє". Дане застосування об'єднує всі інструменти: налаштування і управління устаткуванням, проглядання звітів, отримання інформації про події на графічних планах, реєстрація співробітників, установка має рацію в системі і ін.

Мультіплатформенность - можливість роботи на разных програмно-апаратних платформах забезпечує широкий вибір комп'ютерного устаткування і операційних систем: Microsoft Windows (Intel), Linux, Sun Microsystems Solaris (SPARC)

Відвертість ПК LYRIX для сторонніх розробників дозволяє IT підрозділам підприємства самостійно розвивати систему, підганяючи її під власні потреби. Відвертість забезпечують такі технології, як CORBA (стиковка окремих модулів), формат XML (зберігання налаштувань об'єктів, їх експорт і імпорт), JDBC (робота з базою даних)

Можливість тісної інтеграції з інформаційними системами підприємства дозволяє задіювати ресурси систем безпеки для оптимізації і підвищення ефективності загальних бізнес-процесів компанії

Швидке доопрацювання під вимоги замовника, надійна і оперативна технічна підтримка з боку розробника, компанії ААМ Системз, робить програмний комплекс LYRIX однаково привабливим як для замовника, так і для інсталятора

2.4.1.2 Інтегрована система охорони «Рубіж»

Науково-виробнича фірма «Сігма - Інтегровані Системи» є одним з провідних розробників і виробників інтегрованих систем безпеки. Прилади «Рубіж-07-3» і «Рубіж-08» служать основою для організації ІСБ середніх і крупних об'єктів, «Рубіж-060» і «Р-020» для організації ІСБ малих і середніх об'єктів. Названі вище прилади застосовуються для організації систем охоронної, тривожної і пожежної сигналізації, управління виконавчими пристроями контролю доступу, технологічної сигналізації, автоматичної пожежогасінні. Всі вказані системи інтегруються на рівні устаткування і функціонують незалежно від наявності ПЕВМ, що забезпечує високу надійність ІСБ в цілому.

Компьютер використовується для інтеграції з телевізійною системою спостереження, створення декількох автоматизованих робочих місць (АРМ), зручності роботи з ІСБ, передачі інформації про роботу системи по різних каналах (GSM, E-mail). Організація системи відеоспостереження здійснюється з використанням плат введення і оцифрування телевізійних аналогових сигналів «Рмвідео-4» і «Рмвідео-16-50», що встановлюються в Певм.Для ПЕВМ системи безпеки розроблено спеціальне програмне забезпечення «ПО Рубіж-08», що дозволяє створювати АРМ різних служб системи безпеці.

Апаратним способом інтегруються підсистема охоронної і тривожної сигналізації, підсистема пожежної сигналізації, система контролю і управління доступом (апаратна частина - считыватели, замки і так далі), система контролю технологічного устаткування і управління виконавчими пристроями. Апаратний спосіб інтеграції - на основі устаткування без участі ПЕВМ, забезпечує максимальну надійність і швидкодію системи.

Програмним способом інтегруються система охоронного телебачення (СТІЛЬНИК), система синхронізованою цифровою відео і аудіо реєстрації, система фотоідентифікації, система передачі сповіщень (SMS, E-mail), системи обліку робочого часу і бюро пропусків, система організації закритих каналів зв'язку для проведення конфіденційних телефонних переговорів, система шумоочистки аудіоданих.

ІСБ "Рубіж" дозволяє реалізувати на об'єкті:

- систему охоронної і тривожної сигналізації;

- систему пожежної сигналізації і систему управління пожежогасіннею і протипожежною автоматикою;

- систему контролю і управління доступом (СКУД);

- систему контролю технологічного устаткування;

- систему управління виконавчими пристроями (пожежогасіння, СКУД, газового, водяного, електропостачання, електроприводів і т. п.);

- систему охоронного телебачення (СТІЛЬНИК);

- систему синхронізованою цифровою відео і аудіо реєстрації;

- систему фотоідентифікації;

- систему передачі сповіщень (SMS, E-mail);

- систему обліку робочого часу і бюро пропусків;

- систему організації закритих каналів зв'язку для проведення конфіденційних телефонних переговорів;

- систему шумоочистки аудіоданих.

ІСБ «Рубіж» реалізує апаратно-програмне об'єднання підсистем охоронної, пожежної сигналізації, контролю і управління доступом, системи телевізійного спостереження. Має адресно-радіальну структуру побудови. Забезпечує можливість роботи і програмування без комп'ютера, і можливість об'єднання в локальну мережу з управлінням від ЕОМ і нарощування розгалуженої структури.

«Рубіж-08» має модульну архітектуру, а всі периферійні елементи уніфіковані. Це дозволяє створювати системи, оптимальні по критерію вартість/ефективність, а також реалізувати побудову ІСБ шляхом поетапного нарощування системи за принципом від простого до складного.

Основним елементом системи служить блок центральний процесорний (БЦП). Це могутній контроллер, що забезпечує побудову різних варіантів систем, на базі невеликої кількості типів периферійних елементів (адресних лінійних блоків, мережевих контроллерів управління доступом, адресних релейних блоків). Використання БЦП дозволяє виключити ПЕВМ з управління, що дозволяє забезпечити високу надійність, перешкодостійкість і живучість системи. У ІСБ «Рубіж-08» ПЕВМ використовується як додатковий елемент, що забезпечує зручність роботи з системою, а також реалізацію програмного способу інтеграції.

Прибор приймально-контрольний охоронно-пожежний з елементами телевізійного спостереження, управління устаткуванням контролю доступу і життєзабезпечення «Рубіж-08» призначений для створення систем комплексної безпеки і автоматичного (автоматизованого) управління життєзабезпеченням середніх, великих і особливо важливих об'єктів і багатооб'єктових комплексів. Багатооб'єктові комплекси будуються з використанням спеціального програмного забезпечення, яке є мережевим і забезпечує можливість створення необмеженого числа автоматизованих робочих місць (АРМ) і

автоматизованої процедури підтримки ухвалення оперативних рішень. Основу системи складає центральний процесорний блок (БЦП), який може забезпечити автономне управління всією системою навіть без присутності ЕОМ або при порушенні зв'язку і несправності комп'ютера. Новий БЦП має ряд особливостей, основні з яких:

- вісім вбудованих радіальних шлейфів сигналізації;
- чотири вбудовані релейні виходи виконавчих пристроїв.
- дві адресні лінії, які дозволяють підключати до 256 адресних пристрої;
- ЖКИ дисплей, що забезпечує високу інформативність повідомлень;
- вбудований блок живлення з резервним акумулятором;

БЦП також має в своєму складі інтерфейс для підключення ПЕВМ (RS232), інтерфейс для об'єднання блоків в мережу (RS485), інтерфейс для підключення принтера (Centronix). ЖКИ дисплей забезпечує значно зручніше управління приладом, дозволяє виводити інформацію у вигляді текстових повідомлень, вводити команди за допомогою системи меню. Є можливість вибору мови інтерфейсу.

Наявність двох адресних ліній для підключення периферійних блоків дозволяє гнучкіше будувати архітектуру системи. Як інтерфейс адресних ліній вибраний інтерфейс RS485, який володіє хорошою перешкодостійкістю, забезпечує високу швидкість обміну даними і дозволяє використовувати стандартні схеми підключення всіх периферійних мережевих пристроїв.

«Рубіж-08» забезпечує можливість підключення блоків з складу системи «Рубіж-07-3» за допомогою спеціального перехідного модуля.

За принципом побудови система «Рубіж-08» є сукупністю адресних, розподілених апаратно-програмних елементів. Цей принцип дозволяє реалізувати апаратно-програмний спосіб інтеграції. При цьому елементи системи утворюють ієрархічну, модульну, розподілену апаратно-програмну структуру, що забезпечує реалізацію різних топологий ліній зв'язку: радіальною, кільцевою деревовидною. Окрім цього забезпечується робота кожного елементу, як у складі приладу, так і автономно.

- Мережевий контроллер шлейфів сигналізації **СКШС-01** призначений для організації охоронно-пожежної сигналізації і має в своєму складі 4 універсальних шлейфу сигналізації (ШС).
- Мережевий контроллер шлейфів сигналізації **СКUJC-02** призначений для організації охоронно-тривожної сигналізації і має в своєму складі 8 охоронних ШС.
- Мережевий контроллер шлейфів сигналізації **СКШС-03-4 (8)** призначений для підключення виходів зворотного зв'язку пристроїв пожежної автоматики, а також іншого технологічного устаткування і має в своєму складі 4 (8) гальванічно розв'язаних ШС.

- Мережевий контроллер шлейфів сигналізації **СКШС-04** призначений для організації охоронно-тривожної сигналізації і має в своєму складі 16 охоронних ШС.
- Мережевий контроллер виконавчих пристроїв **СКИУ-01** призначений для підключення виконавчих пристроїв і має в своєму складі 4 реле з перемикальними контактами.
- Мережевий контроллер пристроїв прочитування коди **СК-01** призначений для організації точок доступу (підсистема СКУД) і терміналів управління. СК-01 має в своєму складі 2 комплекти входів/виходів для підключення пристроїв прочитування коди (считывателей) і устаткування дверей (реле управління виконавчим пристроєм, датчик положення дверей, кнопка виходу).
- Пульт управління об'єктовий **ПУО-02** призначений для організації об'єктового терміналу управління охоронною сигналізацією на рівні зон: постановка на охорону, зняття з охорони, проглядання стану. ПУО-02 оснащений рідкокристалічним текстовим дисплеєм з підсвічуванням, що значно підвищує зручність його використання. До одного БЦП можна підключити до 16 ПУО-02.
- Мережевий пристрій прочитування коди **УСК-02С** призначений для організації точок доступу (підсистема СКД) і терміналів управління. УСЬК-02С має в своєму складі считыватель проксимити-карт стандарту HID Wiegand26, вихід для управління замком, входи для датчика положення дверей і кнопки виходу.
- Мережевий контроллер лінійних блоків **СКЛБ-01** призначений для використання у складі ППКОП "Рубіж-08" блоків лінійних ЛБ-06, ЛБ-07 (ЛБ) з складу ППКОП Рубіж-07-3", ППКОП "Рубіж-07-4". До одного СЬКЛБ-01 може бути підключено до 32 ЛБ.
- Мережевий контроллер адресних пристроїв **СКАУ-01** призначений для підключення адресно-аналогових пожежних извещателей і адресних модулів System Sensor серії 200/500. До одного СЬКАУ-01 може бути підключене до 99 извещателей і 99 модулів.
- Мережевий контроллер управління пожежогасіннею **СКУП-01** призначений для побудови автоматичної системи пожежогасінні (АСПТ). СКУПИЙ-01 має 4 виходи управління (піропатрони, електромагнітні клапани і так далі) і два входи для підключення сигналізатора тиску (СДУ) і датчика наявності огнетушащего речовини (ОТВ).
- Пульт пожежник об'єктовий **ППО-01** призначений для об'єктового управління і індикації стану АСПТ. ППО-01 встановлюється біля входу в приміщення, що захищається. До ППО-01 підключаються: світлове табло "Газ (порошок) йди", світлове табло "Газ (порошок) не входь", світло-звукове табло "Пожежа", датчик положення дверей. ППО-01 дозволяє: здійснювати перемикання режимів роботи АСПТ (автоматичний / ручний} за

допомогою електронних ключів Touch Memory; здійснювати ручний пуск АСПТ за допомогою кнопки, захищеної від ненавмисного натиснення; здійснювати відміну пуску.

- Пульт пожежник диспетчерський **ППД-01** призначений для управління і індикації стану до 8 напрямів АСПТ. ППД-01 встановлюється в приміщенні чергового поста охорони.
- Мережевий контроллер аналогових сигналів **СКАС-01** призначений для підключення датчиків із стандартними аналоговими виходами. Підтримуються наступні типи виходів: 4-20 mA, 0-20 mA, 0-5 mA, 0-5 V, 1-5 V, 0-10 V. СЬКАС-01 має 4 аналогових входу для підключення датчиків.
- Блок інтерфейсний **БІ-02** призначений для підключення БЦП до локальної обчислювальної мережі, що задовольняє стандартам IEEE 802.3/802.3u (Ethernet/Fast Ethernet). При використанні БІ-02 БЦП може підключатися до ПЕВМ через локальну мережу. БЦП має вбудований WEB-сервер, що дозволяє дістати доступ до консолі БЦП для конфігурації і управління приладом через стандартний WEB-браузер (Internet Explorer).
- Мережевий контроллер радіоканальних пристроїв прочитування коди **СКУСК-01Р** призначений для організації управління системою за допомогою радиобрелоков: СКУД; управління шлагбаумами, комірами і т.п.; використання радиобрелоков як ношені термінали управління
- Мережевий кодонаборное пристрій **УСК-02КС** призначений для організації об'єктового терміналу управління охоронною сигналізацією на рівні зон: постановка на охорону, зняття з охорони, запит стану.
- Пульт управління **ПУ-02** призначений для організації робочого місця оператора системи безпеки і реалізує видалену консоль управління. ПУ-02 дозволяє виконувати всі дії з конфігурації і управління приладом.
- Джерело безперебійного живлення **ІБП 1200/2400** призначене для організації безперебійного живлення устаткування систем безпеки. ІБП передає в БЦП стан своїх входів і виходів.
- Блок індикації станів **БІС-01** призначений для індикації стану до 64 об'єктів системи безпеки на вбудованому світлодіодному табло.

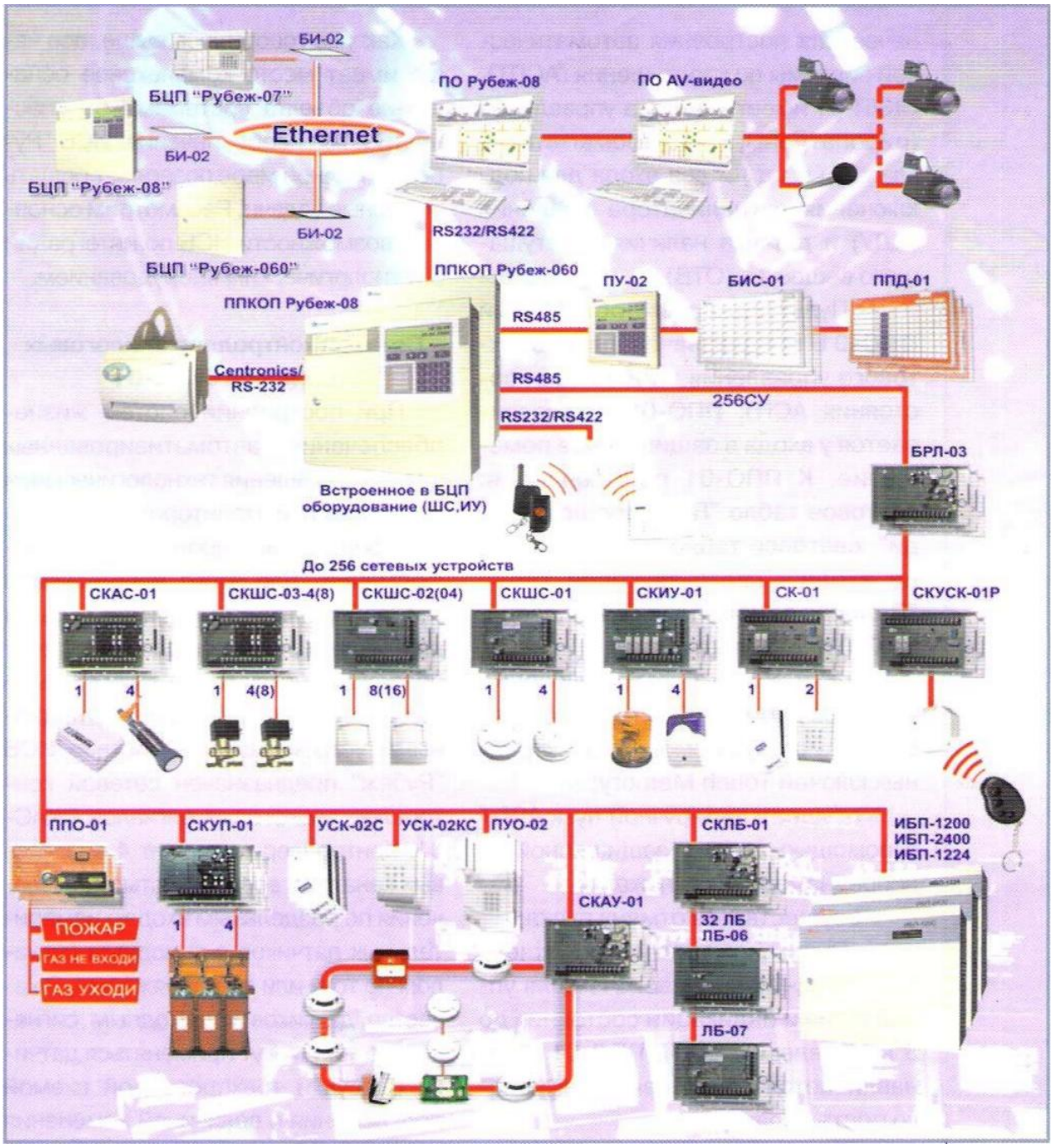

Рисунок 2.1 Схема підключення обладнання «Рубіж -08»

2.4.1.3 ІСБ «Оріон»

Система призначена:

Для збору, обробки, передачі, відображення і реєстрації сповіщень про стан шлейфів охоронної, тривожної і пожежної сигналізації

Для контролю і управління доступом (управління пристроями типу, що перегороджують, шлагбаум, турнікет, ворота, шлюз, двері і тому подібне)

Для відеоспостереження і відеоконтроля об'єктів, що охороняються

Для управління пожежною автоматикою об'єкту

Для управління інженерними системами будівель

Система забезпечує

Модульну структуру, що дозволяє оптимально обладнати як малі, так і дуже великі розподілені об'єкти

Низькі витрати з розрахунку на один шлейф або одну точку проходу

Захищений протокол обміну по каналу зв'язку між пультом і приладами

Микропроцессорный аналіз сигналу в шлейфах сигналізації, можливість вимірювання опору шлейфу для запобігання саботажу

Контроль і управління доступом через точки входу типу дверей, турнікети, шлюзи, шлагбауми

Відеоспостереження, відеоконтроль і реєстрація тривожних ситуацій

Управління пристроями автоматичної пожежогасінні, сповіщення, дымоудаления, кондиціонування

Технічна реалізація ІСО «Оріон» заснована на використанні головного (ведучого, керівника) мережевого контроллера системи (як яке може бути пульт контролю і управління «С2000» або комп'ютер з АРМ «Оріон»), інтерфейсу RS-485, що опитує по лінії, підключені до нього пристрої системи «Оріон». Максимальні функції системи можуть бути реалізовані тільки при використанні мережевого контроллера.

Разом з тим, ряд приладів ІСО «Оріон» допускає і автономну роботу. При автономній роботі реалізуються функціональні можливості самого приладу, такі як охоронно-пожежна сигналізація, функції управління і контролю доступу, управління пожежогасіннею.

Основою об'єднання приладів в систему служить лінія зв'язку інтерфейсу RS-485. Особливості технічних рішень, застосованих при розробці приладів, дозволяють використовувати не тільки шинну структуру по виділеній лінії зв'язку, властиву стандартному інтерфейсу RS-485, але і, в достатній мірі, довільну топологію із застосуванням повторителей інтерфейсу з гальванічною розв'язкою С2000-пі і різних каналів зв'язку (виділена лінія, «зайнята» лінія, оптоволоконний канал зв'язку, цифровий канал зв'язку в потоці Е1, локальна мережа по протоколу Ethernet, стільниковий канал зв'язку, радіо канал зв'язку).

Прилади і пристрої, що входять до складу системи, можна розділити на шість груп.

Перша група — це прилади, що мають радіальні шлейфи сигналізації. До цієї групи приладів відносяться «Сигнал-20», «Сигнал-20П» і «С2000-4». Прилади цієї групи можуть працювати в автономному режимі («Сигнал-20», «С2000-4») і у складі системи, під управлінням мережевого контроллера («Сигнал-20», «Сигнал-20П» і «С2000-4»).

Друга група приладів складає підсистему передачі сповіщень — «СПИ С2000а». До цієї групи відноситься контроллер «С2000-кдл» і адресні розширювачі, извещатели і сигнально-пускові блоки: «С2000-ар1», «С2000-ар2», «С2000-ар8», «С2000-іп», «ДІП-34А», «ІПР 513-3А», «С2000-ік», «С2000-ст», «С2000-смк», «С2000-сп2». Контроллер цієї групи має одну адресну лінію зв'язку, до якого підключаються адресні розширювачі, адресні извещатели і сигнально-пускові блоки, при цьому контроллер може працювати тільки у складі системи, під управлінням мережевого контроллера.

Третя група — прилади, що забезпечують функції контролю доступу. До цієї групи відносяться «С2000-4», його модифікації «С2000-4-01», «С2000-4-02» і «С2000-2». «С2000-2» є контроллером, що реалізовує функцію контролю доступу «вхід/вихід» для одних дверей або функцію «вхід» або «вихід» для двох дверей. «С2000-4» реалізує тільки функцію «вхід» або «вихід» для одних дверей. Контроллери можуть використовуватися для управління доступом на пристроях, що перегороджують, типу «двері», «турнікет», «шлагбаум», «шлюз» і тому подібне Прилади цієї групи можуть працювати у складі системи, під управлінням мережевого контроллера або автономно.

Четверта група — пристрої управління, індикації і передачі сповіщень на зовнішні системи. До цієї групи приладів відносяться «С2000-к», «С2000-кс», «С2000-бі», «С2000-іт», «С2000-сп1». Пристрої цієї групи призначені для забезпечення функцій управління узяттям під охорону, зняття з охорони розділів, контролю і управління доступом, відображення стану розділів системи, управління виконавчими пристроями, а також для передачі сповіщень на пульти централізованої охорони і користувачам системи.

Устройства цієї групи не володіють можливістю автономної роботи і призначені для функціонування тільки у складі системи, під управлінням мережевого контроллера (окрім «С2000-іт»).

П'ята група — прилади управління виконавчими пристроями пожежної автоматики. До цієї групи входять прилади «С2000-аспт» і «С2000-кпб». Прилади призначені для побудови систем пожежогасінні, дымоудаления, управління технологічними системами будівлі з розподіленими виконавчими пристроями. Прилади цієї групи можуть працювати у складі системи, під управлінням мережевого контроллера або автономно (окрім «С2000-кпб»).

Шоста група — мережеві контроллери і інтерфейсні перетворювачі. До цієї групи приладів відносяться «С2000», «С2000-кс» і персональний комп'ютер, зі встановленим на нім програмним забезпеченням АРМ «Оріон» і перетворювачем інтерфейсу ПІ, «ПІ-ГР» або «С2000-пі». Основним призначенням «С2000-пі» є побудова верхнього рівня інтерфейсу управління складною розподіленою системою, що використовує деревовидну топологію

інтерфейсу, а також подовження інтерфейсу RS-485 і локалізацію короткого замикання лінії інтерфейсу RS-485, при реалізації кільцевої або деревовидної структури ліній інтерфейсу. У складній розподіленій системі може використовуватися комп'ютерна мережа, яка також дозволяє використовувати довільну топологію.

2.5 Аналіз представлених систем

Об'єктом цього курсового проекту є будівля – офісний центр малих розмірів. Необхідно з розглянутих систем забезпечення комплексної безпеки вибрати найбільш відповідну для даного об'єкту.

Основою вибору ІСБ буде підбір оптимальної для даного об'єкту сукупності параметрів, виходячи з критеріїв подібних систем:

Виходячи з опису об'єкту можна зробити вивід, що він відноситься до класу малих або середніх об'єктів.

При організації захисту малих і середніх об'єктів використовуються далеко не всі функції комплексної системи, тому бажане використання ІСБ з модульною архітектурою, що б купувати тільки потрібних функціонал, а не всю систему цілком.

Крупним підприємствам часто вигідно співробітничати з одним виробником устаткування для уніфікації всіх використовуваних систем і висновку довгострокових контрактів на обслуговування. Але для малих об'єктів вигідно мати доступ до устаткування всіх виробників. Тому доведеться відкинути системи, що використовують тільки своє устаткування, і вибирати систему з найбільшою інтеграцією.

Для забезпечення зручності установки і експлуатації, система повинна мати як можна менш складну внутрішню інфраструктуру з найменшою можливою кількістю вузлів. Центральною частиною системи має бути сервер обробки інформації на базі IBM – сумісного комп'ютера.

Перевіримо запропоновані ІСБ на відповідність цим параметрам.

ІСБ «LyriX-Server» призначені для побудови на їх основі систем безпеки середніх і крупних підприємств, тому ці системи не підходять для заданого об'єкту.

Системи «Рубіж» і «Оріон» не підходять по третьому пункту, оскільки вони засновані на використанні устаткування виключно власного виробництва.

ІСБ «ГРІФОС» є відповідною по багатьом пунктам, але має обмежену інтеграцію з устаткуванням інших виробників, наприклад з устаткуванням серії «Рубіж» виробника СИГМА-ІС.

Так як саме на цьому устаткуванні будуватиметься апаратна частина системи безпеки(цей вибір буде обгрунтований пізнішим), це є критичним чинником і цю систему теж необхідно відкинути.

Апаратна частина обидві ІСБ однакова, оскільки основою їх служить сервер(IBM сумісний комп'ютер підвищеної надійності) і системи ОПС, СКУД і комплекс відеокамер інших виробників. Тому вартість впровадження грунтуватиметься на вартість комплексу програмного забезпечення, необхідного для роботи.

Визначимо можливості, які повинно надавати це ПО.

Наявність системи збору і обробки інформації, що працює на основному сервері.

Наявність видаленого робочого місця(УРМ) для моніторингу системи з декількох робочих місць. Це потрібно, оскільки контроль здійснюватиметься з кімнати охорони, а моніторинг так само з кімнати охорони із за стійки ресепшн.

Інтеграція з системою ППКОП «Рубіж»

Робота з чотирма ip-видеокамерами.

Можливість резервного копіювання відеоданих

Розглянемо вартість системи:

Таблиця 2.5.1«Интеллект»

ПО Ядро системи	14 000
ПО Видалене робоче місце (УРМ)	8 736
ПО Архіватор (Оперативний Архів)	14 000
ПО інтеграції з ППКОП «Рубіж-60»(включаючи СЬКД)	8 400
ПО обробки IP-камер (список див. на сайті)	3 500
Разом:	48600

Таблиця 2.5.2.«SecurOS»

АРМ "SECUROS"	12880
ПО підключення цифрових камер Axis, за IP адреса	3500 * 4
ПО ППКОП "Рубіж-08" (вимагає наявність "Ліцензія "Рубіж-08")	6440
ПО видаленого робочого місця Адміністратора, за кожне робоче місце	12880
ПО видаленого робочого місця - моніторинг, за кожне робоче місце	2800
ПО резервного копіювання відеоданих (ініціалізація даної функції	12880

вимагає наявність АРМ SECUROS)	
Разом:	61900

У результаті, відкинувши невідповідні по різних параметрах ІСБ, була вибрана ІСБ «SecurOS», на якій і буде побудована комплексна система безпеки об'єкту.

3. АНАЛІЗ ОБ'ЄКТУ ПРОЕКТУВАННЯ

Можливі типи небезпек: пожежа, крадіжка, просочування інформації, рейдерский захоплення.

Опис: Об'єкт вдає із себе двоповерхову офісну будівлю, не оточену огорожею. Є один парадний(Вхід 1) і два службові(Вхід 2, Вхід 3) входи в приміщення. На території будівлі офісу можуть знаходиться тільки співробітники і службовий персонал, за винятком кімнати прийому відвідувачів. При прийомі відвідувачів керівником, вони повинні супроводитися співробітниками охорони до кімнати переговорів і назад.

Контроль безпеки об'єкту ведеться з кімнати охорони(9), де встановлений центральний пульт охорони з можливістю стеження за станом всіх датчиків, а також можливість виклику пожежної служби і наряду міліції у разі потреби. У кімнаті охорони позмінно ведеться круглостуочное чергування охранны у складі мінімум однієї людини.

Методи протистояння погрозам:

Таблиця 3.1. Матриця безпеки об'єкту

№ приміщення	Функціональне призначення	Категорія зони режимної	Наявність охорони	Наявність ТСО
Територія, Вхід 1	Прилегла територія	0	-	Засоби спостереження
Вхід 2, Вхід 3	Службовий вхід	2	+/-	Засоби спостереження, система контролю доступу
9	Кімната охорони	1	+	П/о сигналізація, механічне посилення, система контролю доступу, центральний пульт ТСО
11	Кімната прийому посететелей	2	+	П/о сигналізація, засоби спостереження
10, 21	Робочі місця співробітників	3	-	П/о сигналізація, захист від витоку інформації
16, 19	Кабінет керівника, кімната переговорів, бухгалтерія	4	-	П/о сигналізація, захист від витоку інформації, механічне посилення, кнопка виклику охорони

5,18	Сховище матеріальних цінностей	4	-	П/о сигналізація (засоби спостереження, механічне посилення)*2,система контролю доступу
1, 2, 4, 15, 17	Коридор	3	-	П/о сигналізація, засоби спостереження
6, 7, 8, 12, 13, 20	Господарські приміщення	3	-	П/о сигналізація
3, 14, 22	Кімнати відпочинку персоналу	3	-	П/о сигналізація, захист від витоку інформації

3.1 Аналіз можливих ситуацій

1. Пожежа

Метод запобігання загрозі: у всіх приміщеннях мають бути встановлені датчики пожежної сигналізації з виходом на центральний пульт і з можливість автоматичного сповіщення пожежної служби.

Необхідні технічні засоби:

Датчики пожежної сигналізації.

Зв'язок пульта управління з пожежною службою та автоматичною системою пожежогасіння

Автоматичні системи пожежогасіння досить ефективні для ліквідації загоряння на його ранніх стадіях. Автоматичне пожежогасіння застосовується спільно з системою пожежної сигналізації або автономно, повністю виключаючи людський фактор при його запуску. Варто зазначити, що проектування і монтаж систем автоматичного пожежогасіння – заходи дуже відповідальні, так як визначають ефективність і безпеку системи в процесі експлуатації.

Про безпеку сказано не випадково – деякі типи установок пожежогасіння, при порушенні вимог нормативних документів за вибором, проектування, монтажу, при спрацьовуванні можуть представляти серйозну загрозу здоров'ю, життю людей. Це залежить від того, що гасіння полум'я досягається, в тому числі, за рахунок обмеження доступу кисню в зону горіння з усіма наслідками, що випливають звідси можливими наслідками для людини. Тому, проміжок часу між виявленням автоматичною пожежною сигналізацією загоряння або іншою спонукальною системою, і запуском установки пожежогасіння повинен бути достатнім для забезпечення евакуації людей з небезпечної зони. З іншого боку, чим більше цей час – тим вище ступінь розвитку пожежі. Так що дотримання "золотої середини" тут дуже важливо.

Досягається це:

поділом об’єкта на зони таким чином, щоб запуск автоматичної системи пожежогасіння був максимально локалізована по відношенню до вогнища спалаху; обладнанням об’єкта системою оповіщення, управління евакуацією виконаної за зональним принципом з пріоритетним оповіщенням в зонах загоряння; грамотно складеним планом евакуації, нарешті.

Системи водяного пожежогасіння в якості вогнегасної речовини використовують воду, можливо – з додаванням піноутворювача. Ці системи забезпечують поверхневе гасіння полум’я за рахунок охолодження зони горіння, а при застосуванні піноутворювача – також обмежують доступ до полум’я кисню. Для людей найменш небезпечні, ефективні для гасіння великих площ, тому широко використовуються в великих торгових центрах, паркінгах, виробничих приміщення та складах . Крім того установки водяного пожежогасіння здатні створювати водяні завіси для локалізації вогнища загоряння, зрошувати стіни будівлі, підвищуючи їх вогнестійкість.

Застосування водяного пожежогасіння там, де є неізольовані електромережі, можливо тільки після автоматичного відключення напруги.

Водяне пожежогасіння вимагає прокладки системи трубопроводів, установки насосних станцій, іншого обладнання, що визначає досить високу його вартість.

Водозаповнена система

Водозаповнена система є найпоширенішим типом спринклерних систем. У такій системі мережа розподільчих трубопроводів повністю заповнена водою під тиском. Проектується для приміщень з мінімальною температурою повітря 5°С і вище.

Повітряна (суха) система

Такі спринклерні системи розроблені спеціально для неопалюваних приміщень, де існує небезпека замерзання води в трубопроводах. У таких системах, починаючи від водоповітряного вузла керування, система не заповнена водою, лише стиснутим повітрям.

3.2 Вибір устаткування

3.2.1 Охоронно-пожежна сигналізація

Проміжною ланкою між системами пожежної сигналізації, контролю доступу і центральним сервером безпеки є система збору і обробки інформації з датчиків ПОС і СКУД. Безліч фірм пропонує таке устаткування, наприклад 2 провідних вітчизняних фірми: «СИГМА-ІС» з серією «Рубіж» і «Болід» з серією «С2000».

Ми зупинимося на продукції компанії «СИГМА-ІС», оскільки для офісної будівлі невеликих розмірів бажано всі вузли ПОС і СКУД об'єднати в одному місці усередині одного

приймально-контрольного пожежно-охоронного приладу (ППКОП). Серія рубіж якраз відповідає такій вимозі, коли як устаткування фірми «Болід» надає більшою мірою можливість побудови розподіленої системи.

Із списку можливих для підключення до ІСБ «Інтелект» ППКОП виберемо модель «Р-060», тому що именного вона призначена для створення інтегрованих систем безпеки малих і середніх об'єктів.

ППКОП 01059-100-4 «Р-060»

Рис.3.1 Загальний вид ППКОП 01059-100-4 «Р-060»

Призначення.

Прилад призначений для створення інтегрованих систем безпеки малих і середніх об'єктів. Повний набір підсистем з розвиненими можливостями: охоронна сигналізація, тривожна сигналізація, пожежна сигналізація, технологічна сигналізація, контроль і управління доступом, управління виконавчими пристроями, а також апаратна інтеграція підсистем на рівні устаткування і незалежність роботи від комп'ютера дозволяють створювати дійсно надійні системи.

Основные возможнсти.

· Апаратна інтеграція підсистем на рівні устаткування

· Підтримка до 128 (256 – в розширеній версії БЦП) об'єктів технічних засобів (шлейфів сигналізації, точок доступу, виконавчих пристроїв) сигналізації

· Підключення до 32 (64) мережевих пристроїв до лінії зв'язку, що забезпечує обмін інформацією по протоколу RS485 (можливе підключення будь-яких мережевих пристроїв з

складу ППКОПУ «Р-08», окрім пристроїв вживаних в АСПТ: СКУПИЙ-01 IP20, СКУПИЙ-01 IP65, ППО-1 і ППД-01)

· Контроль шлейфів пожежних извещателей всіх типів (ДІП, ІДПЛ і т. п.)

· Підключення тривожних радіокнопок

· Використання радиобрелоков для СЬКД, управління сигналізацією, ІУ і тому подібне

· Контроль шлейфів технологічних систем (газоаналізаторів, датчиків витоку води, газу і ін.)

· Організація роботи тамбур-шлюзов

· Постійний контроль ліній зв'язку і шлейфів сигналізації

· Вбудована мова макропрограмування Рубіж Скрипт

· Сучасний дружній інтерфейс оператора, що дозволяє видавати повідомлення на дисплей ПУ-02 (Пульт управління оператора) в термінах об'єкту охорони, з вказівкою назв приміщень.

· Підтримка російської і англійської мов інтерфейсу, можливість локалізації під будь-який язик

· Багаторівнева система розмежування повноважень операторів і користувачів системи (глибина призначення дозволів аж до конкретної дії над конкретним об'єктом в заданий час)

· Вбудований блок безперебійного живлення

· Виконання всіх мережевих пристроїв в конструктивах IP20 і IP65

· Документування подій на принтері

· Розвинене прикладне ПО для конфігурації і адміністрування (поставляється безкоштовно)

· ПО для організації АРМ різних служб системи безпеці (ПО Р-08)

Рис. 3.2 Комбінований пожежний извещатель Іп212/101-2-а1r

Сумісність практично з будь-якими пожежниками приймально-контрольними приладами (ПКП), у тому числі і із знакозмінною напругою в шлейфі сигналізації, наприклад, з "ППК-2", "ВЕСЕЛКА", Промінь, "СИГНАЛ-20П", "ВЭРС-ПК", УОТС, "РУБІЖ".

Розширений діапазон робочих температур извещателей серії ECO1000 від - 30°C до +70°C забезпечує роботу в опалювальних і неопалювальних приміщеннях.

Ізвещатель Іп212/101-2-a1r - поєднує в собі функції димового оптико-електронного і теплового максимально-диференціального датчика, завдяки чому він спрацьовує при будь-якому типі спалаху: як задимленням, що супроводиться, так і підвищенням температури.

У комбінованому извещателе Eco1002 проста логіка АБО (тобто спрацьовує або димовий або тепловий канал) замінена інтелектуальним алгоритмом обробки даних від обох каналів.

Стабілізація струмів вбудованого світлодіода і виносного оптичного сигналізатора, забезпечує постійну високу яскравість їх свічення у всьому діапазоні робочої напруги живлення.

Забезпечені простота і зручність включення тесту - дистанційно, при передачі кодованого сигналу з лазерного тестера ЛТ на світлодіод датчика, проводиться його включення і формується сигнал "Пожежа" для перевірки системи.

Зручний новий знімач Xr-1000 з телескопічною штангою дозволяє швидко встановити і зняти извещатели серії Eco1000 на висоті без використання сходів.

Для захисту димових камер від пилу извещатели Іп212/101-2-a1r поставляються з надітими на них пластмасовими технологічними кришками.

Базові підстави захищають извещатели серії ECO1000 від несанкціонованого витягання і забезпечують надійне кріплення в умовах транспортного трясіння при їх установці на рухомих об'єктах.

Використання друкарської плати з екрануючим шаром підвищило стійкість датчика до дії зовнішніх електромагнітних перешкод.

Високий захист від корозії забезпечений спеціальним покриттям і герметизацією окремих секторів монтажної плати.

Таблиця 3.1 Технічних характеристик Іп212/101-2-a1r

Діапазон чутливості відповідає оптичній щільності середовища:	0,05 - 0,2 дБ/м
Інерційність спрацьовування димового каналу:	10 сік
Температура спрацьовування при повільному підвищенні:	58°C
Спрацьовування при швидкості підвищення температури	8°C/мин і більш
Клас теплового каналу	A1R
Середня площа, контрольована одним извещателем:	до 110 м2

Допустимий рівень дії фонової освітленості:	12000 лк
Допустима швидкість повітря:	до 20 м/с
Робоча напруга:	від 8 до 30 В
Амплітуда пульсацій напруги живлення:	±2 У, макс.
Номінальний струм в черговому режимі:	не більше 85 мкА
Допустимий струм в режимі "Пожежа":	50 мА, макс.
Висота з базою E1000в:	50 мм
Діаметр:	102 мм
Вага з базою E1000в:	120 грам
Розмір лазерного тестера ЛТ:	83x30x15 мм
Вага лазерного тестера ЛТ:	30 грам
Діапазон робочих температур:	-30°C +70°C
Максимально допустима відносна вологість:	95%
Ступінь захисту оболонки извещателя:	IP23

Рис.3.3. Ізвещатель охоронний поверхневий суміщений «ОРЛАН» (Іо315-1)

Назначение і особливість

Призначений для використання у складі систем охоронної сигналізації, суміщаючи два незалежні канали виявлення:

акустичний канал - виявлення руйнування всіх видів будівельних стекол: звичайного, загартованого, візерунчастого, армованого, багатошарового, такого, що ламінує, а також скляних порожнистих блоків;

інфрачервоний канал - виявлення проникнення в простір закритого приміщення, що охороняється.

• Сферична лінза, що забезпечує зону виявлення без спотворень, високу збираючу здатність.

• Зона виявлення ІК-КАНАЛА: об'ємна.

• Наявність екрану захисту пироприемника від комах.

• Контроль розтину корпусу.

• Мікропроцесорна обробка сигналу.

• Світлова індикація стану каналів виявлення і можливість її відключення.

• Вибір чутливості акустичного каналу.

• Вибір чутливості інфрачервоного каналу.

• Індикація "пам'яті тривоги".

• Контроль напруги живлення.

• Температурна компенсація виявляючій здатності при зміні температури навколишнього середовища.

• Роздільні виходи на ШС по АК і ГИК каналам.

• Наявність кронштейна для зміни положення зони виявлення в просторі.

• Можливість установки на стіні або стелі приміщення.

• Ізвещатель видає тривожне сповіщення розмиканням шлейфів сигналізації контактами виконавчих реле окремо по АК і ГИК каналам.

Таблиця 3.2 Технічних характеристик

Дальність дії з АК каналу	6 м
Дальність дії з ГИК каналу	12 м
Мінімальна площа листового скла, контрольована акустичним каналом	0,1 м2
Споживаний струм	35 мА
Ступінь захисту оболонки	IP30
Діапазон робочих температур	-20 . +45° С
Габаритні розмір	124х68х51 мм
Маса	0,15 кг

Рис.3.4. Ізвещателі охоронні точкові магнитоконтактные
ІО 102-29 "ЕСТЕТ", "ЕСТЕТ-СЕЙФ"

Дуже часто в солідних офісах з сучасним дизайном впадають в очі чорні шурупи охоронних датчиків і що псують вид інтер'єру сполучні коробки.

Нові извещатели "ЕСТЕТ", "ЕСТЕТ-СЕЙФ" избавят Вас від цих проблем. Ізвещателі призначені для блокування дверних і віконних отворів, а також блокування інших конструктивних елементів будівель і споруд, на відкриття або зсув з видачею сигналу "Тривога" на приймально-контрольний прилад, концентратор або пульт централізованого спостереження. Конструктивно извещатели складаються з датчика магнитоуправляемого (датчика) на основі геркона і задаючого елементу (магніта), виконаних в корпусах з ABS пластика фірми BAYER AG.

Извещатель "ЕСТЕТ-СЕЙФ" призначений для установки на магнитопроводных контрольованих поверхнях (сейфи, сталеві ворота і двері, конструкції вікон і так далі) це наймініатюрніший накладний датчик на метал.

Відмітна особливість извещателей полягає в тому, що їх кріпильні отвори зверху закриті накладною декоративною кришкою. З'єднання проводів шлейфу сигналізації здійснюється за допомогою підключення до гвинтових клемників, розташованих під декоративною кришкою.

Контакти извещателей знаходяться в замкнутому стані при розташуванні магніта і датчика на відстані 10 мм і менш, і в розімкненому стані на відстані 25 мм і більш.

Максимально допустима співісна кріплення датчика і магніта извещателя "ЕСТЕТ" - 5 мм, а извещателя "ЕСТЕТ-СЕЙФ" -3 мм. Тому установка цих датчиків вимагає, щоб контрольовані поверхні були позбавлені від різного роду вільних люфтів, зсувів і так далі

Технічні характеристики:

Комутований струм: від 0,001 до 0,5А

Комутована напруга: від 0,02 до 72В

(макс. комутована потужність не більш 10Вт)

Габаритні розміри:

датчика 40х13х10

магніта 40х13х10

Маса не більш:

датчика 0,01 кг

магніта 0,015 кг

Діапазон температур: від -40°С до +50°С

Відносна вологість: 98% при 35°С

Опір замкнутих контактів: не більше 0,5 Ом

Рис.3.5 ІО-101-2 "КНФ-1" (НИЦЬ Охорона)

Ізвещатель ІО-101-2 "КНФ-1" (кнопка тривожної сигналізації), що встановлюється на об'єкті, призначений для організації тривожного сигналу на об'єктовий прилад приймально-контрольний (ППК). До складу ІО-101-2 "КНФ-1" входить мікроперемикач. При спрацьовуванні кнопки (розмикання контактів мікроперемикача) на вході ППК відбувається розрив шлейфу сигналізації. Повернення в початкове положення можливе тільки за допомогою ключа і замку.

Використовується так само для розблокування електрозамків.

3.2.2 Система контролю доступу

Рис. 3.6. AVC-105 Activision Виклична панель аудиодомофона накладного кріплення

Рис. 3.7 ML-194 K (Б/е) NEW електромагнітний замок

автоматики пожежних і запасних виходів, а також в приміщеннях, де пред'являються найжорсткіші вимоги Електромагнітні замки серії ML-194K призначені для використання в системах контролю доступу і до виконавчого механізму:

- висока надійність;
- виняткова зносостійкість;
- вандалозащищенность.

Особливістю даного модельного ряду є величина максимального зусилля на відрив, яка складає не менше 500 кг і велика пропускна спроможність.

Корпус замку суцільнолитий, матеріал — силумін. Покриття — стійка фарба, стандартного колірного виконання — «мідний антик».

Всі робочі поверхні магнитоблока і якорі мають цинкове покриття товщиною не менше 12мкм. У замку передбачений відсік для установки контроллера управління.

Характеристики електромагнітного замку ML-194K наступні:

- напруга живлення, постійна, — 12В;
- споживаний струм, не більш — 0,64А;
- нульова залишкова намагніченість;
- розмір відсіку блоку електроніки: 36?66?36 мм;
- діапазон робочих температур: від -30оС до +50оС;
- габарити: 270?75?45 мм;
- маса комплекту – 5,6 кг

3.2.3 Відеоспостереження

Використання ІСБ дозволяє інтегрувати підсистему відеоспостереження в комплекс «Інтелект». Існують два принципово разных типу систем відео спостереження – цифрові(мережеві ip) камери і аналогові. Розглянемо доцільність застосування на об'єкті повністю цифрової системи.

3.2.3.1 IP-видеонаблюдение: переваги і недоліки

IP-видеокамера може встановлюватися в будь-якому місці, де є мережа LAN, а так само може бути підключена безпосередньо, через модем, стільниковий телефон, або безпровідний адаптер зв'язку. Для передачі живого відеозображення в мережу необхідно просто включити в неї IP-камеру. Перегляд, таким чином, здійснюється через web-браузер, і немає необхідності в спеціальному програмному забезпеченні. Установка IP-камеры проста і зводиться до привласнення нею IP-адреса. Для таких камер відеоспостереження властива висока якість зображення, що отримується з використанням форматів стискування зображення MOTIONJPEG і MPEG-4. Завдяки всім цим якостям, формат

IP (internet protocol) практично став стандартом передачі даних в комунікаційних мережах. Не обійшов він стороною і охоронні системи відеоспостереження.

При побудові схеми охоронного відеоспостереження здійснюється робота тільки з цифровими даними, які транслюються і обробляються в загальній мережі. Аналоговий відеосигнал оцифровується або самою відеокамерою (IP-камера), або це виконує IP-видеосервер. Далі цифрові відеодані можуть бути записані на будь-якій, зокрема видалений, відеореєстратор або декілька відеореєстраторів. Перегляд здійснюється або з підключеного в мережу персонального комп'ютера, або на екрані охоронних моніторів через IP-сервер.

Всі ці функції можуть бути реалізовані в будь-якому, довільному порядку і спільно. Наприклад, з персонального комп'ютера можна вивести картинку окремої IP-камеры і записане зображення з будь-якого відеореєстратора.

Загальна вартість мережевої системи відеоспостереження в середньому вище в порівнянні з аналоговою, а можливості IP-видеонаблюдения, в порівнянні з аналоговим варіантом, значно ширше.

На відміну від аналогової охоронної камери відеоспостереження, IP-камера залишає можливості для формування відкритої архітектурної схеми, при якій можна проглядати зображення з камери в реальному часі і управляти через web-браузер ПК видалено. Цифровий сигнал при цьому не втрачає своєї якості. Кабельна мережа IP-камер проста, оскільки поодинці стандартному кабелю може передаватися зображення з сотень камер одночасно. Системи цифрового відеозапису і відеоспостереження на базі нових технологій, дозволяють будувати будь-які комплекси просто і недорого, спостерігати за тим, що відбувається ви зможете з будь-якої точки Миру, де є Інтернет, і з будь-якого комп'ютера локальної мережі вашого підприємства, офісу, удома або будь-якої установи. IP-камеры можна використовувати для відеоконференцій і контролю з одночасним записом звуку.

Переваги IP (мережевих, Інтернет) відеокамер для організації відеоспостереження і відеоконференцій очевидні. Це:

- Можливість побудова як складних систем відеоспостереження, камер, що складаються з декількох десятків, так і простих, таких, що складаються з 1 камери.
- IP-камера працює автономно, комп'ютера не вимагається.
- IP-камера підключається до комп'ютерної мережі, а не до комп'ютера.
- Доступ до IP-видеокамере можливий з будь-якого комп'ютера локальної мережі і Інтернет.
- Не треба додатково прокладати дроту — використовується вже існуюча комп'ютерна мережа. Прямо на її базі можна побудувати систему відеоспостереження.
- Трирівневий датчик руху відеокамери дозволяє записувати відео і звук тільки в ті моменти, коли був який-небудь рух.
- Передача інформації по мережі відбувається в зашифрованому вигляді, що дозволяє уникнути перехоплення або підміни передаваної інформації, що дуже актуально для охоронних систем відеоспостереження.

Однією з істотних переваг систем мережевого IP-видеонаблюдения полягає в можливості проводити відеореєстрацію будь-яких видалених об'єктів (офісів, філій, складів, удома, прилеглій території). Причому відстань не має особливого значення. Систему IP-видеонаблюдения також використовують для реєстрації людей (відвідувачів), входи, виходи, як лічильник відвідувачів, для невеликого маркетингу, аналізу, для фіксації шахрайства, крадіжок і як стандартне охоронне відеоспостереження.

Система видаленого IP-наблюдения потрібна, перш за все, для контролю. Окрім того, що під час своєї відсутності на роботі або удома можна мати уявлення, що там відбувається, ви зможете ще оперативно реагувати на події. IP-камеры відмінно застосовні для організації оглядового і технологічного спостереження, наприклад, на залізниці, бензозаправках, заводах, розважальних установах і тому подібне

Оцифрування зображення відбувається в камері, що дає можливість розвантажити центральне устаткування системи відеоспостереження і зайняти його вирішенням інших насущних завдань. Детектування і запис в IP-системах може здійснюватися децентрализованно.

Застосування рішень з використанням IP-видеонаблюдения дозволяє різко скоротити кількість комунікацій. Використання комп'ютерних технологій передачі інформації дозволяє значно збільшити відстань від камери відеоспостереження до відеореєстратора. Застосування цифрових камер дозволяє відмовитися від використання чересстрочной розгортки, що істотно підвищує якість відтворного зображення, що виводиться на монітор відеоспостереження.

IP-камеры можуть приймати і обробляти сигнали тривоги, що поступають з датчиків і управляти зовнішніми виконавчими пристроями через цифрові порти введення/виводу. Все це дозволяє використовувати менше кабелю, засобів, збільшити функціональні можливості системи відеоспостереження і розширити можливості інтеграції.

Ціна IP-видеокамеры вища, ніж ціна на аналогову відеокамеру, але ця різниця втрачається на тлі загальних вкладень в IP-проект. Нижча вартість систем IP-видеонаблюдения виходить із-за використання в них мережевого і комп'ютерного устаткування, що підтримує відкриті галузеві стандарти, які використовують всі виробники в IT-секторе, на відміну від часто не сумісних між собою апаратних засобів аналогових систем відеоспостереження, у тому числі і DVR (відеореєстраторів). Це радикально спрощує управління і витрати на устаткування, особливо для великих систем, де пристрої зберігання інформації і сервери — істотна частина загальної вартості рішення. Додаткову економію забезпечує використання єдиної комунікаційної інфраструктури. Мережі на основі IP — Internet, LAN, WAN, що використовують різні методи зв'язки, як дротяні, так і безпровідні, можуть паралельно використовуватися іншими застосуваннями і є дешевшою альтернативою традиційним аналоговим мережам.

При невеликій кількості камер відеоспостереження, місць перегляду і високої пропускної спроможності мережі особливих проблем при побудові рішень на базі IP-камер не виникає.

При організації передачі відео інформації через Internet, а останнім часом все більше стало саме таких запитів від клієнтів, основною проблемою є вибір пропускної спроможності каналу зв'язку і вибору якості зображення.

Зазвичай в системах відеоспостереження, що використовують для передачі зображення мережу Internet, канали зв'язку не володіють такою високою пропускною спроможністю. Максимальна швидкість доступного клієнтам каналу зв'язку на практиці не перевищує 2 Мбод, тому або знижується якість зображення, або підвищується ступінь стискування, або зменшується кількість камер спостереження, або знижується швидкість передачі відеозображення. Оскільки мережа завжди працює із швидкістю найповільнішого свого сегменту, дуже велику увагу слід приділяти всім сегментам мережі від джерела інформації до станцій моніторингу.

Системи IP-видеонаблюдения дозволяють просто масштабуватися. Вони дають можливість використовувати рентабельніші рішення, такі як стандартні сервери, для запису і зберігання відеоданих. Є можливість вибору програмного забезпечення, створеного для управління відео і забезпечення необхідної аналітичної підтримки. Крім того, такі рішення дозволяють організувати децентрализованную обробку і зберігання інформації.

Ці системи легко реконфігуруються і переносяться. Система відеоспостереження вмонтовується на час будівництва, а потім переїздить на новий об'єкт і так далі В цілому, мережеві системи відеоспостереження знаходять хороше застосування для видаленого контролю стану об'єктів, контролю касових операцій в супермаркетах і складних системах, не вимагаючого запам'ятовування і аналізу дрібних деталей зображення. Це можливість необмеженого копіювання даних без втрати якості і універсальність протоколів, як передачі, так і зберігання.

При багатьох перевагах, IP-системы відеоспостереження мають і ряд недоліків, які поки стримують їх масове застосування і повне витіснення аналогових камер. Цей недолік - якість зображення у зв'язку з обмеженням пропускної спроможності каналів зв'язку. Так само виникають складнощі з інтеграцією приладів різних виробників в систему з ПО третьої фірми, тобто складна інтеграція різнорідних систем безпеки. Все різноманіття аналогових камер має, як мінімум, один інтерфейс - композитний відеосигнал, який є промисловим стандартом і підтримується будь-яким устаткуванням. На цифровому світі все набагато складніше. Багато виробників, захищаючи свою нішу на ринку, підтримують всі протоколи передачі даних, проте ретельно приховують алгоритм кодування зображення, вимушуючи клієнтів користуватися тільки їх утилітами перегляду або архівації зображень.

3.2.3.2 Виводи по аналізу відеоспостереження:

В цілому використання мережевих відеокамер помітно здорожує систему, але переваги їх використання, як частини інтегрованої системи, очевидні:

1) Немає необхідності використання відеореєстраторів для обробки і зберігання інформації – відео в цифровому вигляді обробляється центральним сервером «Інтелект», що дозволяє застосовувати інтелектуальні системи розпізнавання відеозображення і автоматичного ухвалення рішень.

2) Високий дозвіл, що дозволяє розпізнавати дрібні деталі зображення, зокрема осіб. Це особливо актуально, оскільки відеокамера використовуватиметься для контролю доступу співробітників через службові входи.

3) На об'єкті вже існує розподілена ЛВС(LAN). При невеликій кількості використовуваних камер не буде потрібно створення нової інфраструктури.

4) На об'єкті присутній персонал, відповідальний за роботу мереж, тому не доведеться наймати нових фахівців для підтримки відеомережі.

Тому підсистема відеоспостереження буде побудована з використанням комплексу ip-камер спостереження.

Мережеві камери Smartec повністю інтегровані для роботи з підсистемою спостереження ІСБ «Інтелект». Так само камери цієї фірми мають хороші показники відношення «цена/качества», тому доцільне їх використання для побудови відеосистеми.

Рис.3.8 Кольорова мегапиксельная відеокамера STC-IPM2090A з об'єктивом, аудіоканалом і дозволом до 1280x1024 пикс.

Малогабаритна IP-видеокамера STC-IPM2090A мазкі Smartec використовує високоякісну 1,3-мегапиксельную КМОП-матрицю з чутливістю до 0,5 лк, яка формує інформативний відеосигнал з дозволом до 1280x1024 пикс. Цифрові відеопотоки у форматах MPEG-4 або M-JPEG ця мегапиксельная відеокамера може передавати по IP-сети з дозволом від 640x480 до 1280x1024 пикс. і частотою від 30 до 8 к/с, відповідно, а також дозволяє організувати аудіозв'язок між оператором і об'єктом відео спостереження через аудио-вхід/вихід. Окрім цього відеокамера оснащена мегапиксельным об'єктивом 4,2 мм, детектором руху з чутливістю, що настроюється, і тривожними входом/виходом, а також підтримує технологію POE. STC-IPM2090A комплектується русифікованим ПО NVR на 32 відеоканали і сумісна з ПО XProtect компанії Milestone.

Однією з особливостей STC-IPM2090A є застосування технології формування і паралельної передачі по мережі чотирьох відеопотоків в одному з форматів стискування – MPEG-4 або M-JPEG. За рахунок цього мегапиксельная відеокамера може одночасно транслювати відеопотоки з різним фрэймрейтом, які можуть використовуватися для відображення відео, його запису, передачі по Інтернет і тому подібне Відеопотік з мегапиксельным дозволом 1280x1024 пикс. (SXGA) у кожному з форматів відеокамера передає із швидкістю 8 к/с. Для інших трьох відеопотоків можна задати дозвіл HD720 (1280x720 пикс.) або VGA (640x480 пикс.), які STC-IPM2090A транслюватиме з частотою 10 к/с або 30 к/с, відповідно, що цілком достатньо для IP-систем відео спостереження багатьох об'єктів.

3.2.3.3 Застосування мегапиксельной бюджетною КМОП-матриці

На відміну від багатьох аналогів, STC-IPM2090A використовує високоякісну КМОП-матрицю з прогресивною розгорткою, яка значно дешевше ПЗС-МАТРІЦ високого дозволу, тому ця мегапиксельная відеокамера може стати найбільш вдалим вибором при створенні бюджетних систем IP-видео спостереження. Крім того, алгоритму прогресивної розгортки КМОП-матриці запобігає утворення «гребінки» по краях зображення рухомих об'єктів, а функції автоматичного балансу білого, АРУ, компенсації зустрічного засвічення і мерехтінь дозволяють настроювати якість зображення з відеокамери під різні умови освітлення.

3.2.3.4 Ефективна робота STC-IPM2090A в низькошвидкісних мережах

До локальної мережі мегапиксельная відеокамера підключається через мережевий інтерфейс 10BaseT/100BaseTX Ethernet і може транслювати відео по каналах із смугою від 28 Кбіт/с до 3 Мбіт/с. STC-IPM2090A має вбудований веб-сервер-сервер, тому все відео, що поступає з неї, з синхронним аудіосупроводом можна переглядати на будь-якому комп'ютері, підключеному до мережі, у вікні стандартного веб-сервера-браузера. Для авторизації доступу до відео досить набрати IP-адрес відеокамери в адресному рядку браузера, а також пароль доступу.

3.2.3.5 Програмне забезпечення для перегляду, запису, пошуку відео і управління по мережі

У комплект постачання STC-IPM2090A входить русифіковане програмне забезпечення NVR, яке підтримує всі необхідні функції запису, пошуку, відтворення відео і налаштування IP-видеокамеры і розраховано на одночасну роботу з 32 IP-устройствами Smartec. При покупці ліцензій на додаткові канали число обслуговуваних ПО NVR відеокамер або відеосерверів Smartec можна довести до 64. Окрім цього, мегапиксельная відеокамера може працювати і під управлінням ПО XProtect данської компанії Milestone Systems, яке використовується, як правило, для організації охоронного IP-видео спостереження на крупних і територіально-розподілених об'єктах і дозволяє управляти роботою як IP-оборудования Smartec, так і IP-видеокамер/IP-серверов більш ніж 35 виробників.

3.2.3.6 Підтримка технології POE і двонаправленої передачі звуку

При роботі у складі системи IP-видео спостереження мегапиксельная відеокамера дозволяє організувати двосторонній аудіозв'язок між центральним пунктом відео спостереження і приміщенням, де встановлена відеокамера. Для цього досить підключити в аудіовходу STC-IPM2090A зовнішній мікрофон, а до її аудіовиходу – активний динамік.

Ще однією гідністю STC-IPM2090A є підтримка технології POE (Power over Ethernet), завдяки якій мегапиксельная відеокамера може отримувати електроживлення по вільних жилах тієї ж витої пари, по якій транслюються відеопотоки. У багатьох випадках це дозволяє скоротити час монтажу і інсталяції відеокамери, і виключити додаткові витрати на кабель електроживлення і його прокладку. Як альтернатива POE на STC-IPM2090A можна подавати живлення через 12 В адаптер постійного струму, який входить в комплект постачання.

3.2.3.7 Настроювання алгоритмів реакції відеокамери на сигнали тривоги

Для виявлення руху в зоні відео спостереження мегапиксельная відеокамера може використовувати вбудований детектор руху з трьома областями детекции і чутливістю, що настроюється, або зовнішній охоронний датчик. Підключити датчик до STC-IPM2090A можна через тривожний вхід, а через TTL-выход відеокамера здатна управляти роботою одного виконавчого пристрою. При цьому оператор може набудувати реакції відеокамери так, що під час вступу сигналу тривоги з детектора або датчика буде активований відеозапис, приведений в дію виконавчий пристрій, відправлена тривожна послідовність і повідомлення про тривогу на e-mail або FTP-сервер .

Таблица 3.3. Основних технічних характеристик на мегапиксельные відеокамери Smartec STC-IPM2090A:

Параметри	Значення
Чутливий елемент	1/3” КМОП-матриця Micron Progressive Scan
Кількість пікселів	1280x1024
Чутливість	0.5 лк (F1.8, 30 IRE, макс. АРУ)
Дозвіл відеокамери	SXGA (1280x1024) при 8 к/с
	HD720 (1280x720) при 10 к/с
	VGA (640x480) при 25 к/с
Формати стискування	MPEG-4/MJPEG
Об'єктив	Мегапіксельний без АРД 4.2 мм/F1.8 (у комплекті)
Електронний затвор	1/10-1/2000 з
Баланс білий	6 режимів (Авто/ручной/фікс./Внутр.1/Внутр.2/Внеш.1/Внеш.2)
Компенсація зустрічного засвічення	Є
АРУ	Авто (що настроюється)
Відношення сигнал/шум	>44 дБ
Синхронізація відеокамери	Внутрішня
Аудіостискування	8 кГц, моно, PCM
Детектор руху	Апаратний, 3 області детекции
Тривожні входи/виходи	TTL, 1 вхід, 1 вихід
Швидкість передачі даних	От 28 Кбіт/с до 3 Мбіт/с
Підключення до мережі	Ethernet 10/100Base-T, RJ-45
Підтримувані протоколи	TCP, UDP, IP, HTTP, DHCP, PPPoE, RTP, RTSP, FTP, SMTP, DNS, DDNS, NTP, ICMP, IGMP, ARP, 3GPP
Безпека	Захист паролем; зміна налаштувань відеокамери –

	тільки адміністратор
Веб-сервер-браузер	Internet Explorer 6.0 або вище
Діапазон робочих температур	0?. +50? З
Напруга живлення	POE (IEEE 802.3af), клас 3 або 12 В пост. струму +/-10
Споживана потужність	3.3 Вт (DC 12 V) 4.3 (POE)
Габарити	67x55x129.5 мм
Маса	400 грам

Рис.3.9 Універсальні термокожухи Smartec серії STH-1230

Термокожухи Smartec серії STH-1230 мають ступінь пыле- і вологозахисту IP66 і призначені для захисту камер відеоспостереження при їх роботі у вуличних умовах. Моделі цієї серії з одним обігрівачем забезпечують діапазон робочих температур від -40о до +50оС, а з двома обігрівачами – від -55о до +50оС. Також випускається модифікації з імпульсним джерелом живлення і без нього. У пристроях цієї серії верхня кришка відкривається повністю, що забезпечує вільний доступ до камери, яка розташовується на кріпильній пластині з можливістю регулювання її положення.

Як і будь-який термокожух мазкі Smartec, термокожухи цієї серії оснащені ущільненими виводами для кабелю, а конструкція штатного кронштейна передбачає часткову крізну проводку кабелю із закладенням в стіну або виведенням його назовні у підстави кронштейна. Імпульсний блок живлення на 800 мА, встановлений в моделі STH-1230S-PSU1 і STH-1230D-PSU1, дозволяє живити камери, що працюють від 12 В пост. струму.

3.2.3.8 Кліматичні випробування, що підтвердили характеристики STH-1230

Для перевірки характеристик термокожухов, заявлених виробником, були проведені незалежні кліматичні випробування, в ході яких вони поміщалися в спеціальну термокамеру.

При цьому в термокамері і в термокожухе встановлювалася температура +20°С, яка потім змінювалася із швидкістю 1°/мин. Усередині кожного кожуха були встановлені стандартна чорно-біла камера спостереження з об'єктивом і два датчики для вимірювання температури (один в центрі кожуха над камерою, а інший над об'єктивом).

У моделях з одним обігрівачем при зміні температури в термокамері від -46° до +42°С температура в центрі термокожуха змінювалася від -15° до +42°С, а температура над об'єктивом – від 0° до +45°. У моделях з двома обігрівачами, при зміні температури в термокамері від -56° до +41°, термокожух підтримував температуру в центрі від -12,9° до +39,9°С, а над об'єктивом від +5° до +45,6°С.

4 ЕКОНОМІЧНА ЧАСТИНА

4.1. Розрахунок економічної ефективності

При розрахунку економічної ефективності системи безпеки в основному спираються на порівняння повної вартості впровадження такої системи порівняно із збитком, який може нанести реалізація погроз безпеці, на запобігання яким направлена ця система.

Економічна доцільність застосування ТСО розраховується на основі можливостей і економічної вигоди, яке дає це застосування в порівнянні з наймом служби охорони.

Розрахуємо кінцеву вартість отриманої системи безпеки.

Таблиця 4.1 Розрахунок вартості рішення:

ІСБ «SecurOS» ПО	50000	1	50000
Сервер обробки і зберігання даних	100000	1	100000
ППКОП 01059-100-4 «Р-060»	22000	1	22000
Пожежний извещатель Іп212/101-2-а1r	400	18	7200
Ізвещатель охоронний «ОРЛАН»	1000	15	15000
Ізвещатель магнитоконтактный ІО 102-29 "ЕСТЕТ"	70	5	350
Тривожна кнопка ІО-101-2 "КНФ-1"	240	3	720
Виклична панель домофона AVC-105	500	3	1500
Електромагнітний замок ML-194 K (Б/е)	1700	3	5100
Мережева відеокамера STC-IPM2090A	15000	4	60000
Термокожух Smartec серії STH-1230	2000	4	8000
LCD монітор 24’	10000	2	20000
Кабелі і витратні матеріали			20000
Монтаж			50000
Разом:			360000

Очевидно, що витрати на створення системи безпеки значно менше збитку, який може бути нанесений при реалізації будь-якій з погроз.

Дана сума достатня для найму 1-2 охоронців строком на рік з рівнем зарплати 15000-30000 грн. Але при цьому така служба охорони не може забезпечити всіх можливостей, що надаються введенням в експлуатацію ТСО, а особливо інтегрованої системи безпеки. До того ж термін служби устаткування складає від 3 до 5 років, з чого виходить, що, в розрахунку не весь термін експлуатації, створення системи безпеки на основі ТСО має високу економічну ефективність.

5 ОХОРОНА ПРАЦІ

5.1 Правила техніки безпеки при роботах по монтажу технічному обслуговуванню і ремонту технічних засобів систем безпеки і інших електроустановок

Дотримання правил техніки безпеки є головною умовою попередження виробничого травматизму. Найдосконаліші умови праці і новітні технічні заходи щодо техніки безпеки не зможуть дати бажані результати, якщо працівник не розуміє їх призначення. Знання виробничих трудових процесів, вживаного устаткування, пристосувань, інструменту і безпечних способів і прийомів в роботі створюють умови для продуктивної праці без травматизму.

Велике значення для цього мають інструктажі по техніці безпеки.

По характеру і часу проведення вони підрозділяються на ввідний, первинний на робочому місці, повторний, позаплановий і поточний.

«Міжгалузеві правила, що діють в даний час, по охороні праці (правила безпеки) при експлуатації електроустановок» введені в дію I липня 2001 р. Вони розповсюджуються на працівників організацій незалежно від форм власності і організаційно-правових форм і інших фізичних осіб, зайнятих технічним обслуговуванням електроустановок, провідних в них оперативні перемикання, організуючих і виконуючих будівельні, монтажні, налагоджувальні, ремонтні

роботи, випробування і вимірювання. З введенням даних правил скасовані «Правила техніки безпеки при експлуатації електроустановок» і «Правила техніки безпеки при експлуатації електроустановок споживачів».

Недотримання правил безпеки і необережне поводження з електротехнічним устаткуванням може привести до тяжких наслідків і навіть до смертельних результатів.

Завдання техніки безпеки полягають в створенні таких умов роботи на об'єкті монтажу, при яких забезпечується високопродуктивна праця монтажного персоналу і повністю унеможливлюється травм.

Адміністрація монтажних організацій повинна забезпечувати систематичний контроль за дотриманням електромонтажниками правил безпеки, застосуванням запобіжних пристосувань, спецодягу і інших засобів індивідуального захисту. Посадові особи, що не забезпечили виконання цих вимог, притягуються в установленому порядку до адміністративної або кримінальної відповідальності згідно чинному законодавству.

Електрозахисні засоби і засоби індивідуального захисту, використовувані при будівельно-монтажних роботах (діелектричні рукавички, покажчики напруги, інструмент з ізолюючими рукоятками, запобіжні пояси, каски і тому подібне)

повинні відповідати вимогам державних стандартів і «Правил застосування і випробування засобів захисту, використовуваних в електроустановках».

Робочі і службовці електромонтажних організацій допускаються до виконання робіт тільки після проходження ввідного інструктажа (загального) і інструктажа на робочому місці (виробничого) по техніці безпеки. Всі електромонтажники повинні пройти курсове навчання по техніці безпеки і спеціальне технічне навчання. Навчання проводиться адміністрацією по типових програмах. Відповідальність за своєчасність, повноту і правильність навчання по техніці безпеки несе керівник монтажної ділянки, організації, підприємства. Після закінчення навчання кваліфікаційна комісія приймає іспит і привласнює навчаним відповідну кваліфікаційну групу по електробезпеці.

До персоналу, що вмонтовує електроустановки, пред'являються особливі вимоги. При прийомі на роботу по монтажу електроустановок той, що поступає обов'язково проходить медичний огляд в поліклініці.

Во уникнення травматичних випадків адміністрація монтажної організації зобов'язана приймати заходи для їх попередження.

До них відносяться:

• своєчасна і належна підготовка фронту робіт;

• забезпечення електромонтажників справним індивідуальним і бригадним монтажним інструментом, пристосуваннями і устаткуванням;

• надання в розпорядження електромонтажників справних і перевірених засобів механізації і електрифікованого інструменту;

• забезпечення електромонтажників своєчасно випробуваними і перевіреними засобами захисту і спецодягом, відповідними характеру їх роботи, напрузі електроустановки, умовам навколишнього середовища;

• надійна огорожа робочих місць;

• забезпечення стандартними плакатами по техніці безпеки, вказуючими місце безпечної роботи, такими, що забороняють або вирішують виробництво робіт, застережливими про небезпеку поразки електричним струмом;

• забезпечення об'єкту монтажу відповідними засобами для роботи на висоті (ліси, підмости, сходи, драбини, підйомники і так далі);

• подача до місця монтажу електричної мережі напругою 12 або 36 В, якщо за умовами роботи або навколишнього середовища використовувати електроустаткування

вищої напруги небезпечно для життя людей або заборонене відповідними правилами або інструкціями;

• інструктаж електромонтажників на робочому місці;

• перевірка знань персоналом правил техніки безпеки і вимог пожежної безпеки.

5.2 Заходи безпеки при роботі на висоті

Роботи, при виконанні яких електромонтажник знаходиться вищим 1,5 м від поверхні робочого наздогнала, перекриття або грунту, називаються роботами на висоті.

До роботи на висоті допускаються особи не молодше 18 років, що пройшли медичний огляд, навчання вимогам безпеки праці, що отримали спеціальне посвідчення.

Особи, допущені до роботи на висоті, проходять медичний огляд щорічно.

Електромонтажні роботи на висоті можна проводити з лісів або подмостей з настилами шириною не менше 1 м, що мають надійну огорожу у вигляді поручнів заввишки не менше 1 м, а також із справних драбин і приставних сходів. Розсувні

сходи-драбини повинні мати пристрої, які унеможливлюють їх мимовільного розсовування. Приставні сходи, що встановлюються в місцях руху транспорту або людей, захищають або охороняють.

У необхідних випадках працювати на висоті можна з необгороджених поверхонь або з постійно укріплених сходів, але з обов'язковим застосуванням перевірених і випробуваних запобіжних поясів.

Запобіжні пояси мають бути забезпечені паспортами і бирками. Користуватися поясами, на які немає паспортів, забороняється. Карабін запобіжного поясу повинен мати міцну замикаючу пружину. Застосовувати карабіни із слабкою або зламаною замикаючою пружиною не допускається. Запобіжні пояси через кожних 6 міс. випробовують на статичне навантаження 30 Н протягом 5 мин. При роботі з приставних сходів

і драбин прикріплятися до них запобіжними поясами забороняється.

Забороняється працювати зі сходів і драбин біля працюючих машин, устаткування і над ними, а також поблизу токоведущих частин, що знаходяться під напругою і не захищених від випадкового дотику до них. При необхідності роботи в таких місцях машини і устаткування мають бути відключені, а токоведущие частини відключені і заземлені.

Для перенесення і зберігання інструментів, метизів, настановних елементів особи, що працюють на висоті, мають бути забезпечені індивідуальними сумками або інструментальними ящиками.

При виконанні робіт на висоті забороняється підніматися і опускатися по тросах і канатах, користуватися для цієї мети підйомними монтажними механізмами, переходити по незакріплених конструкціях і працювати на них, а також перелазити через огорожі і сідати на них.

Забороняється підкидання яких-небудь предметів для подачі що працює вгорі. Інструменти, матеріали і інші предмети необхідно подавати за допомогою мотузка, до середини якої їх прив'язують. Другий кінець мотузка повинен знаходитися в руках у працівника, що стоїть внизу, який утримує предмети, що піднімаються, від розгойдування.

У разі ожеледі, сильного вітру (більше шести балів), снігопаду або дощу монтажні роботи на висоті на відкритому повітрі припиняють.

5.3 Техніка безпеки при роботі на комп'ютері

5.3.1 Вимоги безпеки перед початком роботи

Перед початком роботи слід переконатися в справності електропроводки, вимикачів, штепсельних розеток, за допомогою яких устаткування включається в мережу, наявності заземлення комп'ютера, його працездатності

5.3.2 Вимоги безпеки під час роботи

Для зниження або запобігання впливу небезпечних і шкідливих чинників необхідно дотримувати: санітарні правила і норми, гігієнічні вимоги до відеодисплейних терміналів, персональних електронно-обчислювальних машин і організації роботи. Щоб уникнути пошкодження ізоляції проводів і виникнення коротких замикань не вирішується: вішати що-небудь на дроти, закрашувати і білити шнури і дроти, закладати дроти і шнури за газові і водопровідні труби, за батареї опалювальної системи, висмикувати штепсельну вилку з розетки за шнур, зусилля має бути докладене до корпусу вилки.

Для виключення поразки електричним струмом забороняється: часто включати і вимикати комп'ютер без необхідності, торкатися до екрану і до тильної сторони блоків комп'ютера, працювати на засобах обчислювальної техніки і периферійному устаткуванні мокрими руками, працювати на засобах обчислювальної техніки і периферійному устаткуванні, що мають порушення цілісності корпусу, порушення ізоляції проводів, несправну індикацію включення живлення, з ознаками електричної напруги на корпусі, класти на засоби обчислювальної техніки і периферійному устаткуванні сторонні предмети.

Забороняється під напругою очищати від пилу і забруднення электрооборудование.

Забороняється перевіряти працездатність електроустаткування в непристосованих для експлуатації приміщеннях із струмопровідними підлогами, сирих, не дозволяючих заземлити доступні металеві частини.

Неприпустимо під напругою проводити ремонт засобів обчислювальної техніки і перифейного устаткування. Ремонт електроапаратури проводиться тільки фахівцями-технікою з дотриманням необхідних технічних вимог.

Щоб уникнути поразки електричним струмом, при користуванні електроприладами не можна стосуватися одночасно яких-небудь трубопроводів, батарей опалювання, металевих конструкцій, сполучених із землею.

При користуванні элетроэнергии в сирих приміщеннях дотримуватися особливої обережності.

5.3.3 Вимоги безпеки в аварійних ситуаціях

При виявленні несправності негайно знеструмити електроустаткування, оповістити адміністрацію. Продовження роботи можливе тільки після усунення несправності.

При виявленні дроту, що обірвався, необхідно негайно повідомити про це адміністрації, прийняти заходи по виключенню контакту з ним людей. Дотик до дроту небезпечно для життя.

У всіх випадках поразки людини електричним струмом негайно викликають лікаря. До прибуття лікаря потрібно, не втрачаючи часу, приступити до надання першої допомоги постраждавшему.

Штучне дихання ураженому електричним струмом проводиться аж до прибуття лікаря.

На робочому місці забороняється мати вогненебезпечні речовини

У приміщеннях забороняється:

а) запалювати вогонь;

б) включати електроустаткування, якщо в приміщенні пахне газом;

в) палити;

г) сушити що-небудь на опалювальних приладах;

д) закривати вентиляційні отвори в електроапаратурі

Джерелами займання є:

а) іскра при розряді статичної електрики

б) іскри від электроборудования

в) іскри від удару і тертя

г) відкрите полум'я

При виникненні пожароопасной ситуації або пожежі персонал повинен негайно прийняти необхідні заходи для його ліквідації, одночасно оповістити про пожежу адміністрацію.

Приміщення з электроборудованием мають бути оснащені вогнегасниками типу ОУ-2 або ОУБ-3.

5.3.4 Вимоги безпеки після закінчення роботи

Після закінчення роботи необхідно знеструмити всі засоби обчислювальної техніки і периферійне устаткування. У разі безперервного виробничого процесу необхідно залишити включеними тільки необхідне устаткування.

5.3.5 Вимоги до персоналу, що експлуатує засоби обчислювальної техніки і периферійне устаткування:

До самостійної експлуатації електроапаратури допускається тільки спеціально навчений персонал не молодше 18 років, придатний за станом здоров'я і кваліфікації до виконання вказаних робіт.

Перед допуском до роботи персонал повинен пройти ввідний і первинний інструктаж по техніці безпеки з показом безпечних і раціональних примемов роботи. Потім не рідше за один раз в 6 мес проводиться повторний інструктаж, можливо, з групою співробітників однакової професії в складі не більше 20 чоловік. Позаплановий інструктаж проводиться при зміні правив по охороні праці, при виявленні порушень персоналом інструкції після техніки безпеки, зміни характеру роботи персоналу.

В приміщеннях, в яких постояннно експлуатується електроустаткування мають бути вивішені в доступному для персоналу місці ?Инструкции по техніці безопасности|, в яких також мають бути визначені дії персоналу у разі виникнення аварій, пожеж, електротравм.

Керівники структурних підрозділів несуть відповідальність за організацію правильної і безпечної експлуатації засобів обчислювальної техніки і периферійного устаткування, ефективність їх використання; здійснюють контроль за виконанням персоналом вимог справжньої інструкції по техніці безпеки.

5.4 Види небезпечних і шкідливих чинників

Що експлуатує засоби обчислювальної техніки і периферійне устаткування персонал може піддаватися небезпечним і шкідливим дії, які за природою дії підрозділяються на наступні групи:

поразка електричним струмом

механічні пошкодження

електромагнітне випромінювання

інфрачервоне випромінювання

небезпека пожежі

підвищений рівень шуму і вібрації

5.5 Вимоги електробезпеки

При користуванні засобами обчислювальної техніки і периферійним устаткуванням кожен працівник винен уважно і обережно поводитися з електропроводкою, приладами і апаратами і завжди пам'ятати, що зневага правилами безпеки загрожує і здоров'ю, і життю людини

Щоб уникнути поразки електричним струмом необхідно твердо знати і виконувати наступні правила безпечного користування електроенергією:

1. Необхідно постійно стежити на своєму робочому місці за справним станом електропроводки, вимикачів, штепсельних розеток, за допомогою яких устаткування включається в мережу, і заземлення. При виявленні несправності негайно знеструмити електроустаткування, оповістити адміністрацію. Продовження роботи можливе тільки після усунення несправності.

2. Щоб уникнути пошкодження ізоляції проводів і виникнення коротких замикань не вирішується:

а) вішати що-небудь на дроти;

б) закрашувати і білити шнури і дроти;

в) закладати дроти і шнури за газові і водопровідні труби, за батареї опалювальної системи;

г) висмикувати штепсельну вилку з розетки за шнур, зусилля має бути докладене до корпусу вилки.

3. Для виключення поразки електричним струмом забороняється:

а) часто включати і вимикати комп'ютер без необхідності;

б) торкатися до екрану і до тильної сторони блоків комп'ютера;

в) працювати на засобах обчислювальної техніки і периферійному устаткуванні мокрими руками;

г) працювати на засобах обчислювальної техніки і периферійному устаткуванні, що мають порушення цілісності корпусу, порушення ізоляції проводів, несправну індикацію включення живлення, з ознаками електричної напруги на корпусі

д) класти на засоби обчислювальної техніки і периферійному устаткуванні сторонні предмети.

3. Забороняється під напругою очищати від пилу і забруднення электроообоpудование.

4. Забороняється перевіряти працездатність електроустаткування в непристосованих для експлуатації приміщеннях із струмопровідними підлогами, сирих, не дозволяючих заземлити доступні металеві частини.

5. Ремонт електроапаратури проводиться тільки фахівцями-технікою з дотриманням необхідних технічних вимог.

6. Неприпустимо під напругою проводити ремонт засобів обчислювальної техніки і перифейного устаткування.

7. Щоб уникнути поразки електричним струмом, при користуванні електроприладами не можна стосуватися одночасно яких-небудь трубопроводів, батарей опалювання, металевих конструкцій, сполучених із землею.

8. При користуванні элетроэнергией в сирих приміщеннях дотримуватися особливої обережності.

9. При виявленні дроту, що обірвався, необхідно негайно повідомити про це адміністрації, прийняти заходи по виключенню контакту з ним людей. Дотик до дроту небезпечно для життя.

10. Порятунок постраждавшего при поразці електричним струмом головним чином залежить від швидкості звільнення його від дії струмом.

У всіх випадках поразки людини електричним струмом негайно викликають лікаря. До прибуття лікаря потрібно, не втрачаючи часу, приступити до надання першої допомоги постраждавшему.

Необхідно негайно почати проводити штучне дихання, найбільш ефективним з яких є метод (рот в рот) або (рот в ніс) а також зовнішній масаж серця.

Штучне дихання ураженому електричним струмом проводиться аж до прибуття лікаря.

5.6 Вимоги по забезпеченню пожежної безпеки

На робочому місці забороняється мати вогненебезпечні речовини

У приміщеннях забороняється:

а) запалювати вогонь;

б) включати електроустаткування, якщо в приміщенні пахне газом;

в) палити;

г) сушити що-небудь на опалювальних приладах;

д) закривати вентиляційні отвори в електроапаратурі

Джерелами займання є:

а) іскра при розряді статичної електрики

б) іскри від электроборудования

в) іскри від удару і тертя

г) відкрите полум'я

При виникненні пожароопасной ситуації або пожежі персонал повинен негайно прийняти необхідні заходи для його ліквідації, одночасно оповістити про пожежу адміністрацію.

Приміщення з электроборудованием мають бути оснащені вогнегасниками типу ОУ-2 або ОУБ-3.

5.7 Санітарно-гігієнічні норми при роботі на ПК

Численні користувачі персональних комп'ютерів часто забувають, а деколи і просто не знають про те, що тривала робота за комп'ютером негативно позначається на багатьох функціях нашого організму:

вищій нервовій діяльності

ендокринній, імунній і репродуктивній системах

на зорі і кістково-м'язовому апараті людини

Що це може означати для простої людини?

І чи можна від цього захиститися?

Найбільша шкода здоров'ю користувача наносять пристрої введення-виводу: монітор, клавіатура, миша.

Комп'ютер є джерелом:

електростатичного поля

електромагнітних випромінювань в низькочастотному, наднизькочастотному і високочастотному діапазонах (2 Гц - 400 кГц)

випромінювання оптичного діапазону (ультрафіолетового, інфрачервоного і видимого світла)

рентгенівського випромінювання

Електромагнітне випромінювання несприятливо діє на зір, викликає зниження працездатності, головні болі. Тому відстань від імені людини до монітора має бути не менше 60-70 див. Електростатичне поле сприяє осіданню пилу і аерозольних частинок на обличчі, шиї, руках, що може викликати у людей, особливо чутливих до подібної дії негативні шкірні реакції – сухість, алергію.

ЖК-мониторы можна назвати майже «зеленими» пристроями, що зберігають здоров'я людей. Без особливих побоювань за здоров'я з ними можуть працювати і жінки, і діти.

Нерухома і напружена поза оператора, протягом тривалого часу прикованого до екрану монітора, приводить до втоми і виникнення болів в озвоночнике, шиї, плечових суглобах.

Під час роботи за комп'ютером необхідно дотримувати правильну поставу.

Основні вимоги до конструкції крісла: воно повинне забезпечувати рівномірність розподілу сил тяжіння частин тіла на опорні поверхні для уникнення статичної напруги великих м'язових груп і хребетного стовпа.

Інтенсивна робота з клавіатурою викликає больові відчуття в ліктьових суглобах, предплечьях, зап'ястях, в кистях і пальцях рук.

Основний блок клавіш на клавіатурі розбитий на дві частини, розгорнені таким чином, що користувачеві хочеш не хочеш доводиться розсовувати руки і розставляти лікті. Фірмою Microsoft розроблена ергономічна клавіатура, яка своєрідною конструкцією покликана понизити навантаження на руки.

5.8 Правильне положення за комп'ютером

Приміщення під час роботи з комп'ютером має бути добре освітлене. Освітлення в приміщеннях ПК має бути змішаним: природним, - за рахунок сонячного світла, - і штучним. Забороняється робота з комп'ютером в темному або напівтемному приміщенні!

Хоча картина дії комп'ютерів на організм людини, описана вище, виглядає досить похмурою, потрібно пам'ятати, що подібні наслідки можливі лише у разі абсолютного ігнорування мерів безпеки і гігієнічних норм.

Профілактичні і оздоровчі методики і технології дозволять звести до мінімуму негативну дію комп'ютера на Ваше здоров'я, зробити роботу на ПК приємним і увлекательным заняттям. Сьогодні це вже можливо!

Висновки

Була спроектована система комплексної безпеки заданого об'єкту. Аналіз можливих погроз і методів їх запобігання показав, як правильно організувати систему безпеки для захисту від подібних погроз. Були вибрані види технічних засобів і варіанти їх застосувань. Також були побудовані графіки вірогідності виявлення порушника, які підтвердили ефективність вибраного плану захисту.

Було ухвалено рішення реалізувати інтегровану систему безпеки, оскільки вона дає можливість об'єднання в себе всіх підсистем безпеки і реалізує новий рівень в зручності установки і експлуатації цих систем, новий рівень захищеності об'єкту і недоступні раніше інтелектуальні засоби ПОС, СКУД і відеоспостереження.

Був проведений аналіз трьох подібних систем, розроблені критерії вибору ІСБ. На основі цих критеріїв була вибрана найбільш відповідна для даного об'єкту система.

Узявши цю систему за основу, були підібрані компоненти ПОС і СКУД. Був обгрунтований вибір використання системи цифрового відеоспостереження і підібраний комплекс мережевих відеокамер. А також вибрана система автоматичного керування пожежосасінням.

Останнім кроком стало економічній обгрунтування створення системи безпеки на основі технічних засобів охорони. Створення такої системи виявилося обгрунтованим і з економічної точки зору і з погляду нових функціональних можливостей, що підвищують загальний рівень захищеності об'єкту.

СПИСОК ЛІТЕРАТУРИ

1. Системи технічної безпеки: актуальні реалії (http://www.video-control.ru/surveillance_systems.html)

2. Розподілений апаратний інтелект - наступний ступінь в еволюції систем відеоспостереження (http://www.secnews.ru/articles/7512.htm)

3. SecurityNews (http://www.secnews.ru/)

4. IP-видеонаблюдение: переваги і недоліки (http://www.visionpro.ru/art97)

5. Охоронні системи. Інформаційне видання. Випуск 4, М., «Солон», 2018 р.

6. Гавріш В. Практіческоє посібник із захисту комерційної таємниці. Симфе рополь. «Тавріда». 2018 р.

7. Підприємництво і безпека. М., Універсум. 2018 р.

8. Алексєєнко С. Н., Сокольський Б. Е. Системи захисту комерційних объек тов. Технічні засоби захисту. М., 2018 р.

9. Бізнес і безпека. М., КМЦ «Центуріон». 2018 р.

10. Кисельов А. Е. і ін. Комерційна безпека. М., Іноро Арт. 2019 р.

11. Технічні засоби охорони, безпеки і сигналізації. Довідник. BIMI, 2019 р.

12. Никулін О. Ю., Петрушин А. Н. Системи телевізійного спостереження. М., «ОБЕРЕГ-РБ», 2019г.

13. Рейці Ч. Д. 55 електронних схем сигналізації. М., Енергоатоміздат, 2017 р.

14. Андріанов Ст. І., Соколів А. В. Охранниє пристрої для автомобілів. «Лань» Спб. 2017 р.

15. Винограду Ю. А. Електронная охорона (елементи і вузли охоронних систем). М., «СИМВОЛ-Р», 2017г.

16.N. V. P. R. Durga Prasad, T. Lakshminarayana, et al., “Automatic Control and Management of lectrostatic Precipitator”, IEEE Transactions on Industry Applications, pp. 561-567, Vol. 35, No. 3, May/June, 1999.

17.Ralf Joost and Ralf Salomon. “Advantages of fpga-based multiprocessor systems in industrial applications”. In 31st Annual Conference of the IEEE Industrial Electronics Society (IECON 2005). IEEE-I ECON, November 2017.

18.Hyman, Anthony. Charles Babbage, pioneer of the computer. — Oxford University Press, 2014.

19. Randell, Brian. The Origins of Digital Computers: Selected Papers.. — 2018.