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

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Комп'ютерна інженерія»

Група: 2БКС-26

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

здобувача освіти денної форми навчання

БКС.26.21.000.КРБ

ЩЕДРОВА
ДАНИЛА
МИКОЛАЙОВИЧА

м. Одеса
2022 р.

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

Спеціальність: **123 «Комп'ютерна інженерія»**
Освітня програма: «**Комп'ютерна інженерія»**
Група: **2БКС-26**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційній роботі бакалавра на тему:_____

«Дослідження безпроводових технічних засобів охорони»

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

Виконавець _____ (Щедров Д.М.)
Керівник _____ (Кільдишев В.Й.)

Консультанти:
з охорони праці_____ (Чорновол Н.І.)
з дотримання вимог ЄСКД _____ (Петрашова В.І.)
старший консультант _____ (Скорнякова О.В.)

До захисту допущений
Завідувачка кафедри _____ (Іванова Л.В.)
Завідувач відділення _____ (Суліма Ю.Ю.)

Захист «____»_____ 2022 р. Протокол ДКК №_____
Оцінка ДКК _____

Секретар ДКК _____

АНОТАЦІЯ

Метою даної роботи є дослідження безпроводових технічних засобів охорони.

В бакалаврській роботі розглянуто основні етапи впровадження автоматичних систем пожежної сигналізації АСПС на об’єктах згідно національного стандарту ДСТУ-Н CEN/TS 54-14:2009. Детально досліджено склад систем протипожежного захисту (АСПС, СПЗ, СОУЕ), наведено декілька класифікацій датчиків пожежних сповіщувачів. Згідно завдання, розглянуто застосування безпроводових технологій. Досліджено компонентний склад ОПС, розраховано технологічні параметри. Розглянуто критерії ефективності безпроводових систем пожежної сигналізації.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

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

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

Освітня програма **«Комп'ютерна інженерія»**

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР_____

_____

"_____"_____2022 р.

З А В Д А Н Н Я

на кваліфікаційну роботу бакалавра

Здобувачеві (здобувачці) освіти Щедрову Данилу Миколайовичу

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи

Дослідження безпроводових технічних засобів охорони

30 грудня 1 306-А2-ОД

затверджена наказом по коледжу від "____"_____202___р. №_____

2. Термін здачі кваліфікаційної роботи_____

3. Вихідні данні до проекту (роботи) Об'єкт аналізу – системи охоронного телебачення як елемент ТЗО. Системи аналогового відеоспостереження високої чіткості. Транспортне середовище СОТ – проводове, безпроводове. Класи загроз – інфраструктури, обладнання, ПЗ, мережеві, з боку персоналу

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

1Вступ. 1. Базові відомості щодо напряму технічних засобів охорони. 2. Порівняння безпроводових технологій за масштабом мереж 3. Системи безпроводового відеоспостереження. 4. Безпроводові системи охоронної сигналізації. 5. Охорона праці. Висновки. Перелік використаних джерел. Додато

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

Презентація (10 слайдів)

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Основний	Кільдішев В.Й.	*30.11.2021*	18.05.2022
Охорона праці	Чорновол Н.І.	*04.05.2022*	18.05.2022
Нормоконтроль	Петрашова В.І.	*04.05.2022*	18.05.2022
Старший консультант	Скорнякова О.В.	*04.05.2022*	18.05.2022

7. Дата видачі завдання

_____30.11.2021_____

Керівник _____

(підпис)

Завдання прийняв до виконання _____

(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1	Архітектура та базові відомості щодо		
	напряму технічних засобів охорони	**27.05.2022 р.**	
2	Аналіз безпроводових технологій при		
	використанні технічних засобів охорони	**02.06.2022 р**	
4	Дослідження безпроводових рішень в		
	напрямку ТЗО	**04.06.2022 р.**	
5	Виконання розділу «Охорона праці»	**08.06.2022 р.**	
6	Виконання графічної частини роботи	**13.06.2022 р.**	
7	Чистове оформлення пояснювальної		
	записки кваліфікаційної роботи	**15.06.2022 р.**	
8	Підготовка доповіді та презентації до захисту	**17.06.2022 р.**	
9	Отримання рецензії, відповіді на		
	зауваження рецензента	**21.06.2022 р.**	
10	Захист роботи	**24.06.2022 р.**	

Виконавець _____

(підпис)

Керівник _____

(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 26.21.000.00 КР	*Кваліфікаційна робота*		
А4			***БКС 26.21.000.00 КР ПЗ***	*Пояснювальна записка*		
			БКС26.21.000.00 КРБ МП	*Мультимедійна презентація*		

Ізм.	Арк.	№ докум.	Підпис	Дата	*БКС 26.21 000.00 БКР ПЗ*		
Розробив		Щедров Д.М.			Дослідження безпроводових технічних засобів охорони	Літ.	Аркуш 3 / Аркушів
Перевірив		Кільдішев В.Й.				Н Д П	
Н. Контр.		Петрашова В.				ВСП «ОТФК ОНТУ» гр.БКС-26	
Затверд.		Іванова. Л.В.					

ЗМІСТ

ВСТУП 6
……
1 АРХІТЕКТУРА ТА БАЗОВІ ВІДОМОСТІ ЩОДО НАПРЯМУ ТЕХНІЧНИХ ЗАСОБІВ ОХОРОНИ…….. 7
1.1 Системи охоронно-тривожної сигналізації……..… 7
1.2 Системи пожежної сигналізації…… 9
1.3 Система відеоспостереження…… 11
1.4 Система контролю та управління доступом…… 15
2 АНАЛІЗ БЕЗПРОВОДОВИХ ТЕХНОЛОГІЙ ПРИ ВИКОРИСТАННІ ТЕХНІЧНИХ ЗАСОБІВ ОХОРОНИ……..… 17
2.1 Види безпроводових технологій……. 17
2.2 Порівняння безпроводових технологій за масштабом мереж 23
3 ДОСЛІДЖЕННЯ БЕЗПРОВОДОВИХ РІШЕНЬ В НАПРЯМКУ ТЗО 26
3.1 Системи безпроводового відеоспостереження…… 26
3.1.1 Класифікація безпроводових відеокамер…….…. 26
3.1.2 Застосування обладнання на базі брендів Trassir та CISCO…… 32
3.1.3 Аналіз параметрів системи безпроводового IP-відеоспостереження……... 34
3.2 Безпроводові системи охоронної сигналізації……..…… 40
3.2.1 Охоронна сигналізація на базі обладнання Ajax……..…. 40
3.2.2 Охоронна сигналізація на базі обладнання Каліпсо……..… 43
3.2.3 Охоронна сигналізація на базі обладнання Лунь Р……...… 45
4 ОХОРОНА ПРАЦІ……...…… 48
ВИСНОВКИ …… 50
ПЕРЕЛІК ПОСИЛАНЬ…… 51

ВСТУП

Питання наявності охоронної сигналізації стають все більш актуальними. Щорічна статистика міністерства внутрішніх справ говорить про збільшення кількості грабежів в різних регіонах України. Наприклад, у середньому, тільки в столиці сьогодні здійснюється близько 40 квартирних крадіжок на добу. В цілому, розкриття даного виду злочинів складає 30% .

Аналіз крадіжок, що сталися останнім часом, показує, що зловмисники проникають, насамперед, у ті приміщення та будівлі, де технічна укріпленість слабка – пустотілі дерев'яні двері, замки низької секретності, дешеві і низькоякісні елементи захисту. Особливо вразливими об'єктами посягання є перші поверхи житлових будинків. Популярні металопластикові вікна давно не є бар'єром для зловмисника. Залізні двері з хитромудрими замками, грати на вікнах – це перепони серйозніше, але також не зупиняти кваліфікованого зловмисника. Преса та телебачення рясніють повинними стрічками про розтин найновіших замків, дверей, в інтернеті є багато інформації про методи дій порушників і їх методиках обходу інженерно-технічних елементів укріпленості.

Найбільш надійно захищені від крадіжки ті приміщення, де окрім надійних дверей і решіток доданий ще один елемент – охоронна сигналізація з виведенням сигналу тривоги на ПЦС МВС або приватної охоронної компанії. Звичайно ж, охоронна сигналізація не зможе перешкоджати проникненню злодія всередину приміщення, що охороняється, але по сигналу, поданого на пульт позавідомчої охорони, прибуде наряд міліції, і якщо чи не затримає злочинця на місці, то розкриє крадіжку за «гарячими слідами» і поверне вам ваше майно.

1 АРХІТЕКТУРА ТА БАЗОВІ ВІДОМОСТІ ЩОДО НАПРЯМУ ТЕХНІЧНИХ ЗАСОБІВ ОХОРОНИ

1.1 Система охоронно-тривожної сигналізації

Охоронна сигналізація – це набір електронних пристроїв для виявлення несанкціонованого доступу на об'єкт, генерування сигналу тривоги та передачі на пульт охорони.

Можна виділити такі основні компоненти системи:

- датчики;

- приймально-контрольні прилади (ПКП);

- оповіщувачі.

Структурна схема об'єктової охоронної сигналізації представлена рис.1.1.

Оповіщувачі або охоронні датчики, по суті, є органами почуттів усієї охоронної системи. Вони перетворюють контрольований параметр навколишнього середовища електричний сигнал і передають його на обробку в приймально-контрольні прилади. Існує багато різних детекторів. За принципом дії можна поділити їх на дві основні групи:

- пасивні: інфрачервоні, акустичні, магнітоконтактні, барометричні, інерційні;

- активні: радіохвильові, ультразвукові.

Використовуються і комбіновані активно-пасивні датчики, а також спеціалізовані: ємнісні, електромагнітні, індукційні.

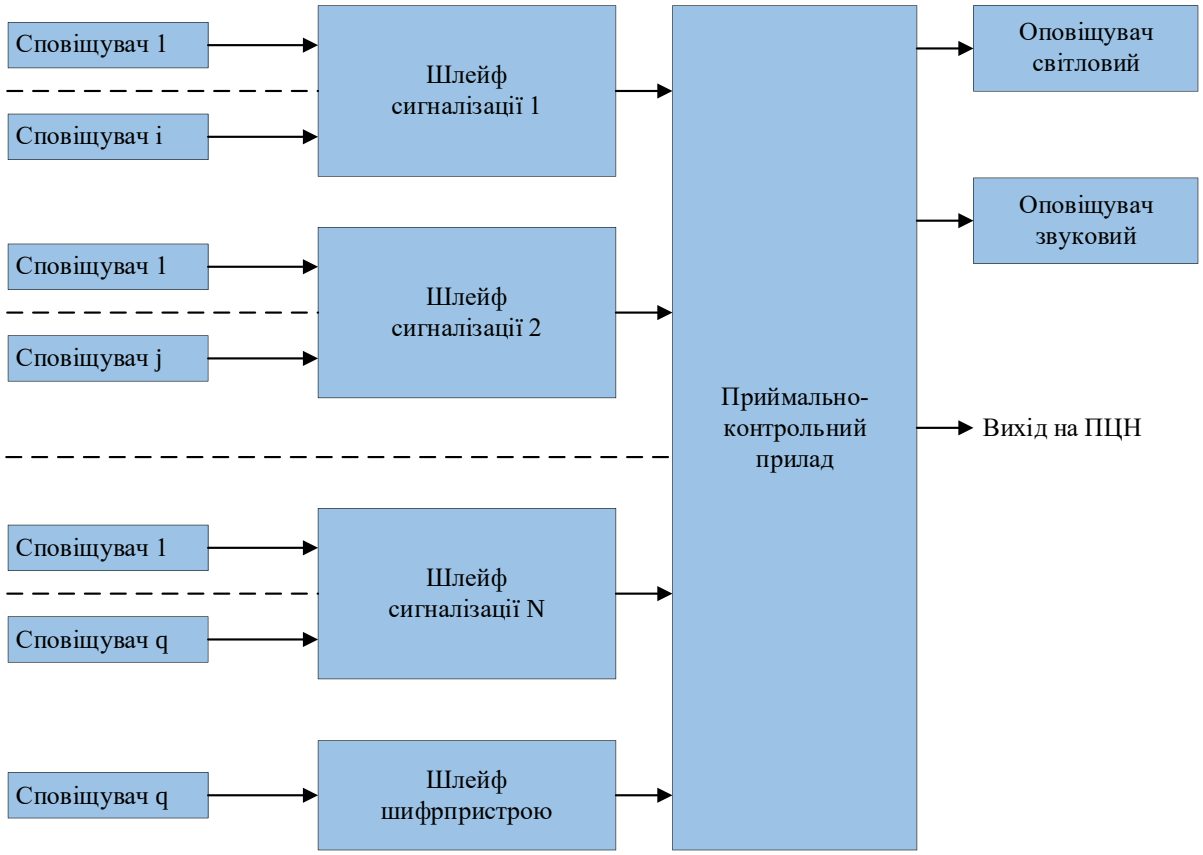
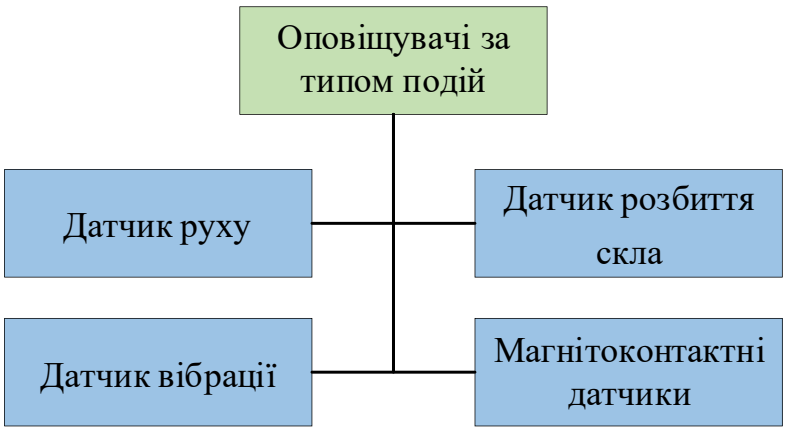


Рисунок 1.1 – Структурна схема об'єктової охоронної сигналізації

За типом подій, на які реагує оповіщувач, можна виділити:



Датчик руху - ІЧ-датчик, що вловлює теплове випромінювання PIR елементом і за допомогою спеціальних лінз, що відстежує переміщення їхнього джерела.

Датчик вібрації - пристрій, що реагує на вібрацію, що використовується для захисту від пролому стін, розкриття сейфів, розбиття вікон.

Датчик розбиття скла - акустичний прилад, що сприймає гучні звуки у певному діапазоні частот, характерному для дзвону розбитого скла.

Магнітоконтактні датчики - пристрої, що спрацьовують при розриві магнітокерованого контакту під час відкриття дверей або вікон.

Мозковим центром системи охоронної сигналізації є приймально-контрольний прилад (ПКП). На нього надходить інформація щодо спрацьовування від встановлених датчиків. У системах охоронно-пожежної сигналізації ПКП призначені для:

- контролю стану шлейфів (датчиків) системи;

- індикації режимів роботи апаратури;

- формування (у деяких випадках та передачі) тривожних та службових повідомлень;

- управління іншим обладнанням та системами.

1.2 Системи пожежної сигналізації

Враховуючи, що однією з найважливіших складових загальної безпеки будь-якого сучасного об’єкту є його надійний захист від пожеж, то і система управління пожежною безпекою має посісти відповідне місце у сфері загального управління.

Установка пожежної сигналізації – це сукупність технічних засобів, призначених для виявлення пожежі, обробки та надання в заданому вигляді повідомлення про пожежу на об'єкті, що захищається, для видачі команд на включення автоматичних установок пожежогасіння та управління іншими технічними засобами.

В склад будь-якої установки пожежної сигналізації входять пожежні сповіщувачі, приймально-контрольні прилади, світлові і звукові оповіщувачі,

технічні засоби передачі інформації до пультів централізованого спостереження, пультів зв'язку пожежних частин та інше.

При плануванні та побудові установки пожежної сигналізації необхідно враховувати велику кількість чинників. Уявлення оператора, який проводить проектно-пошукові роботи з проектування автоматичного протипожежного захисту, повинні співпадати з вимогами відповідних регіональних контролюючих органів, нормативних документів, відомчих норм і рекомендацій.

Планування і побудова автоматичного протипожежного захисту, зокрема пожежної сигналізації, завжди прив'язане до певного проекту, тобто повинні враховуватися конкретні характеристики об'єкта, захист якого необхідно забезпечити. На рис. 1.2 зображено загальну схему системи пожежної сигналізації.

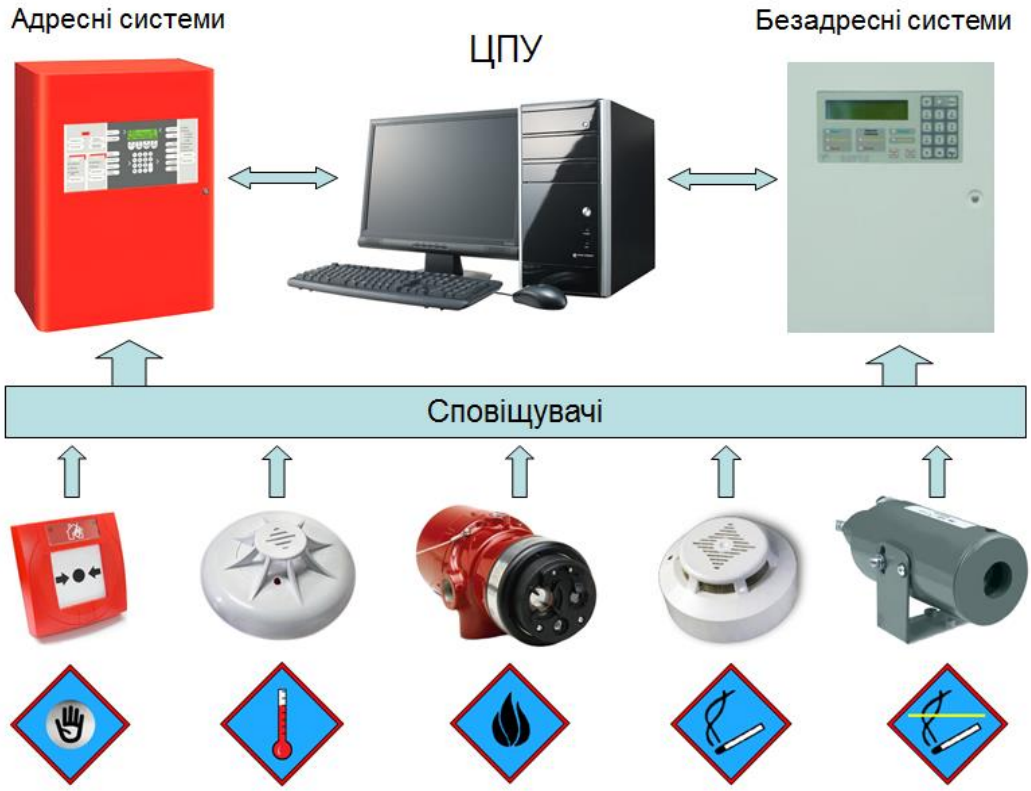


Рисунок 1.2 – Загальна схема системи пожежної сигналізації

1.3 Система відеоспостереження

Сьогодні на ринку відеоспостереження (охоронного телебачення) представлено два основних напрямки – аналогове та цифрове.

Однак більш правильно сучасні системи відеоспостереження розділяти по типу сигналу на аналогові, комбіновані (цифро-аналогові), гібридні, мережеві. Загальну класифікацію систем відеоспостереження за базовими ознаками представлено на рис. 1.3.

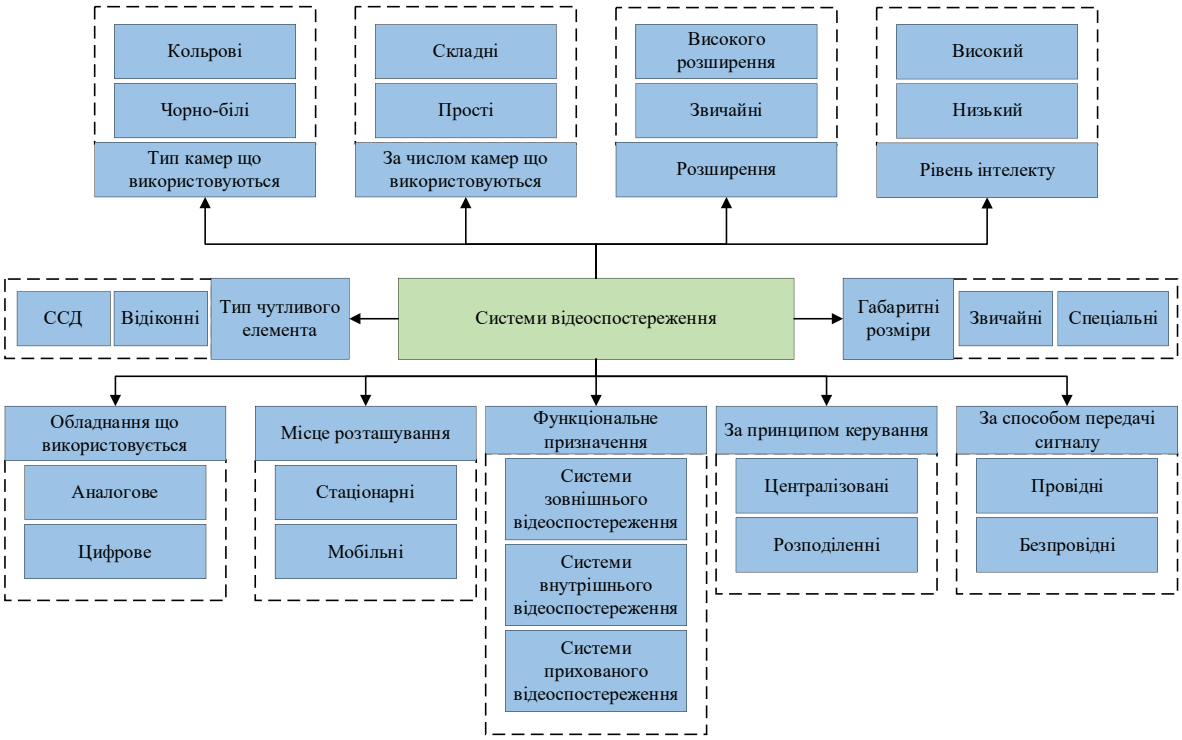


Рисунок 1.3 – Класифікація систем відеоспостереження за базовими ознаками

Залежно від типу використовуваного обладнання системи відеоспостереження поділяють на аналогові та цифрові.

Аналогові системи відеоспостереження використовуються там, де необхідно організувати відеоспостереження у невеликій кількості приміщень та сигнал із відеокамер записувати на відеомагнітофон: у невеликих офісах,

складських приміщеннях, автостоянках та інших об'єктах. Основу аналогових систем відеоспостереження складають камери відеоспостереження. Ці камери являють собою оптичні пристрої, ПЗЗ-матриці яких формують відеосигнал зі світлового потоку, що проходить через об'єктив та групу лінз і потрапляє на матрицю. Аналогові відеокамери можна модернізувати, використовуючи блок перетворення аналогового відеосигналу на цифровий. Такі модернізовані відеокамери можна використовувати у цифрових системах відеоспостереження.

Переваги аналогових систем відеоспостереження полягають у невисокій вартості обладнання, високій надійності, простоті конструкції та експлуатації, що дозволяє використовувати їх персоналом невисокої кваліфікації. Недоліками таких систем прийнято вважати необхідність постійного обслуговування (заміна відеокасет, архівування знятого матеріалу, обслуговування відеомагнітофонів) та деяку функціональну обмеженість, зумовлену використанням аналогової апаратури.

Цифрові системи відеоспостереження використовуються для безпеки особливо відповідальних або територіально-розподілених об'єктів. Ці системи можуть інтегруватися у комплексні системи безпеки.

Переваги цифрового запису очевидні: це необмежений час зберігання запису, практично миттєвий доступ до будь-якого сюжету з архіву, можливість простої передачі відеоінформації локальними та глобальними обчислювальними мережами, можливість обробки кадрів з використанням різних алгоритмів фільтрації та підвищення якості зображення з подальшим роздрукуванням на звичайному принтері. При цьому апаратна частина цифрових систем відеоспостереження скорочується до трьох компонентів: цифрової відеокамери, плати відеовведення (відеозахоплення, відеообробки) та персонального комп'ютера зі спеціальним програмним забезпеченням (відеосервер). Починаючи з деякого рівня складності, цифрові системи відеоспостереження виявляються економічно ефективнішими за аналогові. Крім того, можна вказати такі переваги цифрових систем відеоспостереження:

- якісна картинка відео;
- можливість комп'ютерної обробки та аналізу відеоматеріалу;
- застосування дешевих цифрових носіїв інформації для відеоархіву;
- висока швидкість доступу до відеоархіву;
- використання стандартних комп'ютерних ліній зв'язку;
- можливість передачі інформації мережами LAN/WAN;
- можливість транслювання відеозображення в Інтернет;
- високий рівень інтеграції з сучасними системами безпеки.

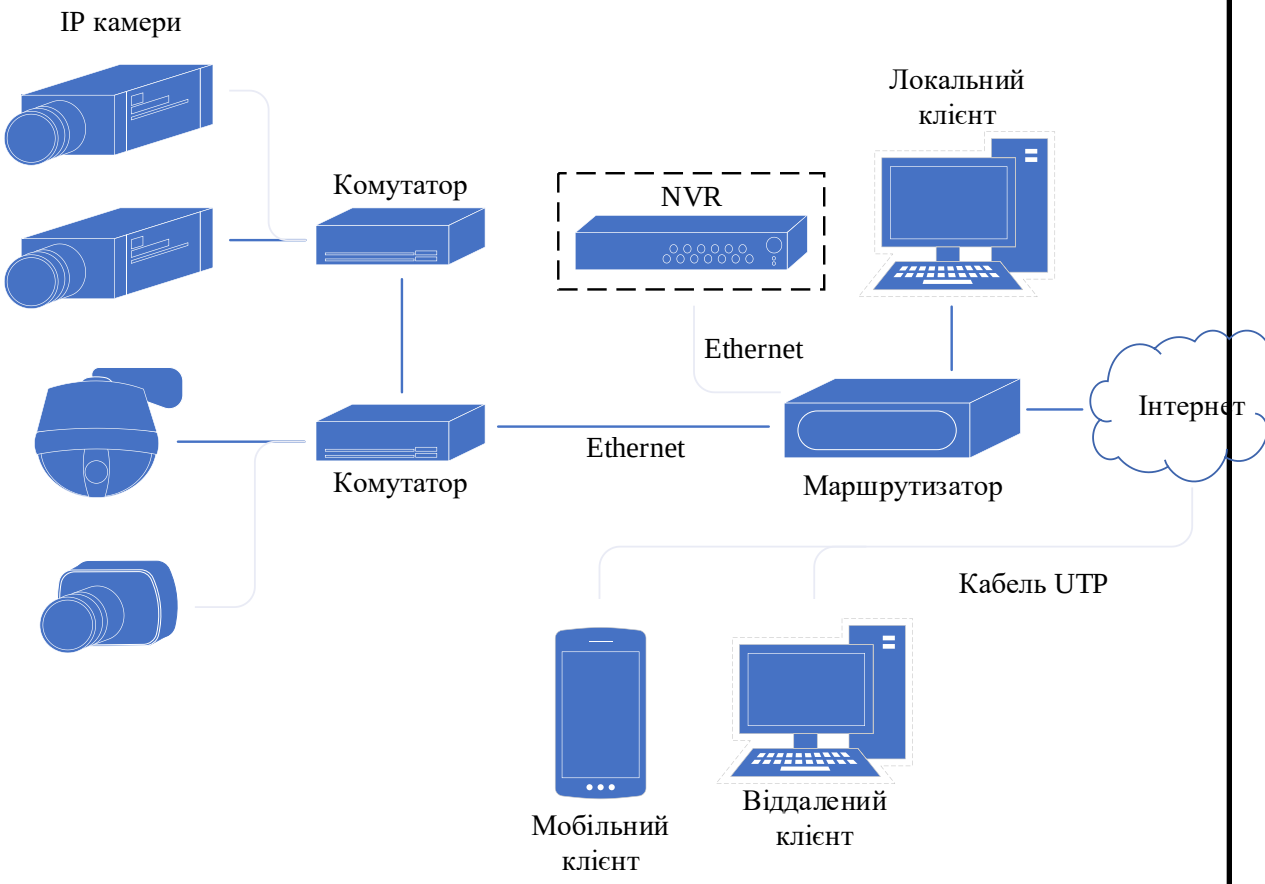


Рисунок 1.4 – Цифрова система відеонагляду на базі IP-камер та NVR

Основними елементами СОТ є:

- камери відеоспостереження - аналогові або IP-відеокамери, як джерело відеосигналів;

- відеосервери та відеореєстратори - компютери або апаратні пристрої з встановленим програмним забезпеченням для здійснення прийому, обробки, зберігання та передачі відеосигналу, що надходить від відеокамер;

- робочі місця оператора (АРМ) - комп'ютери з попередньо встановленим програмним забезпеченням для роботи оператора відеоспостереження, яка в основному зводиться до перегляду відео в реальному часі та відео з архіву. Робоче місце оператора може бути організоване безпосередньо на відеосервері та відеореєстраторі або віддалено, через мережу, через програму-клієнт;

- системи зберігання даних - рішення з урахуванням пристроїв зберігання даних тривалого зберігання видеорхива.

1.4 Системи контролю і керування доступом

Системою контролю і управління доступом (СККД) називають сукупність програмно-технічних засобів і організаційно-методичних заходів, за допомогою яких чоловік може вирішувати завдання контролю відвідування співробітниками окремих приміщень, управління цим процесом, оперативного контролю переміщення персоналу і за часом його находження на території об’єкту. Дійсно, СККД не лише апаратура і програмне забезпечення, це продумана система управління руху персоналу.

Традиційні методи ідентифікації особистості, в основі яких перебувають різні ідентифікаційні карти, ключі або унікальні дані, такі як, наприклад, пароль не є надійними в тім ступені, що потрібно на сьогоднішній день. Природним кроком у підвищенні надійності ідентифікаторів стали спроби використання біометричних технологій для систем безпеки.

Сучасна система контролю і керування доступом повинна:

–забезпечувати контроль доступу і управління ним на різних типах контрольно-перепускних пунктів (людських, автомобільних, з/д);

–захищати від провезення в ті або інші місця заборонених предметів (зброї, вибухових речовин, матеріалів, що діляться, і т. п.);

–затримувати потенційних порушників;

–підтримувати різні способи посвідчення осіб, що проходять, у тому числі біометричні;

–мати відкриту для цілей інтеграції програмно-апаратну платформу;

–мати високі адаптивні властивості;

–забезпечувати автоматизацію процесів керування службами безпеки об’єкту і координацію їх діяльності;

–функціонувати в умовах поразки компонентів системи і в інших надзвичайних ситуаціях.

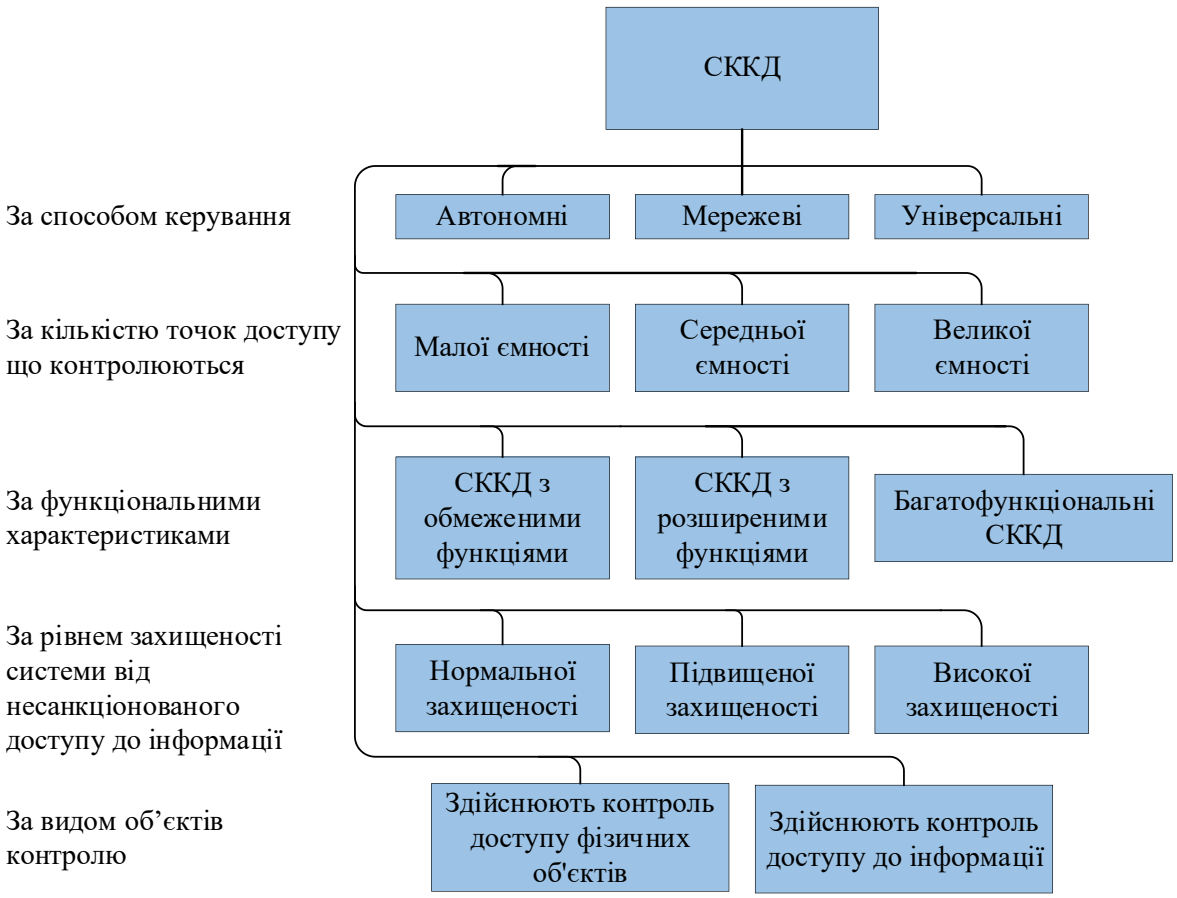


Рисунок 1.5 – Загальна класифікація СККД

2 АНАЛІЗ БЕЗПРОВОДОВИХ ТЕХНОЛОГІЙ ПРИ ВИКОРИСТАННІ ТЕХНІЧНИХ ЗАСОБІВ ОХОРОНИ

2.1 Види безпроводових технологій

Безпроводові технології - підклас інформаційних технологій, служать для передачі інформації на відстань між двома і більше точками, не вимагаючи зв'язку їх проводами. Для передачі інформації може використовуватися інфрачервоне випромінювання, радіохвилі, оптичне або лазерне випромінювання.

В даний час існує безліч безпроводових технологій, найбільш часто відомих користувачам по їх маркетинговим назвам, таким як Wi-Fi, WiMAX, Bluetooth. Кожна технологія має певні характеристиками, які визначають її область застосування. Бездротові технололіі можна класифікувати по дальності дії, по топології, залежно від сфери застосування і т.д. Розглянемо порівняння бездротових технологій більш детально.

Технологія Bluetooth.

Bluetooth – це інтерфейсна безпровідна технологія. Діаметр мережі 1 – 100 м. Працює в багатопунктовому режимі, не обов’язково в зоні прямої видимості. Головне призначення – створення побутових мереж, приєднання мультимедійної периферії та побутової техніки.

У мережі Bluetooth використовують неліцензований частотний діапазон 2.45 ГГц. Однак у цьому діапазоні працюють багато інших технологій і він має багато завад. Під час передавання даних відбувається псевдовипадковий перехід на іншу частоту (FHSS) – до 1600 разів за 1с. Крім того, реалізовано часовий розподіл каналів. Таким чином, метод доступу в такій мережі гібридний – FHSS/TDMA. Швидкість передавання по всьому радіоканалу – 1 Мбіт/с. Такий підхід забезпечує ліпший захист від завад.

В основі технології Bluetooth лежить об'єднання пристроїв у пікомережі (piconet), які представляють собою невеликі за кількістю елементів і відстані між ними бездротові мережі передачі даних. Елементарна пікомережа - це два пристрої з модулями Bluetooth , які називаються master (головний) і slave (підпорядкований).

Причому master виконує ініціацію і підтримку функціонування з'єднання. Максимальна кількість з'єднань для одного майстра - 7 , а сумарна швидкість передачі даних не перевищує максимум для даної версії технології. Функції master і slave жорстко не фіксуються за пристроями і залежно від завантаження можуть змінюватися. Причому, залежно від структури пікомережі пристрій в різних з'єднаннях може виконувати різні ролі, а також може бути як slave для різних master.

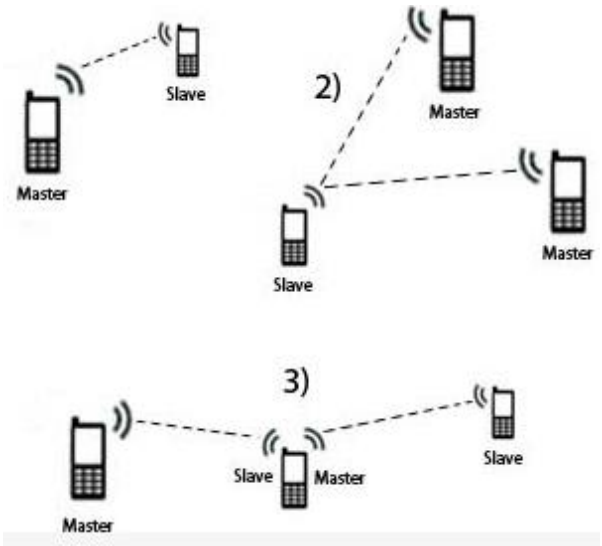


Рисунок 2.1 – Принцип дії технології Bluetooth

Технологія Wi-Fi.

Технологія Wi-Fi – це безпровідний аналог стандарту Ethernet, на основі якого сьогодні побудована велика частина офісних комп'ютерних мереж. Він був зареєстрований в 1999 році і став справжнім відкриттям для менеджерів, торгових агентів, співробітників складів, основним робочим інструментом яких є ноутбук або інший мобільний комп'ютер.

Wi-Fi - скорочення від англійського Wireless Fidelity, що означає стандарт бездротового (радіо) зв'язку, який об'єднує декілька протоколів та має офіційне найменування IEEE 802.11 (від Institute of Electrical and Electronic Engineers - міжнародної організації, що займається розробкою стандартів у галузі електронних технологій). Найбільш відомим та поширеним на сьогоднішній день є протокол IEEE 802.11b (зазвичай під скороченням Wi-Fi мають на увазі саме його), що визначає функціонування бездротових мереж, в яких для передачі даних використовується діапазон частот від 2,4 до 2.4835 гігагерца і забезпечується максимальна швидкість 11 Мбіт/сек. Максимальна дальність передачі сигналу у такій мережі складає 100 метрів, однак на відкритій місцевості вона може досягати й більших значень (до 300-400 м).

Таким чином, Wi-Fi-технологія дозволяє вирішити три важливих завдання:

– спростити спілкування з мобільним комп'ютером;

– забезпечити комфортні умови для роботи діловим партнерам, які прийшли в офіс зі своїм ноутбуком;

– створити локальну мережу в приміщеннях, де прокладка кабелю неможлива або надмірно дорога.

Звичайно, однією точкою доступу мережа може не обмежуватися, що і трапляється при зростанні мережі - базові набори служб утворюють єдину мережу, конфігурація якої носить назву розширеного набору служб (Extended Service Set, ESS). У цьому випадку точки доступу обмінюються між собою інформацією, переданої через дротове з'єднання (рис. 2.2) або через радіомости, що дозволяє ефективно організовувати трафік у мережі між її сегментами (фактично, точками доступу).

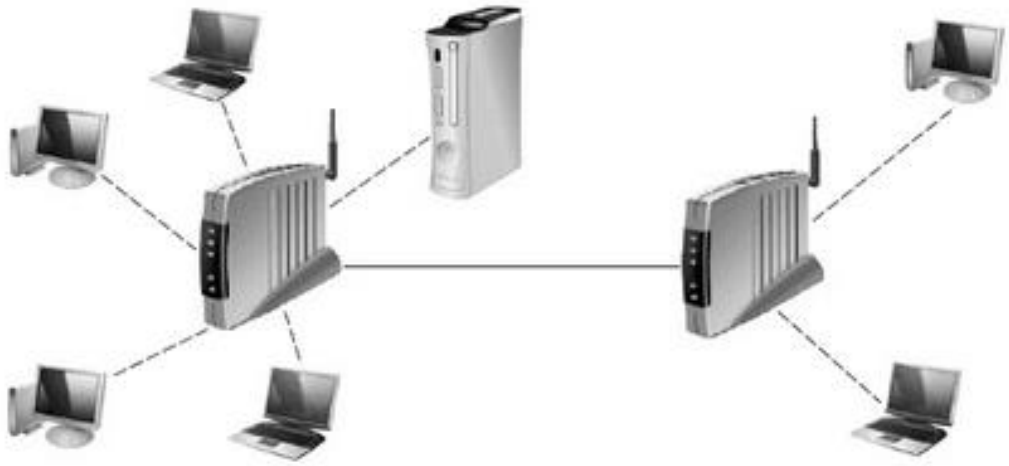


Рисунок 2.2 – Інфраструктурна конфігурація мережі з розширеним набором служб

Технологія WiMAX.

Термін “WiMAX” (Wireless MAN) застосовують для позначення групи технологій для регіональних безпровідних мереж. Топологія мережі WiMAX подібна до топології Wi – Fi. Новий стандарт IEEE 802. 16a, прийнятий у січні 2003 року, визначає технологію, що працює в іншому діапазоні передавання (2 -11 GHz) та не вимагає наявності прямої видимості між передаючою та приймаючою антенами.

WIMAX має схожу з технологією Wi-Fi пропускну здатність, але його перевага у більшому радіусі дії. Мережі WiMAX можуть використовуватися як мережа останньої милі, створюючи недорогу альтернативу для мереж DSL або мереж кабельного телебачення. Її також доцільно застосовувати в місцевостях зі слабкою кабельною інфраструктурою, або там, де прокладати кабельні сполучення недоцільно.

Мережі WiMAX дозволяють передавати дані на відстані до декількох десятків кілометрів зі швидкостями до 70 Мбіт/с в одному радіочастотному каналі.

Між базовими станціями встановлюються з’єднання (прямого сигналу), що використовують діапазон частот від 10 до 66 ГГц, швидкість

обміну даними може досягати 140 Мбіт/с. При цьому, принаймні одна базова станція підключається до мережі провайдера з використанням класичних дротових з'єднань.

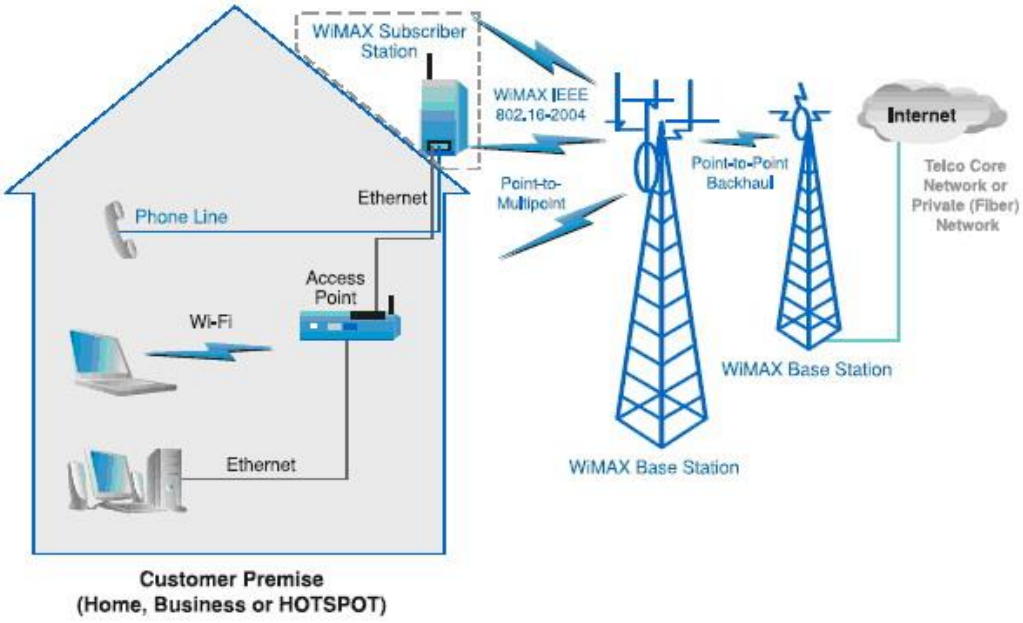
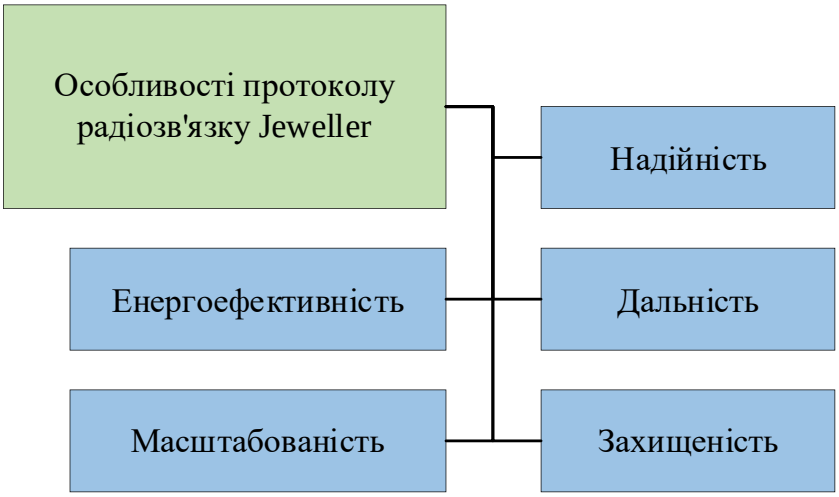


Рисунок 2.3 – Принцип роботи мережі WiMAX

Технології Ajax Jeweller та Wings.

Jeweller - це розроблений компанією Ajax Systems протокол радіозв'язку, що гарантує безперебійну взаємодію хаба та пристроїв системи безпеки. Це пропрієтарний двосторонній радіопротокол

Особливості Jeweller:



Надійність. Радіозв'язок двосторонній, використовуються механізм контролю доставки подій та автоматична зміна частоти при перешкодах. Тривоги передаються менш як за 0,15 секунди.

Дальність. За відсутності перешкод можливий зв'язок між пристроями на відстані до 2000 метрів та до 3800 метрів, коли використовується ретранслятор радіосигналу.

Енергоефективність. Протокол використовує тимчасове розподілення каналів зв'язку з кадрами від 12 секунд, короткі сеанси зв'язку, авторегулювання потужності передавачів пристроїв. І датчики працюють до 7 років від батарей.

Захищеність. Блокове шифрування даних з плаваючим ключем, частотний хоппінг та автентифікація пристрою при кожному сеансі зв'язку виключають заміну пристроїв та сигналів.

Масштабованість. У системі безпеки можуть працювати до 200 пристроїв, не створюючи взаємних перешкод, та використовуватися до 5 ретрансляторів радіосигналу. Максимальна площа покриття однієї системи Ajax досягає 35 км.

Таблиця 2.1 – Технічні характеристики

Дальність зв'язку	До 2000 метрів (за відсутності перешкод)
Потужність радіосигналу	До 25 мВт (саморегульована)

Час доставки тривоги	0,15 секунди
Шифрування	Блочне з плаваючим ключем
Час роботи пристроїв від батарей	До 7 років
Дистанційне налаштування пристроїв	Є
Детектування глушіння	Є
Захист від підробки	Є
Радіочастотний хоппінг	Є
Тип зв'язку	Двостороння
Діапозон частот	868,0-868,6 МГц або 868,7-869,2 МГц залежно від регіону
Кількість пристроїв у системі	До 200 (залежить від моделі хаба)
Період опитування пристроїв	Від 12 до 300 секунд

2.2 Порівняння безпроводових технологій за масштабом мереж

Технології безпроводових технологій на ділянці доступу до мережі можна класифікувати, у першу чергу, по масштабах мережі зв'язку. На рис. 2.4 наведено таку класифікацію.

Починаючи з найменшої зони покриття можна виділити наступні групи мереж:

– BAN (Body Area Network) – петельна мережа, тобто мережа в рамках одного організму тварини або людини. Прикладом такої мережі може служити мережа WSN (Wireless Sensor Network) – безпроводова мережа датчиків;

– PAN (Private Area Network) – персональна мережа. Прикладом може служити мережа, побудована в рамках одного приміщення, організована з використанням Bluetooth або WiFi;

– LAN (Local Area Network) – локальна мережа. Прикладом може служити мережа підприємства або організації;

– MAN (Metropolitan Area Network) – мережа в масштабах міста або населеного пункту;

– WAN (Wide Area Network) – глобальна мережа.

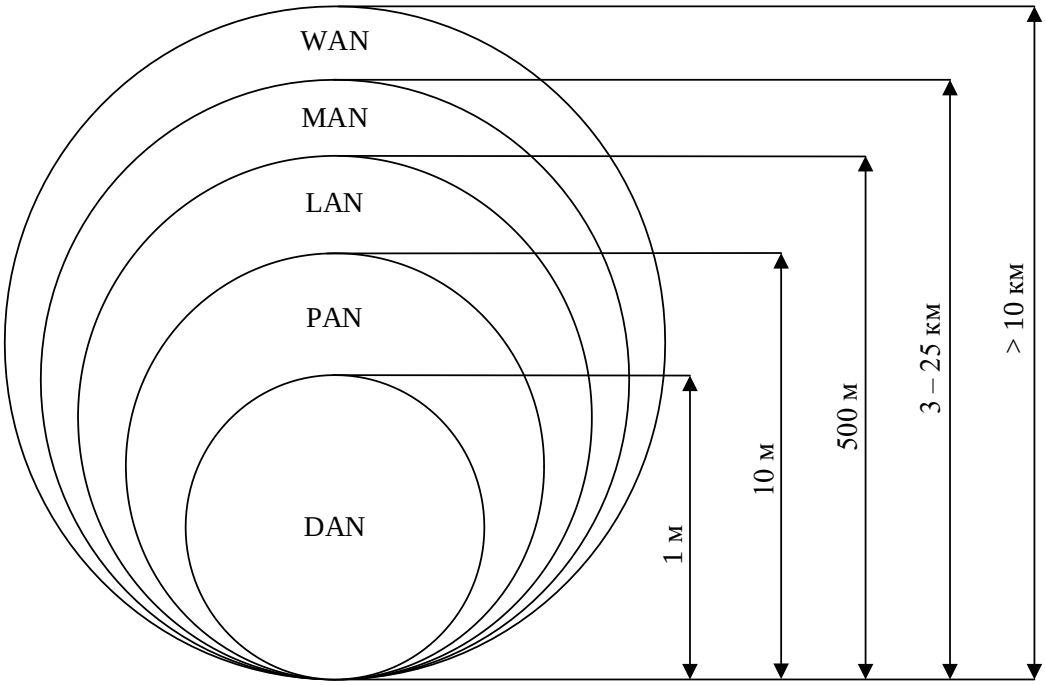


Рисунок 2.4 – Зони покриття безпроводових мереж різного призначення

З погляду операторів зв’язку найбільший інтерес у цей час представляють мережі PAN, LAN і MAN. У цей час для реалізації мереж цих масштабів існують технології доступу Wi-Fi і WiMax, а також технології доступу в мережах другого й третього поколінь.

Залежно від використовуваної технології бездротові мережі можна розділити на три типи:

– локальні обчислювальні мережі;

– розширені локальні обчислювальні мережі;

– мобільні мережі (переносні комп'ютери).

Таблиця 2.2 – Характеристики стандартів по швидкості ПД

Характеристика	Стандарт	Технологія ПД	Макс. швидкість ПД на рівні АД
Технологія 2G–2,75G	GSM	CSD HSCSD GPRS EGPRS (EDGE)	9,6 Кбіт/с 28,8 Кбіт/с 43,2 Кбіт/с 236,8 Кбіт/с
	CDMA–Is95		115200 Кбіт/с
Технологія 3G	WCDMA	HSDPA	3,6 Мбіт/с
	CDMA–2000	EV–D0	3,1 Мбіт/с
	UMTS		8 Мбіт/с
Радіо доступ	DECT		552 Кбіт/с
Радіотехнології, призначені для передачі даних	WiMax	IEEE 802.16 IEEE 802.20 IEEE 802.22	70 Мбіт/с
	LTE		більше 570Мбіт/с
	WiFi	IEEE 802.11x	до 300 Мбіт/с
Персональні мережі PAN	Bluetooth	IEEE 802.15.1	3 Мбіт/с
Сенсорні мережі (WSN)	ZigBee	IEEE 802.15.4	250іт/с

3 ДОСЛІДЖЕННЯ АРХІТЕКТУР ТА КОМПОНЕНТНОГО СКЛАДУ БЕЗПРОВОДОВИХ РІШЕНЬ В НАПРЯМКУ ТЗО

3.1 Системи безпроводового відеоспостереження

3.1.1 Класифікація безпроводових відеокамер

Часто доводиться використовувати системи відеоспостереження там, де поки немає ніяких ліній зв'язку або там, де прокладка кабельних ліній небажана, або неможлива. Наприклад, установка камер в котеджах, цехах, на заводській території, на віддалених об'єктах, на дачі, у квартирі і так далі. Якраз для таких застосувань і призначені безпроводові камери. Ще раз хотілося б підкреслити, що безпроводові камери доцільно встановлювати там, де складно або неможливо провести кабель. Якщо є можливість протягнути кабель, то установка безпроводових камер недоцільна.

Як правило, безпроводові камери використовуються в цифрових мережах (IP-мережах). Аналогова технологія в системах відеоспостереження не дозволяє оптимально використовувати можливості камер. Віддалений доступ в таких системах присутня або тільки на відеореєстратор, як ядро системи СОТ, або використовуються неоптимальні технології безпроводового доступу, розглянуті докладно раніше. Тому в класифікації буде розглянуто лише IP-обладнання.

Безпроводові IP-камери діляться за технологією на аналогові і цифрові. Аналогові бездротові камери сильно схильні перешкод і спотворень, їх застосування практично завжди не дозволене законодавством і, як наслідок, застосування таких бездротових камер безперспективно.

Безпроводові IP -камери набагато менше схильні до дії перешкод, причому перешкоди не позначаються на зображенні, а просто знижують швидкість передачі даних. Безпроводові IP-камери діляться на відеокамери з передачею даних по радіоканалу (безпроводові Wi-Fi камери, безпроводові WiMax камери) і на відеокамери з передачею зв'язку по каналах стільникового зв'язку (безпроводові GPRS-камери, безпроводові CDMA- камери).

Безпроводові камери Wi-Fi

Найдоступніший і недорогий вид безпроводових камер - Wi-Fi камери. Дані камери можуть застосовуватися як для відеоспостереження усередині приміщень, так і на вулиці, як вдень, так і вночі. У приміщеннях безпроводові камери зручні тим, що не доводиться протягувати кабель до кожної з камер. Для установки в приміщеннях добре підходять безпроводові камери з вбудованим Wi-Fi модулем. Слід пам'ятати , що стіни і інші перешкоди зменшують швидкість передачі даних і перед установкою безпроводової камери слід переконатися, що саме в цьому місці швидкості передачі Wi -Fi достатньо для роботи камер.

При проектуванні систем відеоспостереження на основі IP-камер з використанням безпроводових камер необхідно враховувати обмеження пропускної здатності Wi-Fi каналу. На одну точку доступу має припадати не більше 4 камер, крім того, потрібно враховувати, що в стандартному діапазоні Wi-Fi є всього 3 незалежні канали зв'язку, тобто при використанні стандартних засобів вдається підключити не більше 12 безпроводових камер. Для того, щоб обійти це обмеження, існує кілька способів: використання діапазону 5 ГГц, а також використання нестандартних частот в діапазоні 2.4 ГГц. Використовуючи ці способи, можна отримати близько 20 незалежних радіоканалів і підключити близько 80 безпроводових камер до системи відеоспостереження. Ще потрібно пам'ятати про те, що необхідна умова для підключення безпроводових камер - наявність прямої видимості до точки доступу і відсутність будь-яких перешкод на шляху поширення радіосигналу: дерев, будівель, ЛЕП і тому подібного. При наявності перешкод сигнал від

безпроводових камер можна передати з використанням з'єднання типу міст або з використанням ретрансляторів .

Безпроводові камери Wi-Max.

У зв'язку з бурхливим розвитком мереж Wi-Max (Yota, Комстар), стає актуальним підключення безпроводових камер по Wi-Max.

Можливості системи бездротового IP -відеоспостереження через інтернет онлайн: Віддалене аудіо та відеоспостереження з точки світу через web-браузер. Запис відеоархіву і звуку централізовано, з кількох віддалених точок (до 16 камер), за допомогою спеціалізованого програмного забезпечення. Локальний запис відеоархіву на SD-карту, а також стандартний набір функцій для віддаленого управління, виявлення руху, записи по таймеру або по детектору руху, для комплексного та ефективного вирішення вашої безпеки.

Безпроводові камери Wi-Max.

У зв'язку з бурхливим розвитком мереж Wi-Max (Yota, Комстар), стає актуальним підключення безпроводових камер по Wi-Max.

Можливості системи бездротового IP -відеоспостереження через інтернет онлайн: Віддалене аудіо та відеоспостереження з точки світу через web-браузер. Запис відеоархіву і звуку централізовано, з кількох віддалених точок (до 16 камер), за допомогою спеціалізованого програмного забезпечення. Локальний запис відеоархіву на SD-карту, а також стандартний набір функцій для віддаленого управління, виявлення руху, записи по таймеру або по детектору руху, для комплексного та ефективного вирішення вашої безпеки.

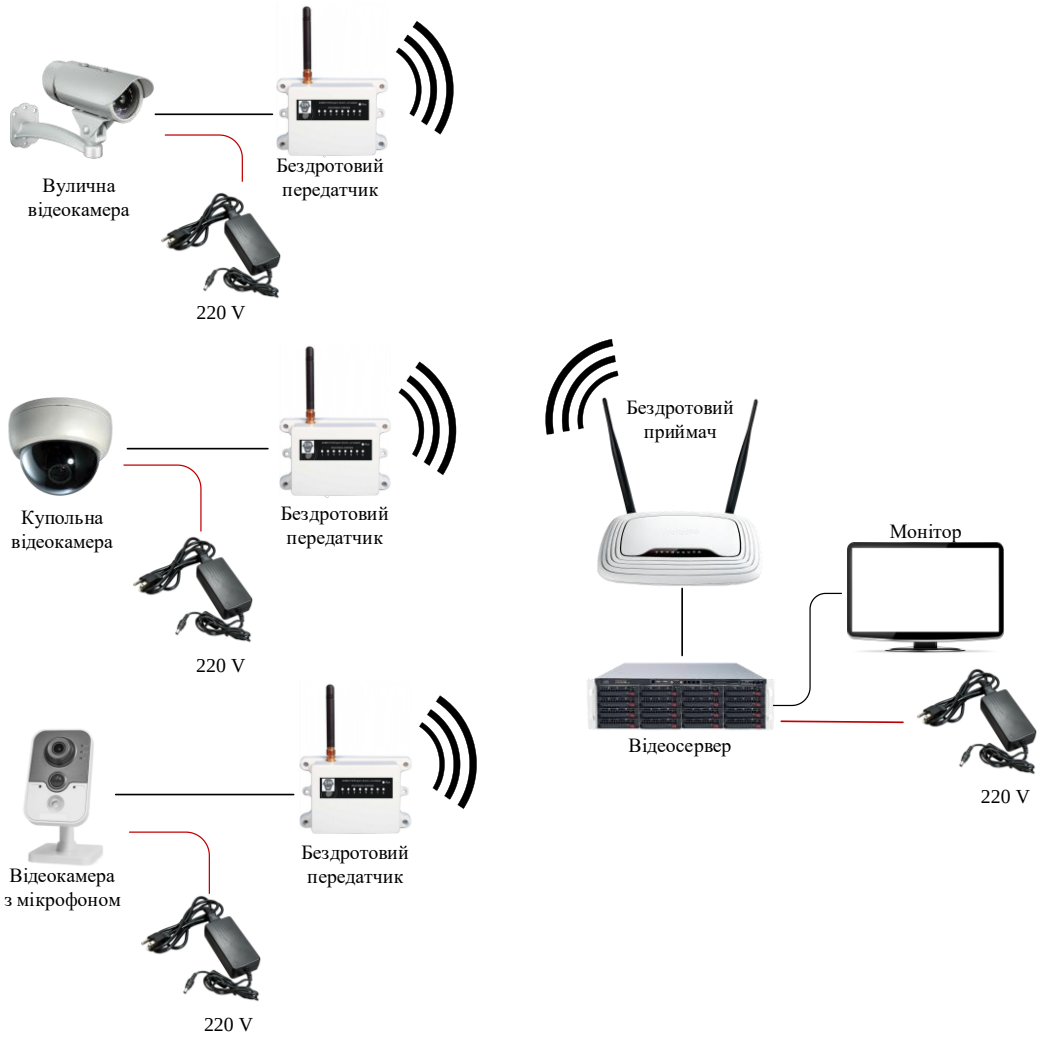


Рисунок 3.1 – Схема wi-fi відеоспостереження

Комплект зазвичай складається з однієї або декількох камер відеоспостереження, що підключаються до блоку управління проводами (до 100м) або по Wi-Fi (до 500 м в прямій видимості). Блок управління складається з модему і 4-х портового маршрутизатора Ethernet-Wi-Fi. При включенні в розетку система відеоспостереження налаштовується і виходить на готовність до роботи вже через 1-2 хвилини. Для доступу до камери безпроводового відеоспостереження з точки світу досить набрати в рядку вашого web - браузера адресу камери, наприклад camXXX.yota77.ru, де XXX - номер контракту, який буде вам виданий при покупці комплекту устаткування. Присутня можливість збереження стоп- кадрів і запису відео і аудіо з Web-

браузера безпосередньо на локальний жорсткий диск без установки спеціального програмного забезпечення для відеоспостереження.

Безпроводові камери GSM (GPRS, EDGE).

Безпроводові GSM-камери застосовуються там, де неможливо використовувати лінії проводового зв'язку і відсутній доступ по Wi-Fi, але є мережа операторів GSM (МТС, Київстар, Life і т.д.), типові приклади: заміський будинок, будмайданчик, котедж, дача, віддалений об'єкт, фермерські господарства, підприємства. У цьому випадку можна використовувати бездротову GSM-камеру, яка передає дані по каналах стільникового зв'язку EDGE або GPRS.

Безпроводові камери CDMA (1xEV-DO Rev.A 450МГц)

Безпроводові CDMA-камери застосовуються там, де неможливо використовувати лінії проводового зв'язку і відсутня доступ по Wi-Fi , але є мережа оператора CDMA (наприклад, Інтертелеком або CDMA-Україна). У цьому випадку можна використовувати бездротову CDMA -камеру , яка передає дані по каналах стільникового зв'язку EV- DO. Середня швидкість передачі даних при такому підключенні бездротової камери буде близько 150-250 кбіт/с , що дозволяє передати до 10-15 кадрів в секунду. Необхідно пам'ятати, що при зверненні до безпроводової CDMA- камері провайдер стільникового зв'язку стягує плату як за доступ в Інтернет, тому слід уважно вибирати абонентські пакети. В даний час мережі пішли в сферу 3G , тому оператори обіцяють максимальні швидкості до 5,5 Мбіт / с.

3G - технології мобільного зв'язку 3-го покоління - це набір послуг, які об'єднують як високошвидкісний мобільний доступ з послугами мережі Інтернет, так і технологію радіозв'язку, яка створює канал передачі даних. В даний час під терміном 3G найчастіше мається на увазі технологія UMTS.

HSPA (High Speed Packet Access - високошвидкісна пакетна передача даних) - технологія безпроводового широкосмугового радіозв'язку, що використовує пакетну передачу даних і що є надбудовою до мобільних мереж WCDMA / UMTS. Максимальна теоретична швидкість передачі даних за

стандартом становить 14,4Мбіт/с (швидкість передачі даних від базової станції до всіх локальних абонентів) і до 5,8 Мбіт/с від абонента.

Вбудовані технології 3G (підтримка SIM-карт в відеокамерах) доступні на даний момент в камерах брендів Brickcom і D- Link. Інші виробники пропонують рішення з використанням додаткових 3G- модулів.

Рисунок 3.2 – Схема системи IP-відеоспостереження на базі 3G

Недоліком даної технології є низька пропускна здатність і пріоритет голосового зв'язку на базових станціях. Перевага буде завжди віддаватися голосовим дзвінкам, і використання 3G IP - камер в зонах з великим скупченням людей, що користуються мобільним зв'язком (бізнес - центри, торгові центри, вокзали тощо) буде практичний неможливим. Ймовірно, з часом дана проблема перестане бути актуальною, оскільки технології постійно вдосконалюються.

На даний момент 3G IP - камери - це оптимальні рішення для віддалених об'єктів, а також об'єктів, важкодоступних для прокладання кабельних комунікацій.

3.1.2 Застосування обладнання на базі брендів Trassir та CISCO

Безпроводова передача відео-та аудіоінформації набуває все більшої популярності у інсталяторів і власників систем відеоспостереження, так як найчастіше простіше організувати канал передачі даних , не використовуючи

провідні технології. У міських умовах це найбільш актуально у зв'язку зі складністю прокладки кабелів. Якщо є необхідність передавати сигнал на далекі відстані (до декількох кілометрів), безпровідне відеоспостереження буде найбільш вдале, тим більше, не потрібно кожні 100-200 метрів ставити підсилювачі сигналу, як у випадку з дротяними системами. На рис.2.6 показана типова архітектура організації відеоспостереження.

Ретрансляційна частина, що включає IP-відеосервер, знаходиться в спеціалізованому термобокси, призначеному для розміщення активного устаткування і використовуваному для роботи всередині приміщення, в місцях, де навколишнє середовище несприятливе за своїми температурним і вологим характеристикам для експлуатації даного обладнання.

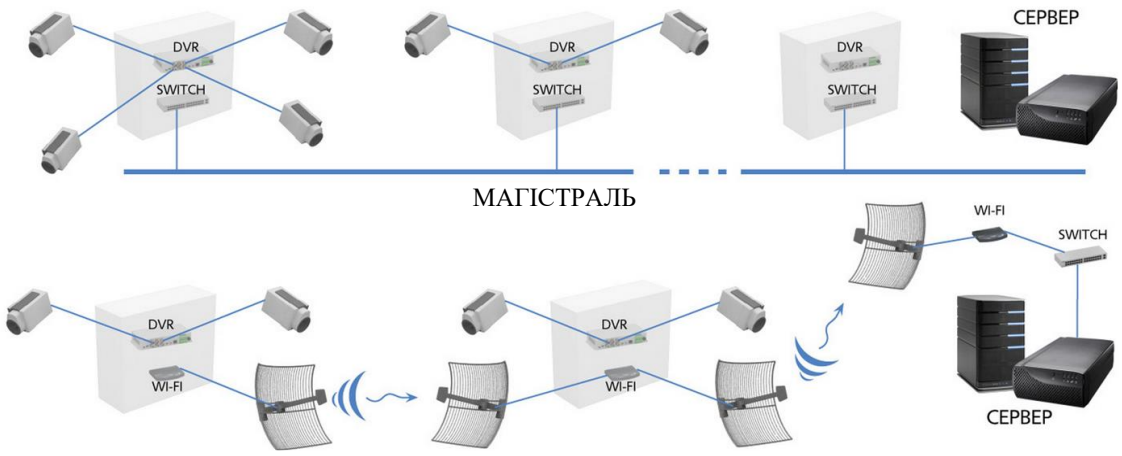


Рисунок 3.3 – Типова архітектура організації відеоспостереження

Система відеоспостереження Cisco (VSM) дозволяє адміністраторам мережі і фахівцям з системної інтеграції створювати мережу відеоспостереження в повній відповідності з наявними вимогами. Комплект програмного забезпечення дозволяє будувати масштабовані, настроюються і прості в управлінні відеосистеми з можливістю доступу до відео в режимі реального часу або в запису в будь-якому місці, з використанням інтерфейсу Web-браузера, на комп'ютерах і смартфонах.

Робота під управлінням операційної системи Linux, апаратне забезпечення і мережеві IP- протоколи, наявні в стандартній конфігурації, забезпечують сумісність з великим числом пристроїв і додатків сторонніх виробників. Авторизовані мережеві користувачі можуть переглядати відеодані з будь-якої кількості IP- або аналогових камер з підключеним енкодером , і управляти ними в режимі реального часу. При цьому можливе використання різних відмовостійких опцій запису і зберігання даних з метою їх відновлення в разі аварії. Набір функцій системи відеоспостереження може збільшуватися при впровадженні нових технологій, коли у підприємства з'являться відповідні комерційні можливості.

Рисунок 3.4 – Структура безпроводового відеоспостереження CISCO VSM

3.1.3 Аналіз параметрів системи безпроводового IP-відеоспостереження

При формуванні систем віддаленого контролю за допомогою відеоспостереження (контроль за віддаленими об’єктами) є параметри, дослідження яких допоможе оптимізувати систему відеоспостереження ще на етапі її проектування, дасть можливість правильно обрати обладнання, інфраструктуру, тощо. Ці параметри – глибина архіву системи відеоспостереження та пропускна спроможність каналів зв’язку між прикінцевим обладнання системи СОТ та серверною частиною.

Для проведення розрахунку задано ланку вихідних даних, а саме – кількість кадрів за секунду, розподільну здатність (якість зображення). Параметри налаштування камери:

Складність кадру – 40%.

Швидкість – 12 кадрів/с.

Розподільна здатність - 4CIF, D1,HD, FullHD.

Відомо, що при використанні безпроводових систем відеоспостереження "вузьким" місцем є саме канал зв'язку між камерою і місцем записи архіву. Проведемо розрахунки щодо вимог до пропускної здатності системи відеоспостереження при різній якості зображення. Отримані результати допоможуть вибрати оптимальні безпроводові технології для побудови і подальшої модернізації безпроводових систем відеоспостереження.

Для розуміння параметрів якості зображення наведемо в табл. 3.1 технічні показники.

Таблиця 3.1 – Параметрів якості зображення

№	Позначення якості зображення	Кількість точок в кадрі	Кількість мегапікселів
1	4CIF	704×576	0,4
2	D1	720×576	0,42
3	HD	1280×720	0,92
4	FullHD	1920×1080	2,07

В табл. 3.1 представлені стандарти з такою якістю зображення, які оптимальні для розгортання безпроводових систем відеоспостереження при побудові систем безпеки для об'єктів великого масштабу. Стандарти якості нижче, ніж 4CIF зазвичай використовуються тільки при спостереженні через мережу при обмеженій пропускній спроможності каналу, а також реєстрації загальної ситуації при малих зонах огляду (від 3 до 5 м). QCIF взагалі використовується тільки при мережевому моніторингу по низькошвидкісних каналах зв'язку з потоком до 56-128 Кбіт / с. Про якість зображення можна сказати тільки те, що «видно якийсь рух», і більш нічого. Використання відеокамер з якістю більше 2-х мегапікселів вимагає швидкісних каналів доступу. Так, на рис. 3.5 представлена залежність пропускної здатності каналу зв'язку при використанні камер з якістю в 5 Мп. Як видно, використання навіть однієї камери потребує потоку на швидкості не менше, ніж 7,15 Мбіт/с.

Звичайно, для охорони територій великого масштабу одиничне застосування камери не застосовується. Застосування принципу "ковдри" з використанням 20 камер виставляють вимоги до пропускної здатності мережі не менше 142,9 Мбіт/с.

Залишимо для об'єктивності таку ж кількість камер та розрахуємо пропускну здатність при якості зображення 4CIF, D1, HD і FullHD. Результати представлені на рис. 3.6. Варто відзначити, що параметри форматів 4CIF, D1 дуже близькі, тому криві на графіку накладаються одна на одну. При розрахунку враховувався єдиний критерій руху в кадрі - 40%. В реальності цей показник динамічний, і навантаження на канал зв'язку, а також вплив на показник глибини архіву також динамічні. Кожна камера бачить "своє" зображення різної динаміки. Але для розрахунку використовувався усереднений показник.

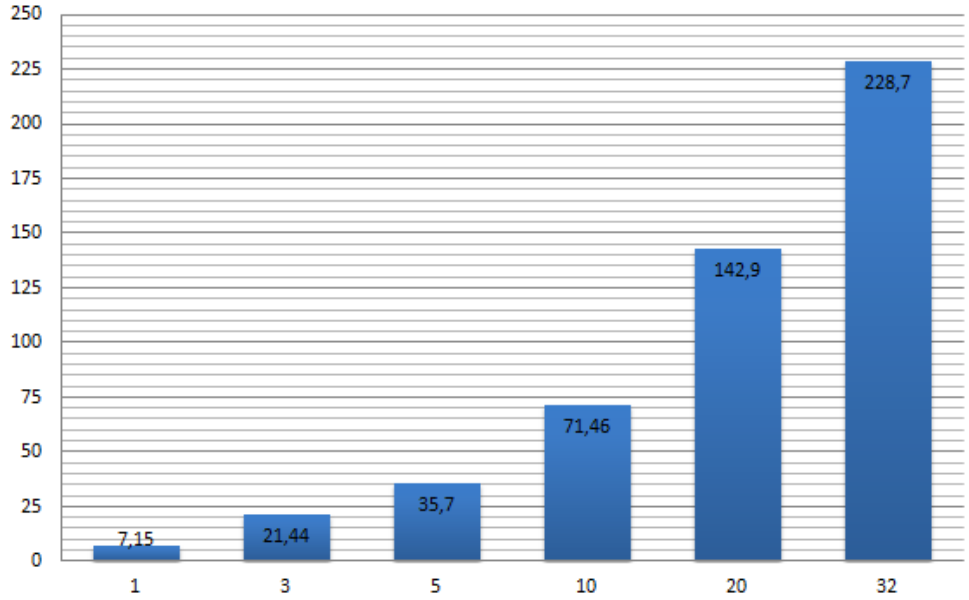


Рисунок 3.5 – Залежність пропускної здатності каналу зв'язку від кількості відеокамер при якості зображення в 5 Мп

Як зазначалося раніше, проведений розрахунок дозволяє визначити оптимальну безпроводову технологію для використання на мережі відеоспостереження. Зведемо в таблицю швидкості технологій, які можуть застосовуватися при побудові безпроводових систем відеоспостереження.

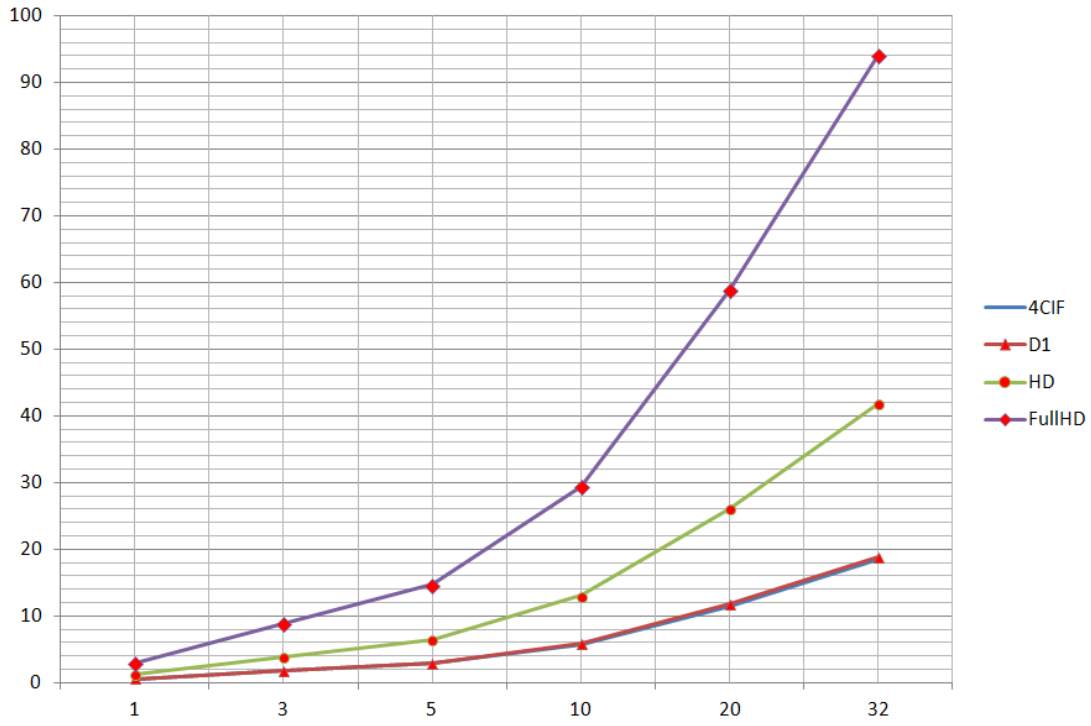


Рисунок 3.6 – Залежність пропускної здатності каналу зв'язку системи відеоспостереження при якості 4CIF, D1, HD і FullHD при зміні кількості камер

Таблиця 3.2 - Безпроводові технології та їх максимальні швидкості

№	Технологія	Максимальна швидкість, Мбіт/с
1	GSM/CDMA (2,5G)	0,39
2	GSM/CDMA (3G)	3,6
3	GSM/CDMA (3,5G)	42
4	IEEE 802.11a (Wi-Fi)	54
5	IEEE 802.11g (Wi-Fi)	54
6	IEEE 802.11n (Wi-Fi)	300
7	IEEE 802.11ac(Wi-Fi)	1000
8	IEEE 802.16d (WiMax)	75
9	IEEE 802.16e (WiMax)	40

Для моделювання встановимо кількість камер в 10 штук. В такому випадку графік перетворюється в вигляд, що представлено на рис. 3.7.

Пунктирними областями на графіку виділені діапазони швидкостей найбільш застосованих технологій - GSM/CDMA та Wi-Fi. Взяті реальні параметри швидкостей, які можна використовувати на території України.

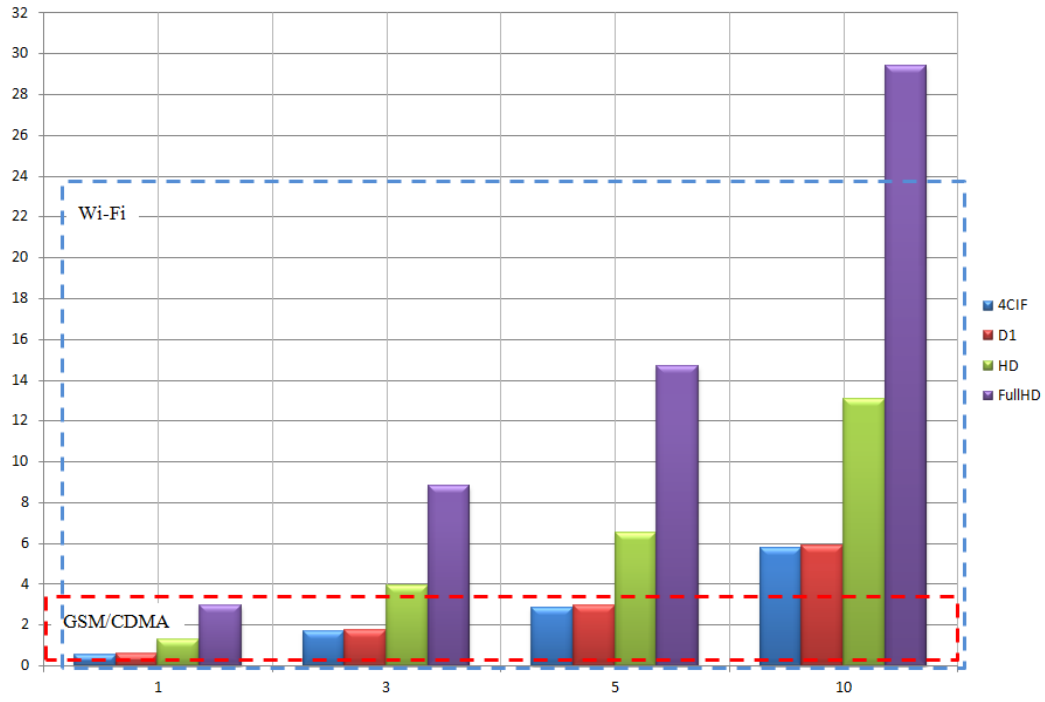


Рисунок 3.7 – Залежність пропускної здатності каналу зв'язку системи відеоспостереження при якості 4CIF, D1, HD і FullHD із зазначенням областей безпроводових технологій

3.2 Безпроводові системи охоронної сигналізації

3.2.1 Охоронна сигналізація на базі обладнання Ajax

Сьогодні лідером в Україні вважається система бездротової сигналізації Ajax. Велика кількість різноманітних за функціоналом охоронних датчиків, кілька видів централей, зручність використання, можливість масштабування системи, адекватне співвідношення ціна/якість, потужна

рекламна кампанія – це дозволило Ajax завоювати вітчизняного споживача. Розглянемо компонентний склад лінійки обладнання компанії Ajax.

Основа системи (центр управління) це хаб. Він контролює роботу всіх пристроїв системи, управляє режимами охорони, а у разі тривоги сповіщає охоронну компанію та клієнта.

Інтелектуальна централь для охоронної сигналізації Ajax Hub контролює коректне виконання моніторингу всіх підключених пристроїв Ajax за допомогою радіопротоколу Jeweller та негайно надсилає сигнал тривоги всім користувачам системи, а також на пульт охорони.

Особливості контрольної панелі для сигналізації Ajax Hub:

– Централь Ajax Hub працює до 15 годин від вбудованого резервного акумулятора.

– Технологія Geofence нагадує користувачам увімкнути сигналізацію при виході з приміщення та вимкнути після повернення.

– Контрольна панель на сигналізацію Ajax Hub обслуговує до 100 пристроїв.

– Можливість підключення відеоспостереження за рахунок камер, що підтримують RTSP-потік.

– Є можливість підключення до 50 користувачів та охоронної компанії до системи моніторингу.

– Централь для сигналізації Ajax Hub зберігає історію всіх зазначених системою подій.

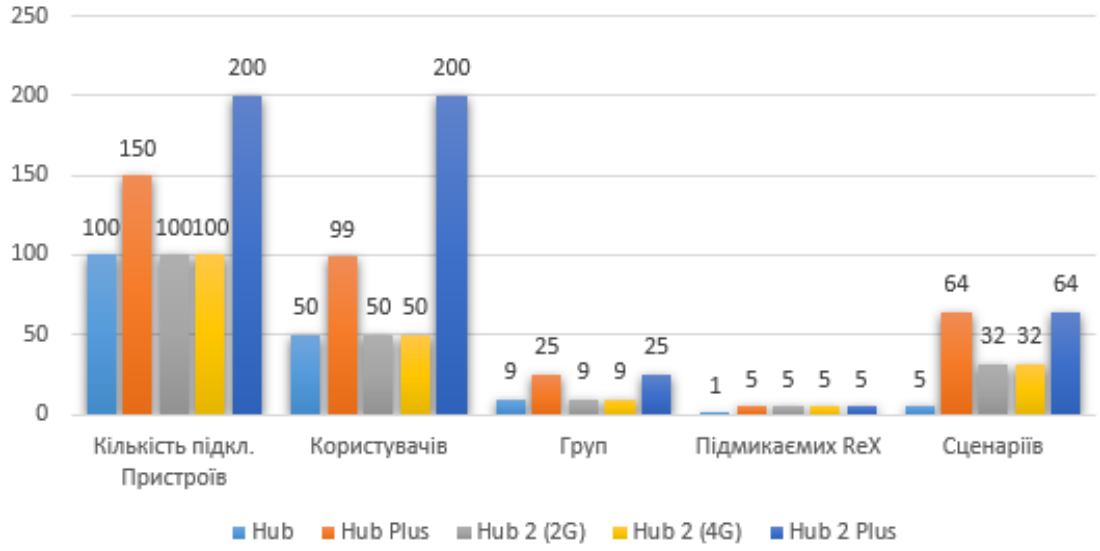
– Контрольна панель повідомляє про зникнення зовнішнього живлення відразу після виявлення проблеми.

– Корпус розумної централі сигналізації захищений тампером від розтину. У разі спроби демонтажу або пошкодження панелі користувач отримає повідомлення про подію

Нижче наведено порівняння охоронних централей (хабів).

	Кількість підкл. Пристроїв	Користувачів	Кімнат	Груп	Підмикаємих сирен	Підмикаємих ReX	Сценаріїв
Hub	100	50	50	9	10	1	5
Hub Plus	150	99	50	25	10	5	64
Hub 2 (2G)	100	50	50	9	10	5	32
Hub 2 (4G)	100	50	50	9	10	5	32
Hub 2 Plus	200	200	50	25	10	5	64

На рисунку представлена візуалізація порівняння низки параметрів охоронних централей від бренду Ajax.



Система є масштабованим під будь-які завдання технічним рішенням. При цьому компонентний ряд може включати:

– централі (Hub, Hub Plus, Hub 2 (2G), Hub 2 (4G), Hub 2 Plus);

– ретранслятори (ReX, ReX2) ;

– датчики для охорони приміщень (MotionCam, MotionProtect, MotionProtect Plus, CombiProtect, MotionProtect Curtain, DoorProtect, DoorProtect Plus, GlassProtect) ;

– датчики для охорони вулиці та територій (DualCurtain Outdoor, MotionCam Outdoor, MotionProtect Outdoor) ;

– пожежні датчики (FireProtect, FireProtect Plus) ;

– клавіатури та тривожні кнопки (KeyPad, KeyPad Plus, Pass, Button, DoubleButton) ;

– сирени (HomeSiren, StreetSiren, StreetSiren DoubleDeck) ;

– засоби автоматизації (Socket (type F), WallSwitch, Relay) ;

– модулі інтеграції (vhfBridge, Transmitter, MultiTransmitter) ;

– блоки живлення (6V PSU, 12V PSU).

3.2.2 Охоронна сигналізація на базі обладнання Каліпсо

Як і обладнання компанії AJAX, бренд Каліпсо – українського виробництва. Центральне обладнання підтримує 32 бездротові зони, 8 провідних зон, 6 протоколів зв'язку. Моніторинг проводиться у різний спосіб - Contact ID (GSM), S IA IP (LAN, GPRS), SMS. Радіоканал: (868 МГц) до 200 м, можливе збільшення радіусу дії за допомогою репітерів.

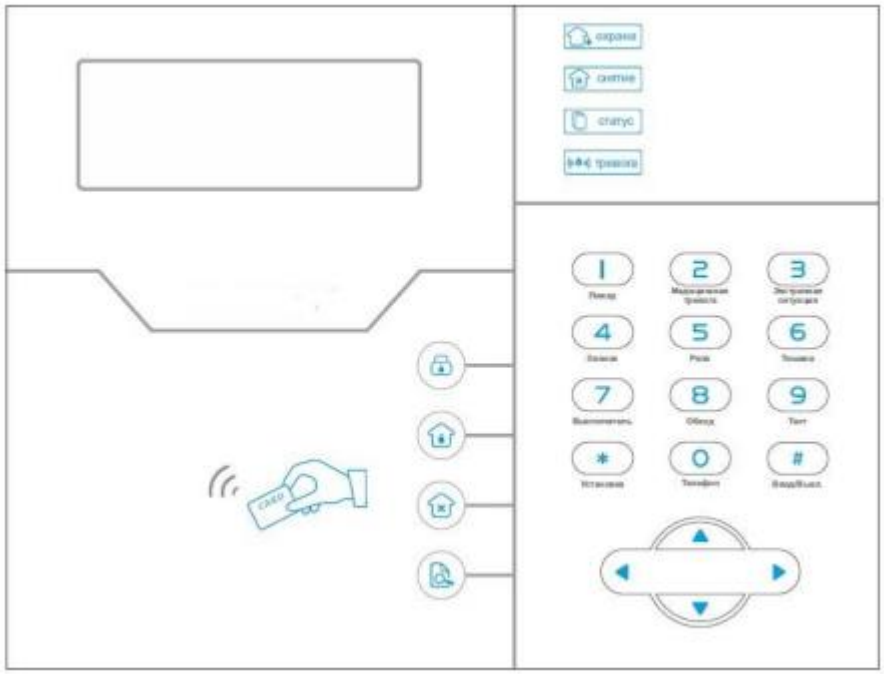
Безпроводові зони	32
Проводові зони	8
Залежні зони (групи)	4
Програмований вихід	1
Пристрої керування	8
Безпроводові вимикачі	16
Користувачі	16
Адміністратор (інсталятор)	1

Сирени	вбудована, провідна, безпровідна
Час роботи контрольної панелі від АКБ (година)	До 12
Середній час роботи батарей у пристроях (рік)	1
Комунікатори	LAN, GSM

Канали оповіщення та управління:

- GSM голосове приватне сповіщення (4 номери);
- SMS (4 номери);
- GSM CID (Contact ID) на ЦМЗ (2 номери);
- LAN (SIA IP) на ЦМЗ;
- GPRS (SIA IP) на ЦМЗ;
- P2P (lля роботи з мобільним додатком);
- WEB інтерфейс.

Зовнішній вигляд представлений на рисунку.



Система підтримуємо велику кількість датчиків та аксесуарів.

3.2.3 Охоронна сигналізація на базі обладнання Лунь Р (LUN-R)

– Обладнання Лунь виготовляється в Україні вже понад 20 років. Базова комплектація обладнання включає централь Лунь 25К з вбудованим радіоприймачем бездротових датчиків, датчик руху PIR R, датчик відкриття дверей та вікон Magnet R та брелок Button R.

– ППК Лунь 25К - це прилад охоронно-пожежний, призначений для побудови охоронної сигналізації з елементами «розумного будинку» на об'єктах великих розмірів. Система на 17 провідних охоронних зон. Вбудовані GSM та Ethernet модулі. Живлення 180 - 240 В від мережі.

Характеристики ППК Лунь 25К:

– 16 базових зон сигналізації, 5 із яких розташовані на платі основного блоку;

– підтримує до 30 бездротових зон/брелоків через додатковий радіоприймач, який встановлюється у корпусі основного блоку;

– передача подій на ПЦН та віддалене управління: GSM (GPRS або Voice), а також WiFi (з наступним виходом в Internet);

– є можливість підключення додаткових провідних зон за допомогою адресних модулів розширення «АМ-11» (до 4 модулів, кожен із яких забезпечує додаткові 3 зони);

– всі зони можуть бути розділені на 2 групи, для управління кожною з яких передбачено до 16 ключів та до 7 номерів мобільних телефонів;

– використовує шифрування AES-128 протоколу зв'язку з ПЦН «Орлан»;

– може працювати автономно — події передаються на центр спостереження «Phoenix-Web» (сторінка зареєстрованого користувача на сайті в мережі Інтернет);

Ця модель централі УІУ "Лінд-27". УІУ (пристрій індикації та управління) є цифровою сенсорною клавіатурою з додатковими світлодіодними індикаторами. УІУ призначено для вбудовування в корпус основного блоку ППКОП та дозволяє відображати:

– стан зон поточної групи;

– системні несправності;

– стан охорони та готовність до постановки на охорону груп 1 та 2.

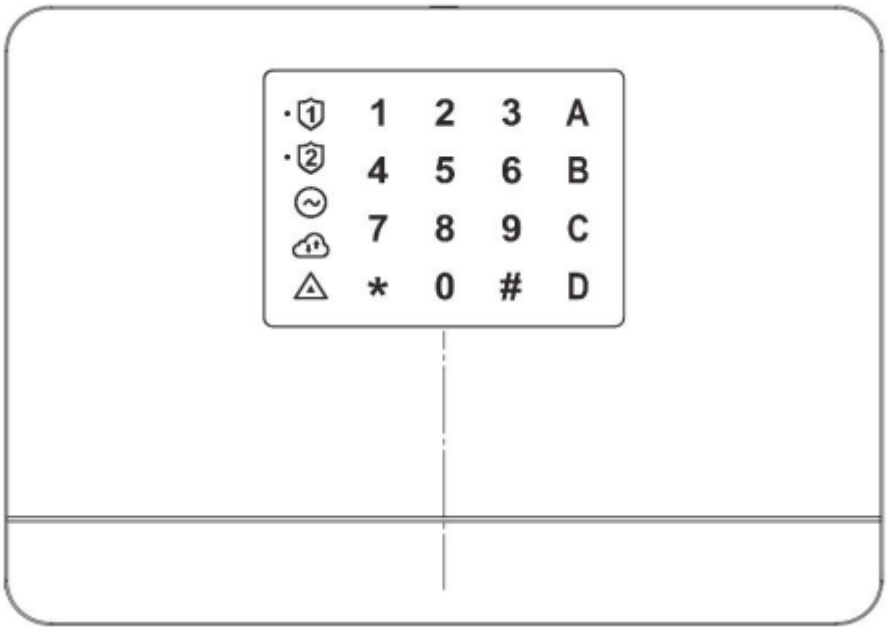


Рисунок 3.8 – Лицьова панель ПВКОП «Лунь-25К»

Варто зазначити, що до лінійки LUN-R входить досить широкий перелік обладнання:

– датчик руху з лінзою типу "штора" PIR-CR;

– датчик розбиття скла GBD-R;

– ретранслятор сигналу Repeater-R;

– радіореле Relay-R, для керування зовнішніми пристроями;

– вуличний датчик руху з імунітетом від тварин PIROUT-R;

– керована розетка Socket-R, за допомогою якої ви можете керувати побутовими приладами;

– датчик затоплення Flood-R;

– оптичний датчик диму Smoke-R;

– сирена Siren-R, яка сповістить світлом і звуком, якщо хтось спробує пробратися до приміщення.

Максимально до системи можна підключити до 30 бездротових пристроїв.

РОЗДІЛ 4. ОХОРОНА ПРАЦІ

ВСТУП.

Державна політика України щодо охорони праці виходить з конституційного права кожного громадянина на належні безпечні і здорові умови праці та пріоритету життя і здоров'я працівника по відношенню до результатів виробничої діяльності.

В реалізації цієї політики значну роль має відігравати постійне поліпшення умов і безпеки праці, зменшення рівнів травматизму та професійної захворюваності.

Широке впровадження комп'ютерної техніки, що дає змогу автоматизувати багато рутинних операцій комп'ютерної обробки інформації, одержати доступ до численних джерел інформації, швидко проводити потрібні розрахунки і т. ін. підвищує продуктивність праці. Проте активне впровадження у практику персональних комп'ютерів має і негативну сторону – з'являються фактори, які несприятливо впливають на здоров'я працюючої людини.

Згідно темі кваліфікаційної роботи бакалавра робоче місце користувача послуг складається з персонального комп'ютеру з програмним забезпеченням та призначено для застосування безпроводових технічних засобів охорони в спеціалізованих закладах.

Тому для нього застосовуються звичайні вимоги безпеки праці для користувача персонального комп'ютеру.

4.1 Аналіз небезпечних та шкідливих чинників, що впливають на працівника.

Виявлення та аналіз шкідливих та небезпечних виробничих факторів слід починати з аналізу дотримання вимог, встановлених санітарними правилами і нормами для виробничих приміщень та робочих місць.

Дана робота виконується в приміщені з відеотерміналами та ПЕОМ, де діють нижче перераховані шкідливі та небезпечні виробничі фактори.

Показниками гігієнічних вимог є рівень освітлення, температура, вологість, шум, вібрація, токсичність, загазованість, обмежена загальна м'язова активність (гіподинамії), дія електростатичного поля, неіонізуючих та іонізуючих електромагнітних випромінювань.

4.2 Розробка заходів з охорони праці

В Україні діють Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСАНПіН 3.3.2.007-98 «Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин». Ці правила призначені для запобігання несприятливої дії на працівників шкідливих факторів, які супроводжують роботу з ВДТ

4.2.1 Освітлення робочого місця, шум, вібрація

Приміщення зі стаціонарним обладнанням повинно мати природне і штучне освітлення відповідно до ДБН В.2.5-28-2006 «Природне і штучне освітлення». Природне світло повинно проникати через бічні світлопрорізи, зорієнтовані на північ чи північний схід, і забезпечувати коефіцієнт природної освітленості (КПО) не нижче 1,5%. Вікна приміщень з відеотерміналами повинні мати регулювальні пристрої для відкривання, а також жалюзі, штори, зовнішні козирки тощо.

Зазначення освітлення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300 - 500 лк. Світильники місцевого освітлення слід встановлювати таким чином, щоб не створювати бліків на поверхні екрана, а освітленість екрана має не перевищувати 300 лк.

Світильники місцевого освітлення слід встановлювати таким чином, щоб не створювати бліків на поверхні екрана, а освітленість екрана має не перевищувати 300 лк.

Система загального освітлення має становити суцільні або переривчасті лінії світильників, розташовані збоку від робочих місць (переважно ліворуч),

паралельно лінії зору працюючих. Допускається використання світильників таких класів світорозподілу:

1. прямого світла - П;
2. переважно прямого світла - Н;
3. переважно відбитого світла - В.

Рівні вібрації підчас виконання робіт у виробничих приміщеннях не повинні перевищувати допустимих значень, визначених в СН 3044-84 "Санитарные нормы вибрации рабочих мест", затверджених Міністерством охорони здоров'я СРСР, та ДСанПіН 3.3.2-007-98.

4.2.4 Мікроклімат робочої зони працівників, вентиляція.

Параметри мікроклімату, іонного складу повітря, вміст шкідливих речовин на робочих місцях, оснащених відеотерміналами, повинні відповідати вимогам ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень».

Для підтримки допустимих значень мікроклімату та концентрації позитивних та негативних іонів необхідно передбачати установки або прилади зволоження та/або штучної іонізації, кондиціювання повітря. Рівні інфрачервоного випромінювання не повинні перевищувати граничних

Рівні інфрачервоного випромінювання не повинні перевищувати граничних відповідно до ТОСТ 12.1.005. Вміст озону в повітрі робочої зони не повинен перевищувати 0,1мг/м3; вміст оксидів азоту - 5мг/м3; вміст пилу - 4мг/м3.

4.2.5 Організація робочого місця користувача ПК

Розміщення робочих місць з ПЕОМ у підвальних приміщеннях, на цокольних поверхах заборонено.

Площа на одне робоче місце становить не менше ніж 6,0 м2, а об’єм – не менше ніж 20,0 м3, відстань між робочими столами – щонайменше 2,5 м у ряду і 1,2 м між рядами. Стіни приміщень потрібно фарбувати у пастельні тони з коефіцієнтом відбиття 0,5 – 0,6.

Організація робочого місця повинна передбачати:

1) достатній простір для людини-оператора;

2) вільну досяжність органів ручного управління в зоні моторного поля: відстань по висоті - 900-1330мм, по глибині - 400-500мм:
3) розташування екрана відеотермінала під кутом ± ЗО градусів від лінії зору оператора, а також зручність використання відеотермінала;
4) відстань від екрана до ока працівника повинна відповідати вимогам вищевказаних пунктів;
5) можливість повертання екрана відеотермінала навколо горизонтальної та вертикальної осі.

Робочі місця з ВДТ слід так розташовувати відносно світових прорізів, щоб природне світло падало збоку переважно зліва. При розміщенні робочих столів з ВДТ слід дотримувати такі відстані між бічними поверхнями ВДТ 1,2 м, відстань від тильної поверхні одного ВДТ до екрана іншого ВДТ – 2,5 м.

Робоче місце користувача складається зі столу, крісла і підніжки, які дають змогу зберігати раціональну робочу позу впродовж усього робочого дня.

Конструкція робочого місця користувача відеотермінала (при роботі сидячи) має забезпечувати підтримання оптимальної робочої пози з такими ергономічними характеристиками: ступні ніг - на підлозі або на підставці для ніг; стегна - в горизонтальній площині; передпліччя - вертикально; лікті - під кутом 70-90 градусів до вертикальної площини; зап'ястя - зігнуті під кутом не більше 20 градусів відносно горизонтальної площини; нахил голови - 15-20 градусів відносно вертикальної площини.

Рекомендовані розміри столу: висота - 725мм, ширина - 600-1400мм, глибина - 800-1000мм.

Робоче сидіння користувача відеотермінала та персональної ЕОМ повинно бути підйомно-поворотним, таким, що регулюється за висотою, кутом нахилу сидіння та спинки,

Для зниження статичного напруження м'язів рук необхідно застосовувати стаціонарні або знімні підлокітники довжиною не менше 250мм, шириною - 50-

70 мм, що регулюються по висоті над сидінням у межах 230 ± 30мм та по відстані між підлокітниками в межах 350-500мм.

Поверхня сидіння, спинки та підлокітників має бути напівм'якою, з неслизьким покриттям.

Розташування екрана відеотермінала має забезпечувати зручність зорового спостереження у вертикальній площині під кутом ±30 градусів від лінії зору працівника.

Клавіатуру слід розміщувати на робочій поверхні окремо від столу на відстані 100-300 мм від краю, ближчого до працівника.

Розміщення принтера на робочому місці має забезпечувати добру видимість екрана відеотермінала, по висоті 900-1300мм, по глибині 400-500мм

Виробничі приміщення повинні обладнуватись шафами для зберігання документів, полицями, стелажами, тумбами тощо, з урахуванням вимог до площі приміщень. Приміщення з ВДТ мають бути оснащені аптечками першої медичної допомоги.

4.3 Пожежна безпека

Робоче приміщення відповідно до ПБЕ та ОНТП 24 –86 по вибухово-пожарній безпеці можна віднести до категорії "В".

Можливими причинами виникнення пожежі в приміщенні є:

1) коротке замикання проводки;
2) користування побутовими електрорадіоприладами .
3) не дотримання умов протипожежної безпеки.

У зв'язку з цим відповідно до ПУЕ необхідно передбачити наступні заходи щодо пожежної безпеки: ретельна ізоляція всіх струмоведучих провідників до робочих місць; періодичний огляд і перевірка ізоляції; суворе дотримання норм протипожежної безпеки на робочому місці;

Для гасіння пожеж на робочому місці користувача ПК використовують вуглекислотні та порошкові вогнегасники.

- ✓ Вуглекислотні вогнегасники випускаються як ручні (ВВК-5);

- ✓ Порошкові вогнегасники ВП-2, ВП-5, ВП-10 та ін.

З метою своєчасного оповіщення, на дільниці необхідно встановити протипожежну сигналізацію. Проходи та запасні виходи повинні бути вільними. Пожежний щит повинен розміщуватись в доступному місці та містити первинні засоби пожежогасіння: вогнегасник, лопату, відро, простирадло, ящик з піском. Відповідальний за пожежну безпеку керівник виробничої дільниці.

ВИСНОВКИ

Сьогодні використання технічних засобів охорони на об'єктах стало нормою, а не винятком. Стосується це і застосування систем пожежної сигналізації. Варто відзначити, що на відміну засобів охоронної сигналізації, відеоспостереження та контролю доступу, застосування систем пожежної сигналізації строго регламентоване нормативними документами України, які носять обов'язковий, а не рекомендаційний характер. Розуміння нормативної бази, компонентного складу і етапів впровадження АСПС важливо при проектуванні, експлуатації та обслуговуванні технічних засобів охорони. По роботі можна зробити наступні висновки

1. Представлений розширений склад систем протипожежної безпеки об'єктів.
2. Проведено аналіз датчиків (сповіщувачів) АСПС. Результати представлені у вигляді класифікацій.
3. Розглянуто системи АСПГ і СОУЕ.
4. Проведено аналіз складу бездротових АСПС.
5. Представлено техніко-економічне обґрунтування впровадження систем ПС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Воронов В. А. Системы контроля и управления доступом: учебник / Воронов В. А., Тихонов В.А. – М. Горячая линия – Телеком, 2010. – 272 с.
2. Новиков Ю. В. Основы микропроцессорной техники: учебник / Новиков Ю. В., Скоробогатов П. К. – М. ИНТУИТ.РУ. «Интернет – Университет Информационных технологий», 2003. – 440 с.
3. STMicroelectonics DataSheet, IEEE Press, 2015. – 199 p.
4. Андронников И. П. STM32F4 это же просто и на русском языке: учебник / Андронников И.П. МФТИ-ЧГУ, 2014, 348 с.
5. Страуструп Б. Программирование: принципы и практика использования С: учебник / Страуструп Б. – «Вильямс», 2011 – 1239 с.
6. Расчёт показателей надёжности радиоэлектронных средств: учебное пособие для вузов / [С. М. Боровиков, И. Н. Цырельчук, Ф. Д. Троян]; под ред. С. М. Боровиков. – М.: БГУИР, 2010. – 68 с.
7. Дание с сайта Habr.com Сканеры отпечатков. Классификация и способы реализации.
8. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации. Справочное пособие. – С.-Пб.: Лань, 2006. – 272 с.
9. Анин Б.Ю., Петрович А.И. Радиошпионаж. – М.: Международные отношения, 1996. – 448 с. Предпринимательство и безопасность/Под ред. д.ю.н. Ю.Б. Долгополова. В 2-х кн. м М.: Издательство “Универсум”, 2001.
10. Барабаш А.В., Шанкин Г.П. История криптографии. Ч.l. м М.: Гелиос АРВ, 2002. — 240 с.
11. Батурин Ю.М., Жодзишский Н.М. Компьютерная преступность и компьютерная безопасность. – М.: Юрид. лит., 2001. – 160 с.
12. Бендат Дж., Тирсол А. Прикладной анализ случайных данных: Пер. с англ. — М.: Мир, 1989. – 540 с.

13. Болдырев А.И., Василевский И.В., Сталенков С.Е. Методические рекомендации по поиску и нейтрализации средств негласного съема информации. Практическое пособие. м М.: НЕЛК, 2001. – 138 с.

14. Введение в криптографию/Под общей ред. В.В. Ященко. – С-Пб.: Питер, 2001. – 288 с.

15. Вербицький О.В. Вступ до криптології. – Львів: Видавництво науково-технічної літератури, 1998. – 248 с.

16. Вєртузаев М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник/За ред. С.Г. Лаптєва. – К.: Видавництво Європейського університету, 2001. – 201 с.

17. Всемирная история шпионажа/Авт.-сост. М.И. Ушаков. – М.: Олимп; ООО “Фирма «Издательство АСТ»”, 2000. – 496 с.

18. Гавриш В.А. Практическое пособие по защите коммерческой тайны. – Симферополь: Таврида, 2004. – 112 с.

19. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. – М.: Энергоатомиздат, 2004.

20. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Яхтсмен, 2006. – 67 с.