**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

Факультет аеронавігації, електроніки та телекомунікацій

Кафедра телекомунікаційних та радіоелектронних систем

**ДОПУСТИТИ ДО ЗАХИСТУ**

Завідувач кафедри

\_\_\_\_\_\_\_\_\_проф. Г.Ф. Конахович

“ \_\_\_\_ ” \_\_\_\_\_\_\_\_\_\_2020 р.

**ДИПЛОМНА РОБОТА**

**(ПОЯСНЮВАЛЬНА ЗАПИСКА)**

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЮ

**«МАГІСТР»**

**Тема:** Система охоронного відеоспостереження розумного будинку

**Розробив:** А.І. Заморій

**Керівник:** М.Ю. Заліський

**Консультанти з розділів:**

**Охорона праці** І.В.Якимець

**Охорона навколишнього середовища** І.М.Горбач

**Нормоконтролер з ЄСКД (ЄСПД)** М.М. Малоєд

**Київ 2020**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

Кафедра телекомунікаційних та радіоелектронних систем

Спеціальність 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Апаратура радіозв’язку, радіомовлення і телебачення»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_проф. В.М. Васильєв

“ \_\_\_\_ ” \_\_\_\_\_\_\_\_\_\_2019 р.

**ЗАВДАННЯ**

**на виконання дипломної роботи студента**

ЗАМОРІЙ АНДРІЯ ІГОРОВИЧА

1. **Тема проекту**: Система охоронного відеоспостереження розумного будинку, затверджено наказом ректора від «\_\_» \_\_\_\_\_\_\_\_\_ 2020 р. № \_\_\_\_\_\_\_\_.

2. **Термін виконання роботи**: з 25 жовтня 2019 р. по 3 лютого 2020 р.

3. **Вихідні дані до роботи**:

План-схема будинку.

Принципи функціонування "Розумного будинку".

Відеоспостереження за фасадом та внутрішніми приміщеннями.

Живлення від джерела змінного струму 220В 50Гц.

Відеоархівація не менше 24 год.

Дубляж відеоархіву.

4. **Зміст розрахунково-пояснювальної записки**:

(перелік розроблюваних питань):

Аналіз принципів побудови систем відеоспостереження.

Проектування системи відеоспостереження.

Експлуатація системи відеоспостереження.

Охорона праці

Охорона навколишнього середовища

5. **Перелік графічного матеріалу**:

(із зазначенням обов’язкових креслень)

Структурна схема системи відеоспостереження.

Графічні зображення компонентів системи відеоспостереження.

Графічні пояснення до розрахунків параметрів системи відеоспостереження.

6. **Консультанти проекту**

|  |  |  |  |
| --- | --- | --- | --- |
| **Розділ** | **Консультант** | **Підпис, дата** | |
| **Завдання видав** | **Завдання прийняв** |
| Охорона праці | І.В.Якимець |  |  |
| Охорона навколишнього середовища | І.М.Горбач |  |  |

7. **Дата видачі завдання** «25» жовтня 2019 р.

Керівник М.Ю. Заліський

Завдання прийняв до виконання А.І. Заморій

**КАЛЕНДАРНИЙ ПЛАН**

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **п/п** | **Найменування етапів роботи** | **Термін виконання етапів роботи** | **Примітка** |
| 1 | Ознайомлення з тематикою дипломних робіт. Вибір теми | 25.10.19 |  |
| 2 | Обробка матеріалів за темою дипломної роботи: журнали, Інтернет, науково-технічні джерела | 01.11.19 |  |
| 3 | Виконання першого розділу | 10.11.19 |  |
| 4 | Виконання другого розділу | 28.11.19 |  |
| 5 | Виконання третього розділу | 13.12.19 |  |
| 6 | Виконання четвертого розділу | 10.01.20 |  |
| 7 | Питання охорони праці та навколишнього середовища | 15.01.20 |  |
| 8 | Графічний матеріал | 20.01.20 |  |
| 9 | Оформлення електронного варіанту ПЗ та графічного матеріалу до ПЗ | 24.01.20 |  |
| 10 | Подання на кафедру  Усунення недоліків  Оформлення пояснювальної записки | 29.01.20 |  |
| 11 | Електронна версія доповіді, ілюстративний матеріал доповіді | 03.02.20 |  |

Студент-дипломник А.І. Заморій

Керівник роботи  М.Ю.Заліський

УДК 656.7.075

*Заморій А.І.* Система охоронного відеоспостереження розумного будинку / Керівник доц. М.Ю. Заліський, кафедра телекомунікаційних та радіоелектронних систем. Національний авіаційний університет. − К.: НАУ, 2019.

У пояснювальній записці до дипломної роботи наведений аналіз інтелектуальних систем "Розумний будинок" в частині проектування та експлуатації підсистем охоронного відеоспостереження. Виконано обгрунтування та розрахунок компонентів системи, розроблено структурну схему.

Розглянуті питання технічної експлуатації систем відеоспостереження, охорони праці та навколишнього середовища.

Стор. 100, рис. 38, табл. 5, список літ.: 19 джерел

**ЗМІСТ**

[СПИСОК ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ **Ошибка! Закладка не определена.**](#_Toc30786323)

[ВСТУП 8](#_Toc30786324)

[1. ІНТЕЛЕКТУАЛЬНА СИСТЕМА РОЗУМНИЙ БУДИНОК 10](#_Toc30786325)

[1.1. Загальні принципи побудови системи «Розумний будинок» 10](#_Toc30786326)

[1.2. Структура системи «Розумний будинок» 12](#_Toc30786327)

[1.3. Система відеоспостереження та контролю доступу 20](#_Toc30786328)

[1.4. Система охоронно-пожежної сигналізації 23](#_Toc30786329)

[1.5. Підсистема GSM-моніторингу 27](#_Toc30786330)

[2. ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ РОЗУМНОГО БУДИНКУ 29](#_Toc30786331)

[2.1. Структура систем відеоспостереження 29](#_Toc30786332)

[2.2. Типи відеокамер відеоспостереження 31](#_Toc30786333)

[2.3. Обладненя системи відеоспостереження 37](#_Toc30786334)

[2.4. Надійність і рівні ризику впливу для виділених загроз Розумного   
будинку 40](#_Toc30786335)

[3. РОЗРОБКА ПРОЕКТУ СИСТЕМИ ОХОРОННОГО ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ РОЗУМНОГО БУДИНКУ 46](#_Toc30786336)

[3.1. Аналіз об’єкту охорони 46](#_Toc30786337)

[3.2. Розробка структури системи відеоспостереження 49](#_Toc30786338)

[3.3. Розрахунки характеристик відеокамер 51](#_Toc30786339)

[3.4. Розробка схеми розташування відеокамер із зонами огляду 61](#_Toc30786340)

[3.5. Проектування системи відеозапису 63](#_Toc30786341)

[3.6. Засоби захисту системи відеоспостереження 65](#_Toc30786342)

[4. ЕКСПЛУАТАЦІЯ СИСТЕМИ ОХОРОННОГО ВІДЕОСПОСТЕРЕЖЕННЯ РОЗУМНОГО БУДИНКУ 67](#_Toc30786343)

[4.1. Правові аспекти використання системи відеоспостереження 67](#_Toc30786344)

[4.2. Технічне обслуговування систем відеоспостереження 68](#_Toc30786345)

[4.3. Регламент обслуговування системи відеоспостереження 70](#_Toc30786346)

[5. ОХОРОНА ПРАЦІ 71](#_Toc30786347)

[5.1 Вступ 71](#_Toc30786348)

[5.2. Небезпечні і шкідливі чинники що діють на суб’єкта 72](#_Toc30786349)

[5.3 Організаційні та конструктивно-технологічні заходи для зниження впливу шкідливих виробничих факторів ескплуатації РЕА, а також ЕОМ 74](#_Toc30786350)

[5.4. Забезпечення пожежної та вибухової безпеки при обслуговуванні електричного обладнання ЕОМ та РЕА 82](#_Toc30786351)

[5.5. Висновок 85](#_Toc30786352)

[6. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА 86](#_Toc30786353)

[6.1. Вступ 86](#_Toc30786354)

[6.2. Законодавча база охорони навколишнього середовища 87](#_Toc30786355)

[6.3. Влив випромінювання оптичного діапазону 89](#_Toc30786356)

[6.4. Лазерне випромінювання 94](#_Toc30786357)

[6.5. Висновки 97](#_Toc30786358)

[ВИСНОВКИ 98](#_Toc30786359)

[ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 99](#_Toc30786360)

**СПИСОК ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ**

ВДТ - Візуальні дисплейні термінали

ЕОП - Електронно оптичний перетворювач

ІКД - Інфрачервоне випромінювання

ЛЕП - Лінії електропередачі

НВЧ - Надвисокі частоти

ОНС - Охорона навколишнього середовища

ОПС – Охоронно-пожежна сигналізація

ОС – Система охоронної сигналізації

ПАТ – Пункт автономної охорони

ПК – Пристрої кінцеві

ПЗ - Програмне забезпечення

ПЗЗ - Прилад із зарядним зв'язком

ППК – Приймально-контрольний прилад

ПЦО – Пункт централізованої охорони

ПЦС – Пульт централізованого спостереження

РЕА - Радіоелектронна апаратура

СКД – Системи контролю доступу

СО – Система охорони

СПС – Система передачі сповіщень

СТЗ - Скриті технічні засоби

ТВЛ - Телевізійні вертикальні лінії

ТО - Технічне обслуговування

УФ - Ультрафіолетові промені

ШС – Шлейф охоронної сигналізації

**ВСТУП**

На сьогодні, питання безпеки будинку є дуже актуальним як і для жителів великих міст, так і для тих, хто проживає далеко за містом. Саме тому існує велика кількість різних елементів, що дозволяють створити безпеку у будинку. Завдяки технічному прогресу, сьогодні реально об‘єднати всі ці компоненти в єдину систему. Саме для таких випадків вже винайдено систему «Розумний будинок», яка захищає будинок не лише від непрошених гостей, а й запобігає виникненню неприємних ситуацій, які можуть створити небезпеку для життя та здоров’я людини. При цьому задачею даної системи є не просто забезпечення безпеки людини під час виникнення небезпечних ситуацій, а функціонування системи безпеки у тандемі зі злагодженою роботою усіх служб, що забезпечують комфортне проживання.

Призначення комплексу «Розумного будинку» являє собою такі основні пункти як: дистанційний контроль управління роботою обладнання інженерних систем; побудова єдиного середовища обміну даними систем контролю і управління; отримання оперативної інформації про стан і параметри обладнання систем; реєстрація створення архіву технологічних процесів і дій експлуатаційних служб; скорочення витрат; підвищення надійності та безпеки

Останній пункт розглянемо детальніше. Система «Розумний будинок» включає в себе сукупність датчиків: руху, освітлення, температури, клімату, вологи та інші. Вона передбачає розумний сенсорний пульт, за допомогою якого ви можете дистанційно моніторити і керувати роботою обладнання. Завдяки сенсорам, що розташовані по периметру усього жилого простору помешкання, система «розумний дім» отримує інформацію про стан жилого приміщення у даний момент часу. Саме це є важливим фактором, тому що при зміні стану помешкання появі надзвичайної ситуації, чи яких-небудь небезпек, система може миттєво відреагувати (затримка реагування коливається в межах сотні пікосекунд) і попередити наслідки завдання шкоди помешканню чи життю та здоров‘ю людей, що знаходяться в цей момент в приміщенні. Загалом, система «Розумний будинок» включає в себе: контролер (керуючий пристрій, що з‘єднує всі елементи системи один з одним, а також із зовнішнім світом); датчики (пристрої, що отримують інформацію); актюатори (виконуючі пристрої, що виконують команди).

Автоматика може попередити про дуже велику кількість неприємних ситуацій, навіть таких, як капітальний ремонт, через затоплення водою, або пожежу через витік газу. Система безпеки може вести спостереження за вашими близькими, родичами літнього віку чи маленькими дітьми.

У «Розумному будинку» присутня пожежна система, що у своєму складі має датчики визначення диму, пропану, вуглекислого газу, тепла і багатьох інших речовин. Автоматика допомагає людям вийти з приміщення, автоматично зупинить проникнення кисню в середину приміщення, перекриває всі вентиляційні входи та виходи (при чому, система вентиляції автоматично вимикається), система автоматично відключить електроживлення, подачу газу в дім, проінформує власника про виникнення небезпечної ситуації, якщо його немає вдома.

Тому об’єктом дипломного проектування є процес убезпечення системи «Розумний будинок», а предметом є розробка системи відеоспостереження сигналізації приватного будинку.

**1. ІНТЕЛЕКТУАЛЬНА СИСТЕМА РОЗУМНИЙ БУДИНОК**

### 1.1. Загальні принципи побудови системи «Розумний будинок»

Розумний дім (розумний будинок/ smart home, digital house) – будинок, дача або приміщення комерційного призначення (бутік, офіс, будь-яка установа), які мають якісні системи забезпечення та операційний multi-room. За допомогою останнього, функціонально пов’язуються між собою усі електроприлади будівлі, якими можна керувати централізовано – з пульта-дисплею. Прилади можуть бути під’єднані до комп’ютерної мережі, що дозволяє керувати ними за допомогою персонального комп’ютера (ПК) та надає віддалений доступ до них через Інтернет. Завдяки інтеграції інформаційних технологій у домашні умови, усі системи та прилади узгоджують виконання функцій між собою, порівнюючи задані програми та зовнішні показники (обстановки) [1; 2].

Розумний дім створюється за допомогою професійного [проектування](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F) та [програмування](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F) компаніями, що займаються розробкою проектів smart-home. Програми, що вводяться до алгоритмів multi-room розумного дому, розраховані на певні потреби мешканців та ситуації, пов'язані із зміною середовища або безпекою. Особливістю smart-home є керування з пульта, на котрому людина може натиснути одну-єдину клавішу з метою створення певної обстановки. При цьому, сама система мульти-рум аналізує навколишню ситуацію та параметри усередині приміщення, та, керуючись власними висновками, виконує задані користувачем команди із відповідними налаштуваннями. Окрім того, електронні [побутові прилади](https://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D0%B1%D1%83%D1%82%D0%BE%D0%B2%D1%96_%D0%BF%D1%80%D0%B8%D0%BB%D0%B0%D0%B4%D0%B8), встановлені у розумному будинку, можуть бути об'єднані у домашню [Universal Plug'n’Play](https://uk.wikipedia.org/wiki/UPnP)-мережу із виходом в Інтернет, як це наведено на рис. 1.1.



Рис. 1.1. Керування «Розумним будинком» за допомогою гаджету

Розумні будинки, як і більшість досягнень сучасної техніки, початково з’явилися на сторінках фантастичних оповідань. Але втілюватись ідея почала лише у ХХ-му сторіччі після широкого введення електрики у будівлях і розвитку інформаційних технологій. Перше повідомлення про віддалені прилади контролю можна віднести до розробки Ніколою Тесла дистанційного керування судами та транспортними засобами у 1898 році.

Електричні побутові прилади почали з’являтись між 1915 та 1920 рр. І одразу продемонстрували готовність суспільства замінити роботу домашнього персоналу дешевими механічними пристроями. Правда на той час, проблема енергозбереження при використанні нових технологій ще вирішена не була. Тому, певний час, новітні технологій були доступні лише дуже заможним людям.

Ідеї більш розвинені до понять сучасних систем автоматизації будинку були продемонстровані на ярмарках у Чикаго (1934) та Нью-Йорку. У «великому яблуці» трохи пізніше (1964-65), представили плани електрофікованих та автоматизованих приміщень. У решті-решт перший серйозний аналог розумного дому з'явився у 1966 році. Це була експериментальна система домашньої автоматизації – «домашній комп'ютер Эхо IV». Його винахідник – Джим Сазерленд. Його технологія була приватним, некомерційним проектом. Перші «дротові будинки» були зведені американськими винахідниками-любителями у 1960-х, але вони були суттєво обмежені можливостями тогочасних технологій.

Уперше термін «Розумний будинок» був вигаданий Американською Асоціацією Housebuilders у 1984 році. Із винаходом мікроконтроллерів, вартість на електроприлади швидко падала. Ця ж установа зазначила, що таке помешкання відмінне від звичайного своєю здатністю забезпечувати продуктивне та ефективне використання робочого та житлового середовища.

За цим, віддалені інтелектуальні технології керування були прийняті будівельною промисловістю, яка поступово почала вводити їх не лише у бізнес установах, але і у домашніх помешканнях. Під час активної домашньої автоматизації 90-х років інформатика та телевізійні системи були поєднані для підтримки інтелектуальних можливостей приміщень. У 1995 році винахідники технологій Java оголосили одним із основних призначень даної технології – «збільшення інтелекту побутових приладів».

Сьогодні технології дозволяють збирати домашню автоматику покомпонентно: обирати лише ті функції розумного будинку, які дійсно потрібні користувачу. Тепер новітні технології керування приміщенням з'являються щодня. Навіть речі, котрі раніше розглядалися лише як красиві предмети інтер'єру тепер можуть виконувати ряд мультимедійних або побутових функцій.

### 1.2. Структура системи «Розумний будинок»

Майже у кожній літературі, тим або іншим боком що відноситься до «Розумного Будинку», наводиться хитромудра картинка. На ній зазвичай зображують котедж в розрізі, з тією або іншою мірою деталізації інженерних нутрощів. До цих нутрощів ведуть стрілки з різними поясненнями, наприклад, "управління освітленням", "управління кліматом", "охоронна сигналізація", "захист від протікань", "управління воротами" і так далі. Тим самим уся сукупність можливих додатків домашньої автоматизації підрозділяється на окремі складові частини - системи, кожна з яких може розглядатися і функціонувати значною мірою автономно, тобто сама по собі, але при цьому усі вони можуть контролюватися і управлятися за допомогою єдиного комплексу технічних засобів, в т.ч. і через Інтернет. Типова ілюстрація системи «Розумний будинок» показана на рис. 1.2.



Рис. 1.2. Типова ілюстрація до поняття "Розумний Будинок"

Залежно від складності завдань, концепції розробника, потреби замовника і можливостей використовуваної технічної платформи ділення на складові частини може бути різним [3]. Проте склалася загальноприйнята класифікація базових систем, згідно який виділяються:

1. Системи управління освітленням.

2. HVAC (Heating, Ventillation and Air Conditioning) – системи опалювання, вентиляції і кондиціонування.

3. Мультирум – системи управління аудіо-відео апаратурою.

4. Системи безпеки – домофон, відеоспостереження, кодові замки, охоронна і пожежна сигналізація, системи контролю витоків газу і протікань води і так далі.

Загальними для цих систем є комунікації, пристрої, що управляють, а також засоби відображення інформації і введення команд, що управляють. При цьому можливо і взаємовплив систем, що вимагає погодженого управління ними. Наприклад, система управління освітленням може бути пов'язана з системою управління жалюзі, а система управління кліматом може розглядатися як об'єднання декількох підсистем - управління опалюванням, вентиляцією, кондиціонуванням, відкриттям вікон і контролю внутрішніх і зовнішніх кліматичних параметрів.

В цілому, багато хто з цих систем був відомий ще до приходу ери "Розумного Будинку" і були включені в загальну концепцію вже пізніше, з розвитком техніки дистанційного контролю і управління, про яку говорилося у введенні. Але, слід сказати, інтеграція вже існуючих систем в загальну концепцію комплексної домашньої автоматизації не була простим приєднанням і несла багато нового. Одна тільки можливість бачити на екрані комп'ютера або смартфону стан і параметри усіх домашніх інженерних систем сама по собі великий плюс, не кажучи вже про підвищення зручності взаємодії людини з цими системами і оптимізації їх роботи.

Розглянемо більш детальніше систему управління освітленістю.

У простому виді завдання управління освітленням зводиться до можливості включення-виключення і контролю стану джерел світла з декількох місць. Наприклад, при виході з будинку перевірити, чи не залишилося десь щось включеним і вимкнути те, що не треба, або вимкнути взагалі все одним натисненням кнопки. При вході ж навпаки - відразу включити світло, де потрібно, щоб не спотикатися в темряві. У більшості випадків саме така перша потреба, що відчувається, пов'язана з "розумним будинком". Власне, приблизно цю задачу вирішували перші системи смарт-будинку. У більше просунутому варіанті система управління світлом передбачає управління загальним режимом освітлення - регулювання яскравості і включення заданої комбінації джерел світла. Взагалі кажучи, регулятори яскравості ламп - діммери, існують і застосовуються давно і самі по собі, без всяких претензій на смарт-будинок.

Домашня ж автоматика привносить сюди ту ж можливість дистанційного керування із заданих місць в квартирі, а також можливість включення одним натисненням заданого сценарію освітлення: включити те на 100%, це - на 50%, а решта - вимкнути. У максимальних варіантах управління світлом передбачає ряд автоматичних функцій, наприклад: автоматичне виключення або приглушення світла за відсутності кого-небудь в приміщенні, для чого потрібно спеціальні датчики присутності; автоматичне регулювання освітлення залежно від рівня природної освітленості, для чого також потрібно відповідні датчики; погоджене управління світильниками і жалюзі. Крім того, просунуті системи передбачають можливість налаштування і активації натисненням кнопки, якою-небудь подією або за часом різних сценаріїв – "відбій", "підйом", "нікого немає удома", "прийом гостей", і ін., надаючи необмежений простір фантазіям мешканців.

Типова схема управління освітленням наведена на рис. 1.3, 1.4.

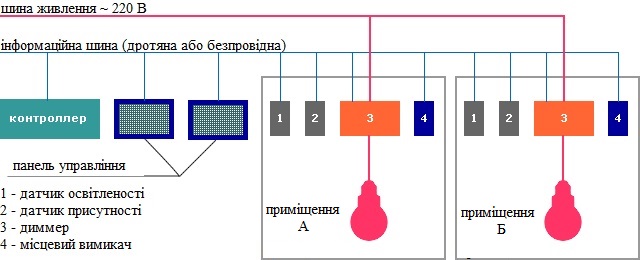


Рис. 1.3. Типова схема управління освітленням



Рис. 1.4. Екран системи управління освітленням фірми Sensio

Стосовно клімат-контролю він же HVAC призначений для контролю і підтримки заданих кліматичних параметрів в житлових і підсобних приміщеннях при одночасному забезпеченні необхідного об'єму вентиляції. У більшості випадків обмежуються температурою і вологістю повітря, але в особливо просунутих варіантах до них може додаватися ще запилена і міра іонізації, в т.ч. кількість озону. Клімат-контроль (рис. 1.5, 1.6) – найбільш значима і відповідальна система "Розумного будинку". Від неї залежить не лише комфорт і здоров'я мешканців, але і витрата енергоресурсів.

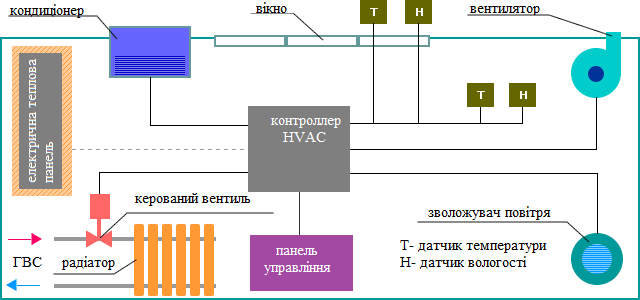


Рис. 1.5. Можливий варіант системи климат-контролю



Рис. 1.6. Екран системи климат-контролю фірми Crerstron

Для управління кліматом потрібно відповідне технічне забезпечення – система припливно-витяжної вентиляції, кондиціонери, електричні регулятори подання теплоносія в радіатори опалювання, зволожувачі, приводу для вікон і кватирок, повітряні фільтри, іонізатори, маса всяких датчиків і ін. В простому випадку використовується стандартна електрична HVAC-система з нагрівачем, охолоджувачем і вентилятором і один датчик температура.

Алгоритми управління при цьому не прості, оскільки все в цій мішанині взаємопов’язано. Проте, сучасні HVAC-системи дозволяють підтримувати задані параметри не лише в цілому по будинку, але і по окремих зонах, в т.ч відповідно до заданих сценаріїв. Наприклад, в заданий час перед сном в спальні може автоматично робитися провітрювання, температура з настанням ночі – знижуватися, забезпечуючи міцний і здоровий сон, а до ранку піти на підвищення. За відсутності мешканців опалювання з метою економії можна приглушити до заданої межі, а до їх появи запустити в штатному режимі.

Втім, є і скромніші варіанти. Серед домашніх умільців дуже популярні саморобні домашні метеостанції, що вимірюють кліматичні параметри в потрібних зонах квартири і за її межами. Заміряти температуру і вологість в різних кімнатах і за вікном, відобразити для загального огляду, та ще отримати графіки зміни по днях і годиннику вже саме по собі велика справа. А відкривати або закривати кватирки і вентилі не забороняється і вручну.

Однією з підсистем «Розумного будинку» є мультирум.

Мультирум (multiroom - мульти-комнатный) – комплекс, що об'єднує усі домашні мультимедійні (тобто аудіо-відео) пристрої, дозволяє з будь-кого, оснащеної ним кімнати діставати доступ до каналів радіо- і телемовлення, домашнім колекціям музики, фільмів, фотографій, а також до мультимедійного вмісту Інтернету.

Будинок, оснащений мультирум-системою, нагадує зореліт. Кожна кімната в нім, як каюта члена екіпажа, оснащена акустичною системою, вбудованою в стіни або в стелю, відеоекраном або відеопроектором і пультом управління. Десь в коморі-радіорубці знаходиться мультимедиа сервер, тобто комп'ютерний системний блок, до якого підключені різноманітні джерела аудіо-відео графічної інформації: різні тюнери і ресівери, приймаючі ефірні або кабельні теле- і радіопрограми, відеоплеєри, відеомагнітофони, сканери, і т.д. На ньому ж зберігаються бібліотеки аудіо- і відеозаписів, фотоархіви і інший мультимедійний матеріал. Легким рухом руки у своїй кімнаті можна відкрити глобальне меню і запустити на вибір улюблений хіт улюбленої співачки, або супутниковий канал, футбольний матч, ролик з Ютуба і так далі. Можливий варіант системи мультирума показано на рис. 1.7, 1.8.

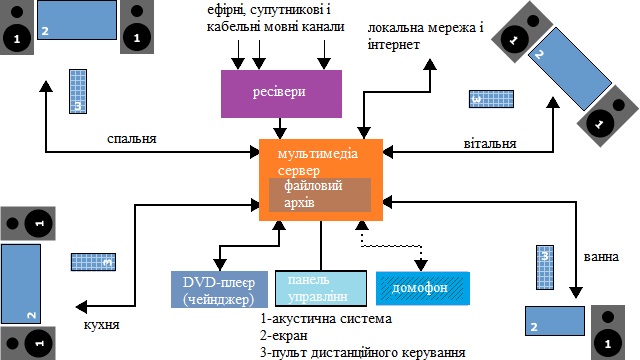


Рис. 1.7. Можливий варіант системи мультирума



Рис. 1.8. Екран мультирума фірми Opus

Взагалі-то в примітивному виді ця потреба відчувається в кожному будинку, оскільки телевізорів зараз менше двох-трьох вже немає ні у кого, але плеєр можна підключити тільки до одного, супутниковий канал у кращому разі до двох, але від одного провайдера, а вийти на ютуб можна тільки з комп'ютера, але з нього не можна вийти на кабельне ТБ, і так далі і ін. Мультирум вирішує усі ці завдання, забезпечуючи взаємодію все зі всим, навіть з домофоном.

Розглянемо систему безпеки «Розумного будинку».

Системи безпеки (рис. 1.9, 1.10) – найважливіші компоненти сучасного помешкання. Раніше, квартири ставили на охорону ще в застійний часи, обважуючи усі вікна і двері датчиками, купою дротів і підключаючи усе це до телефону. В основному, подавало неправдиву тривогу – то кватирка відійде, то дріт десь обірветься, то хазяїн, повернувшись додому, забуде зняти сигналізацію з контролю. Зараз датчики стали досконалішими, можуть не лише фіксувати відкриття вікон і дверей, але і переміщення по квартирі непізнаних об'єктів, теплове випромінювання тіл і ін. І можна зовсім без дротів - все по радіо, як телефонна трубка. При цьому до функцій виявлення і попередження несанкціонованого доступу додалися ще і функції виявлення і парирування катастрофічних ситуацій – пожежі, витоку газу і затоплення.

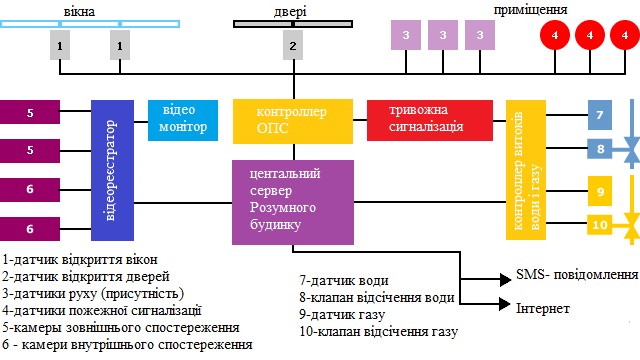


Рис. 1.9. Можливий варіант системи безпеки

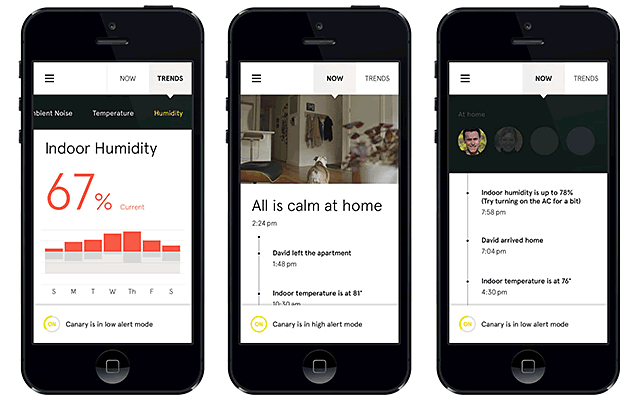


Рис. 1.10. Моніторинг стану системі «Розумний будинок »на екрані смартфона

Sentri Smart Home Security інформує через смартфон про значення вологості і температури у будинку, присутності або відсутності членів сім'ї і інших параметрах. All is calm at home - удома все спокійно.

Як і інші системи, розглянуті вище, системи безпеки застосовувалися і можуть застосовуватися самі по собі, без прив'язки до "розумного будинку". Включення їх в загальну схему інтелектуального житла обумовлене, напевно, тим, що ці системи з часом сильно "порозумнішали", та і можливість стеження за безпекою за допомогою єдиного комплексу засобів відображення інформації "розумного будинку" теж дуже актуальна.

Інші підсистеми «Розумного будинку».

Sentri Smart Home Security інформує через смартфон про значення Окрім розглянутих вище можуть зустрічатися і завдання, що не належать до якої-небудь категорії. Наприклад, просто управляти яким-небудь автономним об'єктом домашнього господарства і отримувати інформацію про його стан. Це може бути вхідна хвіртка або ворота вашої залізобетонної огорожі, жалюзі у вашій кімнаті або по усій квартирі, вентиляція, що не увійшла до системи HVAC, система водопостачання, система каналізації, системи управління поливом, фонтанами і ілюмінацією саду або оранжереї і так далі і ін. Залежно від міри взаємодії з іншими елементами будинку таке управління може розглядається або як самостійний, або як один з функція який-небудь система, куди в якості елемент входить керований об'єкт. Міра "суверенітету" тут визначається різними чинниками, включаючи загальноприйняту практику, точку зору розробника або замовника і так далі.

Часто до систем "Розумного Будинку" зараховують і систему телефонного зв'язку, який може передбачати наявність домашньої МІНІ-АТС, в т.ч. з виходом на різні канали, включаючи інтернет-телефонію, а також домашню локальну комп'ютерну мережу з організацією доступу в Інтернет. Сюди ж іноді відносять і різне новомодне "кібернетичне начиння" - роботи-пилососи, інтелектуальні холодильники і інше хитромудре господарство з претензією на технології "Розумних Речей" і "Інтернету Речей".

### 1.3. Система відеоспостереження та контролю доступу

Відеоспостереження дає можливість бачити в режимі реального часу все, що відбувається у будинку і на присадибній території. Це сучасний і ефективний метод відвертання незаконних проникнень і контролю за діями недоброчесних відвідувачів або співробітників. Встановивши систему відеоспостереження, без зусиль можна вичислити грабіжника і довести його вину. Адже при цьому вже є підтвердження [4].

Комплексні рішення для систем безпеки Розумний будинок завжди включають відеоспостереження. Це дозволяє відстежувати переміщення персоналу, видалено стежити за тим, чим зайняті діти, контролювати пересування зловмисника при його проникненні на територію і т. п. Завдяки цьому управління усіма подіями в Розумному будинку знаходиться в руках власника. При проектуванні охоронної системи враховується можливість отримання сигналу з усіх камер на потрібний певний пристрій (ПК, сенсорну панель, iPhone і інші). Зображення, отримане з камери, поступає на відеореєстратор, який обробляє дані і виводить зображення на монітор. При цьому уся інформація записується на захищений накопичувач. Камери і мережеве сховище підключені до мережі Ethernet і є повноцінною частиною "розумного будинку". Дані, що зберігаються на мережевому накопичувачі, можна переглядати через спеціальне застосування у мобільному пристрої. При цьому можна ретельно вивчити архівні дані або упізнати стан справ у будинку в режимі online.

Система відеоспостереження «Розумний будинок» може бути запрограмований таким чином, що запис почнеться за декілька секунд до проникнення зловмисника на територію. Ця функція реалізується за рахунок установки датчиків руху. Несанкціоноване вторгнення супроводжується поданням звукового сигналу тривоги і повідомленням на пульт служби швидкого реагування.

В усіх системах відеоспостереження «Розумного будинку» зберігаються в захищеному місці, на мережевому накопичувачі. Записи будуть у безпеці: ні зловмисники, ні недобросовісний персонал не зможуть їх видалити.

Висока якість запису системи відеоспостереження «Розумного будинку» забезпечує видимість осіб зловмисників, номерів автомобілів і багатьох інших деталей. Крім того, отримаемо не лише цифрове зображення, але і запис звуку. Можна встановити обмеження на перегляд даних залежно від рівня доступу.

Стосовно систем контролю доступу (СКД), то вони широко використовуються в даний час. Такі системи встановлюють банки, компанії, заводи, бази відпочинку, митниці та ін. СКД дає широкий спектр можливостей з ведення обліку робочого часу і контролю персоналу, проводити контроль заїзду та виїзду автомобільної техніки на об'єкт, а також дозволяє організувати якісний пропускний режим в приміщення, будівлі, робочі зони і т.п.

Системи контролю доступу можуть бути як простими (відкриття-закриття дверей для певного кола осіб) так і більш складними з інтелектуальними функціями (зчитування відбитків пальців, номерів автомобілів, та ін.).



Рис. 1.11. Біометрична СКД по відбитку пальця

Виконавши установку СКД можна:

– автоматизувати контроль над персоналом, його пересуванням і місцезнаходженням;

– відслідковувати відвідувачів;

– розмежовувати доступ персоналу;

– контролювати заїзд і виїзд автомобілів;

Системи контролю доступу і відеоспостереження можна поєднати. Дані системи мають можливість інтегруватися в загальну систему безпеки. Тобто, можливо поєднати відеоспостереження, охоронну та пожежну сигналізацію разом з системою контролю доступу в одну єдину систему безпеки, і всі ці підсистеми будуть працювати спільно, дозволяючи проводити повний моніторинг і охорону Вашого «Розумного будинку».

Стосовно обмеження доступу в приміщення, то СКД побудовані на основі різних електронних замків, зчитувачів, терміналів доступу, контролерів і т.д. Головною їх функцією є обмеження доступу сторонніх осіб до приміщення. При цьому доступ в приміщення здійснюється за допомогою порівняння пред'явленого ключа з базою даних. Ключем в даному випадку можуть виступати: код доступу, безконтактна картка, відбиток пальця і ін. Причому є можливість розмежувати права доступу між окремими особами або групами осіб в контрольовані приміщення або зони.

### 1.4. Система охоронно-пожежної сигналізації

Система охоронної сигналізації (ОС) – це сукупність взаємопов'язаних технічних засобів для виявлення ознак знаходження порушника на охоронюваних об'єктах, збору, обробки, передачі та подання в заданому вигляді інформації споживачам. У функції системи охоронно-пожежної сигналізації (ОПС) входить виявлення як проникнення, так і ознак пожежі на об'єкті. Технічні засоби (ТЗ) ОПС відповідно до ГОСТ 26 342-84 класифікуються за двома ознаками: області застосування і функціональним призначенням.

По області застосування ТЗ підрозділяються на охоронні та охоронно-пожарние.По функціональним призначенням ТЗ поділяються на дві групи:

а) ТЗ виявлення (сповіщувачі), призначені для формування та передачі інформації про стан контрольованих параметрів;

б) ТЗ оповіщення, призначені для прийому, перетворення, передачі, зберігання, обробки і відображення інформації (системи передачі сповіщень, ППК, оповіщувачі).

Сповіщувачем називається первинне технічний засіб для виявлення зміни середовища (проникнення, пожежі) і форматування сповіщення: охоронного, пожежного або обох - охоронного і пожежного.

Сповіщений в техніці ОПВ називається повідомлення, несе інформацію про стан об'єкту, що охороняється, переданого за допомогою електричних, світлових і (або) звукових сигналів. Повідомлення розділяються на тривожні і службові. Тривожне сповіщення несе інформацію про проникнення або пожежі. Службове сповіщення містить інформацію про взятті під охорону, знятті з охорони, несправності апаратури та ін.

Типова структура системи ОПС показана на рис. 1.12.

Шлейф охоронної сигналізації (ШС) – це електричний ланцюг, що з'єднує вихідні ланцюги охоронних сповіщувачів, що включає в себе допоміжні (виносні) елементи (діоди, резистори) і сполучні прилади, призначені для видачі на приймально-контрольний прилад сповіщень про проникнення, пожежу або несправність. У деяких випадках передбачається через шлейф подача електроживлення на сповіщувачі [5 – 8].

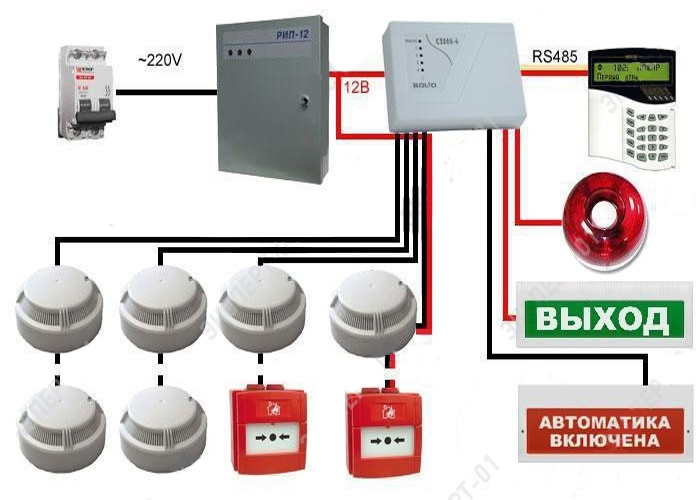


Рис. 1.12. Система охоронно-пожежної сигналізації

Приймально-контрольний прилад (ППК) служить для прийому сигналу від сповіщувачів, обробки його і передачі в зручному вигляді або на центральний пульт, або далі в інший приймально-контрольний прилад.

Охоронно-пожежний оповіщувач - це технічний засіб ОПС, призначене для оповіщення людей про проникнення, спробу проникнення і (або) пожежу.

Система автономної охорони складається з комплексів ОПС з виходом на оповіщувачі і (або) інший ППК, встановлюваний в пункті автономної охорони.

Пункт автономної охорони (ПАТ) – це пункт, розташований на об'єкті, що охороняється в безпосередній близькості від нього, обслуговується службою охорони об'єкту і обладнаний технічними засобами відображення інформації про проникнення і пожежу в кожному з контрольованих приміщень (зон) об'єкта для безпосереднього сприйняття людиною.

Система передачі сповіщень (СПС) – це сукупність спільно діючих технічних засобів, для передачі по каналах зв'язку і приймання в пункті централізованої охорони сповіщень про проникнення на охоронні об'єкти і пожежу на них службових і контрольно-діагностичних повідомлень, а також для передачі і прийому команд телеуправління (за наявності зворотного каналу). СПС передбачає установку пристроїв кінцевих (ПК) на об'єктах, ретрансляторів (Р) на кросах АТС, в житлових будинках та інших проміжних пунктах і пультів централізованого спостереження (ПЦС) в пунктах централізованої охорони.

Пункт централізованої охорони (ПЦО) – це диспетчерський пункт централізованої охорони ряду розосереджених об'єктів від проникнення і пожежі з використанням СПИ.

Залежно від характеристик ГО (протяжність, кількість приміщень, поверховість тощо) і величини матеріальних цінностей, розміщених на об'єкті, його охорона може бути реалізована за допомогою одного або декількох шлейфів сигналізації. У тому випадку, якщо структура охорони об'єкта включає кілька шлейфів, розміщених таким чином, що при проникненні на ГО порушника та рух до матеріальних цінностей, йому необхідно подолати кілька охоронюваних зон, контрольованих різними шлейфами з виходами на окремі номери ПЦН, охорону слід розглядати як многорубежную. Таким чином, шлейф або сукупність шлейфів, контролюючих охоронювані зони на шляху руху порушника до матеріальних цінностей ГО, які мають вихід на окремий номер ПЦН, називається кордоном сигналізації, а сукупність охоронюваних зон, контрольованих кордоном сигналізації, являє собою рубіж охорони. Розглянемо конструкції системи ОПС. Комплекс ОПС по захисту будівель включає в себе:

а) первинні датчики, які безпосередньо здійснюють контроль відведеної території;

б) контролер (контрольна панель), що збирає і аналізує показники датчиків, а також керуючий всієї охоронної системою і виробляє її відповідну реакцію на можливі нештатні ситуації;

в) пульт управління (клавіатура), призначений для постановки приміщення на охорону і зняття з неї.

Існує кілька видів первинних датчиків системи ОПС – залежно від конкретної ситуації можуть застосовуватися ті чи інші пристрої, а також групи пристроїв, контролюючих одну і ту ж територію за різними параметрами. Почнемо з найпоширеніших.

Відповідно до ГОСТ 26342-84 охоронно-пожежні сповіщувачі класифікуються за такими параметрами:

1. За призначенням: для закритих приміщень, для відкритих майданчиків та периметрів об'єктів.

2. По виду зони, контрольованої сповіщувачем: точкові, лінійні, поверхневі, об'ємні.

3. За принципом дії охоронні сповіщувачі поділяються на: обьеміческіе, магнітоконтактні, ударноконтактние, п'єзоелектричні, ємнісні, ультразвукові, оптико-електронні, радіохвильові, комбіновані.

4. За кількістю зон виявлення: Однозонна, багатозонні.

5. За дальності дії ультразвукові, оптико-електронні та радіохвильові охоронні сповіщувачі для закритих приміщень поділяються на: малої дальності – до 12 м, середньої дальності – від 12 до 30 м, великої дальності – понад 30 м.

6. За дальністю дії оптико-електронні та радіохвильові охоронні сповіщувачі для відкритих майданчиків та периметрів об'єктів поділяються на: малої дальності – до 50 м, середньої дальності – від 50 до 200 м, великої дальності – понад 200 м.

7. За конструктивним виконанням ультразвукові, оптико-електронні та радіохвильові охоронні сповіщувачі поділяються на: однопозиційні передавач (випромінювач) і приймач поєднані в одному блоці (може бути декілька передавачів та приймачів в одному блоці) двохпозиційні передавач (випромінювач) і приймач виконані у вигляді окремих блоків, багатопозиційні - більше двох блоків у будь-якій комбінації. За способом електроживлення поділяються на: токонепотребляющіе (використовується «сухий» контакт); живляться від ШС, від внутрішнього автономного джерела живлення, від зовнішнього джерела постійного струму напругою 12-24 В, від мережі змінного струму напругою 220 В; Охоронно-пожежні сповіщувачі за принципом дії поділяються на: магнітоконтактні, ультразвукові та оптико-електронні. За кількістю зон виявлення, дальності дії і конструктивним виконанням охоронно-пожежні сповіщувачі класифікуються аналогічно охоронним сповіщувачем.

Розрахунок здійснюємо за даними таблиць зводу правил 5.13130.2009" Системи протипожежного захисту.

Площа, що контролюється одним точковим димовим пожежним сповіщувачем, а також максимальна відстань між сповіщувачами і сповіщувачем і стіною необхідно визначати по таблиці 1, але, не перевищуючи величин, зазначених у технічних умовах і паспортах на сповіщувачі.

Площа, що контролюється одним точковим тепловим пожежним сповіщувачем, а також максимальна відстань між сповіщувачами і сповіщувачем і стіною визначається за таблицями.

Розрахунок кількості пожежних сповіщувачів на площу розраховується за формулою (1):

 (1);

де Sпом – площа приміщення; hп.п – середня площа контрольована одним сповіщувачем.

### 1.5. Підсистема GSM-моніторингу

Система "Розумний Будинок" – унікальний багатофункціональний інструмент, призначений для контролю і управління електроустаткуванням. Вона складається з безлічі модулів. Але одним з найбільш значимих компонентів є GSM/GPS сигналізація (рис. 1.13). Її наявність дозволить власникові житла покидати будинок на будь-який період, не турбуючись про збереження і цілісність майна. У разі ЧП користувач зможе отримати відповідне сповіщення на мобільний пристрій або електронну пошту, знаходячись як на сусідній вулиці, так і в протилежній точці земної кулі. Вказана сигналізація не обмежується тільки можливістю відправки повідомлень при сторонньому доступі. Її опції великі:

– підключення і відключення вентиляційної системи;

– включення/виключення і налаштування приладів опалювання;

– активація протипожежних пристосувань;

– перекриття електропостачання; прослуховування об'єкту;

– блокування вхідних дверей і вікон;

– безперервний моніторинг за допомогою WEB- камер і інше.



Рис. 1.13. GSM-моніторинг

Розглянемо собливості функціонування GSM- сигналізації.

Алгоритм роботи цього модуля є цілком простим і зрозумілим. На території підконтрольного об'єкту монтуються групи датчиків. Це можуть бути контролери температури, руху, вібрацій, задимленості. При активації датчиків сигнали поступають на охоронний пункт і на мобільний телефон. Існує два типи GSM- сигналізацій - дротяні і безпровідні. Перші відрізняються складністю підключення. Для їх монтажу треба складати індивідуальний проект по прокладенню кабелю. Ключовими перевагами дротяних моделей є висока швидкість відгуку і чіткі сигнали. Передача інформації здійснюється в певних радіодіапазонах. Полягають GSM- сигналізації з декількох важливих блоків. Сюди відносяться центральний модуль, що приймає сигнали з усіх датчиків, контроллери, розміщені в різних місцях, оповісники (сирени і блималки, ліхтарі і прожекторы), функціональні пристрої (блокують).

**2. ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ РОЗУМНОГО БУДИНКУ**

### 2.1. Структура систем відеоспостереження

Основними компонентами систем мережевого відеоспостереження є мережева камера, відеокодер або відеосервер (застосовується для підключення аналогових камер), мережа, сервер і система зберігання, а також програмне забезпечення (далі – ПЗ) для управління системою відеоспостереження і запису відеоінформації. Мережеві камери і відеокодери створені на базі цифрових (комп'ютерних) технологій, тому вони володіють можливостями, недоступними аналоговим камерам. Мережа, системи зберігання та сервери - 12.03.01.2018.438 ПЗ 37 Лист стандартне IT – обладнання. Здатність використовувати звичайне мережеве обладнання – одне з головних переваг мережевого відео. Типова структурна схема системи відеоспостереження представлена на рис. 2.1.

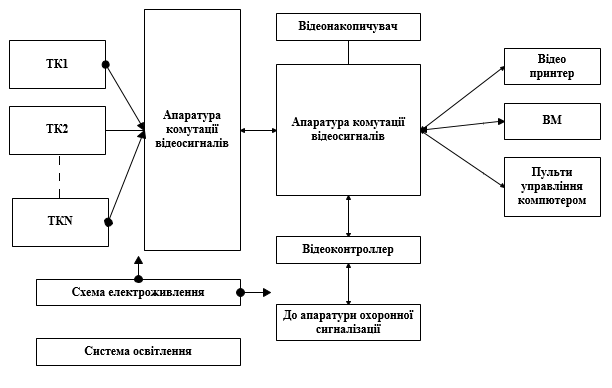


Рис 2.1 Типова структурна схема системи відеоспостереження

Система складається з наступних основних елементів:

– мережеві камери, які встановлюються на віддалених об'єктах, причому на об'єкті можна встановити 1 або кілька камер, в залежності від розміру об'єкта;

– центральний сервер, на якому встановлено ПЗ для централізованого управління моніторингу усіма камерами, а також для запису інформації, одержуваної з камер;

– опціонально можна встановити додаткові комп'ютери в регіонах, наприклад, для локального спостереження за об'єктом. 12.03.01.2018.438 ПЗ 38 Лист Завдання, які дозволяє вирішити дана система:

– централізоване спостереження за декількома об'єктами в режимі реального часу з можливістю одночасного запису зображення на мережеве сховище;

– централізоване спостереження за роботою співробітників в філіях (офісах, магазинах, на складах), які віддалені від центрального офісу на сотні і тисячі кілометрів;

– можливість централізованої запису відео за тривожним сигналом або в постійному режимі;

– повідомлення по телефону або на e-Mail при тривожному подію;

– можливість підключення віддалених робочих місць для перегляду відео, а також перегляд відео з мобільного телефону (смартфону).

Принцип їх дії полягає в тому, що такі камери виробляють захоплення, стиснення у формати MPEG-2, MPEG-4, M-JPEG, і після цього здійснюють передачу зі швидкістю до тридцяти зображень в секунду живого зображення по мережі. IP-камери дають можливість авторизованим користувачам отримувати і переглядати дані зображення, обробляти інформацію, аналізувати її і зберігати.

При підключенні камери їй присвоюється IP-адреса, тобто вона володіє можливостями веб-сервера, FTP-сервера, FTP-клієнта, SMTP-клієнта - можливість передачі інформації за допомогою електронної пошти, обробки сигналів тривоги і програмування. IP-камера з мережі може передавати не тільки відеозображення, а й іншу інформацію, таку як оцифрований звук, повідомлення про тривогу або ж виявленні руху. Також, за допомогою камер можна отримати необхідні дані для можливості напряму їх в потрібну сторону. Це стосується поворотних камер. Для нашого об'єкта структурна схема представлена на рис. 2.2.

Система відеоспостереження складається з 10 купольних камер, 4 з яких знаходяться на вулиці і займаються зйомкою входу в офіс і парковки, 6 камер розташовані в офісних приміщеннях. Як канал зв'язку використовується фольгована вита пара FTP. Сигнал від камер по кручений парі надходить на мережевий комунікатор.

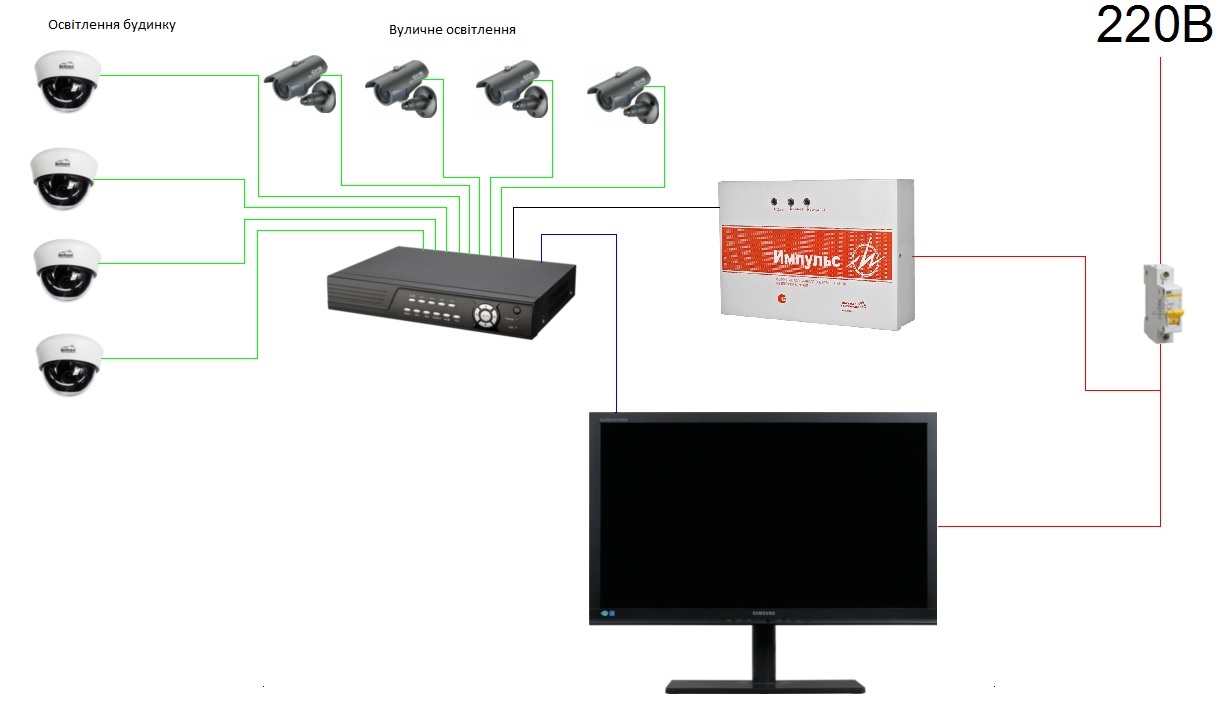


Рис. 2.2. Структурна схема системи відеоспостереження.

З мережевого комунікатора інформація надходить на комп'ютер оператора. Оператор на моніторі може переглядати запис з камер, як в реальному часі, так і з архіву. На комп'ютері оператора є два жорсткі диски ємністю по 4 Тб, на які йде запис зі всіх камер відеоспостереження, а також проводиться резервне копіювання, що забезпечує більшу безпеку. Обсяг жорстких дисків дозволяє зберігати архіви відеозаписів до півроку. Коли жорсткий диск повністю заповнюється, відбувається автоматичне видалення найперших відеозаписів. Також зі свого робочого місця оператор може задавати розклад записи відеокамер. При необхідності зйомку в реальному часі можна включити на мобільному телефоні або іншому комп'ютері.

### 2.2. Типи відеокамер відеоспостереження

Існують наступні типи відеокамер:

1) модульні;

2) мініатюрні;

3) купольні;

4) корпусні;

5) гіростабілізованого.

Модульні камери, вони ж безкорпусні камери відеоспостереження представляють собою плату з закріпленим на ній об'єктивом (рис 2.3).



Рис. 2.3. Зовнішній вигляд модульної камери

Така конструкція одночасно може вважатися і перевагою, і недоліком моделі. З одного боку, модульні камери можна встановлювати в корпус або термокожух потрібної конфігурації або використовувати для прихованого відеоспостереження завдяки маленьким розмірам. З іншого боку, електроніка і оптика камери нічим не захищені і не можуть протистояти негативним впливів середовища або людини при використанні їх в якості самостійний елемент системи спостереження.

Параметри і функціональні можливості відеокамер пріоритетно визначаються:

– матрицею;

– схемою обробки сигналу;

– об'єктивом.

Всі ці компоненти в бескорпусном виконанні присутні, а значить, по характеристикам такі камери потенційно нічим не поступаються іншим видам. Цілком можливо може виникнути питання про доцільність додаткових робіт по збірці, герметизації та ін. Справа в тому, що іноді немає можливості підібрати готовий виріб, відповідне сукупності вимог до технічних характеристик і дизайну. Крім того, при виході з ладу модуля його заміна обійдеться дешевше, оскільки досягається економія на придбанні кожуха. А при пошкодженні останнього відсутня необхідність покупки електронної частини. Можна також розглянути питання меншою безболісності модернізації, при наявності необхідності, з яких-небудь причин, зміни характеристик в кращу сторону.

Природно, не можна скидати з рахунків можливість забезпечення прихованої установки бескорпусной камери, оскільки невеликі розміри модуля дозволяють зробити це досить просто.

Основні характеристики модульних відеокамер:

– модульні камери можуть мати кольорову або монохромну матрицю, як правило, 1/3-дюймову. Вони забезпечують запис відео в досить високому дозволі. Для недорогих пристроїв цей показник становить близько 420 ТВЛ, для більш дорогих - 700 ТВЛ;

– світлочутливість також буде відрізнятися в залежності від цінової категорії обладнання, починаючи від 0,1 Люкс, закінчуючи 0,005 Люкс;

– камери працюють в режимі день / ніч. Для реалізації такої можливості, як правило, встановлюються цифрові інфрачервоні (далі – ІЧ) фільтри;

– найчастіше оснащуються фіксованим об'єктивом з фокусом 2,8 або 3,6 мм;

– діапазон робочих температур від –10 до +50.

Мініатюрні камери мають маленькими розмірами, нерідко використовуються в будівлях і для прихованого спостереження, мають квадратний або циліндричний корпус (рис. 2.4).



Рис 2.4. Зовнішній вигляд мініатюрної камери

Міні камери мають такі переваги:

– мають маленькі розміри, що дозволяє вести приховане спостереження, так як помітити міні камеру дуже складно;

– мініатюрні камери рідко піддаються руйнувань з боку вандалів.

Єдиним недоліком мініатюрних відеокамер спостереження є їх нездатність вести професійне відеоспостереження, де дуже важливі точність передачі кольору і якісна оптика. В цьому відношенні вони значно поступаються звичайним відеокамер. Також варто звернути увагу, що в законодавстві деяких країн передбачена відповідальність за ведення прихованого відеоспостереження, про що також не можна забувати.

Купольні відеокамери на сьогоднішній день є одним з найбільш затребуваних приладів на ринку відеоспостереження. головним позитивним атрибутом цієї відеокамери є багатофункціональність і зовнішня непримітність.

Купольні камери – це камери мають корпус у вигляді півсфери (рис. 2.5, 2.6). Корпус може бути виконаний як з пластика, так і з металу. Під другому випадку, камера вважається антивандальной. основною перевагою купольних відеокамер – це неочевидно для спостережуваного, напрямок огляду відеокамери. Під основним прозорим куполом розташовується другий, як правило, чорного кольору, рідше сріблястого.



Рис.2.5. Зовнішній вигляд купольної камери



Рис 2.6. Зовнішній вигляд купольної поворотної камери

Купольні камери діляться на поворотні і стаціонарні. Поворотні камери відеоспостереження, крім параметрів, властивих іншим камерам, характеризуються:

– величиною кута обертання в горизонтальній і вертикальній площинах;

– швидкістю повороту;

– діапазоном фотографії із близької відстані;

– наявністю певної кількості попередніх (фіксованих кутів повороту, значень фокусної відстані).

Купольні відеокамери так само поділяються на кілька видів:

– купольні відеокамери з фіксованим об'єктивом і не мають можливості регулювання фокусної відстані, тобто фокусна відстань задано один раз, і воно є незмінним;

– купольні відеокамери з варіофокальним об'єктивом, тобто об'єктив з фокусною відстанню, змінним вручну - це особливо зручно, коли немає достовірних даних, про те в яких умовах буде використовуватися відеокамера, тобто на якій відстані буде перебувати об'єкт для спостереження.

Варіофокальний об'єктив зазвичай налаштовують один раз при монтажі відеокамери і в подальшому вже не коригують настройки. Зазвичай в купольні камери встановлюється варіофокальний об'єктив з фокусною відстанню 4-9 мм або 2,8-12 мм.

Якщо купольна камера встановлюється в приміщенні, то кріпиться на стелю таким чином, щоб підстава камери знаходилося паралельно підлозі (Горизонтально), якщо на вулиці - то на стіні будівлі, огорожі або опорі за допомогою спеціального кронштейна, що зберігає горизонтальне положення основи.

За своїми функціональними особливостями купольні пристрої можуть бути:

– з кольоровою матрицею;

– монохромні;

– з можливістю запису звуку;

– з наявністю ІК підсвічування. ІК підсвічування дозволяє бачити спостережуваний об'єкт в повній темряві. У відеокамерах з ІК підсвічуванням може бути встановлений механічний ІК фільтр або електронна ІК корекція.

У системах відеоспостереження корпусні камери займають одну з лідируючих позицій. У ряді випадків вони можуть не комплектуватися об'єктивами, мережевими адаптерами або кронштейнами.

Вуличні відеокамери оснащуються як вбудованими, так і змінними об'єктивами. Останній варіант більш затребуваний в професійних системах безпеки. Установка різних об'єктивів дає можливість підібрати оптимальний варіант для різних завдань, виходячи з характеристик конкретного об'єкта.

У більшості випадків корпусні камера відеоспостереження комплектується приладом із зарядовим зв'язком (далі – ПЗЗ-матриця) високої чутливості. Це сприяє отриманню детального відеоряду контрольованого об'єкта. Більшість камер має досить широкі функціональні можливості. Система настройки дозволяє змінити наступні параметри в автоматичному або ручному режимі:

– шумозаглушення;

– маскування;

– детекция руху;

– компенсація фонової засвітки і інших.

Таким чином вдається легко налаштувати камери в залежності від ситуації. Корпусні відеокамера, як правило, призначена для установки в закритих опалювальних приміщеннях. Однак, відеокамера, вміщена в спеціальний термокожух, отримує захист від попадання вологи, пилу і може бути встановлена на вулиці. За рахунок цього можна без проблем здійснювати відеомоніторинг при самих несприятливих погодних умовах.

Функціональні деталі відеокамери, розміщеної в захисному термокожух, що не можуть бути пошкоджені агресивними впливами зовнішнього середовища.

Зовнішній вигляд корпусних камери представлений на рис. 2.7.



Рис.2.7. Зовнішній вигляд корпусних камери

Гіростабілізовані відеокамери використовуються на рухомих об'єктах. завданням камери є отримання стабілізованого зображення. Цей пристрій може застосовуватися для різних об'єктів, наприклад, трансформаторні підстанції, нафтогазовий сектор, щогли лінії електропередач (далi – ЛЕП). В основному використовуються для огляду місцевості, спостереження за обстановкою, моніторингу надзвичайних ситуацій, проведення пошукових робіт, виявлення об'єктів і вимірювання їх координат. Зовнішній вигляд гіростабілізований камери представлений на рис. 2.8.



Рис. 2.8. Зовнішній вигляд гіростабілізований камери

### 2.3. Обладненя системи відеоспостереження

Квадратори (quad compressor) призначені для одночасного відображення на екрані монітора відеоспостереження зображень від декількох, зазвичай 4 відеокамер, в режимі реального часу. Квадратор ділить екран монітора відеоспостереження на чотири прямокутні області, в кожній з яких міститься зображення від відеокамери, підключеної до відповідного відеовходу квадратора. Одночасно з висновком відеоінформації на монітор, квадрировать зображення через квадратор надходять на відеомагнітофон. Як правило, квадратори встановлюють в невеликі системи відеоспостереження офісів, магазинів, гаражів, автостоянок тощо.

Вступник в квадратор аналоговий відеосигнал спочатку оцифровується, а потім стискається до розміру відповідної області екрану. На виході квадратор формує аналоговий відеосигнал, в якому представлені відеосигнали всіх чотирьох квадрантів. Сучасні квадратори, як правило, оцифровує відеосигнали і видають остаточне зображення розміром 512 x 512 або 1024 x 1024 пікселів. З огляду на те, що картинок на екрані чотири, кількість пікселів кожного зображення в чотири рази менше, ніж повноекранного. І, отже, якість кожного зображення, яке передається на монітор відеоспостереження і записується на відеомагнітофон, помітно гірше, ніж повноекранного.

Квадратори, що перемикаються в повноекранний формат, обробляють відеосигнал по-різному. У найбільш простих моделях квадраторов одне з чотирьох раніше оцифрованих зображень просто розтягується на весь екран. У більш дорогих моделях в повноекранному режимі відеосигнал оцифровується з максимальним можливим для даної моделі дозволом.

Мультиплексори - це пристрої, призначені для роботи в складі системи відеоспостереження. Класичні мультиплексори виконують мультиплексування (перемикання) за часом входять на них відеосигналів з декількох камер відеоспостереження і формують два типи вихідних відеосигналів: один для перегляду на моніторі відеоспостереження, інший для запису на відеомагнітофон (відеорекордер).



Рис.2.9. Приклад мультиплексора

Сигнали зображення, що надходять з виходу мультиплексора на відеомонітор, одночасно формують на його екрані зображення зі всіх відеокамер. Так якщо до мультиплексора підключено 16 відеокамер, то на екрані відеомонітора відображатимуться відеозображення з кожної відеокамери, по одному в кожному з 16 вікон. У той же час оператор може вибрати будь-яку відеокамеру для повноекранного відображення її відеоінформації на відеомоніторі.

Одночасно з цим, на виході мультиплексора, підключеного до відеомагнітофона, формуються розділені за часом мультиплексовані відеосигнали зі всіх відеокамер, вибраних для запису. У цьому випадку принцип роботи мультиплексора аналогічний принципу роботи послідовного комутатора. При цьому мультиплексор обробляє відеосигнали таким чином, що кожен наступний кадр, що посилається на відеомагнітофон або пристрій цифрового запису, виходить від наступної, як правило, один по одному підключеної до нього відеокамери. Мультиплексори, що дозволяють або проводити обробку відеозображень (мультиплексування) для запису на відеомагнітофон, або переглядати зображення підключених відеокамер, отримали назву - симплексний відеомультиплексор.

Що стосовнодуплексних мультиплексорів, то архітектура і принцип роботи симплексного мультиплексора не дозволяють йому виконувати одночасно дві вищеперелічені функції. Одночасне виконання цих завдань реалізують дуплексні мультиплексори, що представляють собою два мультиплексора в одному корпусі. Один мультиплексор призначений для запису відеоінформації на відеомагнітофон або пристрій цифрового запису, а інший для відтворення на відеомоніторі "живого" відео або раніше зроблених відеозаписів.

По роботі мультиплексора в комп'ютерній мережі, то практично всі дуплексні мультиплексори мають мережеві карти і можуть підключатися до мережі Ethernet. При цьому буде можливий перегляд на комп'ютері відеозаписів і відеофрагментів, що зберігаються на мультиплексоре, з можливістю їх передачі по електронній пошті, наступним збереженням і печаткою.

У той же час, через порт RS-485, який присутній у всіх мультиплексорів, дуплексні мультиплексори можна об'єднувати в мережу і керувати ними за допомогою однієї клавіатури. В кінцевому підсумку можна побудувати систему відеоспостереження, яка об'єднує до декількох сотень відеокамер.

Для того щоб одночасно проводити запис відеоінформації, а також переглядати на одному моніторі відеоспостереження комбінацію з "живого" відео і зроблених раніше відеозаписів, застосовуються триплексні мультиплексори.

Сучасне програмне забезпечення і триплексний мультиплексор забезпечує одночасне відеоспостереження на відеомоніторі "живого" відео до 64 камер, високоякісну цифрову запис на жорсткий диск інформації з цих камер і відтворення раніше записаних відеофрагментів.

Використовуючи комп'ютер і мережевий триплексний мультиплексор, оператор системи відеоспостереження може контролювати приєднані до мультиплексору поворотні пристрої і камери, виробляти перефокусировку об'єктива, формувати і активувати предустановки відеокамер. Іншими словами, все, що раніше робилося за допомогою клавіатури управління, тепер виконується за допомогою триплексного мультиплексора і персонального комп'ютера. Екранне меню мультиплексора дозволяє здійснювати пошук відеофрагментів за сигналом тривоги, час, дату, номеру відеокамери.

Переваги сучасних триплексному мультиплексорів:

1. Налаштування мультиплексора і управління камерами відеоспостереження через LAN-мережу [Ethernet / Internet];

2. Цифровий запис відео, перегляд "живого" зображення і відеозапису, зробленого раніше, проводиться одночасно;

3. Налаштування якості запису для кожної підключеної камери;

4. Пряме і реверсивний відтворення відеозаписів з різною швидкістю;

5. Миттєвий доступ до відеозаписів, швидкий пошук по дату, час, номер камери, сигналом тривоги;

6. Автоматичне включення запису по сигналу тривоги;

7. Одночасний перегляд зображення на двох моніторах в мультиекран форматі;

8. Вбудований детектор руху, програмований для кожної камери.

9. Синхронізація кадрів в мультиплексові.

Отримуючи на відеовходи сигнали від різних відеокамер, мультиплексор повинен вибудувати в часі ланцюжок по одному кадру від кожної відеокамери в заданому порядку. Усі вхідні відеосигнали обробляються в мультиплексоре цифровим сигнальним процесором і синхронізуються їм в єдину послідовність кадрів. З огляду на те, що сигнали від різних відеокамер можуть приходити на мультиплексор не одночасно, кадри, які мають затримку щодо оброблюваного сигналу, можуть бути процесором пропущені. Тому досить часто в мультиплексори встановлюють по два процесори синхронізації сигналів на парні і непарні кадри, в результаті чого виробляється цифрове запам'ятовування і правильна їх синхронізація без пропусків

### 2.4. Надійність і рівні ризику впливу для виділених загроз Розумного будинку

Розвиток технології «Розумний будинок» призвело до якісної зміни місця і ролі систем автоматизації та управління будівлями. Все більше людей замислюються про концепцію взаємної ув'язки різноманітного інженерного устаткування будівель та організаційно-технічних рішень по експлуатації з використанням систем автоматизації і управління. Метою використання даної технології є створення системи, здатної підтримувати безпечні та комфортні умови роботи або проживання, а також забезпечувати спрощену систему управління службами і підсистемами будівлі. Сучасна система, побудована за технологією «Розумний будинок» може включати в себе підсистеми управління кліматом і освітленням, охоронної сигналізації та відеоспостереження, водопостачання, віддаленого моніторингу та інші.

В даний час технологія «Розумний будинок» вважається однією з найперспективніших і динамічно розвиваються. У США дана технологія вже давно є широко застосовується в різних сферах автоматизації житлових будівель. У Європі, в тому числі і в Україні, популяризація та розвиток технології

«Розумний будинок» тільки набирає обертів. Найбільш популярними об'єктами для впровадження даної технології є комерційна нерухомість (торговельні центри, офісні будівлі, банки, готелі), державні будівлі (вокзали, аеропорти, спортивні та культурні установи), а також об'єкти домашньої автоматизації.

За даними експертів компанії YORK International, прогнозується щорічне зростання ринку систем, що використовують дану технологію на 20-25% в рік. Цей ріст обумовлений тим, що більш розвинена інженерна та інформаційна інфраструктура «Розумного будинку» дозволяє реалізувати якісно новий рівень надання послуг і істотно підвищити його споживчу цінність.

Однак поряд з очевидними перевагами може виникнути цілий ряд проблем, пов'язаних із забезпеченням інформаційної безпеки організацій та осіб, що використовують дану технологію.

При побудові систем за технологією «Розумний будинок» можна виділити два різних підходи, які мають різну ступінь надійності.

– централізований;

– децентралізований;

– централізований метод реалізації технології.

«Розумний будинок» за своєю суттю є об'єднанням різноманітних датчиків і контролерів в єдину складну телекомунікаційну мережу з центральним контролером. В ролі центрального контролера може застосовуватися сервер, в якості якого використовується будь-який сучасний комп'ютер, і програмне забезпечення з підтримкою необхідного програмного софта і протоколів. Даний контролер є "мозком" системи автоматизації «Розумного будинку». У назві відображена головна суть підходу – до центрального Котроллер системи підключені всі основні і допоміжні блоки, при цьому всі икомпоненти оснащені власними микроконтроллерами, але взаємодіють вони виключно за допомогою центрального контролера.

Телекомунікаційна мережа є основним елементом, що забезпечує функціонування системи життєзабезпечення. Через мережу проводиться з'їм інформації з різного роду датчиків і передача їх головного сервера для обробки. Сервер після обробки інформації здійснює передачу сигналів управління на виконавчі елементи (датчики перекриття води, включення засобів пожежогасіння, блокування дверей і т.д.). Через центральний сервер відбувається настройка і управління «Розумним домом» легальним користувачем, а також через нього при необхідності здійснюється передача заданою інформації господареві квартири (офісу) при його відсутності (наприклад, про несанкціоноване проникнення, протечках, пожежі). Така телекомунікаційна мережа може бути побудована з використанням як провідних, так і бездротових каналів зв'язку, наприклад з використанням Wi-Fi, Bluetooth, або 3G.

Використання даного підходу дозволяє поєднувати пристрої різних виробників, що в свою чергу здешевлює розгортання всієї системи. Основним мінусом є велика залежність від роботи центрального контролера. Також користувач може з метою управління та контролю підключити центральний контролер до мережі Інтернет, тим самим піддаючи всю систему різним загрозам і атакам.

Децентралізований підхід має на увазі розгортання системи з розподіленою логікою. На відміну від централізованого підходу в децентралізованому підході відсутній центральний контролер. В цьому випадку система складається з датчиків, сенсорів і активаторів. Датчики виявляють зміна будь-яких характеристик в будинку, руху або зміни заданих в програмі параметрів, і реагують на ці зміни командою виконуючим пристроям, які включаються активаторами. При децентралізованому підході в разі відмови одного з компонентів порушується тільки функціональна частина, за яку відповідав цей компонент. Тому такі системи є більш безпечними і надійними в порівнянні з системами реалізовані з централізованого методу. Значним мінусом даного підходу є те, що проектування системи вимагає високої кваліфікації і великого досвіду, що в свою чергу позначається і на вартості розгортання системи.

Розглянемо ризики інформаційної безпеки систем, побудованих за технологією «Розумний будинок». Вважаємо, що базовими класичними загрозами інформаційній безпеці є порушення конфіденційності, цілісності та доступності інформації.

Під конфіденційністю інформації ми усвідомлюємо неможливість витоку конфіденційної комп'ютерної інформації організацій (осіб), які експлуатують

Під доступністю інформації ми розуміємо стан системи, при якому легальні користувачі (і сама система), використовуючи елементи «Розумного будинку», можуть реалізовувати дозволені в системі дії (відкривати двері, включати кондиціонування або систему пожежогасіння, моніторити ситуацію і т.д.). Порушення доступності інформації може призвести до неможливості системи реагувати на різні ситуації, в тому числі і аварійні.

Під цілісністю інформації ми розуміємо такий стан системи, при якому легальні користувачі (і сама система) отримують достовірну інформацію про стан підсистем «Розумного будинку». Отримання системи недостовірної інформації про температуру в приміщеннях, наявності пожежу, витоку газу і води і т.п. призведе до неадекватних її діям (наприклад, до включення системи пожежогасіння, перекриття води і т.д.). З прикладів видно, що порушення конфіденційності, цілісності та доступності інформації в системі, побудованої за технологією «Розумний будинок», може привести як до дезорганізації роботи організацій (осіб), її експлуатують, так і до катастрофічних наслідків.

Значення ризику інформаційної безпеки будемо розраховувати на основі ймовірності (частоти) реалізації загроз на вразливі елементи системи, ефективності загроз в разі їх реалізації, а так-же можливого збитку для активів системи. Для визначення значення ризику будемо використовувати якісну шкалу оцінки, яка дає можливість виробити розуміння про ступінь уразливості систем, побудованих за аналізованої технології. Нижче наведені приклади якісних шкал оцінки ризиків інформаційної безпеки.

Під класом активу будемо розуміти роль тієї чи іншої підсистеми (елемента підсистеми) «Розумного будинку» в забезпеченні якості функціонування системи (збитку функціонуванню всієї системи). Так, наприклад, помилкове спрацьовування датчика витоку води і датчика пожежної сигналізації, може привести до різних наслідків. Якісна шкала оцінки рівня класу активу може виглядати в наступному вигляді.

Висока вплив на систему – вплив на конфіденційність, цілісність і доступність елементів системи може заподіяти організації (власникам) значний або катастрофічний збиток. Середнє вплив на систему – вплив на конфіденційність, цілісність і доступність елементів системи може заподіяти організації (власникам) середній збиток. Середній збиток не викликає значних або катастрофічних змін, однак порушує нормальну роботу організації (нормальну життєдіяльність). Низький вплив на систему – вплив на конфіденційність, цілісність і доступність елементів системи не заподіює організації (власникам) будь-якого серйозного збитку. Оцінку ймовірності реалізації загрози на вразливі елементи системи, побудованої за технологією «Розумний будинок», будемо оцінювати через частоту реалізації загрози за певний період.

1. Висока. Ймовірно реалізацію однієї чи кількох скількох загроз в межах року.

2. Середня. Загроза може виникнути в межах двох-трьох років.

3. Низька. Виникнення загрози в межах трьох років малоймовірно.

Оцінку ефективності реалізації загрози на вразливі елементи даної системи будемо оцінювати за наступною шкалою:

1. Висока схильність до впливу. Значний або повний збиток для активу.

2. Середня схильність до впливу. Середній або обмежений збиток.

3. Низька схильність до впливу. Незначний збиток або відсутність такого.

Так, наприклад, такий канал витоку конфіденційної комп'ютерної інформації, як з'їм зловмисником побічних електромагнітних випромінювань сервера, має різну ефективність в різних умовах і може приймати значення від низької до високої схильності впливу. Для обчислення рівня ризику будемо використовувати підхід, запропонований компанією Microsoft. На першому етапі, на підставі значення класу активу і оцінки схильності активу впливу (ефективності реалізації загрози) визначається рівень впливу (таблиця 2.1). На другому етапі, на підставі рівня впливу та ймовірності реалізації загрози визначається ризик інформаційної безпеки (таблиця 2.2). Проведемо оцінку ризиків інформаційної безності системи, побудованої за технологією «Розумний будинок». Як приклад візьмемо приміщення офісу, в якому циркулює конфіденційна інформація, існують вимоги щодо забезпечення доступності та цілісності інформації, а також вимоги щодо нормальної життєдіяльності співробітників. Все офісне обладнання підключено через єдину мережу, яку контролює центральний контролер.

Таблиця 2.1

**Рівні впливу**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Клас активу | Високий вплив | Середній | Високий | Високий |
| Середній вплив | Низький | Середній | Високий |
| Низький вплив | Низький | Низький | Середній |
|  |  | Низький | Середній | Високий |
| Рівень впливу | | |

Таблиця 2.2

**Визначення підсумкового ризику**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вплив (из табл. 2.1) | Високий | Середній | Високий | Високий |
| Середній | Низький | Середній | Високий |
| Низький | Низький | Низький | Середній |
|  |  | Низький | Середній | Високий |
| Рівень ймовірності реалізації загрози | | |

Необхідно відзначити, що точна оцінка ризиків інформаційної безпеки повинна здійснювала вляться для конкретних умов існування організації, до яких відносяться ступінь важливості інформації, що циркулює в організації, її рас положення, які використовуються механізми управління інформаційною безпекою тощо. У даній статті проводиться тільки наближена оцінка ризиків для вироблення розуміння про необхідність викорис тання механізмів забезпечення інформаційної безпеки таких технологій.

Виходячи з результатів оцінки, найнебезпечнішими є ті загрози, при яких зловмисник може брати під контроль всю систему, построєну по аналізованій технології. Тому вкрай необхідним є проведення заходів щодо захисту телекомунікаційної мережі, розмежування прав доступу користувачів, захист від інсайдерів. Небезпечними є ризики втрати електроживлення, пожежа в серверній, поломки устаткування і відмова програмного забезпечення, що відповідає за централізованому управління системою. Реалізація даних загроз може призвести до катастрофічних наслідків для всієї системи.

Тому важливим завданням при проектуванні подібних систем є детальна оцінка ризику для конкретних умов з аналізом всіх потенційних загроз і вразливостей. У подальших дослідженнях будуть розроблені методики оцінки результатів впливу різних загроз на вразливі елементи систем, побудованих за технологією "Розумний будинок".

**3. РОЗРОБКА ПРОЕКТУ СИСТЕМИ ОХОРОННОГО ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ РОЗУМНОГО БУДИНКУ**

### 3.1. Аналіз об’єкту охорони

Об'єктом є приватний будинок, який знаходиться у місті Нікополь, Дніпровської області вул. Сагайдачного 116. Дім має один головних вхід.

Площа: 1 поверху 79.1 м² з висотою h=2.7 , 2 поверху 96.7 м² з висотою h=1.6 і 2.4 м , підвалу 22.2 м² з висотою h=2м.

Фундамент будинку капітальний залізобетонний, стіни капітально цегельні, обшиті гіпсокартоном, стелі приміщень капітальні залізобетонні.

Будинок у собі має:

* Вхід у будинок,

– тамбур,

– хол,

– кухню,

– вітальню,

– 2 спальні,

– 2 ванні кімнати,

– 2 сан вузли,

– дитячу кімнату,

– 2 коридори,

– комору,

– підвал,

– котельню,

– кабінет.

Вікна будинку – склопакети с однією стулкою.

Перехідні двері у всіх кімнатах дерев'яні, мають один урізний замок. Головні вхідні двері: металево броньовані, мають 3 урізних замка. Будинок знаходиться у спальному районі приватного сектору біля якого житлові сусідські будинки. Дім стоїть на перехресті доріг.

Об’єкт охорони зображено на рис 3.1. 3.2.і 3.3.

Рис. 3.1. Перший поверх об’єкту охорони



Рис. 3.2. Другий поверх об’єкту охорони

Пріорітетною кімнатою для охорони і безпеки є кабінет, який знаходится на першому поверсі житлового будинку. Основні цінності (матеріальні, грошові, цінні папери) зберігаються у вогнетривкому сейфі . Доступ до сейфа мають тільки батьки. Найбільш уразливим місцем для проникнення порушника на цей об'єкт є двері і вікна.



Рис. 3.3. Підвал об’єкту охорони

### 3.2. Розробка структури системи відеоспостереження

Основне завдання розроблювальної системи відеоспостереження – одержання, запис і відтворення візуальної інформації про поточні події на охоронюваному об'єкті.

Розроблювана система відеоспостереження є комбінованою й полягає: з аналогових і IP відеокамер, середовища передачі даних, перетворювачів сигналу (відеосервер) записуючого пристрою (відеореєстратор) пристрою відображення й відеоархіву. Кількість IP відеокамер у системі – чотири, кількість аналогових відеокамер – сім. Система відеоспостереження має можливість розширюватися шляхом додавання нових компонентів. Перевагою комбінованої системи відеоспостереження є те, що в одній системі можна використовувати відеокамери з різними параметрами, різними матрицями, різних виробників. Таким чином, на ключові точки огляду на об'єктах доцільно встановлення відеокамери з високою РЗ, а в місцях загального огляду: коридори, периметр досить використовувати відеокамери з невеликою РЗ і більш доступною за ціною. Структура системи відеоспостереження представлено на рис. 3.4.

Структура системи відеоспостереження складається з:

- IP відеокамер;

- аналогових відеокамер;

- відеосервера;

- відеореєстратора;

- відеоархіва;

- персонального комп'ютера;



Рис. 3.4. Структура системи відеоспостереження

З'єднання IP камер з відеореєстратором здійснюється за допомогою витої пари.

З'єднання аналогових камер з відеосервером здійснюється за допомогою коаксіального кабелю.

### 3.3. Розрахунки характеристик відеокамер

Розрахунки величини максимального видалення зони спостереження.

При побудові системи відеоспостереження завжди необхідно визначити максимальну відстань, на яку можуть бути віднесені відеокамери одна від одної для організації безперервної зони відеоконтролю. Ця відстань у значній мірі визначає загальну кількість установлюваних відеокамер на заданій території. Як відомо, застосовуючи об'єктив з більшою фокусною відстанню, можна проводити відеоспостереження за ділянками, розташованими на значному видаленні від місця установки відеокамери. Однак істотне обмеження на величину видалення при цьому накладає ступінь освітленості об'єкта в темний час доби. На рис. 3.5 схематично показане розташування відеокамери й джерела світла на ділянці території.

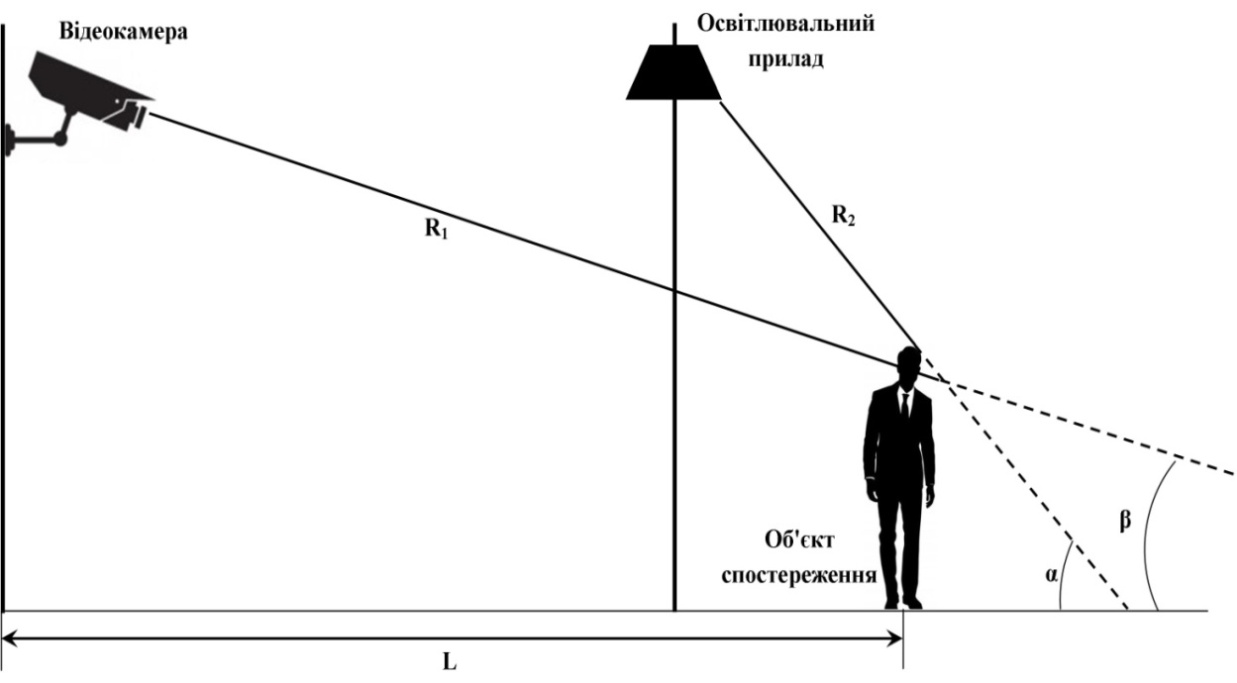


Рис. 3.5. Схематичне положення відеокамери, освітлювального приладу й об'єкта спостереження на ділянці території

Ґрунтуючись на реальних технічних параметрах відеокамер, освітлювального устаткування й характеристиках місцевості, можна розрахунковим методом визначити величину максимального видалення відеокамери від об'єкта спостереження. Для цього необхідно скористатися формулою, по якій визначається рівень освітленості на об'єктиві відеокамери, створюваний освітлювальним приладом:



де *Еv* – мінімально-припустимий рівень освітленості на об'єктиві відеокамери; *Iv* – сила світлового потоку, створюваного освітлювальним приладом; α (17° у конкретному прикладі) кут, під яким освітлювальний прилад висвітлює об'єкт спостереження; *K* – коефіцієнт відбиття світлового потоку; *R1+R2* – сумарна відстань, подолана світловим променем від джерела світла до об'єктива відеокамери.

Для відеокамер з високою РЗ Sony Exview B1073WB2-K12 припустимий рівень освітленості (чутливість) становить величину 0,1 лк. Освітлювальний прилад з галогенними лампами потужністю 50 Вт створюють світловий потік у центрі діаграми спрямованості силою 8000 кд.

Коефіцієнт відбиття світлового потоку для людини на тлі місцевості К=0,22.

Використовуючи попереднє вираження можна визначити сумарну відстань R1+R2.

Після проведення обчислень одержимо величину:

*R1+R2 = 121 м*

*R2 = 20/cosα =21 м*

де 21 – максимальна відстань у метрах від об'єкта спостереження до найближчого освітлювального приладу. R1 =100м – максимальне видалення відеокамери від об'єкта спостереження

*L = R1/Cosβ*=100м,

де β = arcsin H/R1 =1 – кут відбиття світлового потоку; Н = 2.5 м – висота установки відеокамери.

У системах відеоспостереження необхідно виконати вимоги, відповідно до яких на спостережуваному просторі в найбільш віддалену відеокамеру, можна було розпізнати порушника з високим ступенем імовірності. Для цього необхідно правильно вибрати фокусну відстань об'єктива й тип ПЗЗ-матриці (тип відеокамери) за критерієм РЗ .

Для того, щоб розпізнати предмет спостереження мінімального розміру, необхідно, щоб зображення цього предмета займало не менш 5 телевізійних ліній (ТВЛ). У якості тестових предметів спостереження використовуються білі фігури (коло, квадрат, трикутник) розміром 0,3 м, розташовані на чорному тлі. Практичні випробування показали, що якщо оператор здатний розрізняти ці розташовані в найбільш вилученій зоні спостереження предмети на екрані монітора, то оператор здатний ідентифікувати порушника на тлі місцевості. Дослідним шляхом доведене, що білі тестові предмети (коло, квадрат, трикутник) розміром 0,3 м, розташовані на чорному тлі у віддаленій зоні спостереження, добре різняться між собою, якщо на зображення цих предметів на екрані монітора доводиться 5 ТВЛ. Виходячи із цієї умови можна здійснити розрахунок повного розміру видимого об'єкта для обраного типу відеокамери.

Виконаємо розрахунки повного розміру видимого об'єкта в максимально віддаленій зоні спостереження.

Як відомо, мінімальний розмір однієї дискрети зображення на екрані монітора становить величину:

*d=3S/4R;*

де *d* – розмір однієї дискрети зображення; *R –* роздільна здатність відеокамери у ТВЛ; *S* – повний розмір видимого зображення

Розмір тестового предмета висотою й шириною 0,3 м що займає на екрані монітора 5 ТВЛ, буде дорівнює величині 15S/4R= 0,3м;

Звідси повний розмір видимого об'єкта

*S= 1,2R/15 = 0,08R;*

Виходячи з вищенаведеного аналізу випливає, що для відеокамер із середньою РЗ R = 400 ТВЛ повний розмір видимого об'єкта S=32 м, а для відеокамери з РЗ R = 600 ТВЛ S=48 м.

З вищенаведеного можна зробити наступні виводи:

– при однаковому куті огляду довжина сектору огляду для відеокамер з високою РЗ (R = 600) в 1, 5 рази вище, ніж для відеокамер із середньою РЗ (R = 400);

– при однаковій довжині сектору огляду кут огляду для відеокамер з високою РЗ в 1,5 рази вище, ніж для відеокамер із середньою (рис. 3.6).

При відомій відстані L від відеокамери до об'єкта спостереження можна визначити кут зору об'єктива з вираження (рис. 3.7):



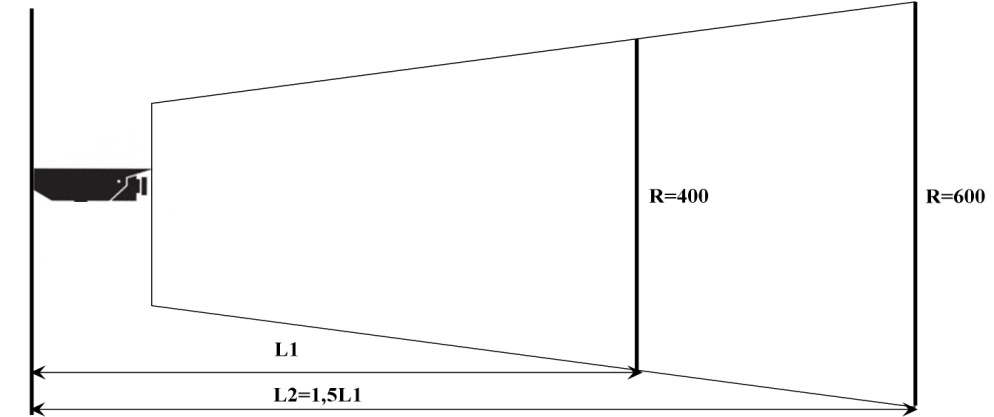


Рис. 3.6. Порівняльна довжина секторів огляду для відеокамер з високою й середньою РЗ при однаковому куті огляду

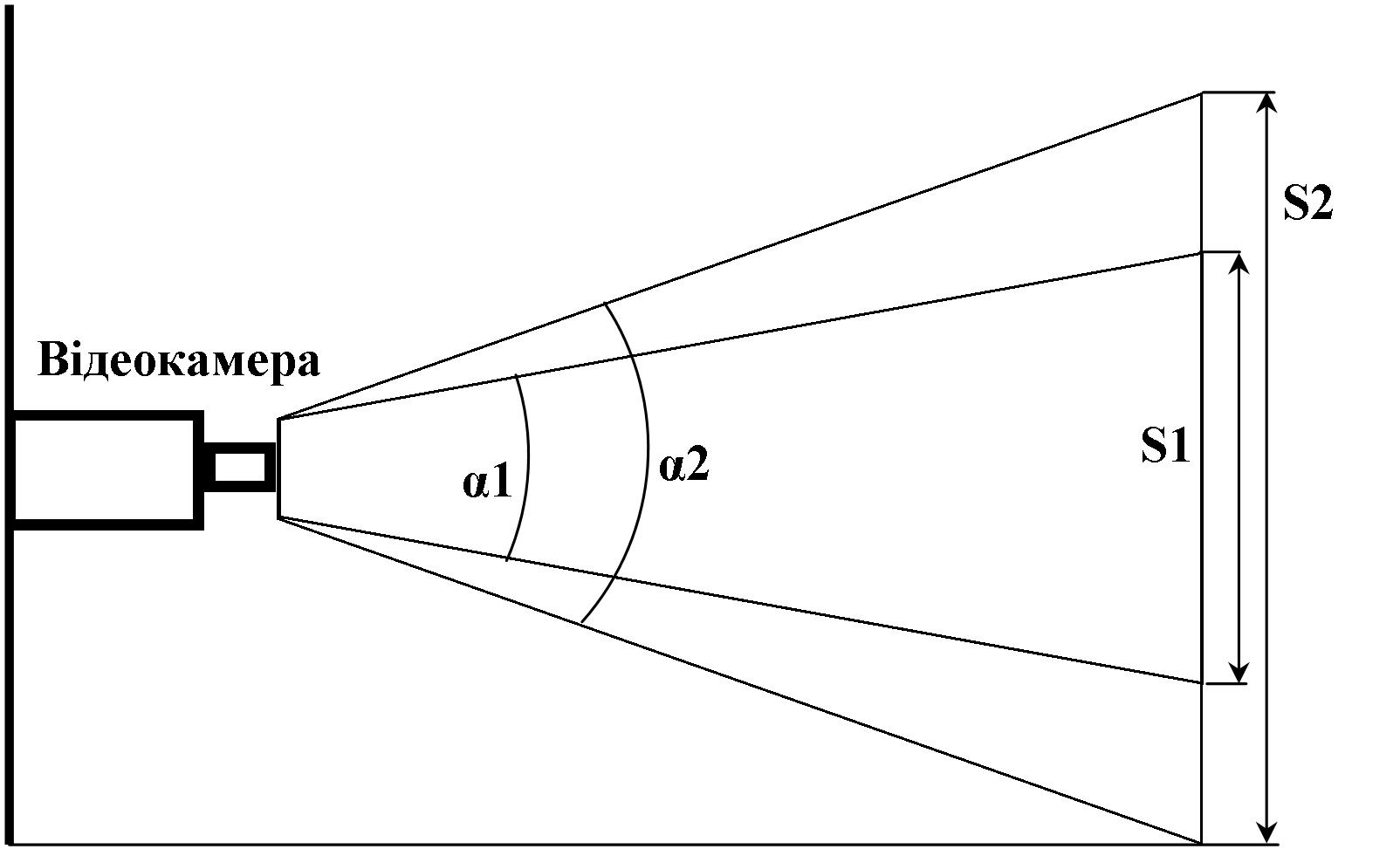


Рис. 3.7. Порівняльна величина кутів огляду для відеокамер з високою й середньою РЗ при однаковій довжині секторів огляду

При відомому куті огляду можна визначити відстань від відеокамери до об'єкта спостереження:



При більш високих вимогах до якості передачі зображення необхідно, щоб на самий дрібний розглянутий предмет доводилася більша кількість ТВЛ (до 8 ТВЛ). При цьому повний розмір видимого об'єкта (при РЗ 400 ТВЛ) буде рівний S= 0,05R =20 м.

З вищевикладеного можна зробити висновок, що бажання підвищити якість зображення у віддаленій зоні відеоспостереження приведе до збільшення кількості відеокамер. Використовуючи пропонований метод, можна завжди з достатньою точністю зробити необхідні розрахунки.

Розрахунки величини дистанції ефективного огляду відеокамер.

На малюнку схематично показане зразкове розташування відеокамер на ділянці периметра. З рис. 2.5 видно, що в горизонтальній площині сектор огляду має «мертву» зону М1 і дистанцію активного огляду D.

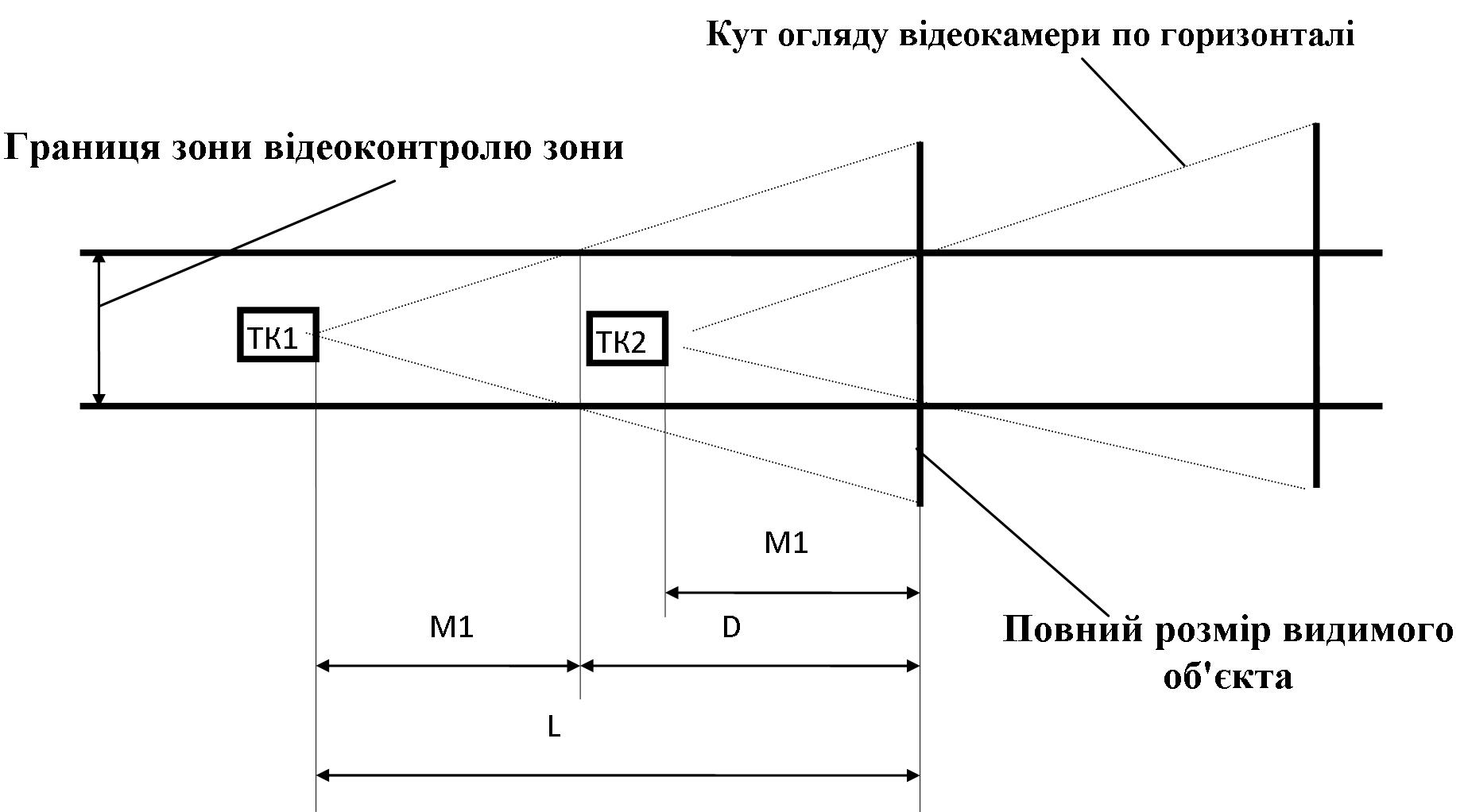


Рис. 3.8. Розташування відеокамер на ділянці периметра

Як видно з рис. 3.8, сектор огляду відеокамери має мертву зону М1, обумовлену значенням кута огляду об'єктива по горизонталі й шириною зони відеоконтролю. Зона відеоконтролю складається із двох ділянок шириною по 3 м. Величина мертвої зони визначається з вираження:





де К – ширина зони відеоконтролю (відповідає ширині зони відчуження периметра, тобто рівна 2 м); α – кут зору об'єктива по горизонталі (у нашому випадку приблизно 160°), як було визначено вище.

Відповідно до попередніх розрахунків максимальне видалення відеокамери від об'єкта спостереження L=67м.

Величина об'єкта спостереження S для телевізійної системи, що має у своєму складі відеореєстратор РЗ 400 ТВЛ:

*S = 0,08R*

де *R* = 400 – РЗ.

При цьому, необхідно відзначити, що РЗ системи, в основному, визначається РЗ самого реєстратора, тому що реєстратор є найбільш вузькою ланкою системи по цьому параметру.

Необхідно також визначити величину мертвої зони, обумовленої значенням кута огляду об'єктива відеокамери по вертикалі (рисунок 3.8).



Рис. 3.9. Сектор огляду відеокамери у вертикальній площині

Згідно з рис. 3.9:

*М2 = Н tg (δ-β)*

*М2 = 2,5·tg (85-75)=0.44м*

де *М2* – величина мертвої зони по вертикалі; *Н* – висота установки відеокамери; *β* – значення кута огляду по вертикалі; *δ* – кут напрямку огляду відеокамери.

*δ = arctg L\H*

*δ= arctg 67\2,5= 87.8°.*

Дистанція ефективного огляду відеокамери становить величину

*D = (L - М1)*

*D=66 м.*

Розрахунки системи відеоспостереження для камер внутрішнього відеоспостереження:

Для об'єктивів без дисторсії кут зображення α можна знайти, знаючи розмір діагоналі світлочутливого елемента *d* і ефективну фокусну відстань об'єктива *F*:

*α*

Для матриці формату 1/3ʺ *d*=6мм.

Перетворимо формулу, і знайдемо необхідний тип об'єктивів для кожної камери, виходячи з потрібного кута спостереження:



Камера К1: Вхід. Необхідний кут огляду α=90°.



Камера К2: Кабінет. Необхідний кут огляду α=90°.



Камера К3: Холл. Необхідний кут огляду α=135°.

F=1.25мм

Камера К4: Вітальня. Необхідний кут огляду α=90°.



Камера К5: Коридор. Необхідний кут огляду α=135°.

F=1.25мм

Камера К6: Спальня. Необхідний кут огляду α=90°.



Камера К7: Спальня. Необхідний кут огляду α=90°.



Камера К8: Дитяча кімната. Необхідний кут огляду α=90°.



Камера К9: Підвал. Необхідний кут огляду α=35°.



Камера К10:Зона-18. Необхідний кут огляду α=135°.

F=1.25мм

Характеристики камер зовнішнього спостереження приведені в табл. 3.1.

Таблиця 3.1

**Характеристики зовнішнього спостереження**

|  |  |
| --- | --- |
| **Характеристика** | **Величина** |
| Фокусна відстань (мм) | 1.25 |
| Формат матриці відеокамери | 1/3ʺ |
| Висота установки камери (м) | 2.5 |
| Кут нахилу камери (°) | 25 |
| Роздільна здатність (ТВЛ) | 500 |
| Відстань до об'єкта (м) | 25 |

Надалі будемо вибирати камери відеоспостереження відповідно до керівних документів і параметрам обчисленим вище в даній роботі.

Добір комплексу програмно-технічних засобів системи відеоспостереження.

Технічні характеристики камери для приміщень (К2-К10) – купольна відеокамера LILIN CMD2422S (табл. 3.2, рис. 3.10).

Кольорова купольна камера відеоспостереження Merit Lilin CMD2422S оснащена ширококутним об'єктивом "риб'яче око", 2-мегапіксельною CMOS-матрицею і високопродуктивним процесором обробки зображення. За ефективністю відеоспостереження ця камера перевершує цілу групу з кількох немегапіксельних камер, оскільки дозволяє оператору в будь-який момент часу бачити всю панораму. Об'єктив з високою роздільною здатністю «риб'яче око», використовуються в бескінематіческіх панорамних мегапіксельних камерах, які дозволяють програмним способом формувати кілька віртуальних камер, оснащених функцією цифрового масштабування, і виводити будь-який фрагмент матриці на екран монітора. Таке обладнання дозволяє контролювати великі площі, забезпечуючи високу деталізацію зображення з можливістю ідентифікації.

Таблиця 3.2

**Характеристики LILIN CMD2422S**

|  |  |
| --- | --- |
| **Характеристика** | **Значення параметра** |
| Передача кольору | Кольорова |
| Матриця | ПЗЗ матриця 1/3ʺ Sony Progressive Scan CMOS |
| Тип камери | Купольна |
| Вбудований об'єктив | 3.6 мм |
| Рабочая температура | -10 °C ~ +50 °C |
| Відношення сигнал/шум | Більш 45 |
| Тип камери | Цифрова |
| Наявність синхронізації | Зовнішня |
| Кут огляду | 180 стандартний, додаткові кути 150,135,110, 90,78, 56, 44, 28 та 25° |
| Напруга живлення | 12В |



Рис. 3.10. Зовнішній вигляд LILIN CMD2422S

Відсутність рухомих механічних вузлів робить цю камеру надзвичайно надійною і довговічною. Одночасно, завдяки 2-х мегапіксельному вирішенню камери, ці зображення мають таку високу деталізацію, що їх масштабування не супроводжується спотворенням дрібних деталей. Тому для ретельного вивчення будь-якої «дрібниці» архівного кадру досить виконати його цифрове збільшення на операторському моніторі.

Інтелектуальні можливості камери забезпечуються процесором, який виробляє обробку вихідного зображення 2 Мп (1600х1200), яке розбивається на чотири сектори, службовців для формування абсолютно незалежних віртуальних поворотних камер відеоспостереження. Процесор обробляє зображення всього простору, що оточує камеру спостереження: на 360 градусів по горизонталі і на 180 градусів по вертикалі. Зображення виводиться на екран у звичній для людського ока формі (табл. 3.3, рис. 3.11). Ці віртуальні камери мають набір функцій, характерним для швидкісних купольних камер. Розмір і положення сектора огляду віртуальних камер визначається оператором і може охоплювати будь-яку частину доступного зображення. Відеопроцесор в режимі реального часу виправляє геометричні спотворення, що вносяться об'єктивом, і виводить отримане зображення на стандартний монітор.

Завдяки надійній конструкції, потужному функціоналу і здатності постійно здійснювати моніторинг просторової перспективи камера оптимально підходить для систем відео спостереження.

Таблиця 3.3

**Характеристики Hikvision DS-2CD2043G0-I**

|  |  |
| --- | --- |
| **Характеристика** | **Значення параметра** |
| Дозвіл | 4 Мп |
| Матриця | ПЗЗ матриця 1/3ʺ |
| Тип | провідні |
| Вбудований об'єктив | 3.6 мм |
| Нахил | 0 ° - 90 ° |
| поворот | 0 ° - + 360 ° |
| Дозвіл і частота запису | Головний потік :: 2560 х 1440, 2304 х 1296, 1920 x 1080 - 25 кадрів / с |
| Нічна зйомка | ІК-фільтр з автоматичним вимикачем Дальність ІЧ-підсвічування: до 30 метрів |
| Напруга живлення | 12 В ± 25 % / 6 Вт, PoE (802.3af) В |
| Температурний режим | -30 °C + 60 °C °C |



Рис. 3.11. Зовнішній вигляд Hikvision DS-2CD2043G0-I

### 3.4. Розробка схеми розташування відеокамер із зонами огляду

Усередині будинку розташовується девять відеокамер і одна на зовні будинка. Пять відеокамер розташовані в ключових місцях, які показано на рис. 3.12, 3.13.

Камера № 1 фіксує зону входу в будинок.

Камера№ 2 фіксує зону холлу.

Камера № 3 фіксує вітальню.

Камера № 5 фіксує зону коридору на другому поверсі.

Камера № 4 фіксує найголовнішу зону кабінет.

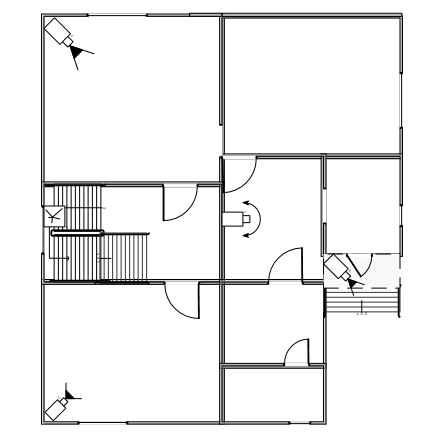


Рис. 3.12. Схема розташування відеокамер на першому поверсі із зонами огляду усередині приміщення

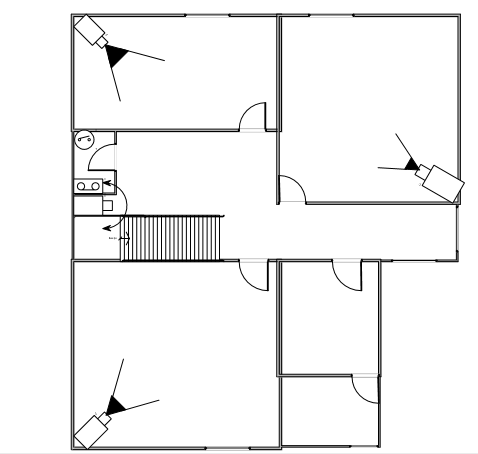


Рис. 3.13. Схема розташування відеокамер на другому поверсі із зонами огляду усередині приміщення

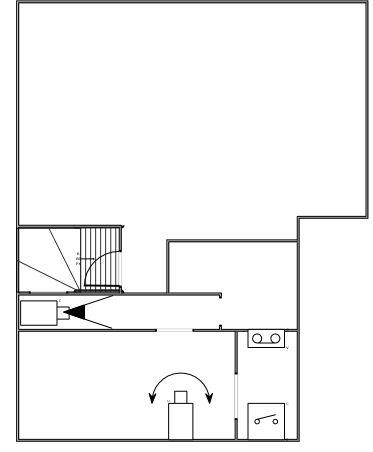


Рис. 3.14. Схема розташування відеокамер підвалу із зонами огляду усередині приміщення

### 3.5. Проектування системи відеозапису

Відеореєстратор служить для запису вхідної інформації від відеокамер.

По суті, відеореєстратор є спеціалізованим комп'ютером, англійською мовою це виглядає так Digital Video Recorder або скорочено DVR. Звичайно запис здійснюється на жорсткий диск. Тому, як правило, система відеоспостереження це в той же час і система відеозапису.

Відеореєстратор є ядром сучасної системи відеоспостереження.

Перш ніж зробити запис, відеореєстратори перетворює вхідний аналоговий сигнал відеокамер у цифровий вид, здійснюють його стиск і, лише потім записує.

Відеореєстратори можна розділити на два типи: відеореєстратори на базі персонального комп’ютера (ПК) і спеціалізовані відеореєстратори.

Процес обробки й стиску найбільш складна процедура, яку виконує система цифрового відеозапису. Саме якість стиску відеосигналу й визначає якість і, відповідно, ціну самого приладу.

При виборі відеореєстратора необхідно визначити потрібний часовий інтервал, протягом якого буде проводитися запис.

Для визначення необхідного дискового простору, потрібно вибрати :

– РЗ, з якою необхідно робити запис (наприклад, запис із РЗ 704х576 займає приблизно в 4 рази більше місця на диску, ніж запис із РЗ 352х288);

– швидкість, з якої необхідно робити запис (наприклад, запис зі швидкістю 25 кбіт/с, займає в 2 рази більше місця на диску ніж запис зі швидкістю 12,5 кбіт/с);

– кількість записуваних відеоканалів.

При необхідності, можна розрахувати його самостійно по формулі, знаючи розмір кадра (параметр F):

*S = N·F·V·T·0,0824*

де *S* – обсяг дискового простору (ГБ); *N* – кількість каналів, по яких ведеться запис; *F* – розмір кадра (кБ) (залежить від формату стиску, який визначається з технічних характеристик відеореєстратора); *V* – швидкість запису на канал (к/с); *T* – час, протягом якого необхідно вести запис (кількість діб).

Виходячи з характеристик нашого відеореєстратора отримаємо 490Гб.

Щоб забезпечити схоронність архіву, у випадку ушкодження жорсткого диска, необхідно, щоб у відеореєстраторові був «дзеркальний» дисковий масив RAID.

Розмір архіву відеореєстратора визначається наступними параметрами:

– кількістю жорстких дисків, які можна встановити у відеореєстратор;

– можливістю підключення зовнішнього дискового накопичувача.

При проектуванні системи відеоспостереження може бути закладена наявність аудіоканалів. Зазвичай, в одному відеореєстраторі їх може бути до 16. На випадок змін вимог до системи відеоспостереження, потрібно передбачити, як мінімум, 1 аудіовхід.

Дуже корисна функція відеореєстраторів – передача по мережі на e-mail, а в деяких випадках і на FTP-сервери, повідомлень про які-небудь події: спрацьовування детектора руху, несправність жорсткого диска, спрацьовування тривожного входу, провалля сигналу від камери, тощо.

Як уже говорилося вище, при використанні відеореєстраторів у мережі перевагу слід віддавати пристроям з форматом стиску відеозображення MPEG4 і H.264, тому що вони забезпечують максимальну швидкість передачі відеоінформації й менше завантажують існуючу мережу. При цьому формат H.264 в 2 рази ефективніше.

Гібридні відеореєстратори мають функціональність DVR відеореєстраторів. Відеореєстратор розташований у кімнаті охорони.

Вибираючи відеореєстратор, потрібно звернути увагу на використовуваний у ньому формат стиску відеоінформації. Звичайно використовуються MJPEG, MPEG4, H.264.

Кожний із цих форматів має свої особливості: MPEG4 - це більш сучасний формат, призначений для стиску потоку аудио- і відеоінформації. Запис, зроблений відеореєстратором, що використовують MPEG4, займає приблизно в 10 раз менше місця дискового простору. Такі відеореєстратори мають більш сучасну елементну базу, отже, їхня ціна вище. У даній роботі буде використовуватися саме відеореєстратор з такою характеристикою.

На підставі розрахунків і аналізу технічних характеристик пристроїв відеозаписи було обрано 16-канальний видеорегістратор Oltec HDVR-016 HD (рис. 3.15).

Це відеореєстратор типу HDVR, що підтримує як аналогові, так і IP-камери.



Рис. 3.15. 16-канальний видеорегістратор Oltec HDVR-016 HD

Технічні характеристики 16-канального видеорегістраторі Oltec HDVR-016 HD:

Виробник- Oltec;

Тривожні входи- 8;

Тривожні виходи -1;

Тип роз'єму- RJ-45;

Формат стиснення -H.264;

Робоча температура -10 ° C / 50 ° C;

Живлення -220В AC;

Email функція –є;

Відеовихід- є;

Кількість відеовходів -16;

Кількість аудіо входів- 16;

Кількість- HDD 2;

Швидкість запису- 25 кадрів / с;

Дозвіл запису- CIF / 4CIF / 960H;

Інтерфейси -USB / RS-485;

MODEL- HDVR-016HD.

### 3.6. Засоби захисту системи відеоспостереження

Для захисту системи відеоспостереження необхідно створення системи зовнішнього захисту від блискавки:

– створення якісного заземлюючого пристрою для відводу на нього імпульсних струмів блискавки;

– екранування устаткування й ліній, що входять у нього, від впливу електромагнітних полів, що виникають при протіканні струмів блискавки по металевих елементах системи захисту від блискавки, будівельним металоконструкціям і іншим провідникам при близькому розміщенні устаткування до них;

– створення системи зрівнювання потенціалів всередині об'єкта або в точці установки відеокамери, шляхом з'єднання за допомогою потенціало-вирівнюючих провідників усіх металевих елементів об'єкта або частин устаткування ( за винятком струмоведучих і сигнальних провідників);

– установка на всіх лініях, що входять до складу об'єкта (або окремо розміщеного устаткування), пристроїв захисту від імпульсних перенапруг з метою вирівнювання потенціалів струмоведучих або сигнальних провідників щодо заземлених елементів і конструкцій об'єкта. Іноді може знадобитися захист і внутрішніх ліній, що з'єднують різне устаткування, наприклад, шини постійного струму на виході випрямляча;

– захисні скляні світлофільтри виконують подвійне завдання: зменшують інтенсивність ультрафіолетових променів, що попадають в об'єктив, і перешкоджають контакту передньої лінзи з пилом і бризків. Якість захисного фільтра визначається в основному сортом скла (воно не повинне вносити колірних викривлень), паралельністю площин (щоб не було геометричних викривлень) і точністю шліфування (щоб не знижувалися роздільна здатність і контраст);

– термокожухи призначені для установки в них вуличних камер з об'єктивами із кріпленням. Герметичний корпус оснащений платою термореле, внутрішнім нагрівальним елементом, колодками для підключення вуличної камери й зовнішніх кабелів.

**4. ЕКСПЛУАТАЦІЯ СИСТЕМИ ОХОРОННОГО ВІДЕОСПОСТЕРЕЖЕННЯ РОЗУМНОГО БУДИНКУ**

### 4.1. Правові аспекти використання системи відеоспостереження

Статистика про розкриття правопорушень, говорить про те, що при використанні систем відеоспостереження, успіх упіймання зловмисника підвищується у декілька разів. У торгівельних центрах і магазинах, відеоспостереження забезпечує контроль над вітринами, над входом і виходом відвідувачів, над діями покупців. Як тільки охорона фіксує на моніторі спостереження факт крадіжки або які-небудь підозрілі дії покупця, цю інформацію передають на вихід. За допомогою камер спостереження, керівництво магазину попереджає випадки розкрадання і крадійства, як з боку покупця, так і з боку персоналу, чим економить грошові кошти.

Триста шістдесять п'ять днів в році цілодобово електронні пристрої спостерігають за тим, що відбувається в супермаркетах, на заправних станціях, в магазинах, в автотранспортних потоках, тощо. Камери спостереження встановлюють для захисту свого житла в заміських будинках і котеджах.

Відеоспостереження в офісі викликає особливе невдоволення у співробітників офісів. Адже працедавець може побачити, яка кількість робочого часу витрачається співробітниками на «перекури», перерви на каві, і чим вони займаються в робочий час. Покупці супермаркетів і магазинів хочуть знати, за чим же саме стежить камера.

Після відкриття нового терміналу в аеропорту Борисполя до ЕВРО2012, керівництво аеропорту, виявивши турботу про безпеку своїх пасажирів, обладнало термінали сучасною системою безпеки і відеоспостереження. Роботизовані керовані камери спостереження допомагають працівникам аеропорту забезпечувати надійну і зручну роботу.

Приховане відеоспостереження є незаконним. Відеозапис, отриманий таким чином, суперечить Конституції України по частині порушення і вторгнення в особисте життя і переслідується законом. Усі співробітники, за якими ведеться відеоспостереження на робочому місці, мають бути про це попереджені. Приховане відеоспостереження можуть проводити тільки правоохоронні органи, з дозволу суду.

Згідно із законодавством України, за використання негласних технічних засобів з’йому інформації існує кримінальна відповідальність.

«Стаття 359. Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації».

Незаконне придбання або збут спеціальних технічних засобів негласного отримання інформації, а також незаконне їх використання караються штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до чотирьох років, або позбавленням волі на той самий строк.

Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - караються позбавленням волі на строк від чотирьох до семи років.

Дії, передбачені частиною першою або другою цієї статті, вчинені організованою групою або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам чи інтересам окремих громадян, державним чи громадським інтересам або інтересам окремих юридичних осіб, – караються позбавленням волі на строк від семи до десяти років.

Під скритими технічними засобами (СТЗ) слід розуміти: - спеціальні технічні засоби для зняття інформації з каналів зв'язку, інші засоби негласного отримання інформації - технічні засоби, устаткування, апаратура, прилади, пристрої, препарати та інші вироби, спеціально розроблені, виготовлені, пристосовані для негласного отримання інформації, або технічні засоби, запрограмовані з цією самою метою з використанням спеціального програмного забезпечення.

Спірні питання щодо належності до спеціальних технічних засобів конкретного технічного засобу, який розробляється, виготовляється і реалізується суб'єктом господарювання, вирішуються експертно-технічною комісією Служби безпеки України [16].

### 4.2. Технічне обслуговування систем відеоспостереження

Система відеоспостереження – це програмно-апаратний комплекс, призначений для організації відеоконтролю на різних територіях і об'єктах. Будь-яка встановлена система відеоспостереження складається з безлічі компонентів і чим їх більше, тем вище ймовірність виходу з ладу одного (або декількох) з них.

Компоненти систем відеоспостереження, як і будь-які інші електронні й механічні пристрої незалежно від умов експлуатації потребують регулярного технічного обслуговування (ТО). Без якісного й своєчасного обслуговування, елементи системи відеоспостереження можуть втратити свої експлуатаційні якості й перестати відповідати заявленим технічним характеристикам.

Таким чином, у самий невідповідний момент, це може поставити під загрозу функціонування системи відеоспостереження й зажадати терміновий ремонт.

Щоб система відеоспостереження, працювала без збоїв, необхідно регулярно проводити технічне обслуговування відеоспостереження. А це цілий комплекс профілактичних і ремонтних робіт, спрямованих на своєчасне виявлення й усунення поломок устаткування.

Організація сучасних систем безпеки в більшості випадків, крім виконання гарантійних зобов'язань, має на увазі й повноцінне обслуговування відеоспостереження. Багато замовників вважаються, що поняття «обслуговування відеоспостереження» і «гарантійне обслуговування» це одне й теж, але насправді між ними є істотні відмінності.

Гарантійний ремонт – це ремонт або заміна устаткування, що вийшло з ладу через заводський брак або ж через помилки в процесі установки. Справжню причину можуть визначити фахівці на місці установки, а за результатами огляду оформлять акт встановленої форми. При цьому, гарантія не поширюється на устаткування, яке втратило свою працездатність через ушкодження в результаті форс-мажорних ситуацій, фізичного впливу сторонніми особами, перебоїв і стрибків електроенергії, тощо.

Обслуговування відеоспостереження – це в першу чергу проведення профілактичних робіт, спрямованих на підтримку в робочому стані всіх пристроїв систем відеоспостереження протягом усього періоду їх експлуатації. Це роботи входять із проведення навчання робочого персоналу, надання консультацій, налаштуванню устаткування, відновлення ПЗ. Також обслуговування відеоспостереження має на увазі аварійні виїзди фахівців і відновлення працездатності системи відеоспостереження або її окремих компонентів у результаті форс-мажорних ситуацій, фізичного впливу сторонніх осіб, тощо.

Систематичне обслуговування систем відеоспостереження дозволяє досягти безперебійного функціонування всієї системи безпеки й практично виключає можливість виникнення непередбачених ситуацій, таких як непрацюючі камери через погані контакти або ж втрата чіткості зображення. Якщо розглядати багаторівневу систему безпеки із установленими високотехнологічними засобами відеоспостереження, то непрацюючі камери – це найпростіший приклад того, що може трапитися із системою безпеки, якщо їй не приділяється винної уваги.

### 4.3. Регламент обслуговування системи відеоспостереження

Обслуговування згідно з регламентом припускає один щомісячний плановий виїзд фахівця на об'єкт для проведення профілактичних робіт, а також необмежена кількість аварійних виїздів і віддалене адміністрування системи при наявності такої технічної можливості.

Виконання профілактичних робіт передбачає:

1. Щомісяця:

– перевірка працездатності системи в цілому, консультаційні послуги з роботи системи;

– зовнішній огляд комутаційних центрів, відеореєстраторів, моніторів, джерел живлення, відеокамер, кабельної мережі;

– перевірка режимів роботи й правильності функціонування відеореєстраторів;

– очищення, протирання від пилу, бруду, корозії основних вузлів системи;

– діагностика системних ресурсів, перевірка дискових масивів на наявність помилок;

– діагностика можливих несправностей устаткування й дрібний ремонт на місці;

– налаштування напрямків і ракурсів відеокамер.

2. Щокварталу:

– замір живлячої напруги відеокамер;

– перевірка кріплення, підтяжка рознімних механічних і електричних з'єднань;

– очищення й знежирення оптичної системи відеокамер;

– перевірка роботи пристроїв обігріву;

– перевірка працездатності джерел безперебійного живлення й параметрів акумуляторів;

– змащення механічних редукторів поворотних пристроїв;

У зв'язку з різноманітністю модельного ряду устаткування в регламент можуть додаватися/виключатися деякі види робіт.

**5. ОХОРОНА ПРАЦІ**

### 5.1 Вступ

Охорóна прáці – це:

1. Порушення техніки безпеки - електромонтер Миколаївобленерго, віліз на поручні підйомної люльки во время ремонту високовольтної ЛЕП

система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних и лікувально-профілактичних ЗАХОДІВ та ЗАСОБІВ, спрямованостей на Збереження життя, здоров'я і працездатності людини під час Трудової ДІЯЛЬНОСТІ;

2. чинна (что Діє на підставі відповідніх законодавчо та других нормативних АКТІВ) система соціально-економічних, організаційно-технічних, санітарно-гігієнічних и лікувально-профілактичних ЗАХОДІВ та ЗАСОБІВ, Які забезпечують Збереження здоров'я і працездатність людини під час праці.

3. Дозвіл на початок робіт підвіщеної небезпеки, Який необхідній организации чи Підприємству, хто працює в будівництві.

Законодавство про працю містіть норми и вимоги з техніки безпеки и виробничої санітарії, норми, что регулюють робочий час і Час відпочинку, звільнення та переведення на іншу роботу, норми праці относительно жінок, молоді, гігієнічні норми и правила ТОЩО.

Загальний нагляд за додержанням норм охорони праці покладаючи на прокуратуру, Спеціальний - на Професійні спілки. Контроль за безпека праці здійснюють такоже, Державні й відомчі Спеціалізовані інспекції (Держгіртехнагляд, Держенергонагляд ТОЩО).

Охорона праці як система зачіпає практично кожну нішу життя людей, пов'язану з виконанням тих або інших робіт. Вона переплітаєтеся з великою кількістю технічних і гуманітарних наук, виконуючи одне з найбільш важливих завдань - збереження життя і здоров'я людини при безпечному виконанні будь-яких робіт.

В даній дипломній роботі розроблена система відеоспостереження, яка працює у взаємодії з автоматизованим робочим місцем, основу якого складає ЕОМ. Більшість компонентів системи також відносяться до периферійних засобів ЕОМ. Отже питання охорони праці слід розглядати ядля інженера з установки та ескплуатації РЕА, а також для користувача ЕОМ.

### 5.2. Небезпечні і шкідливі чинники що діють на суб’єкта

**5.2.1. Шкідливі та небезпечні і шкідливі виробничі чинники**

Нині майже усі електромонтажні з'єднання РЕА здійснюються пайкою. Технологічний процес пайки включає випалювання ізоляції і лудіння.

При виконанні пайки на працюючих можуть впливати наступні небезпечні і шкідливі виробничі чинники:

запиленість і загазованість повітря робочої зони;

наявність інфрачервоних випромінювань від розплавленого припою у ванні або від паяльника;

наявність електромагнітного випромінювання високої частоти; дія ультразвуку на організм монтажника при пайці хвилею, яка утворюється за рахунок дії ультразвуку на розплавлений припій;

дія електростатичного заряду; незадовільна освітленість робочих місць або підвищена яскравість;

незадовільні метеорологічні умови в робочій зоні; дія бризок і крапель розплавленого припою; поразка електричним струмом;

А також група психофізіологічних шкідливих виробничих чинників: фізичні перевантаження (статичні і динамічні) і нервовопсихічні (монотонність праці, емоційні перевантаження).

**5.2.2. Шкідливі та небезпечні чинники під час експлуатації електронно-обчислювальних машин**

Потенційно шкідливими та небезпечними чинниками під час роботи на ВДТ, ЕОМ. ПЕОМ є:

* підвищене значення напруги в електричній мережі, замикання якої може відбутися через тіло людини; підвищений рівень статичної електрики;
* підвищений рівень «м'якого» рентгенівського випромінювання;
* підвищений рівень електромагнітного випромінювання радіочастотного діапазону;
* підвищений рівень інфрачервоного та ультрафіолетового випромінювання;
* підвищений рівень шуму та вібрації на робочих місцях;
* підвищені або понижені температура, відносна вологість та швид­кість руху повітря робочої зони; підвищена запиленість і загазованість повітря робочої зони; підвищений або понижений вміст пози­тивних і негативних аероіонів у повітрі робочої зони;
* недостатня освітленість робочої зони; підвищена яскравість світла; понижена контрастність між об'єктом і фоном; прямий та віддзеркалений відблиск; підвищена пульсація світлового потоку;
* підвищений вміст у повітрі робочої зони озону й аміаку;
* надмірні статичні та динамічні навантаження;
* розумове перенавантаження; перенавантаження аналізаторів;
* монотонність праці; надмірні емоційні навантаження;
* нераціональна організація робочого місця;
* підвищений вміст мікроорганізмів у повітрі робочої зони.

Кожний із наведених чинників може зумовити небажані наслідки впливу ВДТ, ЕОМ, ПЕОМ на здоров'я користувачів, а їх сумісна дія підсилити цей вплив.

Впровадження ЕОМ у різні галузі виробництва позитивно вплинуло на умови праці, її якість та продуктивність. Разом з тим робота на ВДТ, ЕОМ, ПЕОМ, ПК має низку чинників, які у разі порушення правил експлуатації можуть негативно впливати на стан здоров'я користувачів.

Основними проявами їх впливу с зоровий дискомфорт. Він проявляється як біль в очах, почервоніння повік і очних яблук, відчуття піску в очах, го­ловний біль, подвоєння предметів, швидка втома. Кістково-м'язовий дискомфорт проявляється у вигляді болю різної сили у суглобах та м'язах, скутості, втоми, судоми, оніміння тощо. Частіше кістково-м'язовий дискомфорт проявляється у людей старшої вікової категорії. Також ВДТ і ЕОМ зумовлюють захворювання шкіри. Вони проявляються у вигляді висипу, лущення, рожевих вугрів, деяких видів дерматитів. Стресові чинники, до яких належать несприятливі умови та режим праці, зміст праці, здібності працівника, його сподівання, звички, умови життя, можуть стати причиною виникнення фізіологічних і психологічних змін, погіршення здоров'я та змін у поведінці людини. Фізіологічні порушення можуть супроводжуватись розладами шлунково-кишкового тракту, змінами функцій серцево-судинної системи тощо. До психологічних та поведінкових розладів належать нервозність, роздратування, тривога, порушення сну, втрата апетиту, швидкий розвиток втоми.

Користувачі повинні знати потенційно шкідливі та небезпечні виробничі чинники під час роботи на ВДТ, ЕОМ, ПЕОМ та виконувати вимоги НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно- обчислювальних машин» і ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами ЕОМ» та інших нормативних документі» щодо виключення або зменшення їх негативного виливу.

Стосовно вимогам до приміщень, розміщення в них ВДТ, ЕОМ, ПЕОМ та організації лінії робочих місць, то об'ємно-планувальні рішення будівель і приміщень для роботи з ВДТ, ЕОМ, ПЕОМ мають відповідати вимогам чинних нормативних актів,зокрема СНиП 2.09.04-87 «Административные и бытовые здания», ДСанПіН 3.3.2.007-98, НПАОП 0.00-1.28 10 та іншим і мати ступінь вогнестійкості не нижчу II. Для всіх споруд і приміщень, у яких експлуатують ВДТ і ЕОМ визначають категорію з вибухопожежної та пожежної безпеки відповідно до ОНТП 24-86 «Определение категории помещений и зданий по взрывопожарной и пожарной опасности» і НАПБ В.01.053-2000/520 «Правила пожежної безпеки в галузі зв'язку» та клас вибухонебезпепечних зон відповідно до НПАОП 0.00-1.32-01 «Правила будови електроустановок.

### 5.3 Організаційні та конструктивно-технологічні заходи для зниження впливу шкідливих виробничих факторів ескплуатації РЕА, а також ЕОМ

**5.3.1. Охорона праці при пайці і випалюванні ізоляції**

Операції пайки, лудіння і випалення ізоляції супроводжуються забрудненням повітряного середовища в приміщеннях парами свинцю, олова, сурми і інших елементів, що входять до складу припою; парами каніфолі і різних рідин, вживаних для флюсу, змиву і розчинення різних лаків, які застосовуються для покриття друкованих плат; парами соляної кислоти; газами(окисел вуглецю, вуглеводня) і т. д. Пари, потрапляючи в атмосферу цеху, конденсуються і перетворюються на аерозоль такої конденсації, частки якої по своїй дисперсності наближаються до димів.

Знаходячись в запиленій атмосфері, робітники піддаються дії пилу і пари; шкідливі речовини осідають на поверхні шкірного покриву, потрапляють на слизову оболонку порожнини рота, очей, верхніх дихальних шляхів, із слиною заковтуються в травний тракт, вдихаються у легені. Разом із забрудненням повітряного середовища забруднюються робочі поверхні, одяг і шкірні покриви працюючих.

Особливо шкідливі при пайці олов'яно-свинцевими припоями пари свинцю. Свинець і його з'єднання отруйні. Частина свинцю, що поступив в організм, виводиться через кишечник і нирки, а частина затримується в кістковій речовині, м'язах, мозку, печінці. За несприятливих умов свинець починає циркулювати в крові, викликаючи явища свинцевого отруєння. Свинець викликає зміни у складі крові, вражає нервову систему, нирки і печінку.

Властивість свинцю накопичуватися в організмі призводить до хронічного отруєння при систематичному надходженні в організм навіть малих його кількостей. Для запобігання гострим і професійним захворюванням вміст свинцю в повітряному середовищі не повинен перевищувати гранично допустимої концентрації — 0,01 мг/м3.

У виробництві радіоелектронної апаратури окрім олов'яно-свинцевих припоїв знаходять застосування припої, до складу яких входять мідь, літій, срібло, кадмій і інші метали. В деяких випадках пайка здійснюється шляхом занурення в розплавлені хлористі солі кадмію, натрію, бору, літію з додаванням активних присадок – фтористих солей. Пари більшості з перерахованих речовин, що утворюються при пайці, можуть чинити шкідливу дію на організм працюючих.

Найбільш небезпечні пари окислу кадмію, міді і фтористі сполуки. Не байдужі для організму також літій і хлористий цинк, що чинять подразливу дію на шкіру і дихальні шляхи.

Пайка в атмосфері звичайними припоями робиться із застосуванням флюсів.

Біологічна дія флюсів на організм людини залежить від компонентів, що входять до складу паяльних флюсів. Одні компоненти(каніфоль соснова, етилацетат, олеїнова кислота та ін.) мають подразливу дію; інші (спирт етиловий) — наркотичним; треті (семікарбазид гідрохлорид, етилгліколь) – високою токсичністю; дія четвертих(кремнійорганічна рідина) на організм ще вивчено недостатньо.

Деякі марки флюсів (ФГСп, ФДФс, ФСкСп та ін.) через високу токсичність рекомендується не застосовувати або обмежувати їх застосування. У усіх флюсах слідує етилгліколь замінювати гліцерином, оскільки він здатний проникати в організм навіть через неушкоджену шкіру.

Для видалення залишків флюсів після пайки залежно від марки флюсу застосовуються різні миючі середовища, які мають токсичні властивості.

Кожному різновиду процесів пайки і лудіння притаманні певні шкідливі і небезпечні фізичні, хімічні, біологічні та психофізіологічні фактори, що відрізняються як кількісними, так і якісними характеристиками. При цьому деякі види паяння і лудіння утворюють одночасно кілька таких виробничих факторів, які можуть призвести до травмування та профзахворювань або виникнення пожеж і вибухів.

Такими потенційними небезпечними і шкідливими виробничими факторами можуть бути:

* запиленість і загазованість повітря робочої зони;
* наявність інфрачервоних випромінювань від розплавленого припою у ванні або паяльника;
* наявність електромагнітного випромінювання високої частоти;
* дія ультразвуку на організм монтажника при пайці хвилею, яка утворюється за рахунок дії ультразвуку на розплавлений припій;
* вплив електростатичного заряду;
* незадовільна освітленість робочих місць або підвищена яскравість;
* незадовільні метеорологічні умови в робочій зоні;
* впливу бризок і крапель розплавленого припою;
* ураження електричним струмом;
* група психофізіологічних шкідливих виробничих факторів: фізичні перевантаження (статичні і динамічні), нервово-психічні перевантаження (монотонність праці, емоційні перевантаження).

Всі різновиди процесів пайки і лудіння супроводжуються забрудненням повітряного середовища аерозолем припою і флюсу, парами різних рідин, застосовуваних для флюсу, змивки і розчинення лаків, парами соляної кислоти, газами (окис вуглецю, вуглеводні) і т.д.

Операції пайки і лудіння супроводжуються забрудненням повітряного середовища в приміщеннях парами оксиду свинцю, олова, сурми та інших елементів, що входять до складу припою, а також парами каніфолі. Пари, потрапляючи в атмосферу цеху, конденсуються і перетворюються в аерозоль конденсації.

Перебуваючи в запилених атмосфері, робочі піддаються впливу пилу і парів; шкідливі речовини осідають на шкірному покриві, попадають на слизову оболонку порожнини рота, очей, верхніх дихальних шляхів, зі слиною потрапляють в травний тракт, вдихаються в легені. Поряд із забрудненням повітряного середовища забруднюються робочі поверхні і одяг працюючих. Ступінь впливу аерозолів залежить від хімічного складу, який визначається хімічним складом припою.

**5.3.2. Охорона праці при зварюванні і інших методах з'єднань матеріалів**

Для отримання нероз'ємного з'єднання деталей і елементів радіоелектронної апаратури застосовується зварювання. Найбільш поширеними є ручне дугове, контактне, електронно-променеве і лазерне зварювання.

При виконанні зварювання, різання, наплавлення і напиленні на працюючих можуть впливати наступні шкідливі і небезпечні виробничі чинники: підвищена запилена і загазованість повітря робочої зони, наявність в нім зварювальних аерозолів; інтенсивне видиме, ультрафіолетове, інфрачервоне і рентгенівське випромінювання; підвищені рівні шуму і вібрації; підвищене значення напруги в електричному ланцюзі, наявність іскр; бризки і викиди розплавленого металу і шлаку; можливість вибуху балонів, що знаходяться під тиском; механізми, що рухаються, і вироби.

Зварювальна аерозоль викликає важке профзахворювання – пневмоконіоз; токсичні пари і гази викликають отруєння, а яскраве видиме випромінювання зварювальної дуги призводить до захворювання очей – електроофтальмії; теплове випромінювання дуги – до опіків шкіри обличчя і рук.

Зварювальні роботи на об'єктах народного господарства незалежно від їх відомчої приналежності повинні виконуватися відповідно до відповідних стандартів і правил.

При виборі способу зварювання слід враховувати рівень їх безпеки і санітарно-гігієнічні умови.

При розробці технологічних процесів зварювання деталей і вузлів повинні передбачатися їх максимальна автоматизація і механізація. При цьому необхідно використати дистанційне керування. Вживані при зварюванні флюси, електродний дріт і покриття, захисні гази і зварювані матеріали повинні виділяти шкідливі речовини в кількості, що не перевищує ГДК.

У випадках виділення в робочу зону пилу і газів необхідно влаштовувати місцеві витяжні пилегазоприймачі, вбудовані в зварювальне устаткування. При зварюванні великогабаритних виробів відсмоктування виконуються у вигляді рухливого повітряприймача, який швидко і надійно кріпиться поблизу зони зварювання.

Джерела зварювального струму повинні приєднуватися до розподільних електричних мереж напругою не вище 660 В. Зварювальні установки цехів повинні мати запобіжники або автоматичні вимикачі з боку мережі живлення. Пересування зварювальних установок і їх ремонт під напругою забороняється.

**5.3.3** **Охорона праці при виробничих випробуваннях РЕА**

В процесі експлуатації радіоелектронна апаратура піддається кліматичним діям, пов'язаним із станом атмосфери, її температурою, вологістю, осіданнями, тиском, сонячною радіацією, забрудненістю пилом, солями, парами, газами, радіоактивними речовинами, зараженістю мікробами; дією температурних змін, викликаних великими швидкостями в щільних шарах атмосфери, внутрішніми джерелами тепла, додатковим розігріванням і т. д.; механічною дією, причиною яких може бути сила тяжіння, сили постійно діючих прискорень, сили інерції, що виникають при зміні швидкості руху, сили, пов'язані з вібрацією роботи двигунів, сили, що виникають при ударах йди експлуатації і при перевезеннях.

Під впливом вказаних зовнішніх дій відбувається погіршення електричних і механічних параметрів РЕА, а також може настати повне руйнування.

При виробництві РЕА проводяться кліматичні і механічні випробування, які мають бути організовані так, щоб працюючим забезпечувалися умови праці відповідно до вимог санітарних норм і правил.

Кліматичні випробування проводяться в спеціально обладнаних камерах або приміщеннях, доступ в які при встановленому кліматичному режимі виключається за допомогою блокувальних пристроїв. Камери і приміщення з кліматичним середовищем герметичні з метою виключення попадання елементів кліматичного середовища(вологи, пилу, газів і т. д.) в повітря приміщень, де постійно перебувають працюючі. Для періодичної дезинфекції повітряного середовища приміщення обладнуються загальнообмінною вентиляцією і протибактерицидними лампами. Працюючі забезпечуються засобами індивідуального захисту від дії високих і низьких температур.

При проведенні механічних випробувань працюючі піддаються дії шуму, вібрації, механізмів, що рухаються і обертаються. Тому необхідно проводити заходи захисту працюючих.

**5.3.4** **Охорона праці при обробці поверхонь деталей і вузлів радіоелектронної апаратури**

Перед нанесенням на деталі захисних покриттів і їх складанням поверхні деталей попередньо обробляють механічними методами (шліфування, крацовку, гідропіскоструйне і дробоструйне очищення, галтовка) і більш ефективними і продуктивними хімічними методами очищення поверхні (знежирення, травлення і т. д.). При цьому застосовуються небезпечні і шкідливі хімічні та отруйні речовини, вплив яких на працюючих залежить від їх фізико-хімічних властивостей, їх агрегатного стану, класу небезпеки, часу і характеру впливу, шляхів надходження в організм, стану організму, наявності інших виробничих небезпечних та шкідливих факторів і від стану засобів колективного та індивідуального захисту.

Під час знежирювання застосовуються їдкі луги, легкозаймисті розчинники та горючі рідини - бензин, ацетон, трихлоретилен, толуол, бензол, ксилол, спирти та ін. При травленні широко використовується сірчана, соляна, азотна, фтористоводнева, ортофосфорна та інші кислоти, при роботі з якими виникає небезпека отруєння виділяються парами і Газами, руйнування зубів, хімічні опіки. Основними заходами щодо охорони праці для попередження отруєння та професійних захворювань є механізація і автоматизація виробничих процесів; герметизація устаткування; заміна токсичних, отруйних і горючих речовин менш токсичними, неотруйними і негорючими речовинами.

Найбільш високий рівень безпеки виробництва досягається при комплексній механізації та автоматизації технологічних процесів. У масовому і великосерійному виробництві застосовують автоматичні лінії, що виконують всі технологічні операції; в цехах з невеликою виробничою програмою застосовують напівавтоматичні установки, призначені для виконання якої-небудь однієї операції. Існують напівавтомати для мийки, травлення і обезжирення виробів. Всі роботи з отруйними і токсичними речовинами необхідно проводити в спеціальних герметизованих боксах або шафах, обладнаних ефективною місцевою витяжною вентиляцією. При вирішенні питання про необхідність і можливість заміни отруйних, токсичних і горючих речовин менш отруйними, нетоксичними і негорючими речовинами технологи керуються вимогами не тільки економічності, але і безпеки. Так, бензин, гас, трихлоретилен та інші токсичні та вогненебезпечні розчинники замінюють на малотоксичні і негорючі (фреон-113, водно-лужні розчини); хлоровані вуглеводні - синтетичними миючими засобами.

Для зменшення виділення водню і парів кислот при травленні в травильний розчин вводять присадки (ОП-7, ОП-10, «Унікол» та ін.) Дільниці та відділення кислотного та лужного травлення, знежирення в органічних розчинниках необхідно влаштовувати в окремих приміщеннях. Матеріали стін і перекриттів не повинні збирати шкідливі речовини, тому їх викладають скляними і керамічними плитками на висоту 2,8 ... 3,2 м, а іншу частину стін і стелі забарвлюють світлою олійною фарбою.

Підлоги виконують з матеріалів, які повинні бути вологонепроникними, стійкими до кислот і лугів, розчинників і іншим середах. Приміщення обладнуються загальнообмінною вентиляцією, а також використовується система місцевої витяжної вентиляції. При роботі з отруйними і токсичними хімічними речовинами необхідно застосовувати засоби індивідуального захисту. Для захисту від дії кислот і лугів застосовують захисні фартухи, робочі халати та костюми, виготовлені з гуми, хлорвінілової пластику, прогумованої тканини, брезенту та інших хімічно стійких матеріалів. Для захисту ніг використовують гумові кислото-лугостійкі чоботи з внутрішньої текстильної прокладкою і рифленою підошвою з підборами, а також напівчоботи.

Для одночасного захисту обличчя і очей від бризок кислот і лугів зручним і надійним засобом є головні захисні щитки (типу ЩН або НБХ). Очі необхідно захищати напівзакритими або герметичними окулярами (типу ЗПС-80, ЗП2-80, ЗПЗ-80).

Для захисту органів дихання від шкідливих газів і парів (крім особливо токсичних) в концентраціях, що не перевищують ГДК більш ніж у 15 разів, рекомендується протигазовий респіратор РПГ-67. Якщо в повітрі крім газів та парів містяться аерозолі, рекомендується застосовувати універсальний респіратор РУ-60М. Для короткочасної роботи (один-два дні) можна застосовувати протипилові респіратори ШБ-1 «Лепесток», «Сніжок КУ-М».

В аварійних випадках необхідно використовувати протигази, які захищають одночасно органи, дихання та очі робітників від шкоди ¬ них газів, пари, пилу, диму й туману. Для захисту рук від механічних пошкоджень і дії слабких розчинів кислот і лугів застосовують рукавиці з вовняних, бавовняних, лляних тканин з підсилювальними і захисними накладками або без них. Для захисту від кислот, лугів і органічних розчинників застосовують кислотозахисні рукавиці з шинельного сукна, гумові кислото- та лугостійкі рукавички.

Захист шкірного покриву здійснюють за допомогою захисних мазей, кремів і паст (пасти ІЕД-1, ІЕР-2, ФС 42-95-72, паста Чумакова та Міколан; креми «Силіконовий», ПМС-200, «Червона троянда»; мазь Селінского ХІОТ-6). Для зняття захисних мазей і паст після роботи застосовують препарати «Кристал» і «Прогрес».

Отруйні і токсичні речовини треба перевозити в справній тарі. Бочки з хімікатами перевозять за допомогою спеціальних тачок. Пляшки і бідони, виготовлені з поліетилену, перевозять на візках зі швидкістю не більше 5 км / ч. Пролиту на підлогу кислоту слід засипати землею або піском, а потім прибрати лопатою. Бризки і краплі кислот (крім сірчаної), що потрапили на тіло, негайно змивають струменем холодної води і уражене місце промивають 1%-ним розчином харчової соди. При опіках сірчаною кислотою промивають мильною водою і потім розчином харчової соди.

При опіках їдкими лугами пошкоджене місце ретельно промивають великою кількістю проточної холодної води протягом 10...15 хв, а потім промивають слабким розчином оцтової (одна чайна ложка столового оцту на склянку води) і розчином борної кислоти, а потім накривають марлею, просоченою 3 %-ним розчином оцтової кислоти. Пожежобезпечність досягається головним чином запобіганням утворення горючої середовища та ізоляцією джерела запалювання.

Запобігання утворення горючого середовища забезпечується регламентацією допустимих концентрацій горючих газів, пару та аерозолів; окремим зберіганням хімічних речовин, займистих при спільному зберіганні.

Приміщення для промивання і знежирення деталей забороняється опалювати газовими і електричними приладами, застосовувати відкритий вогонь. Для запобігання іскроутворення і вибуху двигуни, пускові пристрої та вентилятори повинні бути вибухобезпечного виконання.

Зберігання розчинників в робочих приміщеннях допускається в кількості не більше добової норми і в герметично закритій тарі. Один із заходів профілактики пожеж полягає в особливому розміщенні пожежо- та вибухонебезпечних ділянок та пристроїв протипожежних перешкод з метою попередження поширення вогню по будівлі.

**5.3.5.Розрахунок враження людини електричним струмом**

Під час обслуговування живлення корпусних камер працівник може доторкнутися до струмонесучих частин допоміжного обладнання, ступінь ураження в такому випадку залежить від умов і характеру дотику. Величина струму, котрий при цьому буде протікати крізь людину залежить віл режиму нейтралі, величини струму, стану ізоляції струмонесучих частин, ємності провідників відносно землі та опору тіла людини. Але факт самого дотику не дає підстави вважати, що людина отримає травму. При дотику до струмопровідних частин слід визначити значення напруги дотику людини і струму, що протікає крізь людину, в залежності від характеру дотику, типу мережі, схеми включення людини в електричний ланцюг та інше. Такий аналіз дозволить оцінити небезпеку дотику в тій чи іншій мережі, а потім правильно обрати необхідні засоби захисту.

Змінна напруга 220В 50Гц часто використовується при обслуговуванні живлення корпусниї камери, що розміщуються в термокожухах. Випадкова ситуація може зробити однофазний дотик до двофазної

*r1*

*r2*

*I2*

*I1*

*Rл*

*2*

*1*

*Uжив*

Рис.5.1.Однофазний дотик

Однофазний дотик до двофазної мережі дотик до однієї фази електроустановки, що знаходиться під напругою. Однофазний дотик, є менш небезпечним, ніж двофазний, тому що струм, що протікає крізь людину, зменшується внаслідок послідовного включення з ним опорів ізоляції провідника, підлоги, взуття та інше.

Відповідно до рис.4.1., під час дотику людини до проводу 1, її тіло стає включеним паралельно опору проводу 1 та послідовного опору  проводу 2, отже:

(5.1)

де -напруга дотик; -струм, що протікає через опір ізоляціївідповідно. Якщо брати до уваги те, що:

, (5.2)

де струм, що протікає через людину при дотику; опір людини, рівний 1000 Ом. Для визначення напруги дотику запишем наступний вираз:

(5.3)

де напруга живлення, котра дорівнює 220В.

Для визначення струму, що протікає через людину, можна записати наступний вираз:

 (5.4)

Якщо прийняти до уваги те, що , де опір ізоляція, то для визначення струму, котрий пройде через людину, і напруги дотику можемо записати наступне:

Так як , то визначимо струм та напругу, що буде при дотику:



=115/(2)=30.5 мА.

Величина такого струму є небезпечною для людини. При досягненні величини струму у 100 мА настає параліч дихання через 3 секунди. Величини розрахованого струму входить в діапазон від 10 до 31 мА, при даній величині сили струму починається судорога руки та її ледь можна відірвати від проводу.

**5.4 Забезпечення пожежної та вибухової безпеки при обслуговуванні електричного обладнання ЕОМ та РЕА**

У відповідності до ЗаконуУкраїни «Про пожежну безпеку» та вимог НАПБА.01.001-2004 «Правила пожежної безпеки в Україні» по запобіганню пожежі та пожежного захистурозглянемо необхідні заходи для забезпечення пожежної та вибухової безпеки. пожежа може виникнути у випадку перевантаження електричного обладнання при обслуговуванні ЕОМ, чи РЕА внаслідок пошкодження ізоляції, неякісного з’єднання електричної проводки чи короткого замикання. Для уникнення таких ситуацій електричне обладнання обладнане автоматом захисту у випадку перевантаження та короткого замикання. Крім того періодично проводять перевірку стану ізоляції проводі. Для покращення температурного режиму необхідне обладнання обладнується системами охолодження. Також приміщення де розташовані робочі місця по обслуговуванні ЕОМ, а також РЕА обладнуються засобами сповіщення у випадку виникнення пожежі. Для цього на стелі встановлюються датчики пожежної сигналізації

Приміщення входить до категорії помірно пожежонебезпечних «НАПБ А.01.001-2004 Правила пожежної безпеки в Україні». (Негорючі речовини і матеріали в гарячому, розпеченому або розплавленому стані, процес обробки яких супроводжується виділенням променистого тепла, іскор і полум'я, і (або) горючі гази, рідини і тверді речовини, які спалюються або утилізуються як паливо).

У будинку знаходиться шість датчиків ИПД-А системи автоматичного пожежегасіння. Призначений для виявлення загорянь в закритих приміщеннях будівель і споруд, що супроводжуються виділенням диму, і автоматичної подачі сигналу про виникнення пожежі (тривоги) в адресних установках пожежної сигналізації і автоматики на базі компонентів систем пожежі.

**5.5. Висновок**

Під час роботи з РЕА та ЕОМ на жителів діє декілька шкідливих факторів.

При плануванні заходів по забезпеченню нормальних умов праці технічного та інженерного персоналу потрібно приділяти увагу всім шкідливим факторам, бо кожен з низ може причинити серйозну шкоду здоров’ю людини або навіть її життю.

Знаючи гігієнічні вимоги, пропоновані до з РЕА та ЕОМ, спеціаліст з охорони праці разом з інженером повинен вміти визначати зони нормованого випромінювання, обирати найкращі для кожногї у конкретному випадку заходи захисту особового складу та домагатися втілення їх у життя, спираючись на відповідні регламентуючі документи. Велике значення має постійна санітарно-освітня робота.

**6. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА**

### 6.1. Вступ

Охорона навколишнього середовища характеризується комплексом вжитих заходів, які спрямовані на попередження негативного впливу економічної діяльності на навколишню природу, що забезпечує сприятливі та безпечні умови людської життєдіяльності. Враховуючи стрімкий розвиток науково-технічного прогресу, перед людством постала складна задача – охорона найважливіших складових навколишнього середовища (земля, вода, повітря), схильних сильному забрудненні техногенними відходами і викидами, що призводить до окислення ґрунту і води, руйнування озонового шару землі та кліматичним змінам.

Промислова політика всього світу привела до таких незворотних і суттєвих змін в навколишньому середовищі, що це питання охорони навколишнього середовища стало загальносвітовою проблемою і примусило державні апарати розробити довгострокову екологічну політику зі створення внутрішньодержавного контролю за ОНС.

Основними умовами для поліпшення екології в країні є:

* раціональне використання, охорона і витрата запасів природного резерву;
* забезпечення безпеки екології та протирадіаційні заходи;
* підвищення і формування екологічного мислення у населення;
* контроль над екологією в промисловості.

Охорона навколишнього середовища визначила ряд заходів для зниження рівня забруднень, що виробляється на об’єктах економічної діяльності:

* виявлення, оцінка, постійний контроль та обмеження викиду шкідливих елементів в атмосферу, а також створення технологій і техніки, які охороняють і зберігають природу і її ресурси;
* розробка правових законів, спрямованих на охоронні заходи навколишнього середовища та матеріальне стимулювання виконання вимог і профілактики комплексу природоохоронних заходів;
* профілактика екологічної обстановки шляхом виділення спеціально відведених територій (зон).

Всі норми і правила екологічної та робочої безпеки повинні бути визначені і зафіксовані в певному документі. Екологічний паспорт обєкту економічної діяльності – це комплексна статистика даних, що відображають ступінь користування даним підприємством природних ресурсів і його рівню забруднення прилеглих територій. Екологічний паспорт підприємства розробляється за рахунок компанії після погодження з відповідним уповноваженим органом і піддається постійному коригуванню у зв’язку з перепрофілюванням, змінами в технології, обладнанні, матеріалів, тощо.

### 6.2. Законодавча база охорони навколишнього середовища

Відносини у галузі охорони навколишнього середовища в Україні регулюються законами:

* «Про охорону навколишнього природного середовища від 25.06.1991 № 1264-XII;
* «Про природно-заповідний фонд України» від 16.06.1992 p.;
* «Про охорону атмосферного повітря» від 16.10.1992 p.;
* «Про тваринний світ» від 03.03.1993 p.;
* «Про екологічну експертизу» від 09.02.1995 p.;
* «Про внесення змін і доповнень у деякі законодавчі акти України з питань охорони навколишнього природного середовища» від 06.03.1996 p.;

Постановами Верховної Ради України:

* «Про затвердження порядку обмеження, тимчасову заборону або припинення діяльності підприємств, установ, організацій і об'єктів у випадку порушення ними законодавства «Про охорону навколишнього природного середовища» від 20.10.1992 p.;
* «Про порядок і видачу дозволів на спеціальне використання природних ресурсів і встановлення лімітів використання природних ресурсів республіканського значення» від 10.08.1992р. №459;
* «Про затвердження порядку визначення плати і стягнення платежів за забруднення навколишнього природного середовища» від 13.01.1992 р. № 018;
* «Про затвердження «Положення про державний моніторинг навколишнього природного середовища в Україні» від 23.09.1993 р № 785.

Кодекси України:

* «Земельний Кодекс України» від 18.12.1992 р. зі змінами від 05.05.1995 р.
* «Лісовий Кодекс України» від 21.01.1994 р;
* «Водний Кодекс України» від 06.06.1995 р;
* «Кодекс України про надра» від 27.07.1994 р.

Згідно з цими законами, а також розроблюваними відповідно нього земельним, водним, лісовим законодавством, законодавством про надра, про охорону атмосферного повітря, про охорону і використання рослинного і тваринного світу та іншим спеціальним законодавствами - основними принципами охорони навколишнього природного середовища є:

* пріоритетність вимог екологічної безпеки, обов'язковість додержання екологічних стандартів, нормативів та лімітів використання природних ресурсів при здійсненні господарської, управлінської та іншої діяльності;
* гарантування екологічно безпечного середовища для життя і здоров’я людей;
* запобіжний характер заходів щодо охорони навколишнього природного середовища;
* екологізація матеріального виробництва на основі комплексності у питаннях охорони навколишнього природного середовища, використання та відтворення відновлюваних природних ресурсів, широко-провадження новітніх технологій;
* збереження просторової та видової різноманітності і цілісності природних об'єктів і комплексів;
* науково обґрунтоване узгодження екологічних, економічних та соціальних інтересів суспільства на основі поєднання між дисциплінарних екологічних, соціальних, природничих і технічних наук та прогнозування стану навколишнього природного середовища;
* обов'язковість екологічної експертизи;
* гласність і демократизм при прийнятті рішень, реалізація яких впливає на стан навколишнього природного середовища, формування у населення екологічного світогляду;
* науково обґрунтоване нормування впливу господарської та іншої діяльності на навколишнє природне середовище;
* безоплатність загального та платність спеціального використання природних ресурсів для господарської діяльності;
* стягнення збору за забруднення навколишнього природного середовища та погіршення якості природних ресурсів, компенсація шкоди, заподіяної порушенням законодавства про охорону навколишнього природного середовища;
* вирішення питань охорони навколишнього природного середовища;
* використання природних ресурсів з урахуванням ступеня антропогенної змінності територій, сукупної дії факторів, що негативно впливають на екологічну обстановку;
* поєднання заходів стимулювання і відповідальності у справі охорони навколишнього природного середовища;
* вирішення проблем охорони навколишнього природного середовища на основі широкого міждержавного співробітництва.

### 6.3. Влив випромінювання оптичного діапазону

Випромінювання оптичного діапазону характеризуються довжинами хвиль приблизно від субміліметрового до далекого ультрафіолетового випромінювання. Показані види випромінювання оптичного діапазону (від 0,76 до 0,38 мкм), що використовуються в лазерних установках.

Межі інфрачервоного діапазону (невидимі теплові промені) визначаються приблизно від довгохвильової ділянки видимого діапазону до субміліметрових хвиль включно. За короткохвильової кордоном видимого діапазону простягається велика область ультрафіолетового діапазону (ближній, середній, далекий УФ), аж до рентгенівського діапазону.

Інфрачервоне випромінювання (ІКД) - це теплове випромінювання, що представляє собою частина електромагнітного спектра з довжиною хвилі λ = 780 нм...1000 мкм і володіє хвильовими і світловими властивостями, енергія якого при поглинанні у речовині викликає тепловий ефект.

Джерелом інфрачервоного випромінювання є будь-яке нагріте тіло. Спектр інфрачервоного випромінювання поділяють з урахуванням особливостей біологічної дії натри області: короткохвильову ІКІ-А (λ < 1,4 мкм); середньохвильову ІКІ-B (λ = 1,4...3,0 мкм); довгохвильову ІКІ-З (λ > 3 мкм).

Найбільш активно короткохвильове інфрачервоне випромінювання, так як воно володіє найбільшою енергією фотонів, здатна глибоко проникати в тканини організму і інтенсивно поглинати водою, що міститься в тканинах.

Повна енергія, що випускається в одиницю часу з одиниці площі стінок порожнини, тобто величина віддачі теплоти випромінюванням, залежить від абсолютної температури поверхні тіла (прямо пропорційна четвертого ступеня її температури) і визначається законом Стефана - Больцмана:

*WS = σT4*

де WS - інтенсивність випромінювання (тепловіддача), Вт/м2;   
σ = 5,67 · 10-8 Вт/(м2 · К4) - постійна Стефана-Больцмана; Т - абсолютна температура тіла, К.

Ця енергія випромінюється в тілесному куті Ω = 2π (ΩS/r2); S - площа, вирізана конусом на сфері радіусом r; одиниця виміру тілесного кута в усіх системах - стерадиан). Для кожної температури є свій спектральний розподіл, причому при збільшенні температури максимум енергії випромінювання зміщується в ультрафіолетову область спектру. При цьому величина λmax, що відповідає максимуму випромінювання для даного розподілу, пов'язана з Т співвідношенням:



де h = 6,63 · 10-27 ерг · з - фундаментальна константа природи; с - швидкість світла.

Сувора залежність енергії випромінювання нагрітих тіл від температури існує тільки для абсолютно чорного тіла. Спектральні розподіли випромінювання людини і Сонця близькі до випромінювання абсолютно чорного тіла.

При проходженні інфрачервоного випромінювання через повітря, воно майже не нагрівається. Між двома тілами, що мають різну температуру нагрівання, встановлюється радіаційний теплообмін з віддачою теплоти більш нагрітій поверхнею менш нагрітій:



де Е - тепловіддача, Вт; С1 і С2 - константи випромінювання з поверхонь; Т1 і Т2 - температури поверхонь, К.

Джерела ІЧ-випромінювання можна розділити на дві групи: природного та техногенного походження.

Головним природним джерелом ІЧ-випромінювання в біосфері є Сонце. При температурі зовнішньої поверхні Сонця приблизно 6000 K, 50% енергії випромінювання припадає на ІЧ-діапазон. До числа природних джерел ІЧ-випромінювання належать діючі вулкани, термальні води, процеси тепломасопереносу в атмосфері, усі нагріті тіла, лісові пожежі, тощо. Поверхня Землі випромінює теплове випромінювання в діапазоні довжин хвиль приблизно від 3 до 80 мкм, тобто захоплює всю середню ІЧ-область.

Людська цивілізація, будучи складною диссипативной структурою, неминуче пов'язана з тепловим випромінюванням. Велика частина електричної енергії, виходить за рахунок перетворення теплової енергії, що виділяється при згоранні органічного палива.

Шляхом перетворення енергії органічного палива приблизно 30% енергії перетворюється в електричну, а 2/3 енергії надходять у навколишнє середовище у вигляді теплового забруднення і забруднення атмосфери продуктами згоряння. Теплове забруднення водойм і атмосфери має місце і при експлуатації атомних електростанцій. В даний час встановлена закономірність загального підвищення температури водойм, річок, атмосфери, особливо в місцях знаходження електростанцій, промислових підприємств у великих індустріальних районах. У свою чергу, це призводить до зміни теплового режиму водойм, що позначається на життя біоорганізмів, до виникнення небажаних повітряних потоків із-за підвищення температури в атмосфері, зміни вологості повітря і сонячної радіації і, в кінцевому випадку, до зміни мікроклімату.

Найбільш поширеним джерелом ІЧ-випромінювання техногенного походження є лампа накачування. При температурі нитки лампи розжарювання 2300...2800 К максимум випромінювання припадає на довжину хвилі 1,2 мкм і близько 95% енергії випромінювання - на ІЧ-діапазон. Використовуються для сушки і нагріву лампи розжарювання з вольфрамовою ниткою потужністю 1 кВт випромінюють в ІЧ-діапазоні близько 80% всієї енергії. При зниженні температури загальний зміст ІЧ-випромінювання джерела зменшується. При падінні інтенсивності в 70 разів максимум інтенсивності відповідає λт=10 мкм, а при λт= 18 мкм інтенсивність зменшиться в 700 разів.

До числа джерел ІЧ-випромінювання техногенного походження відносяться також газорозрядні лампи, вугільна електрична дуга, електричні спіралі з ніхромового дроту, що нагріваються пропускається струмом, електронагрівальні прилади, плазмові установки, печі самого різного призначення з використанням різного палива (газу, вугілля, нафти, мазуту, торфу тощо), електропечі, електротехнічні пристрої з неминучим перетворенням частки електричної енергії в теплову, двигуни внутрішнього згоряння, електродвигуни, ракетні та авіаційні двигуни, МГД-генератори, реактори атомних станцій і т. д.

До числа когерентних техногенних джерел з вузькою смугою ІЧ-випромінювання відносяться ІЧ-лазерів (табл. 6.2).

У виробничих приміщеннях з великим тепловиділенням (гарячі цехи) на частку інфрачервоного випромінювання може доводитися до 2/3 виділеної теплоти і тільки 1/3 на конвекційну теплоту.

**Ультрафіолетове випромінювання**

Ультрафіолетове випромінювання (УФВ) – електромагнітне випромінювання оптичного діапазону з довжиною хвилі λ від 200 до 1000 нм і частотою від 1013 до 1016 Гц. УФІ являє собою невидиме оком електромагнітне випромінювання, що займає в електромагнітному спектрі проміжне положення між світлом і рентгенівським випромінюванням. Відноситься до області не іонізуючих випромінювань.

Будь-яке тіло, нагріте до 3000 К і вище, має в своєму спектрі ультрафіолетову компоненту. Чим вище температура тіла, тим у більшій мірі виявляється ультрафіолетова складова спектру.

За способом генерації УФІ відноситься до теплового випромінювання, за характером впливу на речовини - до іонізуючим випромінюванням. По біологічному ефекту виділяють три області УФІ: УФ-А (λ = 400...280 нм); УФ-В (λ = 315...280 нм); УФ-С (λ = 280...200 нм). УФІ більш короткого діапазону (від 180 нм і нижче) сильно поглинається всіма матеріалами і середовищами, у тому числі і повітрям, і тому може мати місце тільки в умовах вакууму.

Виходячи із специфічної біологічної ефективності, область УФІ-З також називають бактерицидною областю спектра, УФІ-В - ерітемной та УФІ-А - загальнооздоровчою.

Ультрафіолетові промені мають здатність викликати фотоелектричний ефект, проявляти фотохімічну активність, викликати люмінесценцію і володіють значною біологічною активністю.

Джерела ультрафіолетового випромінювання (УФ-випромінювання) можна розділити на природні і штучні.

Основним джерелом УФ-випромінювання природного походження є Сонце. З усього спектру УФ-випромінювання Сонця тільки невелика довгохвильова частина досягає земної поверхні (λ > 0,29 мкм). Інша частина УФ-спектра, в особливості короткохвильова, поглинається атмосферою, що надає сильний вплив на атмосферні процеси. Загальний потік УФ-випромінювання в областях А та £ становить 3...4% загальної енергії сонячних променів.

Велика кількість джерел УФ-випромінювання має техногенне походження: техногенні джерела, що мають температуру вище 2000 °С (лазерні установки, електричні дуги від зварювальних робіт, плазма, розплавлений метал, кварцове скло і т. п.), ртутні випрямлячі; люмінесцентні джерела (лампи газорозрядні та дугові ртутні), що використовуються у поліграфії, хімічному та деревообробному виробництві, сільському господарстві, при кіно - і телезйомках, дефектоскопії та інших галузях виробництва, а також у охороні здоров'я.

Інтенсивним джерелом УФ-випромінювання з безперервним спектром є електронні потоки синхротронов, лінійних прискорювачів, потужних приладів НВЧ.

До техногенних джерел УФ-випромінювання належать понад 70 різних лазерних систем, що працюють в ультрафіолетовому та вакуумному ультрафіолетовому діапазоні.

До техногенних джерел УФ-випромінювання відносяться деякі металургійні печі і домни по виплавці високотемпературних металів і сплавів із застосуванням кисневого дуття, потужних електронних і плазмових потоків і т. п.

Величини УФ-випромінювання розрізняються за енергетичною природою і по ефективності впливу на біологічні об'єкти. Для біологічних об'єктів оцінюють бактерицидні і эритемные величини випромінювань.

В залежності від інтенсивності та довжини хвилі УФ-випромінювання діє двояко на живі організми. З одного боку, малі дози УФ-опромінення роблять благотворний вплив на людину і тварин, сприяючи утворенню вітамінів групи D. З іншого боку, УФ-опромінення надає шкідливе (небезпечне) дію на живі організми. Встановити межу дозволеного і згубного у ряді випадків буває дуже складно. Фізіологічна дія УФ-випромінювання проявляється в наступному:

* УФ-А призводить до флюоресценції;
* УФ-викликає зміни в складі крові, шкіри, впливає на нервову систему;
* УФ-С діє на клітини.

УФ-випромінювання від виробничих джерел, в першу чергу електрозварювальних дуг, може стати причиною гострих і хронічних професійних уражень. Найбільш схильний до дії УФ-випромінювання зоровий аналізатор. УФ-випромінювання виробничих джерел здатні змінювати газовий склад атмосферного повітря внаслідок його іонізації. При цьому в повітрі утворюються високотоксичні гази озон і оксиди азоту, становлять велику професійну небезпеку, особливо при зварювальних роботах в обмежених, погано провітрюваних приміщеннях.

### 6.4. Лазерне випромінювання

Квантові генератори чи лазери використовуються:

- для створення точних вимірювальних приладів та інструментів;

- в оптичній локації;

- для передачі інформації;

- прецизійного зварювання;

- свердління тугоплавких матеріалів.

Застосування лазерів у галузі зв'язку і на телебаченні особливо перспективне.

В лазерах генерується когерентне випромінювання оптичного діапазону великої інтенсивності, у вузькому пучку випромінювання, а густина потоку потужності може досягати 1012-1013 Вт/см2.

Випромінювання електромагнітні (лазерні) охоплюють практично весь оптичний діапазон, від ультрафіолетової до інфрачервоної області спектра випромінювання .

Генератори оптичного діапазону працюють на основі змушених випромінювань, джерелами яких є робочі речовини, що генерують електромагнітні випромінювання оптичного діапазону (що створюють лазерний ефект) внаслідок порушення їхніх атомів електромагнітною енергією іншого джерела.

Іншим джерелом у твердо тілих лазерах служать газорозрядні імпульсні лампи, а в газових лазерах - генератори НВЧ.

Робочою речовиною у твердо тілих квантових генераторах застосовують кристали рубіну, скла з домішкою неодиму, диспрозію, вольфрамат кальцію, а в газових генераторах найбільш простого типу - суміш гелію з неоном і азотом. Робоча речовина випромінює хвилі визначеної довжини. Наприклад, рубіновий лазер створює хвилю довжиною X = 0,6943 мкм, неодимовий X = 1,06 мкм, лазер на суміші вуглекислого газу з неоном і азотом X = 10,6 мкм.

Коли лазерні випромінювання потрапляють на біологічні тканини людини, тоді вони чинять теплову, механічну і електрохімічну дію на організм людини. Тепловий вплив виявляється в поглинанні енергії лазерного випромінювання біологічними тканинами і, в першу чергу, шкірою. Шкіра поглинає велику частину енергії, в результаті чого виникають опіки. Ступінь опіку шкіри у великій мірі залежить від інтенсивності і частоти випромінювання, а також від ступеня пігментації шкіри в момент опіку. Чим більша частота, тим сильніший опік. Чим темніше шкіра, тим більша частина енергії нею поглинається і тим сильніший її опік.

Коли велика інтенсивність опромінення впливає на людину, можуть уражатися внутрішні органи, викликаючи набряки, крововиливи, омертвіння тканин. Тоді може мати місце навіть згортання і розпад крові.

Якщо інтенсивності лазерного випромінювання в організмі людини невеликі, можуть виникнути функціональні порушення - в першу чергу в нервовій і серцево-судинній системах, що виявляється в зниженні або підвищенні артеріального тиску, підвищенні пітливості, виникненні головного болю, стомлюваності, дратівливості. Такі зміни оборотні, якщо вжити заходів щодо виключення опромінення і дотримання належного режиму праці й відпочинку.

**Механічний вплив** виявляється в розриві тканин, що виникає в результаті різкого скипання рідинних структур живої тканини, підвищення тиску й ударної хвилі.

**Електрохімічний вплив** лазерного випромінювання зумовлює іонізацію рідинних компонентів і утворення нових структур, не властивих живій матерії.

В першу чергу і найбільш небезпечне лазерне випромінювання для очей. Небезпека виникає тоді, коли промінь лазера фіксується на сітківці ока, що приводить до її коагуляції. Наслідком коагуляції є сліпота ураженої області сітківки. Найбільш небезпечне ураження центральної ямки сітківки - невелика область діаметром 0,2 мм поблизу центра сітківки. Це серйозна втрата зору. Внутрішнє середовище ока допускає випромінювання оптичного квантового генератора з довжинами хвиль 0,33-1,4 мкм на сітківку ока. Найбільша прозорість ока (до 100%) має місце для довжин хвиль 0,5-0,9 мкм, тому випромінювання рубінового генератора з X = 0,6943 мкм проходить до сітківки без втрат і сприймається як червоний колір, а випромінювання генератора, що працює на суміші вуглекислого газу з неоном і азотом з X = 10,6 мкм, поглинається рогівкою ока [20].

Для очей небезпечним є не тільки пряме випромінювання лазера, але й відбите від будь-якої поверхні. Коли від лазерного випромінювання око віддаляється на видиму відстань, то це не врятовує його від ураження, тому що в оптичній системі ока віддалені об'єкти фокусуються на сітківці менше, ніж прилеглі об'єкти.

Шкідлива робота з оптичними квантовими генераторами пов'язана з такими шкідливими виробничими факторами, як: сліпуче яскраве світло лампи накачування, озон, електромагнітні випромінювання НВЧ.

Лазерні квантові генератори слід розміщувати в спеціально призначених для цих цілей приміщеннях, двері яких повинні мати спеціальне блокування з світловим табло, що включається на час роботи лазерних генераторів. Приміщення повинні задовольняти усім вимогам санітарних норм і повинні бути обладнані припливно-витяжною вентиляцією.

Приміщення усередині, а також устаткування і предмети, що знаходяться в ньому, не повинні мати дзеркально відбиваючих поверхонь, у противному разі їх варто фарбувати в темні матові тони.

Квантовий генератор повинен установлюватися таким чином, щоб шлях променя проходив в найменш відвідуваній людиною зоні, а місця фокусування променя під час його роботи були захищені діафрагмами. Наприкінці променя розміщують пастку для поглинання відбитого випромінювання. Для зменшення розсіювання випромінювання лінзи, призми й інші тверді перешкоди на шляху променя повинні бути обладнані блендами. У деяких випадках необхідно відбивати весь хід променя.

Для візуального юстирування пристрої повинні бути оснащені захисними поглинаючими фільтрами. При роботі з оптичними квантовими генераторами їх розташування за польових умов слід позначати спеціальними знаками.

Ширми, що екранують, штори, завіси можна виготовляти з бавовняної чорної фланелі.

Захист очей слід здійснювати захисними окулярами, скло яких має велику оптичну щільність. Закордонні дослідники пропонують використовувати скло щільністю 9 на довжинах хвиль 0,6943 і 1,06 мкм. Для запобігання ушкодження скла випромінюванням оптичного квантового генератора перед ним пропонується розміщувати скло з меншим коефіцієнтом поглинання.

Окуляри СЗС-22, виконані із синьо-зеленого скла, практично непроникні для випромінювань з довжинами хвиль 0,63-1,5 мкм.

Робітники в процесі роботи з оптичними квантовими генераторами для профілактики захворювань повинні два рази на рік проходити медичні огляди за участю терапевта, гематолога, офтальмолога і невропатолога.

Дослідження і обслуговування оптичних квантових генераторів повинні проводити працівники не молодше 18 років, які не мають медичних протипоказань.

### 6.5. Висновки

Розроблений система охоронного відеоспостереження, пов'язана з безпосередньою взаємодією з випромінюванням оптичного діапазону (ІЧ – підсвітка, засоби освітлення, використання ВОС тощо). У розділі були проаналізовані негативні чинники випромінювання оптичного діапазону, які можуть діяти на людину. Особливу увагу було приділено питанням впливу квантових генераторів або лазерів. Саме вони є основним засобом формування інформаційного потоку у система оптико-волоконних ліній зв’язку.

Зважаючи на небезпеку, пов’язану з експлуатацією оптичного обладнання, були розроблені заходи по захисту людини від оптичних віпромінюань.

**ВИСНОВКИ**

На сьогоднішній день стало дуже популярним встановлення системи відеоспостереження. Це обумовлено тим, що люди прагнуть захистити та вберегти власний будинок, від протиправних дій, та недобросовісніх людей, а також шахраїв. Саме по цій причині , СВС вважають найдосконалішими та найінформативнішими системами безпеки. Ці викладки стали основним спонукаючи фактором, для написання даної дипломної роботи.

У цій дипломній роботі були розібрані загальні принципи побудови системи «Розумний будинок», його структурну систему, технічні засоби охорони, а також систему відеоспостереження .

Було розглянуто існуючі види систем безпеки об’єкту та усі складові цих систем, і безумовно усі види відеоспостереження, їх основні характеристики та пристрої, призначені для роботи в складі системи відеоспостереження. Зроблений аналіз дозволив обрати надійні та не дорогі види камер, і усі необхідні прилади для спостереження за об'єктом, які було використано у робочому проекті.

Проведено огляд систем відеоспостереження для системи «Розумний будинок», який показав, що розробка таких систем є перспективним напрямком в частині забезпечення охоронної безпеки об’єкту охорони. Вибір певного обладнання для вирішення поставлених перед СВС вимог, супроводжувався розрахунками та обґрунтуванням з точки зору практичного досвіду їх використання.

Проведене обстеження об’єкту охорони дозволило виявити можливі місця проникнення зловмисників, на основі чого був запропонований проект системи спостереження в інтелектуальній системі «Розумний будинок».

Також, увага була приділена питанням правової бази використання СВС та розглянуті аспекти технічного обслуговування системи.

У останніх розділах були розглянуті питання охорони праці при використанні РЕА та ЕОМ та питання захисту навколишнього середовища від шкідливих факторів, пов’язаних з експлуатацією розробленої системи.

**ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Електронний ресурс [Умный дом. Дом 21 века. Електронний ресурс:http://www.housecontrol.ru/].

2. Електронний ресурс [Сервисное обслуживание системы «умняй дом». <https://smarthouser.by/>].

3. Електронний ресурс [Охранные системы безопасности, системы охраны, обеспечение безопасности. <http://secur.ua/umniy-dom/>].

4. Електронний ресурс [Управление климатом в системе «умный дом».:http://www.klimatvdomi.com/].

5. Електронний ресурс [Система пожарной безопасности "Умного дома" и ее преимущества. <http://baurum.ru/_library/?cat=safety-systems&id=4798>]

6. Електронний ресурс [Умный дом – от идеи к воплощению. <http://homesystems.com.ua/>].

7. ГОСТ 12.1 004 - 91 ССБТ. Пожежна безпека. Загальні вимоги.

8. Корольов С.Г. Правила улаштування електроустановок. Енергоатоміздат.– М.: Екскмо, 2008. – 256 с.

9. Буденний Ф.А. Системи охоронної та пожежної сигналізації. – СПб.: Питер, 2002. – 360с.

10. Синилов В.Г. Системи охоронної, пожежної та охоронно-пожежної сигналізації. – М .: ІРПО; ПрофОбрІздат, 2001. – 267 с.

11. Старшинов Б.П. Системи пожежної безпеки. – М .: Изд-во Москва, 2003. – 164 с.

12. Електронний ресурс [http://allofremont.com.ua/priemno\_ kontrolnye\_pribory\_oxranno\_pozharnoj\_signalizacii\_16].

13. Електронний ресурс [allofremont.com.ua].

14. . Система «умный дом». [Электронный ресурс]. Режим доступа: http://energorus.com/ (дата обращения: 15.11.2018). Загл. с экр.

15. Концепция системы «Умный Дом». [Электронный ресурс]. Режим доступа: http://www.ascentis.ru/ (дата обращения: 15.11.2018). Загл. с экр.

16. Система умный дом: дом века. [Электронный ресурс]. Режим доступа: http://nazarov-gallery.ru/ (дата обращения: 15.11.2018). Загл. с экр.

17. Автоматизированная система управления освещением дома. [Электронный ресурс]. Режим доступа: http://nazarov-gallery.ru/ (дата обращения: 15.11.2018). Загл. с экр.

18. Новый уровень эффективности функционирования системы «Умный дом» Рычкова В.А. Email: [Rychkova658@scientifictext.ru](mailto:Rychkova658@scientifictext.ru)

19. Рычкова Виктория Андреевна - магистрант, кафедра электроэнергетики, Мурманский государственный технический университет, г. Мурманск