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

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Обслуговування комп'ютерних систем і мереж»

Група: 4КС-55

Дипломний проект

здобувача освіти денної форми навчання
КС.55.07.000.ДП

Чалмаєва Андрія Олексійовича

м. Одеса
2022 р.

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

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

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

Група: **4КС-55**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи) на тему:

Розробка системи захисту підприємства на основі обладнання AJAX

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

Дипломник _____ (Чалмаєв А.О.)
Керівник _____ (Стайкуца С.В.)

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

До захисту допущений
Голова циклової комісії _____ (Скорнякова О.В.)
Завідувач відділення _____ (Суліма Ю.Ю.)

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

Секретар ДКК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

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

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

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

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР_____

_____

"_____"_____2022 р.

З А В Д А Н Н Я

на дипломний проект (роботу)

Здобувачеві (здобувачці) освіти _____ **Чалмаєву Андрію Олексійовичу** _____

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) **Розробка системи захисту підприємства на основі обладнання AJAX**

_____

_____

затверджена наказом по коледжу від "**30**" **січня** 202**1** р. № **306-А2-ОД**

2. Термін здачі закінченого проекту (роботи) _____

3. Вихідні данні до проекту (роботи):

Обєкти дослідженнь – офісні приміщення, приватний будинок

Кількість базових складових ТЗО - 6

Основні беспроводові ОС – Hikvision, Калипсо, Лунь-Р, AJAX

Протокол радіозвязку AJAX - Jeweller

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

ВСТУП.

1. **ТЕХНОЛОГІЧНИЙ РОЗДІЛ**
2. **ЕКОНОМІЧНИЙ РОЗДІЛ**
3. **ОХОРОНА ПРАЦІ**
4. **ВИСНОВКИ**

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

Слайд 2 – Базовий склад технічних засобів охорони. Слайд 3 – Класифікація охоронних сповіщувачів ОТС. Слайд 4 – Щодо систем пожежної сигналізації та пожежогасіння. Слайд 5 – Основні ділянки та склад систем відеоспостереження та охорони периметру. Слайд 6 – Аналіз сучасних систем ОС. Слайд 7 – Безпроводові охоронні сигналізації. Слайд 8 – Бренд Ajax Systems. Слайд 9 – Екосистема та компонентний склад AJAX. Слайд 10 – Дослідження хабів від бренду AJAX. Слайд 11 – Розробка системи захисту офісних приміщень на основі обладнання AJAX. Слайд 12 - Розробка системи захисту приватного будинку на основі обладнання AJAX.

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Вступ, 1	Стайкуца С.В.		
2	Копайгородська Т.Г.		
3	Чорновол Н.І.		
Нормоконтроль	Петрашова В.І.		

7. Дата видачі завдання _____

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.	Огляд літератури. Огляд існуючих рішень.		
2.	Формування кінцевого завдання на розробку. Вступна частина дипломного проекту.		
3.	Технологічний розділ. Вибір елементної бази.		
4.	Технологічний розділ. Розробка структурної та принципової схеми пристрою.		
5.	Технологічний розділ. Розробка алгоритму та управляючої програми.		
6.	Економічний розділ.		
7.	Виконання розділу «Охорона праці».		
8.	Підготовка доповіді та презентації для захисту		
9.	Підготовка до попереднього захисту, підготовка до захисту		
10.	Отримання рецензії, відповіді на зауваження рецензента		
11.	Захист роботи		

Дипломник _____
(підпис)

Керівник _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			КС.55.07.000.ДП	Дипломний проект		
А4			КС.55.07.000.ДП. ПЗ	Пояснювальна записка	1	
				Презентація		

Ізм.	Арк.	№ докум.	Підпис	Дата	КС.55.07.000.ДП		
Розробив		Чалмаєв А.О.			Розробка системи захисту підприємства на основі обладнання AJAX	Літ.	Аркуш 3 / Ар-
Перевірив		Стайкуца С.В.				Н Д П	
Н. Контр.		Петрашова В.І.				ВСП ОТФК ОНТУ	
Затверд.		Скорнякова О.В.					

ЗМІСТ

ВСТУП

Система безпеки будь-якого об'єкта – це багатогранна та комбінована структура, яка має цілу низку складових у системі загальної безпеки. Так, залежно від типу об'єкта, виду та масштабів діяльності підприємства можуть застосовуватися організаційна, технічна, криптографічна, мережева, кадрова та інші види безпеки. У даному разі застосування технічних засобів охорони (ТЗО) є частим явищем практично всіх типах об'єктів. Системи пожежної сигналізації, пожежогасіння та димовидалення, охоронної сигналізації та відеоспостереження, контролю доступу та охорони периметра. Разом або окремо, але системи такого роду часто застосовуються для підвищення рівня безпеки об'єктів.

Важливо відзначити, що тип з'єднання центрального обладнання таких систем з кінцевими пристроями, а саме провідний або бездротовий, часто відіграє вирішальну роль при впровадженні систем. Причин тому багато – швидкість побудови системи, зручність, мобільність, витрати на побудову комунікаційного середовища тощо. Висновок однозначний – здебільшого застосування бездротових систем безпеки, особливо у побутовому та офісному сегментах, ефективно. Тому варто виділити високоякісний та титулований український бездротовий бренд безпеки, окрему екосистему безпеки під назвою Ajax та розглянути її можливості.

1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Концептуальні питання забезпечення безпеки компанії

Для створення оптимальної ефективної системи безпеки об'єкта необхідно насамперед розробити обґрунтовану концепцію, яка визначає цілі захисту, характер можливих загроз та ймовірність їх появи, основні напрямки вирішення завдань захисту тих чи інших цінностей від аварій, стихійних лих та неправомірних дій потенційних порушників.

– Предмет захисту – конкретні цінності фірми, які підлягають захисту за допомогою тієї чи іншої системи.

До таких цінностей відносяться:

– люди - персонал об'єкта, відвідувачі та клієнти фірми;

– матеріальні та фінансові цінності (гроші, цінні папери, документи, обладнання);

– інформація конфіденційного характеру.

Пріоритети зазначених цінностей великою мірою обумовлені характером діяльності фірми.

Об'єкт захисту - фізичний простір, де зосереджені ті чи інші цінності, багато в чому визначає можливі дії порушника безпеки та заходи щодо запобігання загрозам безпеки фірми.

Шляхи формування технічної системи охорони значною мірою залежать від характеристик огороджувальних конструкцій приміщень та інженерно-технічних систем об'єкта, їх відповідності вимогам нормативно-технічної документації щодо будівництва, забезпечення безпеки, протипожежних правил. Великий вплив на характеристики ТСО має також стан, в якому знаходиться об'єкт - стадія розробки проекту, будівництва, реконструкції або постійної експлуатації.

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

– кабінети керівництва фірми;

– переговорні кімнати;

– касові приміщення;

– центр обчислювальної та телекомунікаційної мережі – "серверна";

– приміщення установчої АТС та комутаційного обладнання телефонної мережі;

– приміщення з комутаційно-розподільною апаратурою інформаційно-телекомунікаційних систем (ІТКС) та систем безпеки;

– базові приміщення систем інженерного забезпечення (СІО) – вентиляційна камера, електрощитова кімната, приміщення резервного електроживлення та диспетчерської служби;

– приміщення служби безпеки фірми – центральний пост охорони, пост пожежної охорони;

– архів паперових та електронних копій;

– найважливіші технологічні приміщення, виходячи з характеру бізнес-процесу у фірмі.

Загрози безпеки фірми можна класифікувати так: за природою виникнення - загрози випадкового характеру та спричинені навмисними діями порушників; по відношенню до об'єкта, що захищається: зовнішні і внутрішні.

До загроз випадкового характеру (зовнішнім та внутрішнім) відносяться стихійні лиха та катастрофи природного та техногенного характеру, аварії або порушення у роботі систем життєзабезпечення об'єкта, а також помилкові дії персоналу та відмови обладнання.

До зовнішніх загроз входять також криміногенні загрози, недобросовісна конкуренція, промисловий шпигунство навмисно діючих зловмисників. Загрози, спричинені навмисними діями порушників безпеки об'єкта (як зовнішніх, і внутрішніх), виявляються як розкрадань матеріальних цінностей, вандалізму, шкідництва, саботажу, диверсій і терору. Основними мотивами таких загроз можуть бути невдоволення конкретним керівником, бажання самоствердитись, марнославство, корисливе прагнення отримати матеріальну чи іншу вигоду, а також намір реалізувати свої політичні, релігійні та ідеологічні устремління.

Внутрішні загрози - це зловмисні дії персоналу (зазвичай із соціально-психологічними та моральними проблемами). Ініціаторами такого виду загроз виступають, як правило, самі співробітники або зовнішні структури, які діють шляхом підкупу персоналу.

Оцінка загроз, аналіз ризику реалізації та прогнозування можливої шкоди в кожному виду загроз - найважливіший напрям забезпечення безпеки фірми.

1.1.1 Система охоронно-тривожної сигналізації

Охоронно-тривожна сигналізація (ОТС) – це сукупність спільно діючих технічних засобів метою яких є виявлення проникнення або спроби проникнення на територію об'єкта охорони. Така сигналізація забезпечує збір, обробку, передачу та подання службової інформації та інформації про стан безпеки на об’єкті. ОТС може інтегруватися в комплекс, який об’єднує всі встановлені системи безпеки та інженерні системи будівлі. Умовно ОТС можна розділити на два типи:

1. Автономна система. У разі спрацювання такої системи активуються сирени та інші тривожні прилади. Сигнал тривоги нікуди не передається, а служить для оповіщення внутрішньої охорони об’єкта про несанкціоноване проникнення.

2. Сигналізація з підключенням до пульту централізованого спостереження, з, так званою, пультовою охороною. При спрацюванні сигналізації з найближчого пункту охорони на об’єкт направляється група швидкого реагування для з’ясування ситуації, що призвела до спрацювання сповіщувачів.

Класична охоронна система складається з наступних елементів: контрольної панелі; приладу управління (клавіатура, клієнтського ПЗ тощо); сигнальних пристроїв (сирен, світлових оповіщувачів, прилади віддаленого моніторингу); сповіщувачів.

Елементи, що входять до складу системи дозволяють встановлювати найбільш ефективні для кожного конкретного об’єкту параметри сигналу

тривоги та реакції системи. Різноманітні види датчиків дозволяють враховувати такі фактори, як несанкціонований рух, звук розбиття скла тощо. Сигнальні пристрої, у свою чергу, можуть задіяти слухові чи зорові канали, а також передавати заздалегідь записаний сигнал тривоги на мобільні пристрої довірених осіб, відправити SMS чи push повідомлення. Для постановки та зняття режиму «охорона» сигналізації можуть використовуватися різноманітні пристрої: сенсорну клавіатуру, радіо-брелок, електронні ключ чи біометричну систему.

Центром системи є контрольна панель, яка виробляє обробку даних з датчиків, клавіатур і активує сигнальні пристрої у разі тривоги. Вона стежить за станом підключених датчикі. Якщо система знаходиться у режимі «охорона» і один з підключених датчиків переходить в режим «тривога», контрольна панель активує підключені сигнальні пристрої по заданому алгоритму. Сучасні контрольні панелі дозволяють підключені датчики програмно об'єднувати в зони. Нижче представлені основні типи охоронних зон:

– зона входу/виходу. У цю зону включаються охоронні датчики, розташовані на шляху входу і виходу з приміщення. Панель активує сигнальні пристрої по сигналу від датчиків тільки після тимчасової затримки, яка необхідна для постановки або зняття системи сигналізації з охорони.

– прохідна зона. Формує тривожний сигнал після тимчасової затримки. У цю зону включаються датчики, розташовані по шляху руху об’єкта охорони до клавіатури. Затримка тривоги відбувається тільки в тому випадку, якщо порядок отриманих сигналів від охоронних датчиків відповідає заданому.

– 24-годинна цілодобова зона. Якщо контрольна панель сигналізації отримує тривожний сигнал від датчика з цієї зони, то сигнальні пристрої активізуються негайно. Як правило, в цю зону включаються так звана тривожна кнопка, що застосовується для виклику служб реагування.

– тамперна зона. У цю зону включаються не датчики, а їх спеціальні контакти (тампери). Тривожний сигнал формується при спробі демонтажу або розбиття датчика. Тамперні контакти так само можуть підключатися від клавіатур, сирен і будь-яких інших пристроїв ОТС.

Пристрої управління сигналізацією Для постановки та зняття ОТС з режиму охорони використовуються різні пристрої управління:

– сенсорна клавіатура. Може розташовуватися безпосередньо на корпусі контрольної панелі або встановлюватися окремо. Постановка та зняття з охорони здійснюється набором цифрового коду;

– радіо-брелок. Бездротовий пристрій, який дозволяє використовувати сигналізацію і на рухомих об’єктах (автомобіль, транспортний контейнер тощо);

– електронні ключі. Найчастіше використовуються пластикові proximity-картки або ключі Touch Memory тощо;

Сигнальні пристрої – пристрої, що активуються у разі тривоги. Наприклад, звукові сирени. Найбільшого поширення набули п'єзоелектричні та динамічні сирени. Голосові дозвонювачі при активації передають заздалегідь записане голосове повідомлення на довірені телефонні номери.

Сповіщувач – це пристрій, що формує певний сигнал при зміні того чи іншого контрольованого параметра навколишнього середовища. За областю застосування сповіщувачі класифікуються на охоронні та пожежні. За принципом дії вони поділяються на електроконтактні, магнітоконтактні, удароконтактні, п'єзоелектричні, оптико-електронні, ємнісні, звукові, ультразвукові, радіохвильові, комбіновані, поєднані тощо. Наведемо класифікацію охоронних сповіщувачів на рис. 1.1.

1.1.2 Системи пожежної сигналізації

Система сигналізації – це набір спеціально підібраного і встановленого обладнання та ПЗ, здатного виявити ознаки проникнення на об’єкт охорони або виявлення ознак пожеж з фіксуванням місця, дати та часу події, подачі сигналу тривоги та включення виконавчих пристроїв. Головними функціями системи сигналізації є своєчасне визначення місця порушення заданих параметрів, а також формування та передача сигналів, призначених для управління системами оповіщення про виникнення джерела загрози за допомогою спеціальних технічних засобів.

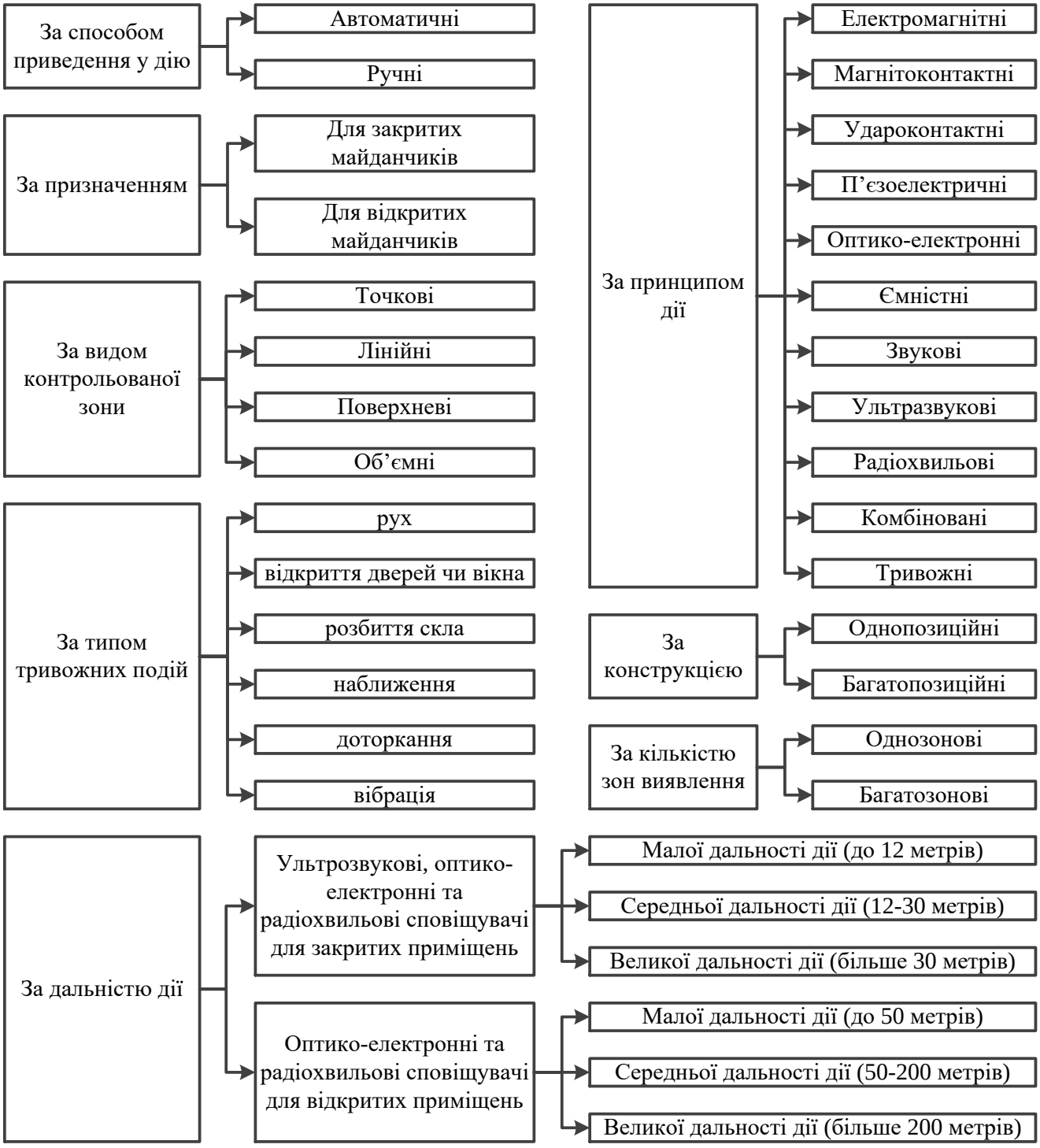


Рисунок 1.1 – Класифікація охоронних сповіщувачів ОТС

Залежно від конструкції такої системи для неї можуть бути передбачені різні завдання. Однак активно протидіяти загрозам системи сигналізації не можуть. Ефективність системи сигналізації полягає у максимально ранньому розпізнаванні небезпеки і в оповіщенні відповідної служби. Спеціалісти виділяють п'ять основних вимог до систем сигналізації:

– щоб знизити кількість помилкових тривог, система сигналізації повинна якомога менше залежати від погодних факторів та інших перешкод;

– система повинна бути підібрана під конкретний об'єкт з урахуванням його вразливих місць;

– управління системою має бути нескладним для користувача;

– монтажні роботи і технічне обслуговування повинне проводитися професіоналами;

– система сигналізації має бути високоякісною.

Система пожежної сигналізації (СПС) – це сукупність технічних засобів, встановлених на об'єкті охорони для виявлення пожежі, обробки, представлення в заданому вигляді повідомлення про пожежу на цьому об'єкті, спеціальної інформації та (або) видачі команд на включення автоматичних установок пожежогасіння та технічних пристроїв.

За способом приведення у дію пожежні сповіщувачі поділяються на ручні та автоматичні. В автоматичних пожежних сповіщувачів контрольованими параметрами можуть виступати: підвищена температура повітря, виділення продуктів горіння, турбулентні потоки гарячих газів, електромагнітне випромінювання тощо. Відповідно до ознак пожежі сповіщувачі поділяються на теплові, димові, полум'яні, газові та комбіновані. Можливо також використання інших ознак. Комбіновані сповіщувачі реагують на два і більше параметрів, що характеризують появу вогнища загоряння. На рис. 1.1 представлено класифікацію пожежних сповіщувачів.

Технічні засоби збору та обробки інформації. До таких засобів належать ППКП, контрольні панелі, сигнально-пускові пристрої, системи передачі сповіщень тощо. Вони призначені для безперервного збору інформації зі сповіщувачів, аналізу тривожної ситуації на об'єкті й її відображення, управління місцевими світловими та звуковими сповіщувачами, індикаторами та іншими пристроями (реле, модемами тощо), а також формування та передачі сповіщень про стан об'єкта на центральний пост або пульт централізованого спостереження.

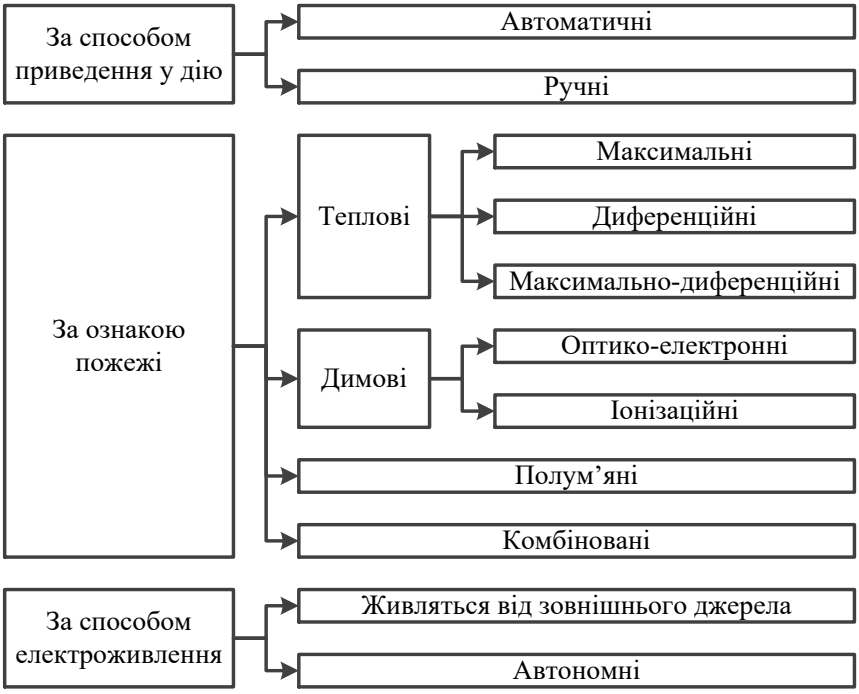


Рисунок 1.2 – Класифікація пожежних сповіщувачів

Шлейф сигналізації – це електричне коло, що об'єднує вихідні ланцюги сповіщувачів і включає в себе допоміжні елементи (діоди, резистори тощо), з'єднувальні дроти і призначена для видачі сповіщень (про проникнення, спробу проникнення, пожежі, несправності), а, в деяких випадках, і для подачі електроживлення на сповіщувачі. Таким чином, шлейф сигналізації призначений для контролю стану деякої зони охорони. Зона охорони – це частина об'єкту, що охороняється, контрольована одним або декількома шлейфами сигналізації. За способом підключення шлейфів можна виділити наступні типи ППКП: з шлейфами радіальної структури, деревовидної структури, адресні.

У ППКП з шлейфами радіальної структури кожен шлейф підключається безпосередньо до самої панелі. Така структура виправдовує себе при невеликій кількості шлейфів (зазвичай до 16) і на об'єктах, які не потребують організації віддалених шлейфів. Застосовуються в основному на невеликих і середніх об'єктах.

ППКП з деревовидною структурою мають спеціальну інформаційну шину з декількох проводів (зазвичай 4). На цю шину підключаються розширювачі. У свою чергу, до розширювачів підключаються радіальні шлейфи. До самого

ППКП можуть також підключатися кілька базових радіальних шлейфів. Загальна кількість шлейфів знаходиться зазвичай в межах 24-128. Розширювачі контролюють стан підключених до них шлейфів, кодують інформацію про їх стан і передають по інформаційній шині на ППКП, що має індикацію стану всіх шлейфів. Такі ППКП використовуються для побудови систем середніх і великих об'єктів.

Адресні ППКП, що використовують шлейфи з адресними сповіщувачами, найчастіше використовуються для створення досить складних ІСБ для великих і відповідальних об'єктів. Адресні сповіщувачі складніше звичайних і більше коштують. Їх застосування та переваги в повній мірі проявляються на складних і великих об'єктах. Існують адресні ППКП, що мають різну побудову своїх шлейфів: променева, кільцева, кільцева з променевим відгалуженням.

Кільцевий шлейф має серйозну перевагу. При його обриві він зберігає свою працездатність, оскільки зберігається лінія обміну інформацією. При замиканні шлейфа спеціальні пристрої, подільники шлейфу, відключають закорочену ділянку, а інша частина шлейфа продовжує функціонувати. ППКП та контрольні панелі є основними елементами, що формують на об'єкті інформаційно-аналітичну систему сигналізації. Такі системи можуть бути автономними або централізованими. У першому випадку ППКП встановлюють в приміщенні охорони, що розміщується на об'єкті, а при централізованій формується об'єктовий комплекс технічних засобів з декількома ППКП.

1.1.3 Системи пожежної безпеки та оповіщення

Важливим компонентом інженерно-технічних засобів захисту інформації є системи пожежної безпеки. Окрім СПС, розглянутих вище, до них слід віднести системи пожежогасіння та оповіщення про пожежу.

Основною функцією таких систем є передача повідомлень про необхідність евакуації при виявленні надзвичайної ситуації у вигляді пожежі та ефективної локалізації вогню для зменшення ризиків життю та здоров’ю людей. У той же час слід відзначити: якщо системи пожежогасіння вузько направлені,

то системи оповіщення використовуються і в інших потребах. Позаяк, підтримувати систему і не використовувати її у повсякденному житті – малоефективне заняття. Саме тому додатковими функціями системи оповіщення про пожежу може бути трансляція фонової музики, реклама чи конференц-зв'язок.

У найпростішому варіанті система вирішує завдання лише речового оповіщення. У більш-складних системах на великих об'єктах можна зустріти такі можливості, як:

– розділення об'єкта на зони з можливістю зонового оповіщення і зі спеціальною чергою оповіщення;

– двосторонній зв'язок зон оповіщення;

– координація роботи системи через управління з пожежного поста;

– включення системи оповіщення від сигналу, який формується, наприклад, СПС.

Склад системи може включати велику кількість обладнання. У тому числі: мікрофони, клавіатури станцій виклику, підсилювачі звуку, контролери оповіщення, пристрої розподілення сигналу і різного роду гучномовці. Останні – кінцевий елемент системи, що є й основним її елементом. Проектування систем оповіщення окреслено такими стандартами, як:

– IEC60849;

– європейські стандарти безпеки до систем класу Voice Alarm System.

При побудові великих систем необхідно, по-перше, обладнання, що могло б компенсувати роботу великої кількості технічних засобів в одному приміщенні, наприклад, у конференц-залі з великою кількістю мікрофонів і гучномовців. Таким обладнанням можуть бути лімітери, експандери, енгансери, еквалайзери, а також різноманітні гейти і компресори, які випускаються виробниками радіоелектроніки. По-друге, під час проектування на деяких об'єктах необхідно використовувати вузькоспеціалізоване обладнання – лінії затримки, тонкоректори, додаткове обладнання шумо- та ехо-приглушення.

Нині однією з найбільш популярних систем аналогового озвучування є Bosch Plena Voice Alarm System, яка підтримує до 60-ти зон озвучування і до 16-ти рівнів пріоритету озвучування, що дозволяє вирішувати завдання для багатоповерхівок і великих об'єктів як вокзали, торгові центри, аеропорти тощо. За останні десять років ринок систем озвучування при пожежі поповнився також повністю цифровими системами. Та ж компанія Bosch випустила систему Praesideo. Відмінною характеристикою таких систем є можливість переключатися на резервні підсилювачі звуку, управління записаними цифровими повідомленнями і інтерфейс з робочою ППКП, можливість моніторингу системи. Таким чином, можна сказати, що цифрові системи оповіщення можуть бути набагато глибше інтегровані з іншими системами безпеки під час побудови ІСБ.

Розглянемо також системи пожежогасіння. Загалом під системою пожежогасіння розуміється сукупність стаціонарних технічних засобів гасіння пожежі шляхом випуску вогнегасної речовини. Завданням цих систем у першу чергу є збереження життя та здоров'я людей шляхом ліквідації пожежі на ранній стадії ще до роботи державної пожежної служби.

Установки пожежогасіння повинні забезпечувати локалізацію або ліквідацію пожежі. Загальна класифікація установок пожежогасіння приведена на рис. 1.3.

За своєю конструкцією системи пожежогасіння поділяються на:

– модульні – нетрубопровідні автоматичні установки пожежогасіння, що передбачають розміщення ємності з вогнегасною речовиною та пусковим пристроєм безпосередньо на об'єкті охорони;

– агрегатні –технічні засоби виявлення пожежі, зберігання, випуску та транспортування вогнегасної речовини конструктивно є самостійними одиницями, монтуються безпосередньо на об'єкті охорони;

– автономні – автоматично здійснюють функції виявлення та гасіння пожежі незалежно від зовнішніх джерел живлення та систем керування.

За ступенем автоматизації:

– автоматичні – автоматично спрацьовують при перевищенні контролюючим фактором (факторами) пожежею встановлених порогових значень на об’єкті охорони;

– автоматизовані – можуть автоматично спрацьовувати при перевищенні контролюючим фактором (факторами) пожежею встановлених порогових значень на об’єкті охорони, або ж контролюватися у оператором системи пожежогасіння чи частково мати деякі автоматичні частини;

– ручні – повністю залежать від дій оператора системи пожежогасіння.

За видом вогнегасної речовини: водяні, пінні, газові, порошкові, аерозольні, комбіновані. За способом гасіння:

– об'ємні – призначені для створення середовища, яка не підтримує горіння на об’єкті охорони;

– поверхневі – впливає на палаючу поверхню на об’єкті охорони;

– локально-об'ємні;

– локально-поверхневі.

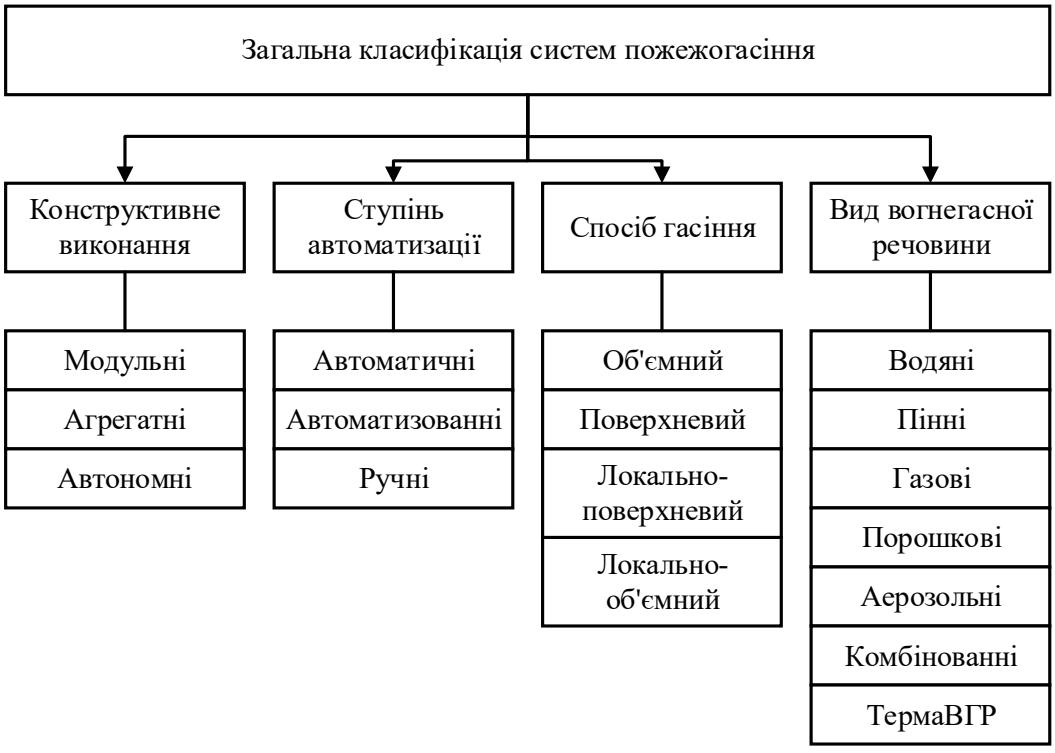


Рисунок 1.3 – Загальна класифікація установок пожежогасіння

Різні види систем пожежогасіння дозволяють успішно вирішувати завдання пожежної безпеки відповідно до конкретних умов на об'єктах, що підлягає захисту. Основними системами пожежогасіння, які застосовуються в даний час, є газові, аерозольні, пінні, порошкові та водяні.

1.1.4 Система відеоспостереження

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

Найбільш звичними як для іноземних, так і для українських фахівців з безпеки на сьогоднішній день є найпоширеніші аналогові системи відеоспостереження. Існуючи вже більше 50 років, вони й донині займають лідируючі позиції за популярністю в усьому світі. Але варто зауважити , що така ситуація актуальна не тому, що аналогові технології запису і передачі відеопотоку чимось краще за інших. Справа в тому, що процес установки та обслуговування аналогових систем досить простий і звичний для більшості інтеграторів систем безпеки. Тому, навіть після появи більш актуальних розробок у сфері відеоспостереження, багато фахівців продовжують довіряти перевіреному обладнанню та встановлювати його більшості клієнтам.

Однак більш правильно сучасні системи відеоспостереження розділяти по типу сигналу на аналогові, комбіновані (цифро-аналогові), гібридні, мережеві. Основні ділянки та компоненти систем відеоспостереження представлено на рис. 1.4.

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.

Рисунок 1.4 – Основні ділянки системи відеоспостереження

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.

Основними елементами системи відеоспостереження 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.

Основними технічними характеристиками системи відеоспостереження є:

- роздільна здатність відеозображення (CIF, D1, 720p, Full HD, 1080p тощо);
- частота кадрів (25 або 30 кадр/сек виходячи із стандартів сигналів PAL та NTSC);
- глибина (тривалість зберігання) відеорхіву (годинник, доба, тижні, місяці);
- наявність додаткових спеціальних можливостей, таких як розпізнавання номерів автомобілів, розпізнавання осіб та інші функції відеоаналітики.

1.1.5 Системи контролю і керування доступом

Система контролю та управління доступом (СКУД) – це сукупність програмно-технічних і організаційно-методичних засобів, за допомогою яких вирішується завдання контролю й управління доступом у приміщеннях об’єкта, а також оперативний контроль за пересуванням персоналу та часу його перебування на території.

На сьогодні існує дуже багато різновидів СКУД різних виробників, а також їх компонентів. Незважаючи на унікальність кожної конкретної СКУД, вона містить 4 основні елементи: ідентифікатор користувача (карта-пропуск, ключ), пристрій ідентифікації, керуючий контролер і виконавчі пристрої. Загальна схема СКУД показана на рис. 1.5:

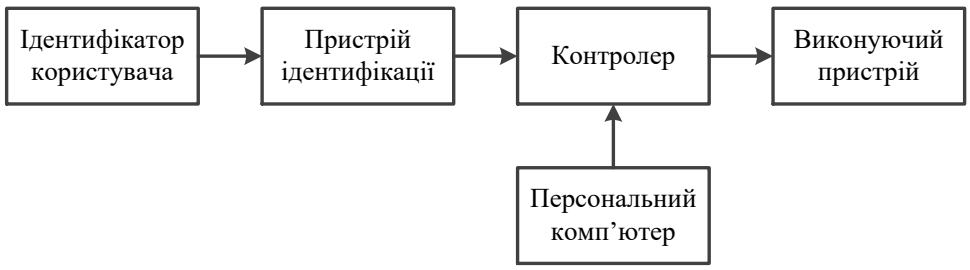


Рисунок 1.5 – Загальна схема СКУД

Ідентифікатор користувача – це пристрій чи ознака, за якою ідентифікується користувач. Для ідентифікації застосовуються атрибутні та біометричні ідентифікатори. В якості атрибутних ідентифікаторів використовують автономні носії ознак допуску: магнітні картки, безконтактні proximity-картки, брелки touch-memory, радіобрелки, а також біометричні фактори особи: зображення райдужної оболонки ока, відбиток пальця, відбиток

долоні, риси обличчя тощо. Кожен ідентифікатор характеризується певним унікальним двійковим кодом. Нині застосовуються:

– безконтактні радіочастотні proxmity-картки. Вони спрацьовують на відстані та не вимагають чіткого позиціонування, що забезпечує їх стійку роботу, зручність використання та високу пропускну здатність;

– магнітні картки. Існують карти з низькокоерцитивною та висококоерцитивною магнітною смугою та з записом на різні доріжки;

– карти Віґанда (Wiegand) – названі іменем американського фізика та винахідника Джона Річарда Віґанда, який відкрив магнітний сплав, що має прямокутну петлю гістерезіса;

– штрих-кодові карти – на карту наноситься штриховий код. Існує складніший варіант – штрих-код закривається матеріалом, прозорим тільки в інфрачервоному світлі, зчитування відбувається в інфрачервоній області;

– ключ-брелок Touch-memory – таблетка, всередині якої розташований чип ROM (від англ. «read-only memory» – пам'ять постійного зберігання).

Контролери – пристрої, призначені для обробки інформації від зчитувачів ідентифікаторів, ухвалення рішення і управління виконавчими пристроями. Саме контролери дозволяють прохід через пропускні пункти. Контролери розрізняються ємністю бази даних і буфери подій, що обслуговують пристрої ідентифікації. Будь-який контролер СКУД складається з чотирьох основних частин: пристроя ідентифікації, контролера, ПК та виконуючого пристроя.

Пристрій ідентифікації передає інформацію на схему обробки сигналів контролера. Далі інформація подається на схему прийняття рішень, яка заносить факт спроби проходу в схему буфера подій, запитує схему бази даних на предмет правомірності проходу і, в разі позитивної відповіді, запускає виконавчий пристрій. На кінець сам факт проходу саме цієї людини заноситься в схему буфера подій.

Серед виконавчих пристроїв СКУД найбільш поширені такі запірні або керовані перегороджуючі пристрої: замки, засувки, турнікети, ліфти тощо.

Переваги біометричних ідентифікаторів на основі унікальних біологічних, фізіологічних особливостей людини привели до інтенсивного розвитку відповідних засобів. Як біометричні ідентифікатори використовуються статичні методи, засновані на фізіологічних характеристиках людини. Відомі розробки СКУД засновані на зчитуванні і порівнянні конфігурацій сітки вен на зап'ясті, зразків запаху, акустичного відгуку середнього вуха людини при опроміненні його специфічними акустичними імпульсами тощо.

1.1.6 Системи охорони периметру

Охорона периметру – це сукупність програмних, технічних, організаційних засобів і заходів, спрямованих на недопущення несанкціонованого проникнення в периметр.

Охорона периметра здійснюється за допомогою технічних засобів охорони і людських ресурсів, причому перші – найбільш надійні і ефективні. Однак, практично всім їм властивий один істотний недолік: сигнал вторгнення проходить лише після несанкціонованого проникнення на територію об'єкта охорони.

Оснащення периметра технічними засобами, що уповільнюють його перетин (колючим дротом тощо) дозволяє дати запас часу силам, які здійснюють охорону об'єкта. Гарного результату можна досягти, оснастивши систему охорони датчиками руху в зонах, прилеглих до периметру зовні та PTZ-камерами. Слід приділити увагу тому факту, що охорона периметра – це завдання, яке вимагає комплексного підходу. Інженерні споруди використовують для уповільнення зловмисника та ускладнення перетину периметру:

- загородження;
- протитаранні пристрої;
- контрольно-пропускні пункти;
- ворота;
- протипідкопні конструкції.

До засобів периметральної сигналізації відносяться різноманітні датчики, які використовують для інформування про зловмисника. Склад системи охорони периметра зображений на рис. 1.6.

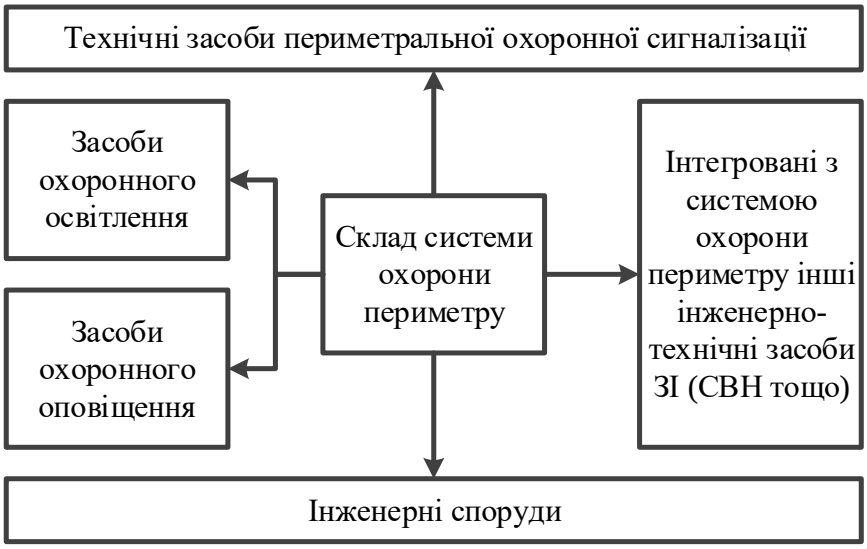


Рисунок 1.6 – Склад систем охорони периметра

Засоби охоронного освітлення забезпечують спроможність оглядати периметр у нічний час, а засоби охоронного сповіщення представляють собою гучномовці, сирени, звукову сигналізацію.

В основі розробки різних систем захисту й організації її функціонування лежить принцип створення замкнутих, послідовних рубежів, що починаються за межами контрольованої зони і концентрично стягуються до особливо важливих приміщень.

На кожному рубежі повинні бути виявлені та, за можливістю, ліквідовані будь-які загрози порушення безпеки. В разі, коли ліквідація загрози неможлива, потрібно у максимально короткий час затримати порушника та задіяти до перешкоджання загрозам наступні рубежі безпеки. Основу планування й обладнання контрольованих зон (організованих рубежами) складають принципи рівнопотужності і комплексності.

Використання системи захисту на основі рубежів обумовлено тим, що система дозволяє забезпечити належний рівень безпеки: при наявності широкого спектру різнорідних загроз (від тероризму до витончених спроб проникнення в

обчислювальну систему); при використанні різних технологій обробки інформації шляхом глобального контролю; за критерієм оптимального розподілу ресурсів системи захисту з урахуванням пріоритету загрози.

1.2 Дослідження напрямку безпроводових систем охорони з позиції охоронно-тривожної сигналізації

1.2.1 Порівняння провідних та бездротових систем безпеки

Система безпеки може бути як дротовою, так і бездротовою. Це означає, що система може мати або бездротову сенсорну мережу та панель управління з провідним стаціонарним з'єднанням, або провідні датчики з панеллю управління, підключеної до зовнішнього світу через стільниковий зв'язок. Найбільш поширена конфігурація поєднує в собі два варіанти, з провідною телефонною лінією як основне з'єднання та резервним стільниковим зв'язком на випадок, якщо телефонні лінії вийдуть з ладу (або обірвуться). Але сьогодні не в усіх будинках є активні стаціонарні телефони. У побутових умовах переваги та недоліки провідних та бездротових систем безпеки зводяться до двох питань: проблеми встановлення та відмінності у продуктивності.

Бездротові системи. Якщо у вашому будинку не встановлено систему безпеки, бездротові системи можуть вирішити кілька проблем. Вам не доведеться турбуватися про свердління отворів або внесення інших змін, тому бездротовий зв'язок є привабливим варіантом для наймачів, історичних будинків або будівель зі значною внутрішньою цегляною, кам'яною або мармуровою конструкцією. Орендарі або домовласники, які змінюють місце проживання, також зможуть скористатися мобільністю більшості бездротових систем – просто відключіть їх та підключіться за новою адресою.

Потенційним недоліком бездротового зв'язку є його надійність. Так само, як маршрутизатори Wi-Fi або мобільні телефони, бездротові системи безпеки схильні до різних типів перешкод, які можуть призвести до того, що ваш датчик не реагуватиме або непередбачувано реагуватиме (наприклад, викликати

помилкову тривогу). Електромагнітні перешкоди можуть бути викликані багатьма іншими пристроями, включаючи радіоняні, пульти дистанційного керування, лінії електропередач, мікрохвильові печі та флуоресцентне освітлення. Структурні перешкоди виникають через стіни, підлоги, стелі або такі речі, як металеві шафи. Однак ці проблеми рідкісні. Щоб допомогти протистояти потенційним проблемам, кожен бездротовий датчик має власну батарею, яка чудово працює, особливо при відключенні живлення. Просто слідкуйте за тим, щоб замінити батареї, щоб вони завжди працювали з максимальною продуктивністю.

Провідні системи. Якщо ваш будинок був заздалегідь підключений до системи безпеки, краще використовувати апаратний варіант, тому що система буде проста в установці. Якщо ви вже знаєте, який провайдер встановив обладнання, активувати вашу систему просто - все, що потрібно - це телефонний дзвінок і, можливо, технічний візит для оновлення панелі управління. Якщо ви хочете використовувати іншого постачальника, встановлення та оновлення системи повинні бути такими ж простими, як програмування нового номера в панелі керування. У деяких випадках може знадобитися перетворювач або навіть нова панель управління, але поки сама проводка не пошкоджена, всі існуючі датчики повинні працювати з обладнанням будь-якого постачальника - всі провідні системи містять по суті одну й ту саму технологію.

Більшість великих постачальників систем безпеки пропонують як дротяні, так і бездротові опції, тому вибір правильного рішення більшою мірою залежатиме від технічного завдання на проектування та вхідних даних по об'єкту.

Детально переваги та недоліки провідних та бездротових рішень систем безпеки на прикладі охоронної сигналізації представлені в табл. 1.1.

Таблиця 1.1 - Переваги та недоліки бездротових систем сигналізації

№	Переваги	Недоліки
1	Найменша кількість видимих елементів	Деяке ослаблення радіосигналу під час проходження через фізичні перешкоди
2	Можливість оперативної зміни місця розташування обладнання	Вартість вище на тлі провідних рішень
3	Можливість комплексної роботи радіоканалів різних діапазонів	Схильність до радіоперешкод
4	Простота встановлення	Залежність від якості та радіусу покриття мережі GSM-оператора
5	Економія на додаткових кріпленнях для монтажу	Складність у ремонті
6	Незалежність від електроживлення	
7	Надійний та ефективний спосіб передачі сигналу	
8	Додатковий захисний ефект за рахунок мініатюрного дизайну	
9	Можливість використання неординарних рішень	
10	Можливість розширення функцій системи сигналізації	

Як видно, перевага – 10, недоліків – 5, що говорить про ефективність застосування бездротових систем сигналізації

Візуалізація переваг застосування бездротових технологій загалом передбачена на рис. 1.7.

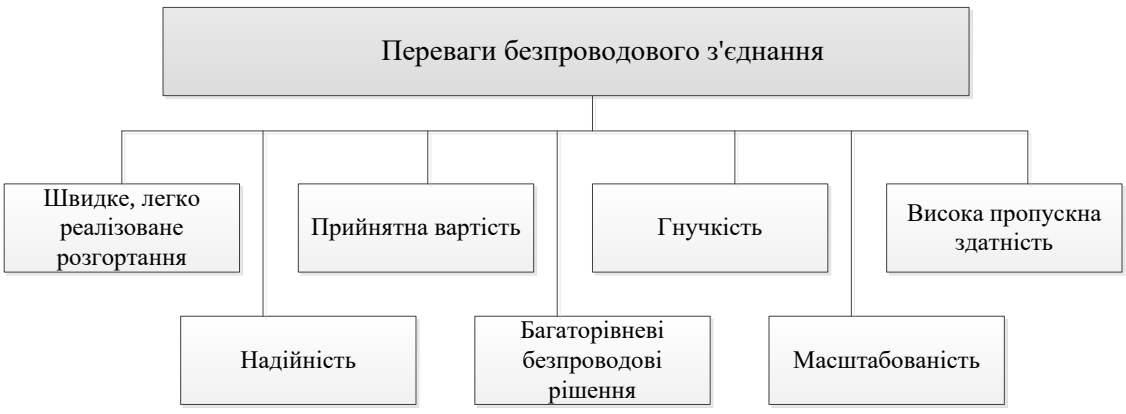


Рисунок 1.7 - Переваги безпроводового з'єднання

1.2.2 Аналіз безпроводових систем охоронної сигналізації

Охоронна сигналізація на базі обладнання Каліпсо

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.

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);

Таблиця 1.2 – ТТХ охоронної централі Каліпсо

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

Зовнішній вигляд представлений на рисунку 1.8.

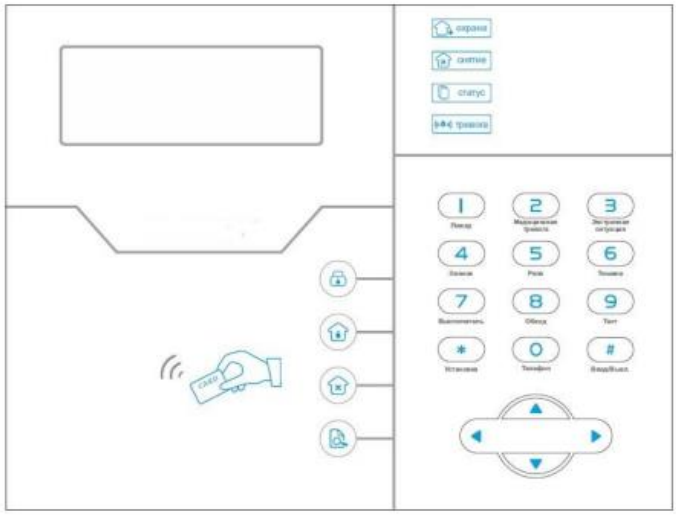


Рисунок 1.8 - Зовнішній вигляд ТТХ охоронної централі Каліпсо

Рисунок 1.8 - Екосистема Каліпсо в сукупності оповіщувачів

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.

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.

Охоронна сигналізація Hikvision AX-Pro

Hikvision AX PRO – сучасне та просунуте рішення як для охорони невеликих квартир, так і для захисту офісних комплексів та заміських будинків.

Це охоронна сигналізація, покликана захищати будинок, офіс та будь-який інший об'єкт – це ціла система гаджетів, яка не буде коректно працювати без централі або хаба управління. Hikvision AX PRO – продукт відомої у сфері безпеки компанії, який поєднує різні пристрої та дозволяє працювати з ними з одного інтерфейсу.

Рисунок 1.9 – Зовнішній вигляд ОС Hikvision AX PRO

Основою охоронної системи Hikvision AX-Pro є централь (хаб). Хаб працює повністю бездротовим радіопротоколом, який дозволяє підключати датчики охоронної сигналізації на відстані до 2000 метрів. Також зв'язок є двостороннім і відбувається у зашифрованому вигляді, при цьому рівень безпеки доведений процедурою сертифікації Grade2.

Також у хаба охоронної сигналізації є низка важливих особливостей:

- дві версії програми: Hik Connect для рядових користувачів та Hik Pro Connect, що використовується професіоналами ринку безпеки;

- широкий вибір каналів зв'язку: Ethernet, WiFi, два слоти під SIM-карти для безперебійного обміну інформацією;

- можливість роботи з датчиками Pircam та підтримка їх функції фотофіксації руху;

- повноцінна відеоверифікація у вигляді семисекундного ролика, що надсилається користувачеві у разі спрацьовування тривоги на датчику.

Централі (хаби), ВКП.

Лідером серед охоронних панелей цього бренду є Hub бездротової сигналізації Hikvision DS-PWA64-L-WE

Hikvision DS-PWA64-L-WE - хаб нового покоління бездротової сигналізації Hikvision серії AX PRO, який здатний підтримувати підключення 142 бездротових пристроїв та 64 бездротових зон охорони. Hub є невеликим за розміром пристроєм, виконаним з пластику білого кольору, який можна розмістити в будь-якому куточку приміщення.

Централь може працювати по Wi-Fi, підтримує TCP/IP, GPRS та сучасні протоколи бездротового зв'язку Tri-X (відстань передачі – до 2000 м) та CAM-X (відстань передачі – до 800 м.).

Особливості централі Hikvision DS-PWA64-L-WE:

– Зони бездротового підключення до 64 бездротових входів/виходів, 8 зчитувачів/клавіатур, 4 оповіщувачів, 2 репітерів,

– Бездротовий протокол нового покоління: Tri-X та Cam-X

– Передача радіосигналу на дальні дистанції до 2000м

– TCP/IP, Wi-Fi та GPRS

– Двосторонній зв'язок із шифруванням AES-128

– Налаштування через веб-клієнт, мобільний клієнт та Convergence Cloud

– Налаштування Hik-Connect та Hik-ProConnect залежить від рівня доступу користувача

– Тривожні повідомлення або через телефонні дзвінки (Один слот SIM картки)

– Перегляд відео в режимі реального часу в Hik-Connect

– Надсилання відео тривожних подій електронною поштою та додаток

– Завантаження звітів про тривоги в ARC

– LED-індикатор для індикації стану системи

– Резервна літієва батарея 4520 мАг

– Протокол SIA-DC09, підтримка Contact ID та формату даних SIA.

Альтернативним рішенням пропонується гібридний приймально-контрольний пристрій Hikvision DS-PHA20-P. Цей прилад, на відміну від попередньої моделі, має не лише бездротові, але й провідні зони на борту. З особливостей:

– Двосторонній зв'язок тривожних подій та інших сигналів через LAN, PSTN, GPRS та 3G/4G з використанням основного та резервного каналів з налаштованим пріоритетом.

– 4 провідних зон на борту та можливість розширення до 20 провідних зон

– До 16 бездротових входів, 18 бездротових виходів, 1 провідна сирена та 2 бездротові сирени

– Попередній (5 с) та посттривожний (2 с) запис для перевірки відео для отримання сигналу тривоги електронною поштою або мобільним клієнтом

– Завантажує події тривоги у центр прийому тривог.

Звичайно, застосування тієї чи іншої ПКП обумовлено особливостями об'єкта, його технічними особливостями та масштабом, кількістю користувачів, вимогами до монтажу тощо. На рис. 1.10 показано порівняння наведених вище ПКП від компанії Hikvision.

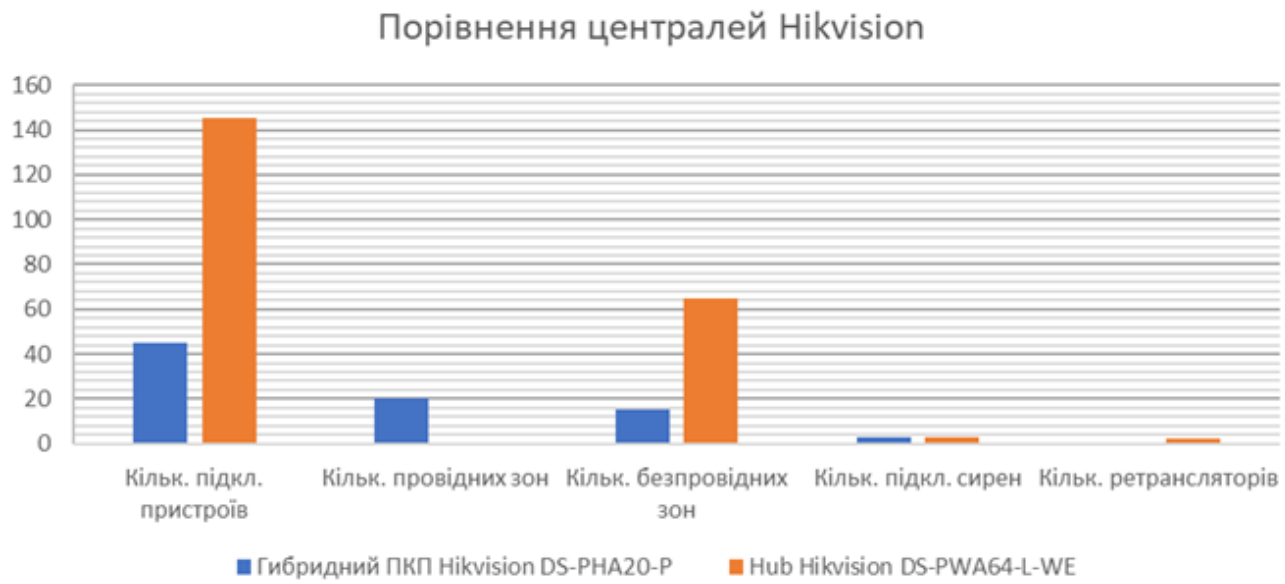


Рисунок 1.10 - Порівняння охоронних ПКП Hikvision за ключовими критеріями

В цілому, компонентний ряд охоронного напрямку бренду включає такі основні групи, як:

- ВКП (хаби).
- Сповіщувачі.
- Бездротові магнітні датчики.
- PIR-датчики.
- Інфрачервоні оптичні оповіщувачі.
- ІЧ-датчики.
- Датчики розбиття скла.
- Датчики диму.
- Датчики протікання води.
- Бездротові внутрішньові сповіщувачі (сирени).

На рис. 1.11 представлена візуалізація вартості компонентів системи. Колірною гамою показані групи обладнання.

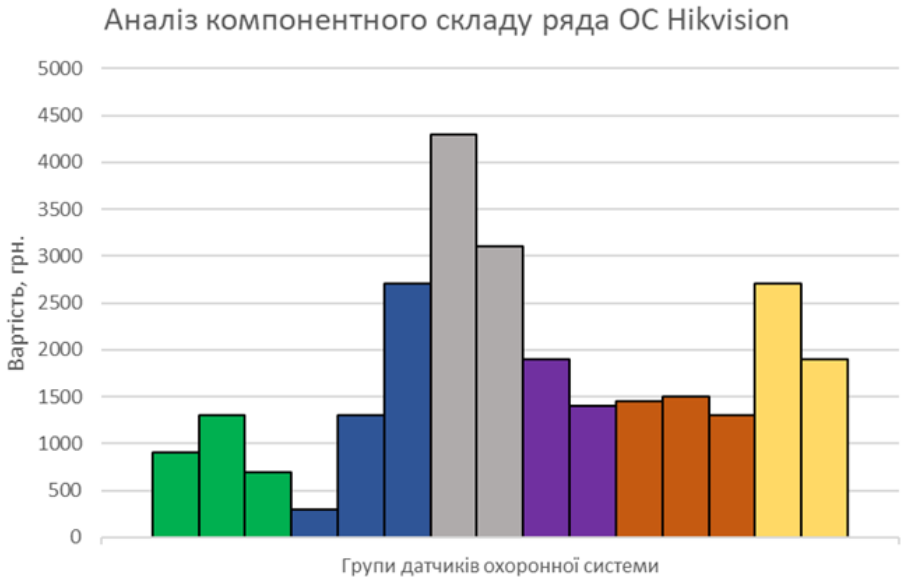


Рисунок 1.11 – Візуалізація вартості компонентів системи

Зелений – бездротові магнітні датчики

Синій – PIR-датчики

Сірий – оптичні сповіщувачі

Фіолетовий – ІЧ-датчики руху

Жовтий – сповіщувачі

Помаранчевий - решта датчиків екосистеми Hikvision, які представлені в лінійці в одній моделі.

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 рис.1.12 представлена візуалізація порівняння низки параметрів охоронних централей від бренду Ajax.

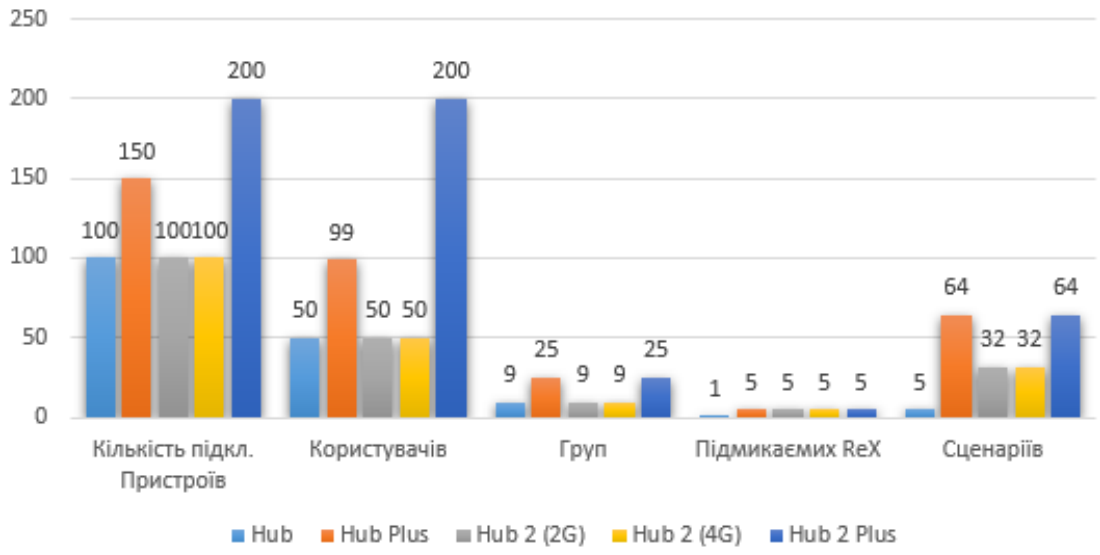


Рисунок 1.12 – Порівняння центрів керування в системі Ajax

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).

Деталізацію щодо компонентного складу та особливості використання екосистеми AJAX розгяленмо в наступному розділі роботи.

1.3 Розробка системи захисту підприємства на базі системи безпеки AJAX

1.3.1 Особливості використання системи безпеки AJAX

Як зазначалося раніше, система безпеки Ajax будується на основі інтеграції різноманітних рішень, кожне з яких виконує своє завдання. При цьому компанія постійно оновлює свої продукти, так і можливості їх взаємодії. А в рамках мультирелізу наприкінці 2019 року кількість пристроїв та функцій ще більше розширилася. Продукцію Ajax з урахуванням функцій можна розділити на кілька груп, вони представлені на рис.

Конкурентною перевагою та особливістю системи безпеки Ajax є використання власних протоколів зв'язку, таких як 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.

Рисунок 1.13 – Компонентний склад системи безпеки Ajax

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

Особливості Jeweller:

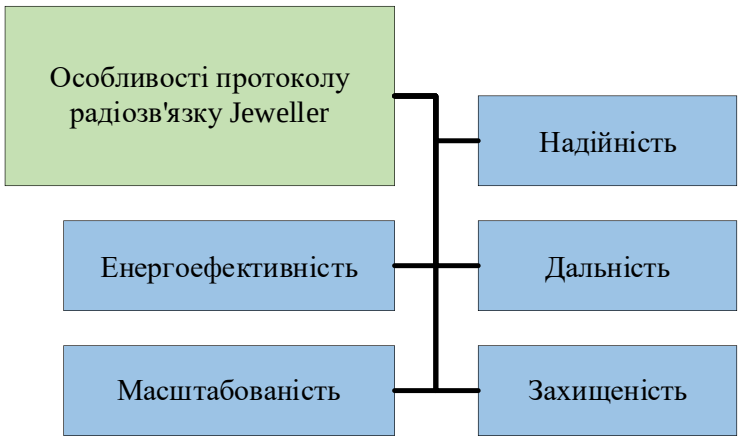


Рисунок 1.14 – Особливості протоколу радіозвязку Jeweller

Радіопротокол Jeweller дозволяє будувати як малі, так і великі системи безпеки з 200 пристроїв під управлінням однієї централі - хаба. Пікової дальності зв'язку між пристроями в 2000 метрів та площі покриття радіомережі до 12 км² достатньо для захисту квартир, приватних будинків, комерційної нерухомості та офісів.

Jeweller працює у оптимальному для охоронного обладнання частотному діапазоні 868,0–868,6 МГц або 868,7–869,2 МГц (залежить від регіону продажу).

Зв'язок між хабом та пристроями двосторонній, що дає системі ряд переваг. Датчики переходять у режим «під охороною» по команді хаба і не розряджають даремно батареї (для порівняння, у системах з одностороннім зв'язком датчики активні завжди). При високій якості зв'язку пристрою автоматично знижують потужність передавачів.

Завдяки вдосконаленій технології тимчасового розподілу каналів (на базі TDMA) кожен пристрій системи безпеки виходить на зв'язок у певний момент на дуже короткий проміжок часу. Решту часу радіомодуль спить, зберігаючи заряд акумуляторів. За синхронізацію механізмів системи відповідають кварцові генератори реального часу. Інтервал сеансів зв'язку регулюється у додатку та становить від 12 до 300 секунд. Від саботажу зв'язок Ajax захищають шифрування, частотний хоппінг та аутентифікація пристроїв. Безглуздо перехоплювати радіопередачу, використовувати кодграбер або намагатися

підлогою брелока зняти з охорони систему безпеки. Дані захищені блоковим шифруванням з плаваючим ключем.

Таблиця 1.3 – Технічні характеристики радіопротоколу Jeweller

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

Система безпеки Ajax дозволяє проводити тести перевірки працездатності підключених пристроїв.

Тести починаються не миттєво, але не більше ніж через 36 секунд при заданому за промовчанням періоді опитування пристроїв у налаштуваннях хаба (меню Jeweller). Тест дозволяє визначити рівень та стабільність сигналу в передбачуваному місці установки пристрою.

Для передачі графічних даних Hub 2 і MotionCam використовують радіопротокол Ajax Wings – високошвидкісний протокол передачі інформації, який був розроблений на основі Jeweller та успадкував його найкращі якості. При цьому Wings використовує виділену антену централі Hub 2 підвищення надійності каналу зв'язку.

Wings гарантує доставку фотографій навіть при нестабільному рівні сигналу та перебоях зв'язку завдяки вбудованим алгоритмам перевірки та дозавантаження пакетів.

Передача серій фотографій.

Використання виділеної антени.

Гарантована доставка даних.

Дальність зв'язку Wings – до 1700 метрів без перешкод. Wings доставляє фотографії навіть при нестабільному рівні сигналу та перебоях у зв'язку, завдяки вбудованим алгоритмам перевірки та дозавантаження пакетів. Оператор охоронної компанії та всі користувачі бачать перший знімок із місця події вже через 9 секунд після тривоги.

1.3.2 Впровадження системи захисту Ajax на прикладі офісу IT-компанії

Вихідні дані:

Приміщення розташоване на 1 поверсі будівлі. Необхідно організувати захист кабінетів, в які можливе проникнення з вулиці. На вікнах встановлені ґрати. Постановку та зняття з охорони виконує: офіс-менеджер, зам. керівника, керівник. Кабінет керівника має ставитися під охорону окремо.

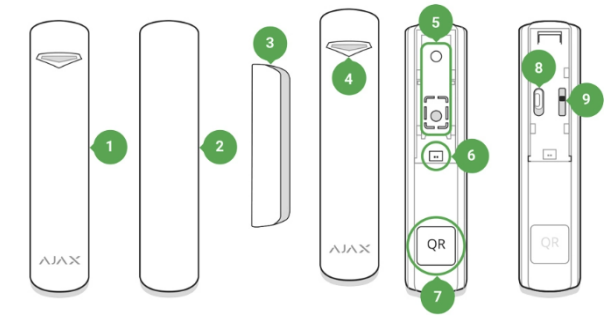
Опис обладнання.

Для побудови системи безпеки в першу чергу нам необхідно встановити датчики відкриття вікон та вхідних дверей – Ajax DoorProtect

Бездротовий датчик відкриття вікон та дверей Ajax DoorProtect – це датчик відкриття внутрішньої установки. Він виявляє проникнення та повідомляє про відкриття дверей або вікна. Монтується на всі види та типи об'єктів. Зовнішній вигляд та функціональні елементи представлені на рис.

Детектор відкриття дверей та вікон на сигналізацію Ajax DoorProtect призначений для виявлення несанкціонованих відкриттів, коли приміщення під охороною. Датчик відкриття спрацьовує за допомогою двох елементів - блоку з герконом та магніту. Принцип роботи бездротового детектора відкриття

виходить з властивостях геркона - деталі, що стає провідником сигналу під впливом магнітного поля.



.

Рисунок 1.15 - Зовнішній вигляд та функціональні елементи бездротового датчика відкриття вікон та дверей Ajax DoorProtect

Для виявлення руху всередині приміщення та контролю цілісності вікон використовуватиметься комбінований датчик руху Ajax CombiProtect.

Бездротовий датчик CombiProtect поєднує функції двох детекторів - розбиття і руху. Пристрій фіксує факт руху людини в приміщенні, що охороняється, на відстані до 12 метрів і визначає розбиття скла на відстані до 9 метрів.

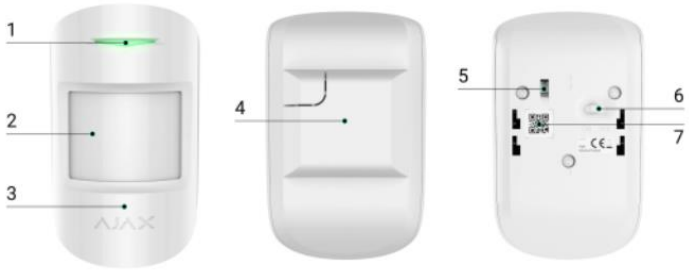


Рисунок 1.16 - Зовнішній вигляд та функціональні елементи бездротового датчика відкриття вікон та дверей Ajax CombiProtect

де:

1. Світловий індикатор.
2. Лінза датчика руху.
3. Отвір мікрофона.

4. Панель кріплення SmartBracket (перфорована частина необхідна для спрацювання тампера при спробі відірвати датчик від поверхні).

5. Кнопка тампера.

6. Вимикач пристрою.

7. QR код.

Принцип роботи бездротового датчика руху та розбиття скла базується на визначенні інфрачервоного випромінювання від живих істот. Коли охоронний детектор фіксує таке випромінювання, він аналізує вагу об'єкта, і якщо він перевищує 20 кг - надсилає тривожний сигнал на центральний блок сигналізації охорони. Алгоритм обробки отриманого сигналу забезпечує ретельну перевірку об'єкта за масою та наявністю руху, що знижує ризик помилкових спрацьовувань від тварин.

За допомогою такого принципу роботи датчик руху і розбиття скла Ajax CombiProtect спрацьовує тільки при визначенні руху людини. Детектор не реагує на переміщення неживих предметів. Якщо в приміщенні впаде одяг з вішалки, або протяг відкриє двері, датчик не активується.

Датчик розбиття скла та руху виявляє та реєструє специфічні низькочастотні та високочастотні звуки від розбиття скла, завдяки спеціальному мікрофону. Якщо в приміщенні, що охороняється, розбивають скляне полотно, детектор вловлює ці звуки і відправляє сигнал тривоги на центральний блок сигналізації по радіоканалу. Охоронний датчик реагує виключно на звук розбитого скла, ігноруючи інші гучні звуки, використовуючи унікальний багатоступінчастий аналіз.

Бездротовий датчик працює на основі бездротової системи радіозв'язку, яка використовує захист від підлоги та шифрування повідомлень. Таким чином, сигналізація захищена від спроб проникнення на територію, що охороняється. Бездротовий комбінований датчик також має високонадійну систему зв'язку, яка дозволяє йому працювати в межах декількох поверхів будівлі або на відстані до 2000 м від центрального блоку сигналізації за відсутності перешкод.

Для встановлення та зняття з охорони застосовується Ajax Keypad.

Коли користувач вводить код доступу на сенсорній клавіатурі, охоронний прилад відправляє сигнал на контрольну панель через радіозв'язок. Панель керування зчитує запит, після чого вмикає або вимикає режим охорони. Бездротова клавіатура KeyPad працює за допомогою системи радіозв'язку Jeweller. Радіопротокол використовує систему шифрування сигналу та захист від підлоги, що робить охоронну систему захищеною від спроб злому або крадіжки. Особливість охоронної клавіатури для керування – блокування пристрою при введенні неправильного коду. Якщо в разі вторгнення код введено неправильно, клавіатура буде заблокована на той час, який власник спочатку фіксує в налаштуваннях. При цьому користувачеві прийде повідомлення про те, що хтось намагається розгадати код. У разі блокування лише користувач з правами адміністратора може розблокувати клавіатуру раніше заданого часу. З Ajax KeyPad є можливість встановлення режиму охорони зон. Тобто, лише певна частина будівлі буде під сигналізацією. Можна встановлювати як загальний пароль всім користувачів системи, і індивідуальний кожному за. За допомогою другого варіанта буде доступний контроль співробітника: коли він прийшов чи пішов. Є варіант настроїти систему так, щоб для кожного користувача був доступ лише до певних зон приміщення. Наявність режиму тривоги на бездротовій клавіатурі дає змогу негайно реагувати на тривогу (пожежну, проникнення) натисканням кнопки.

Для звукового сповіщення тривог використовуватиметься Ajax HomeSiren. HomeSiren – бездротова домашня сирена з потужністю до 105 дБ. Використовується всередині приміщень, швидко встановлюється та настроюється, оснащена світлодіодом (плюс дозволяє підключити зовнішній), працює до 5 років від батареї. HomeSiren працює у складі системи безпеки Ajax, підключаючись по захищеному протоколу Jeweller до хабу. Дальність зв'язку — до 2000 метрів за відсутності перешкод.

Сирена на сигналізацію підвищує ефективність системи безпеки і є найшвидшим засобом реагування на проникнення в приміщення. Ajax Home Siren працює тільки з хабами Ajax та ретрансляторами. Рівень гучності звуку

бездротової сирени налаштовується під користувача, 81-105 дБ на відстані 1 м. Час звучання тривоги також можна налаштувати в діапазоні 3 - 180 с. Доставка сигналу тривоги відбувається менше ніж за секунду, а термін роботи сирени – до 5 років від попередньо встановленої батареї.

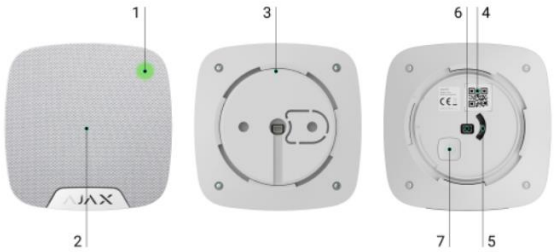


Рисунок 1.17 - Зовнішній вигляд та функціональні елементи бездротової домашньої сирени Ajax HomeSiren

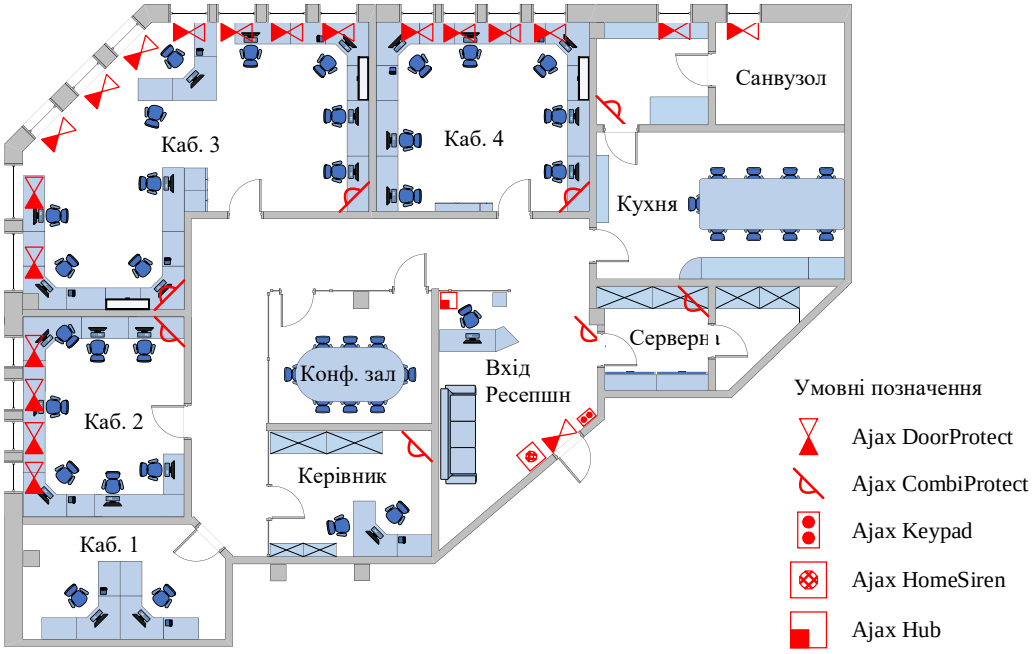


Рисунок 1.18 - Розміщення обладнання системи безпеки Ajax на прикладі офісу IT-компанії

Знаючи технічні принципи роботи даних бездротових датчиків можна перейти до конфігурування системи. У конфігурації нашої системи датчик Ajax DoorProtect буде встановлюватися у верхню частину вікна, щоб унеможливити встановлення на охорону з відкритим на провітрювання вікном. Для вхідної групи у датчиків буде встановлено затримку в 30 секунд, яка дозволить протягом цього часу зняти офіс з охорони. При цьому Ajax HomeSiren відраховуватиме

звуковим сигналом час для зняття з охорони. Клавіатура дозволяє поставити на охорону кілька охоронних груп незалежно один від одного. Також не буде зайвим встановити на смартфон керівника мобільний додаток для контролю постановки/зняття офісу з охорони, на нього також надходитимуть push-сповіщення про тривоги та несправності.

Специфікація обладнання, яке застосовувалося для встановлення системи безпеки на об'єкті, наведено в табл. 1.4.

Таблиця 1.4 - Специфікація комплекту обладнання Ajax під час встановлення в приміщеннях офісу IT-компанії

№	Найменування	Кількість	Вартість, грн.	Ціна, грн.
1	Ajax DoorProtect	21	999,00	20979,00
2	Ajax CombiProtect	7	2099,00	14693,00
3	Ajax Keypad	1	2099,00	2099,00
4	Ajax HomeSiren	1	1499,00	1499,00
5	Ajax Hub	1	4799,00	4799,00

Загальна вартість обладнання (травень 2022 р.) складає 44069,00 грн.

1.3.3 Впровадження системи захисту Ajax на прикладі приватного будинку

Завдання – оснастити заміський будинок системою охоронно-пожежної сигналізації. Кімнати та периметр будинку мають бути у незалежних один від одного охоронних групах. На прохання замовника необхідно встановити датчики диму та затоплення до деяких кімнат будинку. Також слід прописати сценарії роботи деяких охоронних датчиків.

Вибір обладнання для вирішення задачі.

Основою нашої системи буде Ajax Hub 2 Plus. Його технічні характеристики ідеально підходять для вирішення поставлених завдань. Також непоганим бонусом буде підтримка фотоверифікації тривог.

Почнемо побудову охоронної системи з периметру. Нам необхідно закрити всі можливі підступи до будинку, тому що периметр – це наш перший рубіж безпеки, саме він охоронятиме нас у нічний час. Розглянемо додаткові датчики.

Вуличний двонаправлений охоронний датчик руху штора Ajax DualCurtain Outdoor призначений для виявлення та запобігання проникненню на територію під охороною. Детектор ігнорує тварин до 80 см та птахів. Погодні фактори також не викликають помилкових спрацьовувань. Пристрій захищений від несанкціонованого впливу з боку зловмисників - покриття лаком, демонтажу, завішування, захищений від пилу та бризок, працює за температури повітря нижче 0°C, дальність роботи регулюється до 30 метрів.

Вуличний датчик руху для сигналізації Ajax DualCurtain Outdoor визначає рух людини за допомогою двох вбудованих незалежних ІЧ-сенсорів, які фіксують інфрачервоне випромінювання живих істот. Дані, які отримує пристрій, перевіряє двофакторний алгоритм ELSA. Він визначає подібності та спектральні образи між сигналами двох сенсорів, що допомагає уникнути спрацьовування помилкових тривог. Дальність роботи датчика регулюється в діапазоні до 30 метрів по 15 метрів в кожну сторону.

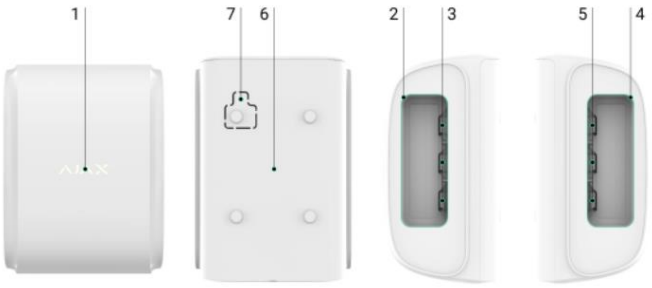


Рисунок 1.19 - Зовнішній вигляд та функціональні елементи вуличного двонаправленого охоронного датчика руху типу "штора" Ajax DualCurtain Outdoor

де:

– логотип Ajax зі світлодіодним індикатором;

– ліва лінза датчика;

– сенсори маскування лівої сторони датчика;

– права лінза датчика;

– сенсори маскування правої сторони датчика;

– кріпильна панель SmartBracket.

DualCurtain Outdoor стійкий до перешкод у роботі. Завдяки тамперу на корпусі пристрою зняти з кріплення його не вийде - спрацює тривожний сигнал. Оптичні системи детектора обладнані сенсорами маскування, які реагують на перешкоди, фарбування корпусу та завішування приладу.

DualCurtain Outdoor оптимізоване енергоспоживання, що дозволяє пристрою працювати до чотирьох років без заміни батарей. Бездротовий датчик заздалегідь попередить користувачів системи безпеки про необхідність заміни елементів живлення.

Другим датчиком охорони периметра, що використовується, буде - бездротовий вуличний детектор руху Ajax MotionProtect Outdoor

Принцип роботи детектора руху Ajax MotionProtect Outdoor заснований на визначенні руху в зоні, що охороняється, за допомогою зчитування ІЧ-випромінювання від об'єкта. Усі живі істоти є джерелами інфрачервоного випромінювання, зокрема і людина. Датчик отримує інформацію за допомогою двох незалежних інфрачервоних сенсорів, що передають дані на центральну панель сигналізації через захищений радіопротокол Jeweller.

Коли система перебуває під охороною, датчик постійно зчитує сигнали із двох PIR-сенсорів. При виявленні руху MotionProtect Outdoor миттєво передає тривогу на хаб і сигналізує блиманням зеленого світлодіода. Тривога на хаб буде надіслана лише при детектуванні двома тепловими сенсорами датчика ідентичних сигналів про рух.

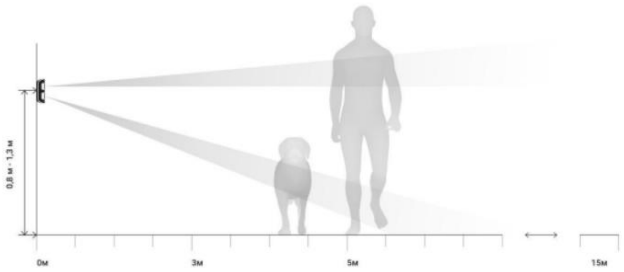


Рисунок 1.20 - Принцип роботи сенсорів MotionProtect Outdoor

MotionProtect Outdoor детектує такі типи маскування:

– перешкода перед обома лінзами (перед датчиком на відстані до 20 см розташований об'єкт, розмірами, який можна порівняти з висотою корпусу датчика);

– перешкода перед будь-якою з лінз (перед однією з лінз розміщено об'єкт на відстані до 10 см);

– зафарбовування або заклеювання непрозорим матеріалом будь-якої з лінз;

– заклеювання фронтальної частини датчика непрозорим матеріалом;

– нанесення фарби або зафарбовування пензлем фронтальної частини MotionProtect Outdoor.

У разі виявлення одного або кількох типів маскування, датчик генерує тривогу про маскування, а зелений світлодіод датчика спалахує на 1 секунду.

Розглянемо внутрішні датчики Ajax.

Найчастіше у господарів приватних будинків усередині будинку є якась домашня тварина, кішка або собака. Враховуючи цей параметр, датчики всередині будинку будуть з «імунітетом» до тварин, тому при інсталяції датчиків руху необхідно провести тести зон виявлення та відрегулювати чутливість кожного датчика. У конфігурації системи будуть використовуватися два види датчиків руху.

Ajax MotionCam – бездротовий датчик руху з фотокамерою для верифікації тривог. Слідом за повідомленням попередження, бездротовий датчик надішле анімовану серію фотографій для оцінки ситуації та підтвердження реакції.

MotionCam – бездротовий датчик руху з фотопідтвердженням тривог для використання всередині приміщення. Датчик працює до 4 років від комплектних батарей, визначає рух на відстані до 12 метрів та вміє ігнорувати тварин, розпізнаючи людину з першого кроку. MotionCam працює у складі системи безпеки Ajax, зв'язуючись з хабом за двома захищеними радіопротоколами. Для передачі тривог та подій датчик використовує Jeweller, а Wings – для передачі фотографій. Дальність зв'язку з хабом за відсутності перешкод – до 1700 метрів.

Бездротовий детектор руху з радіочастотним скануванням перешкод сигналу Ajax MotionProtect Plus використовується для виявлення руху людини на території, що охороняється. Датчик руху визначає появу людини у приміщенні з перших секунд, але ігнорує протяги, рухи домашніх вихованців вагою до 20 кілограм, роботу кондиціонера. Радіочастотне сканування фільтрує перешкоди, які створює теплове випромінювання у комплексі з рухом штор та засвітами. Чутливість детектора руху регулюється користувачем індивідуально.

Бездротовий датчик руху Ajax MotionProtect Plus оснащений системою радіозв'язку, яка використовує захист даних від підробки та шифрування переданих повідомлень. Це забезпечує захищеність сигналізації від спроб злому зловмисниками. Крім того, бездротовий детектор має високонадійну систему зв'язку, яка дозволяє йому працювати в межах декількох поверхів будівлі або на відстані до 1200 м-коду до центрального блоку сигналізації за умови відсутності перешкод.

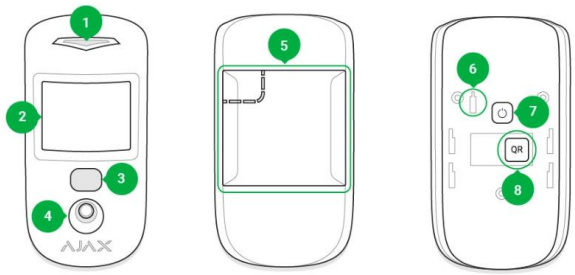


Рисунок 1.21 - Зовнішній вигляд та функціональні елементи бездротового датчика руху з фотокамерою Ajax MotionCam

Також у системі будуть використовуватися пожежні датчики та датчики затоплення. FireProtect Plus - це бездротовий датчик виявлення спалахів у приміщеннях, оснащений сиреною. Пристрій працює до чотирьох років від попередньо встановленої батареї. FireProtect Plus визначає наявність диму в приміщенні або різке зростання температури, реагує на небезпечний рівень чадного газу.

Датчик диму FireProtect Plus працює як частиною охоронної сигналізації із підключенням до контрольної панелі системи безпеки hub, так і автономно. При

автономному використанні, у разі виявлення пожежі, датчик повідомить про тривогу звуковим сигналом та світінням логотипу.

Бездротовий пожежний датчик FireProtect Plus підключається до системи безпеки Ajax захищеного радіопротоколу Jeweller і може працювати на відстані до 1300 м від hub за відсутності перешкод.

Датчик виявляє дим за допомогою оптопари з інфрачервоного випромінювача та фотоприймача, розміщених у димарі. При попаданні диму в камеру фотоприймач виявляє його за спотворенням інфрачервоного променя.

Оскільки деякі матеріали горять без виділення диму, датчик також фіксує зміни температури. Коли функція увімкнена, тривога спрацює, якщо температура приміщення підніметься до 60 ° C і при підвищенні температури на 30 ° за 30 хвилин (навіть якщо вона нижче 60 ° C).

При виявленні пожежі (диму) датчик увімкне зумер - пожежну сирену чутно здалеку, а логотип загориться червоним. При підключенні до охоронної системи датчик також надішле сигнал тривоги на хаб – користувач та охоронна компанія отримають відповідні повідомлення.

При встановленні системи безпеки Ajax, потрібно забезпечити хорошу чутність сирен пожежних датчиків, бажано щоб було видно світлодіодну індикацію пристроїв.

Рекомендується встановлювати димовий сповіщувач FireProtect Plus на стелю. При розміщенні на стіні датчики визначатимуть задимлення та стрибки температури менш ефективно.

Рисунок 1.22 - Зовнішній вигляд та Ajax FireProtect Plus

Не рекомендується встановлювати протипожежний сповіщувач:

– на вулиці та в місцях швидкої циркуляції повітря (біля стельового вентилятора, кондиціонера, витяжки та вікон);

– поблизу металевих предметів та дзеркал – викликають згасання або екранування радіосигналу;

– у приміщеннях з вологістю або температурою, що виходить за межі норми (від 0°C до +65°C);

– у місцях, де утруднений доступ до датчика;

– у безпосередній близькості до кухонних електроприладів.

Бездротовий датчик протікання води Ajax LeaksProtect

Ajax - повноцінна система безпеки, яка може захистити простір, що охороняється не тільки від вторгнень і пожеж, але і від затоплення внаслідок несправності сантехніки або прориву труби. Для встановлення антипотопної системи знадобляться: бездротовий датчик протікання води LeaksProtect, сумісний електроклапан, а також реле WallSwitch або Relay.

За допомогою реле можна налаштувати автоматичне переривання подачі води по тривозі датчика протікання. Користувач також може перекривати воду через програму вручну.

Автономні датчики протікання води можуть виявити затоплення навіть при попаданні на корпус мінімальної кількості води. Система безпеки піднімає тривогу, коли рідина потрапляє на один із чотирьох контактів. Повідомлення отримують всі користувачі системи та охоронна компанія, якщо до неї підключено сигналізацію. А керуючи електроклапаном через реле система Ajax може автоматично перекрити воду до прибуття екстреної служби.

Рисунок 1.23 - Зовнішній вигляд та функціональні елементи бездротового датчика протікання LeaksProtect

Особливості датчика потопу Ajax LeaksProtect:

– До 5 років роботи батареї.

– Захист корпусу від пилу та вологи.

– Установка не потребує використання інструментів.

– Зв'язок з hub на відстані до 1300 м.

– Надсилання сигналу про висихання води після тривоги.

– Живлення бездротового датчика протікання.

– Бездротові датчики протікання води Ajax LeaksProtect працюють на встановлених батареях до 5 років без заміни.

Дистанційне керування електроживленням системи безпеки здійснюється за допомогою силового реле Ajax WallSwitch. Ajax WallSwitch підключається до мережі 110 В/230 і призначене для замикання і розмикання кола по команді. Реле витримує навантаження до 3 кВт, якого вистачає для підключення приладу, що навіть вимагає великої кількості електроживлення. Таку особливість приладу можна дізнатися через Ajax, де користувач може перевірити енергоспоживання завдяки WallSwitch. Ajax WallSwitch захищає прилади системи безпеки від стрибків напруги та перевищення сили струму.

Прилади безпеки Ajax WallSwitch використовують бездротовий зв'язок та захищають від перегорання пристрою безпеки.

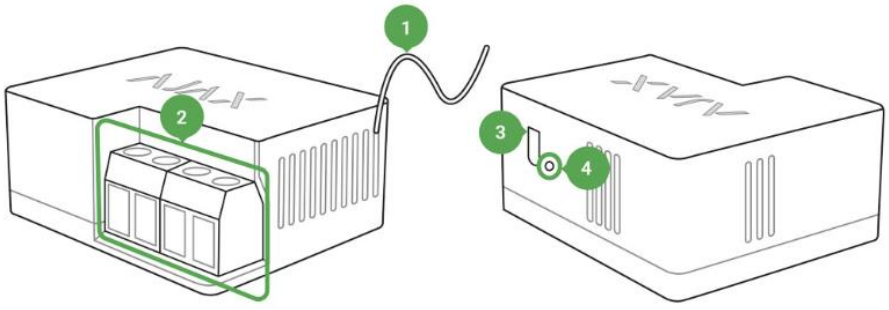


Рисунок 1.24 - Зовнішній вигляд та функціональні елементи реле Ajax WallSwitch

При формуванні ТЗ було визначено, що периметр приватного будинку і кімнати в будинку повинні ставитися під охорону окремими групами. Це можна

реалізувати за допомогою клавіатури (Ajax Keypad) або за допомогою брелока Ajax SpaceControl. Управління нічним режимом/повною охороною здійснюватиметься за допомогою брелока, встановлення окремих кімнат на охорону виконуватиметься за допомогою телефону з мобільним додатком за потреби.

У кожному санвузлі будинку встановлено датчик затоплення Ajax LeaksProtect та силове реле Ajax WallSwitch із сумісним клапаном перекриття води. У налаштуваннях сценаріїв пропишемо, що при спрацюванні певного датчика затоплення реле його перекриє свій клапан. Також така зв'язка встановлена в бойлерній, де обладнано введення води в будинок.

MotionCam датчики руху з фотоверифікацією тривоги – встановлені на входах до будинку, щоб точно розуміти причину спрацювання. Встановлення таких датчиків у всі кімнати будинку можливе, але не доцільне через ціну датчика.

Ajax MotionProtect Plus – використовується для того, щоб виключити помилкові спрацювання при незачинених вікнах у будинку. Оповіщення про тривоги приходитиме на телефон замовника і дублюватиметься Ajax StreetSiren за місцем. На рис. 1.25 представлено розміщення обладнання на плані будинку.

Таблиця 1.5 - Специфікація комплекту обладнання Ajax під час встановлення в приміщеннях приватного будинку

№	Найменування	Кількість	Вартість, грн.	Ціна, грн.
1	Ajax DoorProtect	4	999,00	3996,00
2	Ajax MotionCam	2	3409,00	6818,00
3	Ajax MotionProtect Plus	8	2099,00	16792,00
4	Ajax LeaksProtect	5	1199,00	5995,00
5	Ajax WallSwitch	6	1049,00	6294,00
6	Ajax FireProtect Plus	2	2699,00	5398,00
7	Ajax MotionProtect Outdoor	3	4149,00	12447,00
8	Ajax DualCurtain Outdoor	3	5219,00	15657,00

9	Ajax StreetSiren	1	2999,00	2999,00
10	Ajax Hub 2 Plus	1	9649,00	9649,00
11	Ajax Rex 2	1	4299,00	4299,00

Загальна вартість обладнання (травень 2022 р.) складає 90344,00 грн.

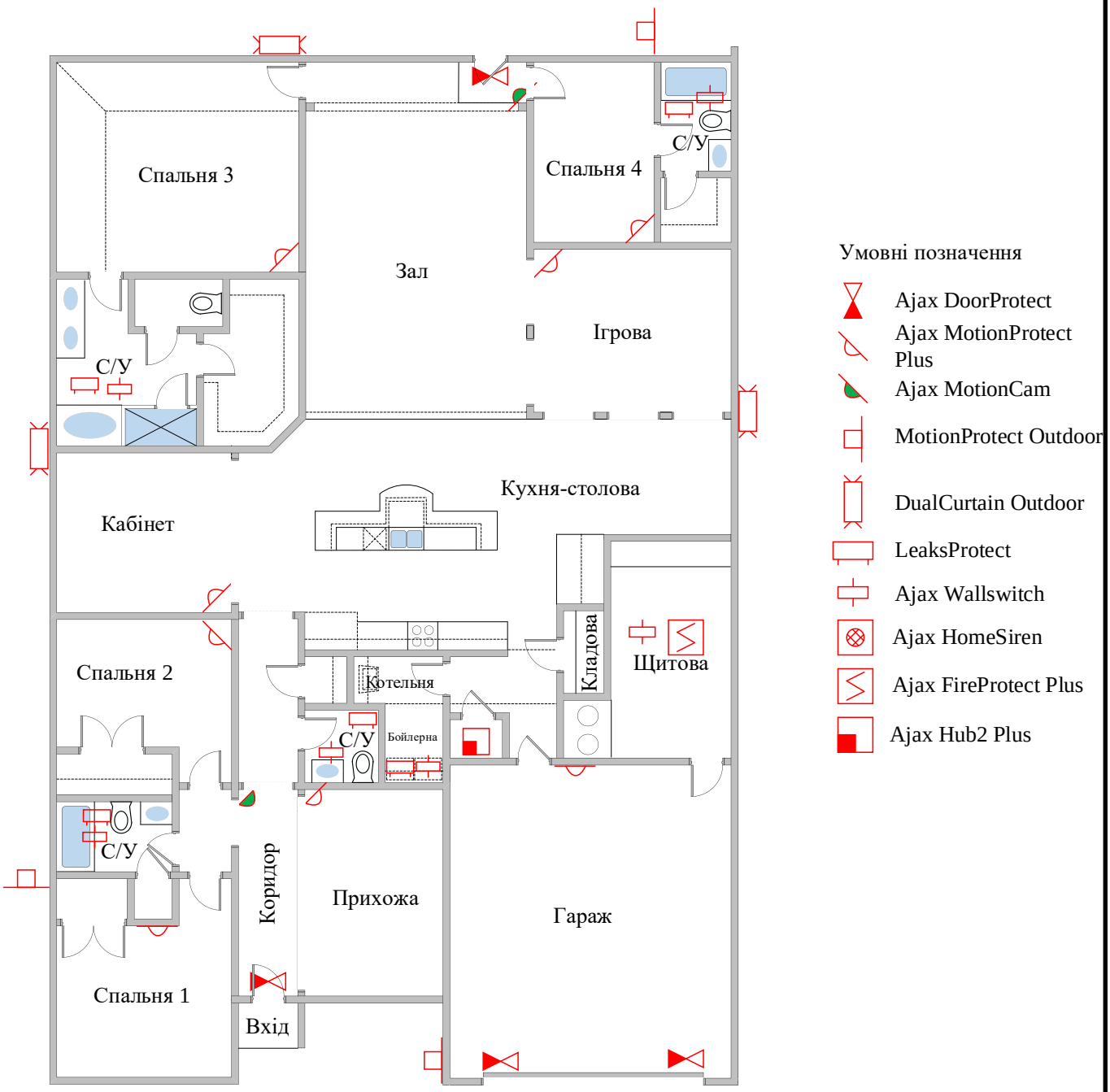


Рисунок 1.25 - Розміщення обладнання системи безпеки Ajax на прикладі приватного будинку

На рис. 1.26 представлено порівняння основного устаткування СБ – хабів охоронної системи з урахуванням Ajax. Для малих об'єктів достатньо застосування першої версії централі - Hub. Вибір інших версій централі залежить від завдань та масштабу системи безпеки об'єктів.

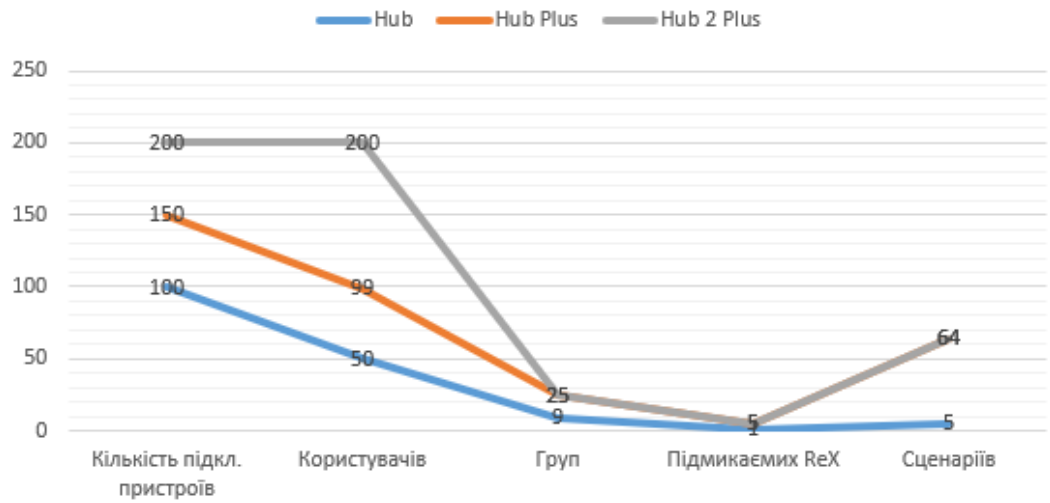


Рисунок 1.26 - Сравнение централей системы безопасности Ajax по 5-ти базовым критериям

2 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою даних розрахунків є обчислення вартості виконання науково-дослідного проєкту на тему «Розробка системи захисту підприємства на основі обладнання AJAX». Система захисту будь-якого об'єкта – це багатогранна та комбінована структура, яка має цілу низку складових у системі загальної безпеки. Так, залежно від типу об'єкта, виду та масштабів діяльності підприємства можуть застосовуватися організаційна, технічна, криптографічна, мережева, кадрова та інші види безпеки. У даному разі застосування технічних засобів охорони (ТЗО) є частим явищем практично всіх типах об'єктів.

Даний вид проекту відноситься до науково-дослідницької розробки. Оцінка якості розробленого проекту включає визначення трудомісткості і вартості його створення.

Розрахунок трудомісткості НДР здійснений в наступній послідовності:

1) Складений перелік всіх етапів і видів робіт, які необхідно виконати в ході даної НДР. Після узгодження з керівником проекту допущено виключення, доповнення, об'єднання окремих етапів і видів робіт;

2) По кожному виду робіт визначений кваліфікаційний рівень виконавців. Перелік етапів і робіт, що виконуються при проведенні НДР, приведений в таблиці 2.1.

Таблиця 2.1 - Розподіл робіт по етапах і видах виконавців

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

	4. Розробка плану проведення досліджень для подальшої розробки.	
Теоретичні і експериментальні дослідження	1.1 Концептуальні питання забезпечення безпеки компанії 1.2 Дослідження напрямку безпроводових систем охорони з позиції охоронно-тривожної сигналізації 1.3 Розробка системи захисту підприємства на базі системи безпеки AJAX	Дипломник керівник консультанти
Узагальнення і оцінка результатів досліджень	1. Узагальнення результатів 2. Оцінка повноти вирішення поставлених завдань. 3.Складання і оформлення звіту. Розгляд результатів проведеною НДР і прийняття результатів в цілому.	Дипломник керівник консультанти

Оцінка тривалості виконання робіт розраховується на основі вірогідних оцінок робіт, що задаються виконавцями.

Таблиця 2.2 - Очікувана трудомісткість робіт

Вигляд роботи	Очікуваний час виконання (дні)
1. Складання і затвердження ТЗ для НДР «Розробка системи захисту підприємства на основі обладнання AJAX».	1
2. Збір і вивчення науково – технічної літератури, технічної документації і інших матеріалів.	3
3. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка.	3
4. Розробка плану проведення досліджень для подальшої розробки.	2
5. Технологічний розділ 5.1 Концептуальні питання забезпечення безпеки компанії 5.2 Дослідження напрямку безпроводових систем охорони з позиції охоронно-тривожної сигналізації 5.3 Розробка системи захисту підприємства на базі системи безпеки AJAX	12
Всього:	21

Розрахунок собівартості і ціни виконання НДР. Виходячи з особливостей створення науково – технічної продукції і її залежності від

інтелектуальної праці, розрахунок собівартості і ціни виконання НДР включає наступні статті витрат: витрати на матеріали, основна і додаткова заробітна плата, відрахування до єдиного соціального фонду страхування, витрати на роботи, що виконуються сторонніми організаціями, і деякі інші.

1) Витрати на матеріали складають 170 грн.

2) До витрат «Основна заробітна плата» відносяться оплата праці виконавців, безпосередньо притягнених до її виконання. Розмір основної зарплати встановлюється виходячи з чисельності різних категорій виконавців, трудомісткості, що витрачається ними на виконання різних видів робіт, а також їх середньої заробітної плати (ставки) за один робочий день. Відповідно до статті 8 «Закону про Державний бюджет України на 2021» встановлено мінімальну заробітну плату у місячному розмірі з з 1 січня 2022 року - 6500 гривень; мінімальну погодинну тарифну ставку – 39,26 грн.

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

$$Зден= п.т.с. * 8;$$

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

8 – тривалість робочого дня,год.

Зден дипломника = 39.26*8 = 314,08 грн.

Зден керівника = 65.00 *8 = 520 грн.

Зден консультантів = 62.00 *8 = 496 грн.

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

Таблиця 2.3 - Витрати на основну заробітну плату

Виконавець	Погодинна тарифна ставка, грн	Денна ставка, грн	Трудомісткість робочих днів	Сума основної зарплати, грн
Дипломник	39,26	314,08	22	6909,76
Керівник	65,00	520	1	520
Консультант по економічній	62,00	496	0,25	124

частині				
Консультант по охороні праці	62,00	496	0,25	124
Нормоконтроль	62,00	496	0,25	124
Всього (Зо)				7801,76

3) Витрати на додаткову заробітну плату визначаються у відсотках від основної. У наукових закладах додаткова заробітна плата складає 10-12% від основної заробітної плати.

$$Зд=11\%Зо;$$

$$Зд= \quad 7801,76*0,11 = 858,19 \text{ грн}$$

4) До складу собівартості НДР включаються податки, збори і інші обов'язкові платежі, встановлені системою оподаткування що діє. Відрахування до єдиного соціального внеску складає:

$$Зєсв=0,22*(Зо+Зд);$$

$$Зєсв=0,22*(7801,76+858,19) = 1905,19 \text{ грн.}$$

5) До накладних витрат відносять витрати на управління і господарське обслуговування, що відноситься до всіх виконуваних НДР.. У наукових закладах накладні витрати складають 40 -120% від основної і додаткової заробітної плати.

$$Рнакл= (З0+Зд)*0,5;$$

$$Рнакл= (7801,76+858,19)* 0,5 = 4329,97 \text{ грн.}$$

На підставі отриманих даних по окремих статтях витрат складена калькуляція планової собівартості в цілому НДР за формою, приведеною в таблиці 2.4.

Таблиця 2.4 - Калькуляція планової собівартості

Статті витрат		Сума, грн.
1.	Матеріали	170,00
2.	Основна заробітна плата	7801,76
3.	Додаткова заробітна плата	858,19
4.	Відрахування до єдиного соціального внеску	1905,19
5.	Накладні витрати	4329,97
Планова собівартість (Спл)		15065,11

Плановий прибуток визначений по формулі:

Ппл = 0,1*Спл = 0,1*15065,11= 1506,51 грн

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

Договірна ціна визначається по формулі

Цнір = Спл + Ппл = 15065,11+1506,51 = 16571, 62 грн.

Ціну реалізації встановлюємо з урахуванням ПДВ

ПДВ = 0,2*Цнір= 0,2*16571, 62 = 3314,32 грн.

Звідси ціна реалізації становить:

Цр = Цнір + ПДВ Цр = 16571, 62+3314,32 = 19885,94 грн.

3 ОХОРОНА ПРАЦІ

Життєвий цикл побудови систем безпеки - відеоспостереження, сигналізації, охорони периметра або СКС для їх взаємозв'язку містить важливий етап, який називається "побудова системи безпеки". Саме на цьому етапі триває реалізація проекту. При цьому при виконанні монтажних робіт працівник може мати справу з низкою небезпечних та шкідливих виробничих факторів. Так, наприклад, монтажник слаботочних систем безпеки може працювати різних кліматичних умовах, тобто. бути схильний до впливу високих і низьких температур, різної вологості і т.д. Для підготовки та прокладання трас систем безпеки потрібне проведення робіт з електроінструментом (перфоратори, шуруповерти, болгарки), на різних висотах (із застосуванням сходів та настилів), часто - проводячи підключення до діючих електроустановок. Інженер займається розлученням обладнання, повинен вміти дублювати роботу своїх підлеглих, а отже – дотримуватись усіх правил безпеки.

Розглянемо детально загальні вимоги щодо охорони праці до інженерного складу команій, які займаються монтажем та пусконалагоджувальними роботами в галузі систем відеоспостереження.

Отже, до роботи в якості інженера (наладчика) засобів зв'язку і відеоспостереження допускаються особи, які досягли 18 років, придатні за станом здоров'я, що пройшли вступний інструктаж і первинний інструктаж на робочому місці, навчання і перевірку знань вимог охорони праці в установленому порядку.

Під час роботи працівник проходить:

1. Перевірку знань вимог охорони праці 1 раз в рік
2. Перевірку знань з електробезпеки для неелектротехнічного персоналу в обсязі 3 групи по електробезпеці - щорічно;
3. Періодичний медичний огляд.

Працівникам необхідно:

- дотримуватися правил внутрішнього трудового розпорядку, режими праці та відпочинку, встановлені в організації;
- дотримуватися вимог пожежної та електробезпеки;
- виконувати вимоги охорони праці при використанні інструменту;
- дбайливо ставиться до отриманим коштам індивідуального захисту.

Під час проведення робіт на об'єктах працівникам необхідно

1. Знати шляхи евакуації при аваріях або пожежі, місця розміщення первинних засобів пожежогасіння, вміти їх застосовувати;
2. Знати місце розташування засобів надання першої (долікарської) допомоги, вміти надавати першу (долікарську) допомогу потерпілим при нещасному випадку;
3. Знати і дотримуватися правил особистої гігієни.

Розглянемо вимоги щодо охорони праці перед початком роботи

Працівники зобов'язані стежити за станом свого робочого одягу, взуття та інших засобів індивідуального захисту. Вони повинні бути справні, надіті без звисаючих частин, застебнуті на всі кріплення, відповідати кліматичним умовам в день роботи. До початку робіт необхідно оглянути робочі місця, перевірити їх підготовленість до роботи, наявність достатнього освітлення, евакуаційних шляхів, відсутність захаращеності. Підготувати необхідний інструмент, пристосування, матеріали та засоби (тару) для їх перенесення.

Перед початком робіт на висоті слід оглянути використовувані майданчики, драбини, настили і інші допоміжні засоби підмощування, перевірити їх справність. Переносні засоби повинні мати непрострочену дату періодичних випробувань, неслизькі підстави і допуск до експлуатації.

Розглянемо деякі вимоги щодо охорони праці під час роботи на об’єкті.

В ході робіт необхідно виконувати вимоги інструкцій за професіями та видами робіт, в тому числі з охорони праці, пожежної та електробезпеки.

1. При роботах на висоті слід керуватися інструкцією з охорони праці при виконанні робіт на висоті, виконувати відповідні вимоги, в тому числі:

- дотримуватися вимог дій на висотних майданчиках (відступи від країв майданчиків, застосування запобіжних поясів, інформування розташованих нижче працівників про небезпеки і небезпечних зонах, огородження небезпечних зон і т.д.);

- дотримуватися вимог роботи з переносних драбин (стійке розташування підстави, кут нахилу сходів, максимальна висота і умови роботи з драбин, підняття вантажу, місця використання цих коштів і т.д.).

Рис.3.1 – Розсувна драбина

2. При виявленні в ході робіт будь-яких невідповідностей, недоліків і небезпек, що виходять за межі завдань і компетенції працівника, необхідно звернутися до відповідних організацій або до свого безпосереднього керівника.

3. Забороняється виконувати роботи в стані алкогольного, наркотичного, токсичного сп'яніння.

4. Забороняється передоручати або залучати до своєї роботи інших працівників без дозволу безпосереднього керівника.

5. Електромонтажні роботи на висоті необхідно проводити з риштувань з настилами шириною не менше 1 м, що мають надійне огородження у вигляді поручнів висотою не менше 1 м, а також з справних драбин і приставних драбин.

6. Забороняється підкидання будь-яких предметів для подачі працюючим нагорі. Інструменти, матеріали та інші предмети необхідно подавати за допомогою мотузки, до середини якої їх прив'язують. Другий кінець мотузки повинен знаходитися в руках у стоїть внизу працівника, який утримує піднімаються предмети від розгойдування.

7. При виконанні монтажних робіт дозволяється застосовувати тільки справний ручний інструмент. Ручний інструмент не повинен мати пошкоджень (тріщин, сколів, вибоїн) робочих крайок, задирок і щербин в місці захоплення інструменту рукою працюючого, тріщин і задирок на потиличній частині рукояток.

8. При роботі в електроустановках напругою до 1000 В, до яких відносяться і системи безпеки, без зняття напруги на струмопровідних частинах і поблизу них необхідно:

- обгородити розташовані поблизу робочого місця інші струмопровідні частини електроустановки, що знаходяться під напругою, до яких можливий випадковий дотик;

- працювати в діелектричних калошах або стоячи на ізолюючої підставці або на діелектричному килимку;

- застосовувати інструмент з ізолюючими рукоятками (у викруток, крім того, повинен бути ізольований стрижень). При відсутності такого інструменту користуватися діелектричними рукавичками;

- працювати в головному уборі і в одязі з рукавами, застебнутими або зав'язаними тасьмами у кистей рук.

Рис.3.2 – Набір одягу для проведення монтажних робіт

9. Перед початком всіх видів робіт в електроустановках напругою до 1000В із зняттям напруги необхідно перевірити відсутність напруги на ділянці роботи.

Після закінчення робіт на об’єкті потрібно:

1. Оглянути свої робочі місця на зовнішніх майданчиках, прибрати їх від сміття, відходів. Вимкнути і зібрати робочий інструмент, пристосування, запчастини, сходи та ін. Перенести і скласти все це в спеціально відведені місця.

2. Здати робочі місця безпосереднього керівника. Повідомити йому про виконані завдання, а також про всі помічені під час робіт несправності.

3. Зняти робочий одяг, взуття, прибрати їх в призначені для зберігання місця.

4. Вимити руки і обличчя з милом, по можливості прийняти душ.

Безпечне виконання робіт на об'єкті, відсутність травматизму та збереження людського життя завжди засноване на знанні та бездоганному дотриманні правил охорони праці, пожежної безпеки та електробезпеки. Це важливо пам'ятати і без порушень проводити будівництво та експлуатацію об'єктів.

ВИСНОВКИ

Застосування бездротових систем безпеки давно стало трендом. Причин тому багато – швидкість побудови системи, зручність, мобільність, витрати на побудову комунікаційного середовища, обслуговування тощо. У більшості випадків застосування бездротових систем безпеки, особливо в побутовому та офісному сегментах, є ефективним. Тішить, що при безлічі рішень різних брендів вже кілька років найкращим залишається український бренд Ajax.

Екосистема цього бренду обширна, і містить безліч пристроїв – хабів, ретрансляторів, різноманіття зовнішніх та внутрішніх датчиків, елементів розумного будинку, систем інтеграції зі сторонніми пристроями. При цьому як вся система, так і кожен пристрій окремо видно зі смартфона, що дозволяє бачити статус системи, параметри виконавчих і кінцевих пристроїв, потужність сигналу і т.д. Важливо відзначити свій протокол передачі даних Jeweller, що дозволило збільшити відстань між датчиком і хабом до 2000 метрів, залишимо конкурентів далеко позаду.

В цілому, рішення Ajax змінили парадигму охоронних систем у світі, показавши користувачеві гарну та надійну ефективність у безпеці.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дворський М.Н., Палатченко С.Н., – Безпека об'єктів підприємництва, том 1, Київ, видавництво А-Депт, 2006
2. Синилов В. Г. Системы охранной, пожарной и охранно-пожарной сигнализации: учебник для нач. проф. Образования / В. Г. Синилов – Москва: Издательский центр «Академия», 2010. – 512 с.
3. Гарсія М. Проектування і оцінка систем фізичного захисту. Пер. з англ. - ТОВ «Издательство АСТ», 2002. - 386 с.
4. ДБН А.2.2-2-96. Державні будівельні норми України. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва.—Держкоммістобудування України.—К., 1996.
5. ВБН.В.2.5.-78.11.01 – 2003 Інженерне обладнання будинків і споруд. Системи сигналізації охоронного призначення - Київ, 2003 р. - 56 с.
6. Керування ризиками на підприємстві / CIDCON CONSULTING COMPANY. - Київ, 2012.
7. Стайкуца С. В. Аналіз ризиків корпоративного середовища з позиції міжнародних стандартів інформаційної безпеки / С. В. Стайкуца, С.О. Дігол, О.М. Берднiков, В.І. Верстаков // Сборник тезисов третьей всеукраинской научно-практической конференции "Перспективные направления защиты информации", ОНАС им. А.С.Попова. – 2017. – С. 68–72.
8. Стайкуца С. В. Анализ и обоснование выбора периметральных систем охраны / С. В. Стайкуца, С. А. Дигол, К. С. Седов. // Сборник тезисов третьей всеукраинской научно-практической конференции "Перспективные направления защиты информации", ОНАС им. А.С.Попова. – 2017. – С. 72–76.
9. Гибридный приемно-контрольный прибор Hikvision DS-PHA20-P [Електронний ресурс] // Корпоративний сайт Hikvision Україна. – 2022. – Режим доступу до ресурсу: https://hikvision.co.ua/hikvision-ds-pha20-p.

10. Обзор беспроводной охранной сигнализации LUN-R (Лунь Р) [Електронний ресурс] // BEZPEKA.CLUB. – 2021. – Режим доступу до ресурсу: https://bezpeka.club/ru/oglyad-bezdrotovoyi-ohoronnoyi-sygnalizatsiyi-lun-r/.

11. Обладнання технічних засобів охорони [Електронний ресурс] // Корпоративний сайт Hikvision Україна. – 2022. – Режим доступу до ресурсу: https://hikvision.co.ua

12. Hikvision AX PRO: обзор 5 интересных датчиков охранной сигнализации [Електронний ресурс] // Pipl. – 2021. – Режим доступу до ресурсу: https://pipl.ua/ru/article/hikvision-ax-pro-oglyad-5-cikavih-datchikiv-ohoronnoyi-signalizaciyi.

13. Обзор централи Hikvision AX PRO [Електронний ресурс] // Pipl. – 2021. – Режим доступу до ресурсу: https://pipl.ua/ru/article/oglyad-centrali-hikvision-ax-pro.

14. Калипсо. Датчики и аксессуары [Електронний ресурс] // Сайт бренду Calipso. – 2022. – Режим доступу до ресурсу: https://kalipso.systems/katalog/datchiki-i-aksessuary.

15. Ajax [Електронний ресурс] // Корпоративний сайт Ajax. – 2022. – Режим доступу до ресурсу: https://ajax.systems/ru-ua/.