Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування закладу вищої освіти)

Навчально-науковий інститут інформаційних технологій і робототехніки
(повне найменування інституту, назва факультету (відділення))

Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

магістр

(ступінь вищої освіти)

на тему **Розроблення системи комплексної кібербезпеки інфокомунікаційної мережі підприємства, на основі стандартів ЄС**

Виконав: студент 6 курсу, групи 601ТТ
спеціальності 172 «Телекомунікації та
(шифр і назва напряму підготовки, спеціальності)
радіотехніка

Міщенко А.С.
(прізвище та ініціали)
Керівник Сокол Г.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)

Полтава - 2022 рік

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інституту Навчально-науковий інститут інформаційних технологій і робототехніки
Кафедра Автоматики, електроніки та телекомунікацій
Ступінь вищої освіти Магістр
Спеціальність 172 «Телекомунікації та радіотехніка»

ЗАТВЕРДЖУЮ

Завідувач кафедри автоматики, електроніки та телекомунікацій

_____ О.В. Шефер
“ ___ ” _____ 2022 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Міщенко Артему Сергійовичу

1. Тема проекту (роботи) **«Розроблення системи комплексної кібербезпеки інфокомунікаційної мережі підприємства, на основі стандартів ЄС»**
керівник проекту (роботи) Сокол Галина Вікторівна, к.т.н., доцент
затверджена наказом вищого навчального закладу від “12 ” 08 2022 року № 544 фа
2. Строк подання студентом проекту (роботи) 07.12.2022 р.
3. Вихідні дані до проекту (роботи) система відеоспостереження, охоронна сигналізація, пожежна сигналізація
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Теоретичні та методологічні основи створення систем комплексної кібербезпеки на основі стандартів ЄС. Обгрунтування вибору програмного та апаратного забезпечення. Розроблення проекту системи комплексної кібербезпеки підприємства на основі стандартів ЄС.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів):
   1) Структурна схема аналогової системи відеоспостереження;
   2) Структура кваліфікаційної роботи магістра;
   3) Нормативна документація країн ЄС;
   4) порівняння комплексних систем кіберзахисту;
   5) обгрунтування вибору програмного та апаратного забезпечення;
   6) обрання способу побудови системи;
   7) принцип роботи та функціональна схема системи;
   8) план розміщення обладнання системи.
6. Дата видачі завдання 01.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів магістерської роботи	Термін виконання етапів роботи			Примітка (плакати)
1	Теоретичні аспекти побудови систем відеоспостереження	13.09.22		15%	Пл. 1
2	Теоретичні аспекти побудови системи охоронно-пожежної сигналізації	27.09.22	I	30%	Пл. 2
3	Дослідження та аналіз стандартів ЄС	10.10.22		40%	Пл. 3
4	Аналіз основних видів загроз та ризиків кіберпезпеки для підприємства	17.10.22		50%	Пл. 4
5	Обґрунтування вибору програмного та апаратного забезпечення	24.10.22	II	60%	Пл. 5
6	Принцип роботи та функціональна схема комплексної системи кібербезпеки	08.11.22		70%	Пл. 6
7	Розрахунок споживаної потужності та вартості системи	07.12.22	III	100%	Пл. 7

Магістрант _____ Міщенко А.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Сокол Г.В.
(підпис) (прізвище та ініціали)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

VHS – Video Home System

IP – Internet Protocol

ПЗ – програмне забезпечення

ПК – персональний комп'ютер

FTP – File Transfer protocol

ОС – операційна система

NVR – network video recorder

ІЧ – інфрачервоний

PoE – Power over Ethernet

TIA – Telecommunications Industry Association

EIA – Electronic Industries Association

ISO –International Organization for Standardization

CCTV – Closed-circuit television

ВСТУП

З кожним роком зростає кількість кібер випадків на промислових підприємствах та критично важливих об'єктів інфраструктури. При цьому наслідки при реалізації таких атак можуть бути виражені як у формі фінансових втрат так і втрати важливої інформації. В теперішній час активно ведуться дослідження різноманітних систем комплексної кібербезпеки, моделей різних атак на компоненти систем і виникаючих від їх реалізації наслідків. Система являє собою засоби по захисту інформації від неавторизованого доступу, руйнування, модифікацій та затримок доступу.

Під системою кібербезпеки розуміється використання спеціальних засобів та заходів, з метою в попередження втрат інформації та власності підприємства. Широкого поширення та розповсюдження обчислювальної техніки різко підвищили вразливість інформації, що зберігається на підприємстві. Для нормального і безпечного функціонування таких систем необхідно підтримувати їх безпеку та цілісність. В сучасних підприємствах системи комплексної кібербезпеки займають ключову позицію забезпечуючи взаємозв'язок всього інженерного обладнання та інших систем підприємства.

Сьогодні проблема інформаційного захисту реалізується за допомогою розробки та введення систем комплексної кібербезпеки, які враховують особливість поведінки потенційних зловмисників та специфіку роботи підприємства.

Для вирішення проблеми розробимо інноваційний та актуальний комплекс кібербезпеки, що відображений в меті даної кваліфікаційної роботи магістра.

Актуальність створення системи комплексної кібербезпеки. Регулярна поява нових загроз вимагає постійного вдосконалення захищеності будь-якого підприємства, адже в іншому випадку підприємству може бути завдано шкоди. Не завжди є можливість організувати роботу спеціалізованих служб, що

забезпечують кібербезпеку підприємств та здійснюють виявлення, попередження та усунення виникаючих загроз.

Об'єкт дослідження: система комплексної кібербезпеки інфокомунікаційної мережі підприємства.

Предмет дослідження: технології та стандарти ЄС для розробки системи комплексної кібербезпеки інфокомунікаційної мережі підприємства.

Метою кваліфікаційної роботи магістра є на основі аналізу методів та технологій країн ЄС розробити та спроектувати систему комплексної кібербезпеки, яка буде захищати інфокомунікаційну мережу підприємства.

Постановка задачі. Задачею дослідження є аналіз сучасних технологій та стандартів ЄС та розроблення системи комплексної кібербезпеки інфокомунікаційної мережі підприємства.

Призначення системи комплексної кібербезпеки. Автоматизує процес збору та обробки інформації від систем та обладнання технічних засобів охорони підприємства, взаємоузгодженого функціонування цих засобів та систем.

1. ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ОСНОВИ РОЗРОБЛЕННЯ СИСТЕМИ КОМПЛЕКСНОЇ КІБЕРБЕЗПЕКИ НА ОСНОВІ СТАНДАРТІВ ЄС.

Здійснення заходів, що до превентивного захисту і адекватної безпеки промислових об'єктів, представляє собою складний неперервний процес, а не одноразові чи випадкові дії, які виконуються від випадку до випадку по мірі виникнення необхідності та вносять неузгодженість в роботу різних служб. Безперервне та стабільне функціонування будь-якого об'єкту неможливе без організації надійного захисту, який включає в себе комплекс заходів направлених на виявлення загроз та створення системи комплексної кібербезпеки об'єкту при визначених обмеження.

Для організації ефективного захисту необхідно розробити системну концепцію безпеки, яка в кожному конкретному випадку повинна бути адаптована до конкретного об'єкта, виходячи з умов його функціонування, розташування, виду діяльності, географічного положення, особливостей навколишнього середовища та інших факторів. Концепція безпеки представляє собою загальний задум організації технічних та організаційних заходів, що до захисту від прогнозованих загроз [1].

1.1. Теоретичні аспекти побудови систем відеоспостереження

Головна причина використання систем відеоспостереження – це прагнення підвищити рівень безпеки і захищеності людей і об'єктів приватної власності.

Відеоспостереження може внутрішнім і вуличним, кількість відеокамер та їх тип найчастіше обмежений тільки фінансовими можливостями. До складу системи обов'язково входять пристрої, що дозволяють передавати та отримувати відеосигнал. За допомогою цих пристроїв можна в режимі реального часу спостерігати відео з камер.

Сучасні системи здатні виконувати задачі відеоаналітики від найпростіших розпізнати рухи в полі зору камери, до автоматизованої ідентифікації особистості, або виявленні залишених предметів [1].

Системи відеоспостереження призначені для організації цілодобового відео та аудіоконтролю будь-якого об'єкту. В залежності від типу обладнання системи поділяють на аналогові та цифрові.

Мінімальна конфігурація аналогової системи зображена на рис. 1.1. [2] включає в себе:

- відеокамери;
- пристрої обробки відеосигналу (квадратори, мультиплексори);
- записуючі прилади (відеомагнітофони, відеореєстратори, відеокодери);
- прилади відтворення інформації (відеомонітори).

Рисунок 1.1 – Структурна схема аналогової системи відеоспостереження

В аналогових системах використовується невелика кількість відеокамер, а вся інформація записується на відеомагнітофони, які можуть записувати до 960 годин відео на одну касету стандарту VHS. Сигнал з магнітофону обробляється мультиплексором, або квадратором, що дозволяє робити запис з декількох камер одночасно. При використанні квадратора швидкість запису збільшується, але якість запису значно знижується. Використавши мультиплексор якість буде краща, так як записується повний кадр, а не зменшений в декілька разів. Проте втрачається швидкість тому що кадри посилаються по черзі з кожної відеокамери [3].

В залежності від кількості камер швидкість запису збільшується (менше камер) або зменшиться (більше камер). Накопичувачем при використанні аналогового способу запису є проста або спеціальна відеокасета. Варто зазначити, що на сьогодні виробники випускають камери із вбудованим блоком перетворення аналогового сигналу в цифровий. Тобто аналогові камери можливо інтегрувати в цифрові системи.

Що стосується самих камер вони можуть бути безкорпусні, маленького розміру, можливо вмонтовані в предмети інтер'єру. Відеокамери що виготовляються в корпусі, маленький розмір дозволяє встановити їх поворотні пристрої. Приховані камери, також невеликого розміру, використовуються для таємного нагляду. Швидкісні купольні камери (зазвичай встановлюють під стелею) мають швидкий поворотний пристрій, за допомогою якого камери можуть розвивати швидкість до 400 градусів горизонтальної площини і повертатися в горизонтальній площині до 160 градусів.

Для передачі відеосигналу аналогові камери використовують класичний коаксіальний кабель. Такі кабелі прокладені на багатьох підприємствах, що є плюсом при модернізації мережі [3].

Аналогові системи відеоспостереження володіють рядом переваг.

Основна та вагома перевага їх невисока вартість, аналогова камера володіє меншим кутом огляду, і якість отримуваного зображення буде гірше, але за вартість однієї цифрової камери, можна придбати дві-три аналогові [3].

По-друге це простота встановлення та налаштування. Підключення аналогових компонентів набагато простіше. Необхідність розраховувати пропускну здатність мережі, підключати роутери, комутатори та виконувати мережеві налаштування не потрібно. Великою перевагою аналогової системи є можливість підключення до уже існуючих кабельних трас. Можливо оновити систему без витрат на монтаж кабелів сигналу та живлення.

По-третє, відсутність затримки при передачі сигналу та зависання зображення. Окрім того трансляція відео с аналогової камери завжди йде в режимі реального часу зі швидкість 30 кадрів на секунду [2].

В четверте висока дальність передачі сигналу без перешкод та використання підсилювачів. При необхідності використання приймачів зможе збільшити дальність передачі сигналу. Відсутність проблем з сумісністю, обладнання різних виробників без проблем працює між собою.

Цифрові системи зазвичай являють собою IP-відеоспостереження один з найпоширеніших методів в сучасних системах відеоспостереження. Вони відрізняються більшими можливостями, кращою якістю зображення і більшим функціоналом, але й значною вартістю. Виробники електроніки намагаються зробити свою техніку сумісною з IP-протоколом він дозволяє приладам підключатися до мережі та взаємодіяти за допомогою ПЗ.

Цифрова система складається з наступних компонентів рис. 1.2. [2]:

- IP відеокамери;
- відео сервери
- прилади відтворення зображення
- додаткові пристрої

Рисунок 1.2 – Структурна схема цифрової системи відеоспостереження

Саме IP відеоспостереження використовують в сучасних системах кібербезпеки, системах виявлення та аналізу предметів, для автоматичного розпізнавання номерних знаків автомобілів. Монтаж відеспостереження на основі IP камер здійснюється разом з організацією локальної мережі, що дозволяє швидко об'єднати всі компоненти, звернутися до камери можна безпосередньо з ПК, досить просто ввести IP адресу камери [4].

IP відеоспостереження це система побудована на мережевих відеокамерах і відеосерверах, які не тільки фіксують зображення, але й відсилають його по бездротовій і локальній мережах, а зафіксовану інформацію можна переглянути на будь-яких приладах, що мають доступ до мережі інтернет [4].

Головна перевага IP технології полягає у можливості побудови системи відеоспостереження не прив'язуючись до відстані. Мережа масштабована і гнучка, що дає можливість інтелектуального аналізу та негайного доступу до відеоданих. В подальшому системи надають безмежні можливості по модернізації ПЗ, що використовується в IP системах. Якість зображення з таких камер дуже висока а сигнал передається майже миттєво.

Камера підключається до мережі інтернет, або локальної мережі через порти Ethernet, далі камері присвоюється ip-адреса. За допомогою ПЗ для FTP-серверу, web-серверу, або E-mail користувача камера буде працювати самостійно [2].

До приладів IP відеоспостереження також відносять відеосервери, котрі призначені для роботи в складі цифрової системи відеоспостереження, вони перетворюють аналоговий сигнал в цифровий формат потім передають його по мережі або на інформаційний носій.

Головні переваги цифрової системи відеоспостереження.

- IP-камера має цифрову матрицю, власний вбудований процесор оперативну пам'ять, процесор, для стиснення та обробки зображень;
- відеодані шифруються і передаються в лише в такому вигляді, доступні лише через введення пароля;

- максимальна простота інтеграції з комп'ютерною мережею через автоматично присвоєну IP-адресу та без необхідності ручного налаштування;
- можливість дистанційного керування та доступу до відеоматеріалів через інтернет.

1.2. Теоретичні аспекти побудови системи охоронно-пожежної сигналізації

Система охоронно-пожежної сигналізації призначені для визначення факту несанкціонованого проникнення до на об'єкт, або виявлення ознак пожежі, ввімкнення сигналу тривоги та спрацювання додаткових засобів (світлових та звукових виконавчих пристроїв) [5].

Система являє собою складний комплекс технічних засобів, що слугують для своєчасного виявлення несанкціонованого доступу в приміщення. Система може інтегруватися в комплекс, який об'єднує в собі системи безпеки з інженерними системами будівлі, забезпечуючи перевіреною адресною інформацією систему сповіщення, пожежогасіння, димовидалення, контролю доступу та інші.

В залежності від масштабу задач, котрі виконує система в її склад входить обладнання трьох основних категорій рис. 1.3:

- обладнання централізованого керування охоронно-пожежною сигналізацією (наприклад, центральний комп'ютер з встановленим ПЗ для керування охоронно-пожежною сигналізацією – пульт централізованого нагляду; в невеликих системах задачі централізованого управління виконує охоронно-пожежна панель);
- обладнання збору та обробки інформації з датчиків;
- сенсорні прилади:
    - технічні засоби виявлення;
    - технічні засоби сповіщення (звукові та світлові сповіщувачі, модеми, системи мовного сповіщення);

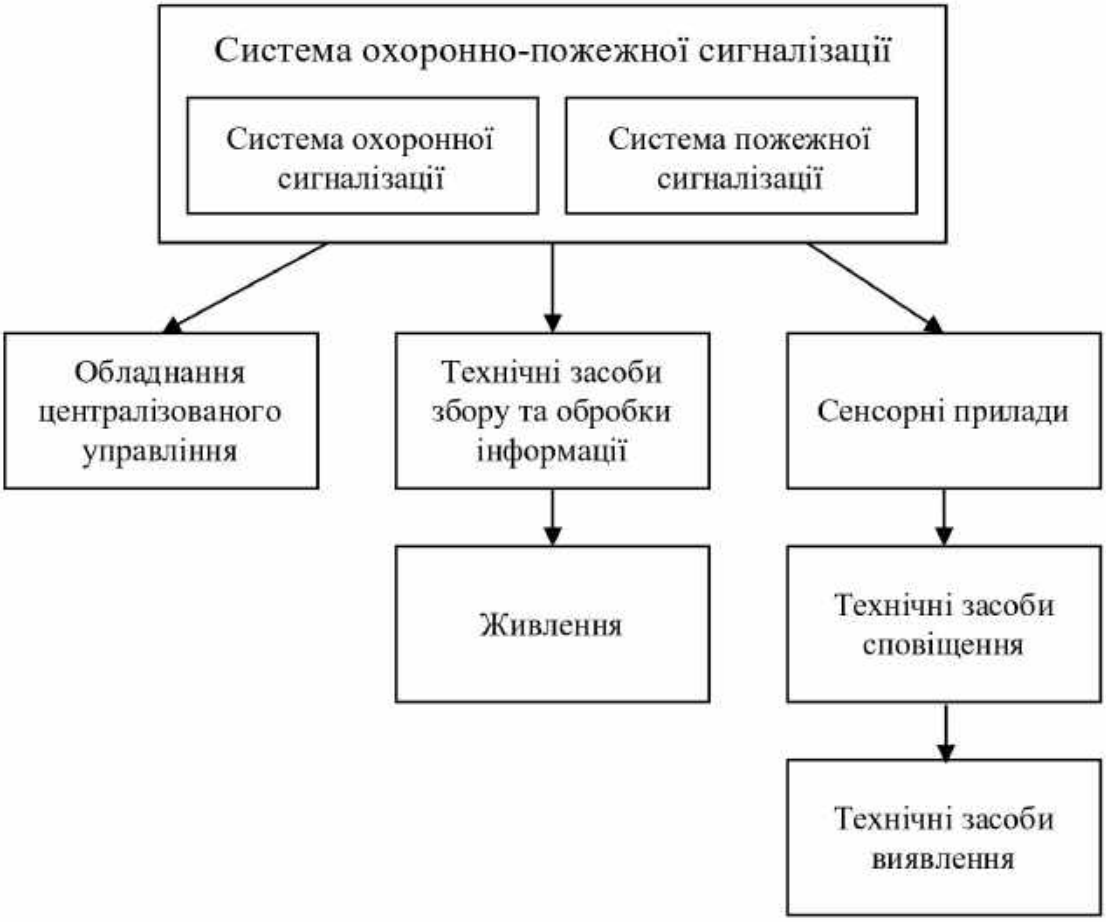

Рисунок 1.3 – Структура охоронно пожежної сигналізації

Кожна система використовує датчики, що контролюють різноманітні фізичні параметри середовища. В залежності від способів виявлення загроз та формування сигналів система поділяється на неадресні, адресні та адресно-аналогові. В неадресних системах датчики мають фіксований поріг чутливості. При цьому група датчиків включається загальний шлейф системи, в якому у випадку спрацювання одного з них, формується узагальнений сигнал тривоги. Адресні системи відрізняються наявністю інформації про адресу датчику, що дозволяє визначити зону порушення з точністю до місця розташування датчика [5].

Адресно-аналогова система є більш інформативною та розвиненою. В такій системі застосовуються інтелектуальні датчики, які передають поточні значення контрольованого параметру разом з адресою шлейфу. Такий спосіб моніторингу застосовується для завчасного виявлення тривожної ситуації,

отримання даних про необхідність технічного обслуговування датчиків внаслідок забруднення чи інших факторів. Крім цього, адресно-аналогові системи дозволяють, не припинивши роботу, на програмному рівні змінювати фіксований поріг чутливості датчиків при необхідності їх адаптації до погодних умов експлуатації на об'єкті.

Кожен тип датчиків має свій перелік основних технічних характеристик, що відповідають належним стандартам. В той же час навіть однотипні датчики мають відмінності в конструктивних особливостях складових частин, зручності експлуатації, надійності, рівню дизайну, що враховується при виборі того чи іншого пристрою або виробника [6].

Інтеграція охоронної і пожежної сигналізацій в складі єдиної системи відбувається на рівні централізованого моніторингу і керування. При цьому сигналізації адмініструються незалежними один від одного постами керування, які зберігають автономність у складі системи охоронно-пожежної сигналізації. У невеликих приміщеннях системою можна керувати за допомогою приймально-контрольними приладами.

Система виконує завдання своєчасного сповіщення про несанкціонований доступ з фіксацією дати, місця та часу проникнення. Технічні засоби виявлення – це датчики побудовані на різних принципах дії. Датчик це пристрій, формуючий певний сигнал при зміні того чи іншого контрольованого параметру навколишнього середовища [6].

Використання додаткових специфічних датчиків дозволяє на одній контрольній панелі організувати комплексну систему кібербезпеки. Всі прилади з'єднуються різноманітними каналами зв'язку, як бездротовими так і дротовими.

Передача сигналів на пульт керування є найважливішою складовою системи сигналізації. Оскільки забезпечує можливість своєчасного реагування, на виявлену загрозу, отже вчасно попередити втрати. Сигнали передаються різними способами по різним каналам зв'язку.

До основних каналів зв'язку можна віднести:

- спеціальні дротові лінії зв'язку;
- спеціалізовані радіо канальні лінії;
- дротові телефонні лінії;
- бездротові телефонні лінії мобільного зв'язку;
- канали передачі даних мобільних мереж;
- комп'ютерні мережі.

Для захисту каналу зв'язку від випадкового або навмисного виходу з ладу доцільно використовувати два канали зв'язку з різноманітними фізичними принципами дії дублювання повідомлень. Для підключення на пульт керування зазвичай потрібні модуль зв'язку або інтерфейси. В деяких системах вони вже вбудовані в контрольну панель пульта керування, В інших випадках потрібно використовувати окремі модулі, або спеціальні кінцеві об'єктові прилади систем централізованого нагляду, що підключаються до контрольної панелі [7].

Датчики сигналізації розташовують на будівельних конструкціях, що мають найбільшу вразливість:

- вікна, вітражі;
- двері, люки;
- некапітальні стіни, перекриття.

Головною характеристикою системи охоронно-пожежної сигналізації є її ефективність. Варто відмітити наступні методи її забезпечення:

1. Надійність – можливість безвідмовної роботи, яка забезпечується виробником обладнання та якістю монтажу системи.
2. Достовірність виявлення проникнення, досягається мінімізацією хибних спрацювань (визначається якістю монтажу, та застосуванням грамотних проектних рішень).
3. Вірогідність виявлення порушників. Визначається повнотою блокування засобами охоронно-пожежної сигналізації вразливих місць.

1.3. Дослідження та аналіз стандартів ЄС

Європейські стандарти, для забезпечення підвищеної безпеки і для бездротових систем, що використовуються в системах кіберзахисту були додані до Європейського стандарту серії EN 50131. Він містить набір стандартів, за яким компанії що займаються встановленням охоронних систем можуть обстежити, встановлювати і обслуговувати об'єкти. Європейські стандарти в даний час мають документ PD 6662, який показує частину британських стандартів, де європейські не застосовуються [8].

Насправді EN 50131 – це ціла серія стандартів для систем кіберзахисту, а сюди вже входять окремі стандарти для різноманітних елементів і складових систем кіберзахисту. Розглянемо всі діючи стандарти в таблиці 1.1.

Таблиця 1.1 – Стандарти систем кібербезпеки країн ЄС

Стандарт	Опис стандарту
EN50131-1	Загальні вимоги до систем кіберзахисту
EN50131-2-2	Пасивні інфрачервоні (ІЧ) датчики
EN50131-2-3	Радіохвильові (СВЧ) датчики
EN50131-2-4	Комбіновані ІЧ/СВЧ датчики
EN50131-2-5	Комбіновані ІЧ ультразвукові датчики
EN50131-2-6	Магнітоконтактні датчики
EN50131-3	Контрольні панелі
EN50131-4	Пристрої сповіщення
EN50131-5-3	Бездротові пристрої
EN50131-6	Джерела живлення

Як можна побачити кожен стандарт може описати тільки визначений тип пристрою. Окремо варто зазначити, щоб отримати сертифікат відповідності країн ЄС недостатньо, створити прилад, що буде відповідати одному з стандартів. Виробник зобов'язаний надати власну розробку в

незалежну лабораторію, де буде проводитися тестування пристрою в продовж декількох місяців, по завершенню цього виробник зможе отримати сертифікат відповідності на свій виріб. Окрім цього в сертифікаті буде вказано якому класу безпеки відповідає обладнання [8].

Як було написано вище вимоги до захисту різних об'єктів повинні буди інакші. Тому в стандарті EN 50131 існує поняття «грейди» (англ. grade) – перекладається як, «клас», «ранг», «ступінь». У випадку ж системи кібербезпеки, мається на увазі клас або ступінь захищеності. Всього існує чотири класи захищеності.

Грейд 1. Найпростіша сигналізація. Дешеве обладнання, але виконує свої функції. Датчиками повинні бути заблоковані очевидні шляхи проникнення, такі як двері та вікна. Система повинна захистити приміщення від недосвідчених, випадкових проникнень зловмисників. Підходить для об'єктів з мінімальним ризиком несанкціонованого доступу.

Грейд 2. Більш складне обладнання, різноманітні типи датчиків, котрі можуть дублювати один одного, або доповнювати. Сигналізація повинна виконувати функції захисту від використання спеціального обладнання. Грейд 2 – самий розповсюджений клас [9].

Грейд 3. Сигналізація повинна протистояти професіоналам, які мають спеціалізоване обладнання для обходу систем кіберзахисту, повинна бути захищена від саботажу. Датчики повинні мати змогу заблокувати не тільки очевидні шляхи доступу до приміщення, а й нівелювати гіпотетичні, такі як гіпсові перекриття, проходи через цокольний поверх, технічні та комунікаційні люки. Така система призначена для охорони великих підприємств, наприклад фінансових установ.

Грейд 4. Система повинна мати змогу протидіяти професіоналам, або навіть терористичним кібератакам. До категорії таких підприємств можна віднести великі кредитні та фінансові установи, державні установи зв'язані з безпекою. Грейд 4 ніколи не використовується для захисту звичайних підприємств, так як вимоги дуже жорсткі та специфічні.

Варто зазначити, що грейд безпеки усієї системи присвоюється ґрунтуючись на елементах найнижчого класу. Наприклад, коли система виконана використовуючи обладнання по нормам та вимогам Грейд 4, а один із датчиків відповідає Грейд 2, то такій системі повинен призначатися другий клас безпеки [9].

Аналізуючи системи комплексної кібербезпеки провідних країн ЄС можна зробити висновок, що на сьогоднішній день не існує єдиної уніфікованої моделі побудови комплексної системи кібербезпеки. Наприклад відповідно до прийнятого 25 листопада 2002 року комплексного нормативно-правового акта у сфері безпеки – закону США «Про внутрішню безпеку» (Homeland Security Act of 2002) – організації, виробники котрі займались системами кіберзахисту, підлягають під контроль цього новоствореного відомства. Закон також збільшив відповідальність за злочини вчинені на інфокомунікаційну мережу (включаючи довічне ув'язнення), зобов'язав інтернет-провайдерів надавати безперешкодний доступ до усієї доступної інформації про клієнтів за першою вимогою правоохоронних органів, що дало змогу розширити їх права щодо можливості перехоплення інформації (прослуховування телефонних переговорів) без рішення суду, визначив основні види діяльності правоохоронних органів з підвищення ефективності захисту критичної інфраструктури США від кібератак, у тому числі об'єктів стратегічного значення, що перебувають у приватній власності [9].

Стратегія кібербезпеки Канади визнає кібертероризм та ворожі дії в кіберпросторі з боку інших країн (кібершпигунство і кібервійну) головними чинниками кібернетичної загрози держави, а ключовим органом, що координує та контролює реалізацію цієї стратегії, реалізація державної політики та координування заходів у сфері кібербезпеки та протидії кіберзагрозам визначене Міністерство громадської безпеки Канади (Public Safety Canada).

ФРН видала закон «Про посилення безпеки інформаційних систем» завданням якого є попередження, реагування на інциденти, викликані

кібернетичними загрозами, керування й координація методів та засобів по захисту критичної інформаційної структури, зокрема у взаємодії з приватним сектором, покладене на Федеральне відомство безпеки інформаційних систем (BSI) ФРН [9].

Основною державною структурою, якій надано права на захист критичної інфраструктури, мінімізації загроз її безперешкодному функціонуванню, в основному від загроз тероризму, ж Центра захисту національної інфраструктури (Centre for the Protection of National Infrastructure, CPNI). Окрім цього наприкінці березня 2013 року Великобританія створила Центр з протидії кібер загроз з метою попередження та нейтралізації кібер атак на об'єкти критичної інфраструктури, а також швидкого реагування на скоєні злочини у цій сфері.

Австрія розробила стратегію кіберзахисту керівником і центральним органом якої було призначено Центр боротьби з кіберзлочинністю Федерального міністерства внутрішніх справ Австрії (Cyber Crime Competence Center (C4) of the Federal Ministry of the Interior).Також, він відповідає за виконання головних функцій щодо здійснення правоохоронної діяльності у сфері кібербезпеки та боротьба з кіберзлочинністю [8].

Головним чинником у забезпеченні кібернетичної безпеки Польщі відповідає Агентство внутрішньої безпеки (АВБ) – польський контррозвідувальний орган. У 2013 році АВБ створило Стратегію кібербезпеки Польщі та ініціювало створення Центру криптології при Міністерстві національної оборони Польщі, котрий виконує завдання захисту інформації, кібероборони та проведення наступальних кібероперацій (активний кіберзахист).

Ключова роль у забезпеченні кібербезпеки Румунії відводиться її спеціальному контррозвідувальному органу – Румунській службі інформації (РСІ) [8].

Аналіз нормативно-правових та організаційних основ системи кібербезпеки провідних країн ЄС свідчить про домінантну роль спецслужб у

забезпеченні кібернетичної безпеки держави, що пов'язано із характером кібернетичних загроз сьогодення, протидія яким потребує інструментарію (повноважень, форм і методів), притаманного виключно спеціальним, а саме, контррозвідувальним органам держави.

1.4. Аналіз основних видів загроз та ризиків кібербезпеки для підприємства

Для побудови системи якісної системи комплексної кібербезпеки, захищеної від реальних загроз, необхідно ясно розуміти що і як загрожує інформаційним та фізичним ресурсам. Аналіз загроз необхідний для якісної та кількісної оцінки, як зовнішніх так і внутрішніх загроз безпеки, актуальних для конкретного підприємства. В результаті отриманої оцінки можна сформулювати повний набір вимог до системи, що забезпечує необхідний захист власності підприємства.

Аналіз загроз дозволяє виділити основні складові загроз – їх джерела та рушійні сили, способи для реалізації. Аналіз виключно важливий для отримання всієї необхідної інформації про загрози, визначення потенційної величини шкоди, як матеріальної так і нематеріальної, та напрацювання засобів протидії [10].

Під загрозою безпеки зазвичай розуміють потенційну подію (вплив, процес чи явище), яке може призвести до заподіяння шкоди чиїмось інтересам. В подальшому під загрозою безпеки будемо розуміти можливість впливу на об'єкт, який може прямо чи опосередковано нанести шкоду [10].

В теперішній час відомо великий перелік загроз кібербезпеки, що містить сотні позицій. Список загроз, оцінки можливості їх реалізації, а також модель порушника слугують основою для аналізу ризику реалізації загроз і формулюванні вимог до системи кіберзахисту [11].

Загрози безпеці на рідкість різноманітні. Зорієнтуватися в цьому різноманітті допомагають переліки загроз, наведені в додатках до стандартів ISO 27005. Одним з найбільш детальніших описів тисяч загроз кібербезпеки

можна зустріти у відкритому німецькому стандарті BSI IT Baseline Protection Manual.

Окрім виявлення потенційних кіберзагроз доцільно виконати аналіз на основі їх класифікації по ряду чинників. Кожний з чинників класифікації відображає одну з узагальнених вимог до системи кіберзахисту. Загрози відповідні кожному чиннику класифікації, дозволяють деталізувати вимоги, що відображені цим чинником [11].

Причини випадкових впливів під час експлуатації системи можуть бути:

- аварійні ситуації із-за стихійних лих, аварійного вимкнення електроенергії;
- відмови та збої апаратної частини;
- помилки в ПЗ;
- помилки в роботі керуючого персоналу та користувачів;
- перешкоди в лініях зв'язку через вплив навколишнього середовища;

Необхідність класифікувати загрози кібербезпеки зумовлена тим, що інформація та власність що зберігається наражається на вплив надзвичайно великої кількості факторів, в силу чого стає неможливо сформувати завдання опису повного переліку загроз. Тому для системи кіберзахисту визначають не повний перелік загроз, а перелік класів загроз [12].

Класифікація можливих загроз може бути проведена за наступними базовими ознакам.

1. За природою виникнення:
   - природні загрози, що відбулися під час впливу на систему фізичних процесів, або стихійних природних явищ;
   - штучні загрози, викликані дією людини.
2. За рівнем навмисності прояви:
   - загрози, що викликані помилками чи недбалістю персоналу;
   - загрози навмисної дії, наприклад діями зловмисників.
3. За безпосереднім джерелом загроз:
   - природнє середовище, наприклад стихійні лиха, магнітні бурі та інші;

- людина, наприклад вербування працівника шляхом підкупу, розголошення конфіденційних даних;
- санкціоновані програмно-апаратні засоби, наприклад видалення даних, відмова в роботі ОС;
- несанкціонована програмно-апаратні засоби, наприклад зараження комп'ютера вірусами з деструктивними функціями.

4. За розташуванням джерела загроз;
   - поза контрольованою зоною системи кіберзахисту, наприклад перехоплення даних по каналам зв'язку, перехват другорядних електромагнітних, акустичних та інших сигналів пристроїв;
   - в межах контрольованої зони, наприклад застосування прослуховуючих пристроїв, викрадення записів, носіїв інформації;
   - безпосередньо в системі кіберзахисту, наприклад некоректне використання ресурсів.
5. За ступенем залежності від активності системи:
   - незалежно від активності системи, наприклад розкриття шифрів криптозахисту інформації;
   - тільки в процесі обробки даних, наприклад загрози виконання та розповсюдження програмних вірусів.
6. За ступенем впливу на систему кіберзахисту:
   - пасивні загрози, які при реалізації нічого не змінюють в структурі системи, наприклад загроза копіювання даних;
   - активні загрози, які при впливі на систему вносять зміни в структуру та вміст, наприклад використання троянських коней та вірусів.
7. За способом доступу до ресурсів системи:
   - загрози, що здійснюються з використання звичайного доступу до ресурсів, наприклад незаконний доступ до паролів та інших реквізитів розмежування доступу з наступним маскуванням під авторизованого користувача;

- загрози, що здійснюються с використанням прихованого нестандартного шляху доступу до ресурсів системи, наприклад несанкціонований доступ до ресурсів системи шляхом використання недокументованих можливостей ОС.

8. За етапом доступу користувачів або програм до ресурсів системи:
   - загрози, що проявляються на етапі доступу до ресурсі, наприклад загрози несанкціонованого доступу до системи;
   - загрози, що з'являються після дозволу доступу до системи, наприклад загрози несанкціонованого чи некоректного використання ресурсів системи.
9. За поточним розташуванням інформації, що зберігається та обробляється в системі:
   - загрози доступу до інформації, що знаходиться на зовнішніх носіях, наприклад, копіювання інформації з жорсткого диску;
   - загрози доступу до інформації, що знаходиться в оперативній пам'яті, наприклад читання залишкової інформації з оперативної пам'яті, доступ до системної області зі сторони прикладних програм;
   - загрози доступу до інформації, що циркулює в лініях зв'язку, наприклад незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача з наступними введенням дезінформації та нав'язування хибних повідомлень;
   - загрози доступу до інформації, що відображена на терміналі, наприклад запис відображеної інформації на приховану камеру.

Проаналізувавши вихідні дані по організаційній структурі підприємства, її інформаційної системи, а також інформаційну безпеку, були знайдені недоліки в організації безпеки. Були встановлені потенційно небезпечні загрози. З найбільш небезпечних можна виділити відсутність відеокамер та контролю роботи пожежної сигналізації. Внаслідок чого можна виділити найбільш небезпечні загрози безпеки: крадіжка носіїв інформації, пожежа та вплив відвідувачів [12].

Висновки до першого розділу

В ході проведеного аналізу теоретичних та методологічних основ створення систем кіберзахисту на основі стандартів ЄС. Розглянуто принципи побудови систем відеоспостереження та сигналізації і попередження несанкціонованого доступу та витоку інформації з метою їх подальшої реалізації. Були виявлені такі проблеми, як необхідність суворого контролю та управління серверами. Названі проблеми посилюються ще тим фактором, що розміщуючи інформацію на сервері, користувачі не завжди можуть контролювати рівень безпеки. Також розглянуті можливі атаки на ресурси системи та виявлені елементи, котрі найбільш вразливі. До них можна віднести канал зв'язку, Web-сервер, комп'ютери користувачів, сервери баз даних, корпоративні сервери.

Структурно інтегрована система кіберзахисту може включати в себе спільно функціонуючі системи відеоспостереження, системи сигналізації, контролю та управлінням доступом, охоронну та пожежну систем, а також ряд додаткових систем, що забезпечують захист від різного рівня загроз.

Для досягнення необхідного рівня системи кіберзахисту необхідно забезпечити протидію різноманітним технічним загрозам та мінімізувати можливий вплив «людського фактору». В даному випадку доцільно передбачити можливість подальшого розвитку системи, шляхом розширення та вдосконалення окремих елементів її частин, а також додавання до існуючих систем у вигляді підсистеми.

Таким чином можна зробити висновок про досягнення мети і вирішення завдань, теоретичної та методологічної побудови системи кіберзахисту та приступити до проектування.

2. ОБҐРУНТУВАННЯ ВИБОРУ ПРОГРАМНОГО ТА АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ

Адекватний на ефективний рівень кібербезпеки може бути забезпечений тільки за допомогою комплексного підходу, який передбачає спрямоване застосування традиційних організаційно-технічних правил надання безпеки на єдиній концептуальні основі з одночасним пошуком та глибоким вивченням нових прийомів та засобів захисту.

Данні положення тією чи іншою мірою актуальні для кожної розвиненої країни, котра прагне до збереження внутрішньої та зовнішньої безпеки. Різняться лише методи та засоби, що застосовуються в різних державах, для досягнення оптимального рівня кіберзахисту.Вибір варіанту системи комплексної кібербезпеки будь-якого приміщення варто розпочинати з його обстеження. Визначивши загальну характеристику об'єкту, варто проаналізувати основні вразливі місця по периметру об'єкта, блокування якого, як правило являє собою перший рубіж захисту [13].

Вибір технічних засобів реалізації системи проведений на підставі аналізу конструктивно-будівельних характеристик і призначення приміщення з урахування завдання, нормативних документів та стандартів ЄС, тактико-технічних характеристик та вартості обладнання. При виборі технічних засобів реалізації системи враховується устаткування і методи установки, які якнайкраще підходять для вирішення завдань системи.

Розгляд взаємодії обладнання, середовища та потенційних порушників важливо для правильного вибору технічних засобів необхідних для реалізації системи. На роботу датчиків впливають конструкція будівлі та приміщення, а також інше обладнання що буде встановлене в приміщення [13].

Зазвичай можна визначити та підібрати прилади, які будуть працювати в заданих умовах, оскільки ці умови для приміщень визначені та контролюються.

Багато пристроїв систем кібербезпеки мають власні програми, за допомогою яких ви можете керувати їх основними функціями. Інші пристрої носять більше загальний характер та використовують популярні стандарти, такі як Zigbee та Z-Wave(бездротові протоколи Bluetooth для зв'язку з хабами), для того щоб керувати пристроями через застосунок в телефоні чи комп'ютері. Деякі пристрої потрапляють в обидві категорії: можна використовувати і застосунки і більшу платформу системи кібербезпеки. Однак деякі платформи обмежують користувача в тому, які прилади можна приєднати до них. При такій великій кількості приладів різних виробників створення системи може здаватися складним завданням, але як і будь-яке інше завдання його можна спростити, розбивши на більш простіші завдання. Можна розпочати з декількох пристроїв і далі масштабувати систему та додавати нові гаджети.

Сьогодні існує багато компаній виробників обладнання, для систем кіберзахисту. Ajax Systems з 2011 року виробляє у Києві професійні системи безпеки для офісних приміщень та дому. Успіхи компанії заключаються у гармонічному поєднанні інноваційних рішень та технологічного дизайну [14].

У їхній доробках поєднуються інженерні інновації, власні ноу-хау та технологічний дизайн. Творці високотехнологічних систем відзначають, що вірять в інтернет речей та розумну безпеку як його основу. Офіси компанії є не лише в Україні, а й у США та Великобританії. [14]

Компанія підкорила не лише найвіддаленіші куточки планети, а й найкращих професіоналів. Команда Ajax Systems уже налічує майже 2000 людей. Серед них — талановиті інженери та розробники, сильні менеджери з досвідом у глобальних корпораціях. Компанія сформувала локальні команди у Великій Британії, Італії, Франції, Іберії, ПАР і готова підкорювати нові вершини.

Основний напрям своїх розробок, направляють бездротову охорону в Україні.. Вдома люди зберігають і накопичують багато цінних та коштовних речей. В нашій країні існує багато охоронних приватних компаній, служба держ-безпеки. Якщо в 2019 році Ajax Systems мала лише 20 охоронних

компаній, як партнерів, то на сьогодні по всій країні є понад 50-60 приватних компаній, а також поліція державної безпеки, які є партнерами Ajax.

Ajax Systems – рідкісний приклад української hardware-компанії, що стрімко розвивається. Вона розробляє компоненти для системи кіберзахисту, що визнані експертами в охоронній індустрії кращими в Європі. Виготовлення техніки знаходиться в Києві – продуктивність виробництва вже досягла 100 000 пристроїв в місяць [14].

Системи Ajax повністю незалежні, так як працюють на захищеному радіо протоколі Jeweller власної розробки. Пікова дальність зв'язку становить 200 метрів, що гарантує нормальну роботу системи навіть в великих приміщеннях. Якщо цього не вистачить в арсеналі виробника є ретранслятори, які завжди можна додати. З ретранслятором дальність при прямій видимості збільшується до 3800 метрів. Виробник заявляє про 35 квадратних кілометрів можливого покриття – це максимальна площа, що доступна для захисту одній системі.

2.1. Аналіз готових проектних рішень

Особиста безпека людей та їх помешкання є однією з самих актуальних проблем на сьогодні. Все більше і більше людей встановлюють на роботі та вдома різноманітні охоронні та протипожежні системи, для того щоб захистити себе та своє майно [13].

Поняття безпеки дуже об'ємне та багатогранне, одним з його пріоритетних аспектів є встановлення комплексних систем кібербезпеки. Підрозділи безпеки підприємств та організацій вирішують широке коло задач, використовуючи при цьому різноманітні інформаційні технології. До найбільш розповсюджених відносять:

- системи контроля і керування доступом;
- системи відеоспостереження та відеоаналітики;
- системи охоронної та пожежної сигналізації.

Останнім часом дані системи часто об'єднують в єдиний комплекс, що називається комплексною системою кібербезпеки. Поряд з вище перерахованим також часто використовують програмно-інформаційні системи збору, аналізу та обробки інформації, необхідної для вирішення завдань, що стоять перед підрозділом безпеки.

З кожним роком все більше об'єктів створюється в ідеології інтелектуального будинку. В якому всі слабкострумові системи зв'язані одна з одною і оператор має можливість на поверхових планах бачити стан охоронної та пожежної сигналізації, контролю доступу, тепло та водо постачання, вентиляції, освітлення, та ін [13].

В Європі та Америці 30% будинків користуються системами кібербезпеки. Найбільшу долю поставок на аналізованому ринку займають компанії Philips Lighting, Honeywell, Belkin, Nest, Ecobee, MyFox, Sonos, Canary, Netatmo та D-Link.

Представимо ряд систем, які розроблені європейськими компаніями:

- комплексна система кібербезпеки Dahua Technology;
- комплексна система кібербезпеки Axis Communications;
- комплексна система кібербезпеки Motorola Solutions;
- комплексна система кібербезпеки Tiandy Technologies.

Проведемо коротку характеристику систем, що базуються на матеріалах, наданих виробниками та розробниками. Кожна з представлених системи комплексної кібербезпеки маж свої особливості, плюси і мінуси в застосуванні.

Система **Dahua Technology** призначена для збору, обробки, передачі, відображення та реєстрації сповіщень про стан шлейфів охоронної, пожежної, тривожної сигналізації, контроля і керування доступом, управління пожежною автоматикою підприємства, відеоконтрольними пристроями, інженерними системами приміщення [13].

Для організації повнофункціонального моніторингу великих територіально розподілених систем і реалізації розширеного функціоналу

керування системами побудованих на базі Dahua Technology, підключаються комп'ютери, для яких компанії розробили понад 20 видів програмного забезпечення. При цьому з'єднання внутрішньої логіки керування контролерів та мережевого управління з єдиного центру дозволяє створити той необхідний баланс централізації та децентралізації системи кібербезпеки, який забезпечує оптимальний співвідношення заданої функціональності з можливістю безперебійної роботи системи у разі виходу з ладу центрального керуючого пристрою.

Комплексна система кібербезпеки Dahua Technology дозволяє гнучко програмувати підсистеми охоронно-пожежної сигналізації. Відмінною перевагою комплексу є використання широкої номенклатури власного обладнання і датчиків. Однак жорстка прив'язка до обладнання не дозволяє використовувати пристрої інших виробників. Закритий протокол не дозволяє підключення інших пристроїв [13].

Комплексна система кібербезпеки **Axis Communications** представляє собою набір з центрального контролера, датчика руху, диму, протікання, відкриття вікон та дверей і модуль в розетку для керування пристроями. Даний комплект є стартовим набором з можливістю розширення. Зв'язок модулів здійснюється за допомогою радіоканалу. Додатково можна включити в систему датчики температури, освітленості, а також іншу модулі для керування електроприладами.

Комплекс від виробника **Motorola Solutions** побудований по принципу адресної розподіленої мікропроцесорної системи з апаратно-програмним способом інтеграції. Комплекс дозволяє об'єднати підсистему охоронно-пожежної сигналізації, відеоспостереження і контролю доступу. Роль центрального мікропроцесорного блоку виконує контролер. Система відрізняється великою надійністю, але такій системі присутня прив'язка до обладнання, закритий протокол унеможливлює підключення пристроїв від інших виробників.

Виробник **Tiandy Technologies** представив свою сучасну багатофункціональну систему для комплексної кібербезпеки підприємств. Вона має оптимальний склад та структуру, володіє широким програмно-апаратними можливостями. Модульна побудова системи, гнучкі програмні налаштування, невеликий склад обладнання та його універсальність забезпечують чудові умови для створення системи різних видів складності і вимог підприємств з урахуванням всіх особливостей [13].

2.2. Охоронна сигналізація

Датчик руху Combi Protect рис. 2.1 [14] бездротовий комбінований датчик руху і розбиття. Вдало виконує завдання захисту приміщення від вторгнення через двері та вікна, додатково контролює цілісність скла. Поєднує в собі функції двох датчиків – руху і розбиття. Виявляє рух у приміщенні на відстані до 12 м і фіксує розбиття скла на віддалі до 9 м від вікна.

Рисунок 2.1 – датчик руху Combi protect

Виявляє рух навіть у жаркому кліматі завдяки методу температурної компенсації. Фільтрує помилкові сигнали тривоги про розбиття внаслідок звуку грози, шуму вантажівки, яка проїжджає неподалік. Швидко підключається до хабу достатньо декілька кліків у мобільному додатку. Монтується за кілька хвилин завдяки кріпленню[14].

За допомогою спеціального мікрофону датчик виявляє і записує специфічні низькочастотні і високочастотні звуки, які виникли при розбитті скла. Якщо в приміщенні, в якому встановлений датчик розбивають скло, уловлює ці звуки і відправляє по бездротовому радіоканалу на центральний блок керування. За допомогою унікального багатоступінчастого аналізу, датчик виключає хибні реагування уловлюючи лише звук розбитого скла, ігноруючи інші гучні звуки.

Пристрій здатний визначити пересування людини через пасивний інфрачервоний сенсор – він вимірює рівень інфрачервоного випромінювання від об'єкта. З метою виключення помилкових спрацьовувань дані вимірювань піддають цифровій обробці [16].

Датчик може використовуватися для виявлення розбиття скла в квартирах, будинках, магазинах, офісних будівлях, готелях, ресторанах, банках, школах, студіях, на складах, тощо.

Таблиця 2.1 – Технічні параметри датчика руху Combi protect

Класифікація	сповіщувач охоронний оптико-електронний комбінований радіоканальний
Тип датчику	бездротовий
Чутливий елемент	PIR-сенсор, електретний мікрофон
Сумісність	працює с хабами Ajax, ретрансляторами, ocBridge, uartBridge
Час доставки сигналу тривоги	0,15 с
Дальність виявлення руху	до 12 метрів
Рекомендована висота встановлення	2,4 метра
Дальність визначення розбиття вікон	до 9 метрів
Кут огляду	180 °

Продовження таблиці 2.1 – Технічні параметри датчика руху Combi protect

Діапазон частот	866,0 – 866,5 МГц 868,0 – 868,6 МГц 868,7 – 869,2 МГц 905,0 – 926,5 МГц 915,85 – 926,5 МГц 921,0 – 922,0 МГц
Проти диверсійний захист	захист від підміни; повідомлення про глушіння; тампер на відкривання та відривання
Клас захисту	2
Відповідність стандартам охоронних систем ЄС	EN 50131-1:2006 / A1:2009 / A2:2017 EN 50131-2-2:2008 EN 50131-2-7-1:2012 EN 50131-2-6:2008 EN 50131-5-3:2017

Датчик відчинення DoorProtect рис.2.2 [14] бездротовий датчик відчинення надсилає повідомлення про виявлення перших ознак вторгнення у приміщення внаслідок злому дверей або вікна. Може бути встановлений на будь-який тип дверей, включно з металевою основою.

Рисунок 2.2 – бездротовий датчик відчинення DoorProtect

Бездротовий датчик відкриття дверей/вікон Ajax DoorProtect застосовується для виявлення відкриття дверей, вікон, тощо. Датчик обладнаний клемною колодкою для підключення додаткових провідних датчиків, в тому числі провідних датчиків відкриття призначених для установки на металеві ворота й люки [14].

Швидко виявляє відчинення вікон чи дверей за допомогою британського геркона hi-end, на який діє магнітне поле. Може працювати у режимі передавача, відправляючи на централь сигнал від звичайного дротового датчика. Складається з двох модулів – датчика та магніту. У комплекті є два магніти: один великий, що встановлюється на віддалі до 2 см, інший малий – до 1 см встановлюється як основний.

Вище згаданий бездротовий датчик відкриття застосовують для охорони будь-яких об'єктів. Головною перевагою датчика є легке і зручне самостійне встановлення, за допомогою кріплення що йде комплекті, для монтажу користувачеві не потрібно розбирати сам датчик [16].

Таблиця 2.2 – Технічні параметри датчика відкриття DoorProtect

Класифікація	оповіщувач охоронний точковий, магнітоконтактний, радіоканальний
Тип датчика	бездротовий
сумісність	працює з хабами Ajax, ретрансляторами, ocBridge Plus, uartBridge
Чутливий елемент	геркон
Поріг спрацьовування	малий магніт — 1 см; великий магніт — 2 см
Ресурс датчика	2 млн. відкриттів
Діапазон частот	866,0 – 866,5 МГц 868,0 – 868,6 МГц 868,7 – 869,2 МГц 905,0 – 926,5 МГц 915,85 – 926,5 МГц 921,0 – 922,0 МГц
Проти диверсійний захист	захист від підміни; повідомлення про глушіння; тампер на відкривання та відривання
Розмір	Діаметр: 20 мм Висота: 90 мм
Клас захисту	2
Відповідність стандартам охоронних систем ЄС	EN 50131-1:2006 / A1:2009 / A2:2017 EN 50131-2-6:2008 EN 50131-5-3:2017 PD 6662:2017 BS EN 50131

KeyPad рис. 2.3. [14] – бездротова сенсорна клавіатура використовується для самостійної зміни режиму охорони для комплексних систем кібербезпеки Ajax. Встановлюється безпосередньо у приміщенні біля вхідних дверей для отримання швидкого доступу до клавіатури.

Рисунок 2.3 – бездротова сенсорна клавіатура KeyPad

Може керувати усіма режимами охорони якщо введено цифровий код на клавіатурі. Має індикацію котра повідомляє про статус охорони, проблеми з датчиками чи обривання зв'язку з хабом. Присутня кнопка тривоги яка, повідомляє про кожну спробу підібрати код і автоматично блокує, у разі перевищення допустимої кількості спроб введення коду [16].

Таблиця 2.3 – Технічні параметри бездротової сенсорної клавіатури KeyPad

Класифікація	клавіатура сенсорна радіоканальна
Тип клавіатури	бездротова, сенсорна
Спосіб встановлення	всередині приміщення
Сумісність	працює тільки з хабами, ретрансляторами Ajax

Продовження таблиці 2.3 – Технічні параметри бездротової сенсорної клавіатури KeyPad

Персональний код користувача	є
Захист від підбирання коду	є
Індикація	є
Термін роботи від батареї	до 2 років
Діапазон частот	866,0 – 866,5 МГц 868,0 – 868,6 МГц 868,7 – 869,2 МГц 905,0 – 926,5 МГц 915,85 – 926,5 МГц 921,0 – 922,0 МГц
Температурний сенсор	є
Антисаботаж	захист від підміни; сповіщення про глушіння; тампер проти злому

2.3. Пожежна сигналізація

Пожежний датчик FireProtect рис.2.4 [14] бездротовий пожежний датчик із вбудованим сенсором температури, що цілодобово відстежує безпеку у приміщенні та своєчасно повідомляє про виявлення диму і різкі стрибки температури.

Рисунок 2.4 – бездротовий пожежний датчик FireProtect

Виявляє дим за допомогою спеціального фотоелементу з сенсором. Якщо горіння відбувається без явного виділення диму, додатковий сенсор фіксує різку зміну температури у приміщенні. Може працювати автономно від хабу, інформуючи про пожежну тривогу за допомогою вбудованої сирени. Кілька датчиків сигналізують про тривогу синхронно. Готовий до роботи з коробки: батарея вже встановлена, тому розбирати датчик не потрібно. [14].

Бездротовий датчик виявлення диму Ajax FireProtect застосовується для виявлення пожежі в приміщенні, що охороняється. Датчик виявляє дим за допомогою інфрачервоного випромінювача і фотоприймача. Елементи змонтовані в спеціальній димовій камері. При попаданні частинок диму в камеру, фотоприймач виявляє спотворення інфрачервоного променю. Якщо диму стає багато, спотворення променю стає сильним, датчик відправляє бездротовий сигнал про пожежну тривогу на розумну централь та включається сирена [16]. Завдяки тому, що пристрій фіксує навіть найдрібніші аерозольні частинки, що виділяються при горінні. Дозволяє моментально реагувати на виникнення вогню та сповіщати про небезпеку.

Таблиця 2.4 – Технічні параметри пожежного датчика FireProtect

Класифікація	оповіщувач пожежний; димо-тепловий; радіоканальний із вбудованою сиреною
Тип датчика	бездротовий
Сумісність	працює автономно або з хабами Ajax, ретрансляторами, ocBridge Plus, uartBridge
Чутливий елемент	фотоелектричний і температурний сенсори
Поріг спрацьовування	+59°C ±2°C
Тип сповіщувача	світлозвуковий
Гучність вбудованої сирени	85 дБ
Час доставляння сигналу тривоги	0,15 с
Фільтр хибних тривог	є
Синхронна тривога кількох датчиків	є
Діапазон частот	866,0 – 866,5 МГц 868,0 – 868,6 МГц 868,7 – 869,2 МГц 905,0 – 926,5 МГц 915,85 – 926,5 МГц 921,0 – 922,0 МГц
Протидиверсійний захист	захист від підміни; повідомлення про глушіння; тампер на відкривання та відривання
Відповідність пожежним стандартам країн ЄС	EN 14604:2005/AC:2008

2.4. Підсистема відеоспостереження

Wi-Fi відеокамера Dahua IPC-D42P IMOU рис.2.5 [16] – Бездротова купольна IP-відеокамера з роздільною здатністю 4 Мрх. Призначена для встановлення всередині приміщень.

Рисунок 2.5 – Wi-Fi відеокамера

Внутрішня купольна відеокамера 4 IMOU Dome Lite (Dahua IPC-D42P) завдяки своїм компактним розмірам та привабливому дизайну буде доречна практично скрізь, де потрібен контроль безпеки: у квартирах та приватних будинках, офісах та салонах, банках та магазинах. Відмінний функціонал та якість зйомки роблять цю модель камер IMOU однією з найпопулярніших серед споживачів [16].

Можливість використання індивідуальних видів сховища. Відеоматеріал, знятий за допомогою Dahua IPC-D42P, можна зберігати (і використовувати для подальшого перегляду) на карті пам'яті microSD об'ємом до 128 Гб, мережевих (NVR) та гібридних (XVR) цифрових відеореєстраторах Dahua, а також у сховище хмар. Головною особливістю цієї моделі IMOU можна вважати можливість одночасного запису даних відразу в три типи сховища, що дозволяє отримати одразу декілька копій в різних місцях

зберігання. Особливості підключення. Крім зв'язку з Wi-Fi-з'єднанням, можна здійснити підключення Dahua IPC-D42P до персонального комп'ютера за допомогою крученої пари через інтерфейс Ethernet RJ-45. Перегляд відео в режимі реального часу можливий за допомогою спеціальної програми. Є

Для використання додаткового функціоналу відеокамери можливе застосування мобільного та десктопного застосунку IMOU, за допомогою якого можна легко керувати камерою, дивитися потокове відео, а також переглядати архів, який можна зберігати на карті пам’яті, або в хмарному сховищі.

Привабливі дизайн. Компактний розмір і купольна форма корпусу надають 4 Мп IMOU Dome Lite візуальної легкості та можливості дуже гармонійно вписуватися в будь-який інтер'єр. До того ж така форма практично невразлива для швидкого демонтажу відеокамери, що збільшує її практичність.

Таблиця 2.5 – Технічні параметри пожежного датчика FireProtect

Матриця	1/3″ Progressive CMOS
Роздільна здатність	4 Мрх (2560×1440)
Фокусна відстань	2.8 мм
Тип об’єктиву	Фіксований
Ethernet порт	1×100 Мбіт/с
Кути огляду	H: 97 °; V: 52 °; D: 115 °
Wi-Fi	IEEE802.11b/g/n
Частота кадрів	30 кад/с
Компресія відео	H.265 / H.264
ІЧ-підсвічування	до 20 метрів
Живлення	12 В DC, 1А
Споживна потужність	5 Вт
Режим день/ніч	Є
Метод зберігання	Micro SD, Cloud, NVR

Продовження таблиці 2.5 – Технічні параметри пожежного датчика FireProtect

Вага	195 г
Мережеві інтерфейси	1 RJ45 100M
Відповідність стандартам охоронних систем ЄС	EN 50131-1:2006 / A1:2009 / A2:2017 EN 50131-3:2009 EN 50131-6:2017 EN 50131-5-3:2017 EN 50131-10:2014 EN 50136-2:2013 EN 50136-1:2016 PD 6662:2017 BS EN 50131

Блок живлення Full Energy BGW-1215 рис.2.6 [16] – Мініатюрний блок живлення для монтажу в підрозетник.

Рисунок 2.6 – блок живлення Full Energy

Мініатюрний імпульсний одноканальний блок живлення у пластиковому вологозахищеному корпусі для монтажу в підрозетник. Пристрій виробляє 12 вольт стабілізованого струму із вхідної напруги 220 В. Вихідний струм – 1.5 А.

Виконує роль джерела стабілізованого живлення для різноманітних малопотужних пристроїв систем безпеки: компонентів сигналізації, відеоспостереження, контролю доступу та ін. Підключення входу – вилка в розетку, підключення виходу – роз'єм живлення.

2.5. Мережеве обладнання

HUB Ajax рис.2.7 [14] – інтелектуальна пристрій, ключовий елемент системи комплексного кіберзахисту, розроблено для використання в приміщеннях. Пристрій конролює роботу всіх датчиків і миттєво відправляє сигнал пульт керування. Збирає інформацію про роботу датчиків у зашифрованому вигляді, аналізує дані у разі тривоги миттєво сповіщає про небезпеку власника системи і безпосередньо на пульт керування.

Рисунок 2.7 – контролер HUB Ajax

Використовує технологію Jeweller для відстеження роботи датчиків і миттєвого реагування на небезпеку. Забезпечує перехід усієї системи на «чисті» частоти під час глушіння, захищений від вірусів на програмному рівні. Налаштовується за допомогою мобільного застосунку, датчики додаються в один клік. HUB потребує доступу до мережі інтернет, для під'єднання до хмарного сервера – для налаштування, управління будь-якої точки світу, передавання повідомленнь про події та оновлення програмного забезпечення. Особисті дані користувачів та детальні логи системи зберігаються під багаторівневим захистом, обмін інформацією з хабом відбувається цілодобово через зашифрований канал [14].

До хаба можна під'єднати до 100 пристроїв. Для зв'язку використовується захищений протокол Jeweller з радіусом дії до 2 км за відсутності перешкод. Має світлову індикацію стану та фізичні роз'єми для підключення рис 2.8 [14].

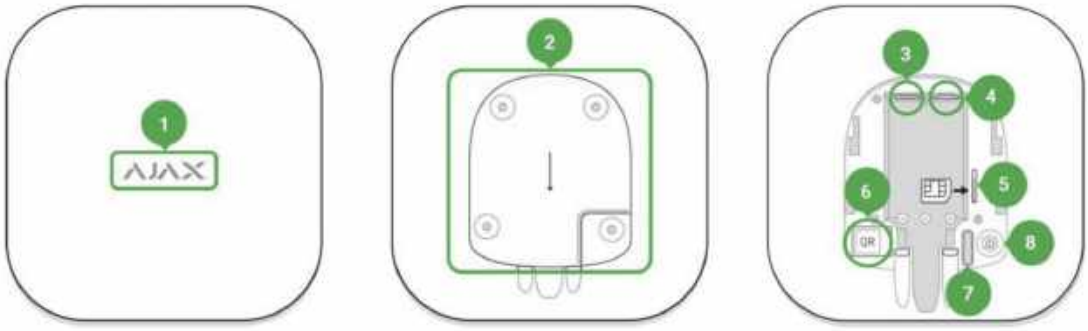

Рисунок 2.8 – роз'єми та індикація контролера HUB Ajax

1. Логотип зі світловим індикатором
2. Кріпильна панель SmartBracket. Перфорована частина необхідна для спрацьовування тампера при спробі відірвати хаб від поверхні.
3. Роз'єм підключення кабелю живлення
4. Роз'єм підключення кабелю Ethernet
5. Слот для встановлення карти стільникового оператора (формату Micro-SIM)
6. QR код

7. Кнопка тампера
8. Кнопка увімкнення / вимкнення

Таблиця 2.6 – Технічні параметри HUB Ajax

Класифікація	централь радіоканальна з модулями GSM і Ethernet
Кількість пристроїв	до 100
Кількість користувачів	до 50
Відеоспостереження	до 10 камер або відеореєстраторів
Живлення	110-240 В AC, 50/60 Гц
Акумулятор	Li-Ion 2 А·г (до 15 годин автономної роботи при неактивному Ethernet підключенні)
Протокол радіозв'язку	Jeweller
Діапазон радіочастот	866,0 – 866,5 МГц 868,0 – 868,6 МГц 868,7 – 869,2 МГц 905,0 – 926,5 МГц 915,85 – 926,5 МГц 921,0 – 922,0 МГц
Максимальна потужність радіосигналу	до 25 мВт
Дальність радіосигналу	до 2000 м (за відсутності перешкод)
Канали зв'язку	GSM 850/900/1800/1900 МГц GPRS, Ethernet
Розмір	163 × 163 × 36 мм
Вага	350 г
Процесор	ARM

Продовження таблиці 2.6 – Технічні параметри HUB Ajax

Підтримка SIM-карт	Micro SIM 2G
Операційна система	OS Malevich
Відповідність стандартам охоронних систем ЄС	EN 50131-1:2006 / A1:2009 / A2:2017 EN 50131-3:2009 EN 50131-6:2017 EN 50131-5-3:2017 EN 50131-10:2014 EN 50136-2:2013 EN 50136-1:2016 PD 6662:2017 BS EN 50131

2.6. Програмне забезпечення для проектування

SecurityProject Zone – онлайн-інструмент, призначений для оптимізації роботи монтажних організацій в процесі підготовки пропозицій у сфері систем безпеки та електрики:

- відеоспостереження;
- системи контролю та управління доступом;
- охоронна сигналізація;
- кабельні мережі;
- електрика;
- світлотехніка.
-

Зручний інструмент для створення моделі плану приміщення та розташування на ньому обладнання, системи контролю та управління доступом, охоронна сигналізація, електрика, світлотехніка, кабельні траси [17].

Доступний з будь-якої точки на планеті, немає необхідності встановлювати програму-проектувальник собі на комп'ютер – SecurityProject Zone працює онлайн в будь-якому браузері (Windows | Mac OS X | Linux). Всі створені проекти та документи надійно зберігаються у хмарному сервісі.

Обладнання від провідних постачальників в каталозі SecurityProject Zone завжди актуальна інформація щодо наявності та ціни, відомі бренди, перевірена якість. Специфікація обладнання та специфікація з'єднань автоматично сформована документація спростить процес монтажу.

Сервіс проектування являє собою функціональний графічний редактор, який складається з поля для проектування рис. 2.9 та панелі інструментів 2.10

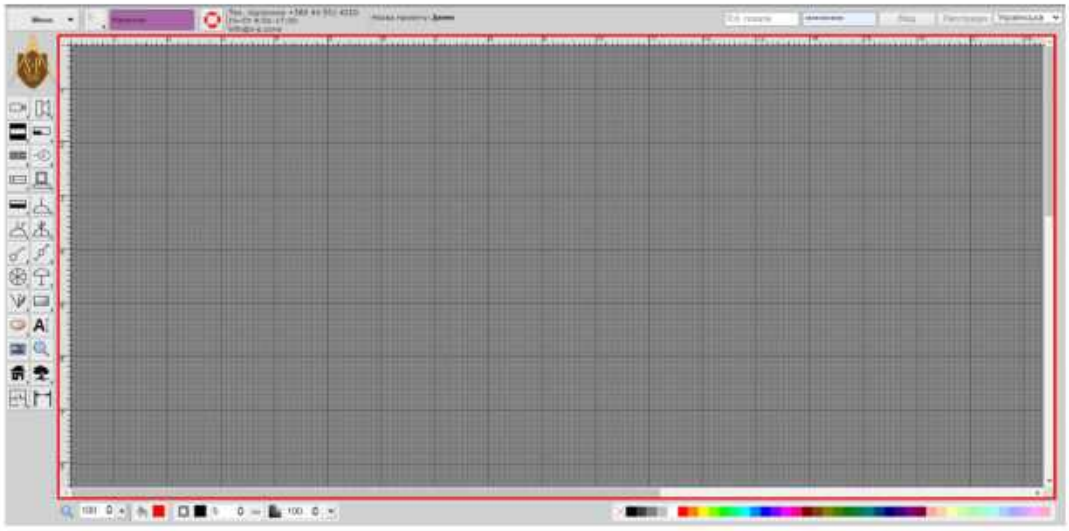

Рисунок 2.9 – поле для проектування сервісу SecurityProject Zone

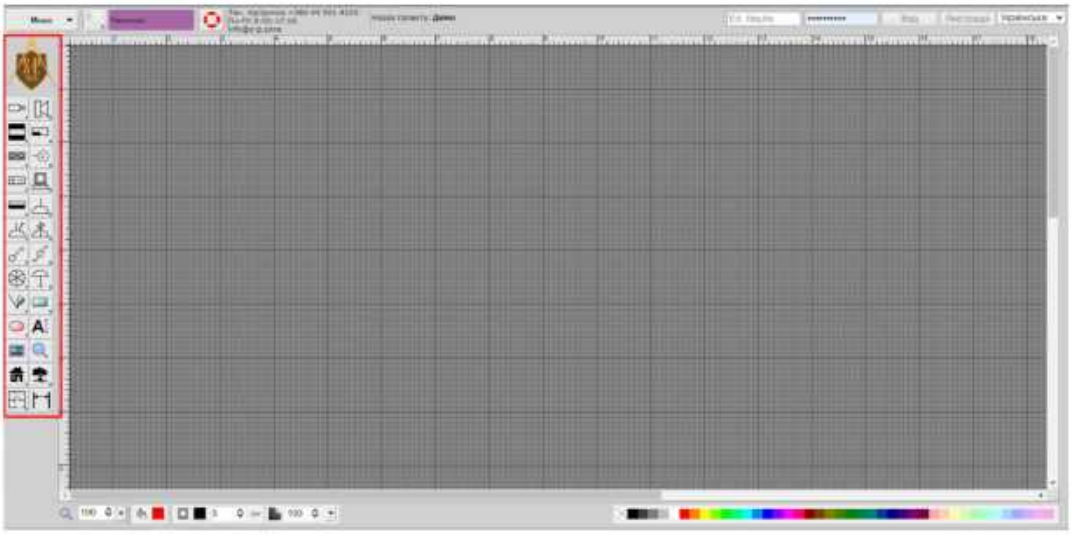

Рисунок 2.10 – панель інструментів сервісу SecurityProject Zone

Для зручного масштабування в верхній та лівій стороні поля для проектування розташована лінійка, а саме поле розділено сіткою, яка прив'язана до лінійки.

Використовуючи панель інструментів та вбудовані графічні елементи можна самостійно спроектувати систему комплексної кібербезпеки в масштабі [17].

IP Video System Design Tool – програмне забезпечення для проектування підсистем сучасного відеоспостереження. З його допомогою можна налаштувати схему розташування відеокамер.

Програма дозволяє моделювати зони огляду камер, розраховувати кути огляду та фокусну відстань об'єктивів та визначити, наскільки добре будуть помітні об'єкти спостереження. На плані приміщень/місцевості підсвічуються зони моніторингу, детекції, розпізнавання та ідентифікації людей, з урахуванням об'єктивів, що використовуються, максимальної роздільної здатності камер і їх розташування в просторі. Крім традиційних камер відеоспостереження, програма підтримує сучасні мережеві IP камери, включаючи мегапіксельні камери.

Програма дозволяє швидко оцінити вимоги до пропускної спроможності мережі та розрахувати обсяг відеоархіву.

Переваги використання IP Video System Design Tool:

- підвищення ефективності системи відеоспостереження шляхом оптимального розміщення камер.
- зниження ризику помилок за рахунок швидкого та наочного розрахунку областей видимості, кутів огляду та фокусних відстаней об'єктивів камер відеоспостереження.
- можливість миттєво оцінити різні варіанти підбору та встановлення камер з відображенням на плані приміщень зон детекції, розпізнавання та ідентифікації людей.
- можливість завантаження планів приміщень або карти місцевості у форматах JPEG, PDF, PNG, TIFF.

Створення вражаючої проектної документації - програма дозволяє друкувати проекти, експортувати їх у PDF. Отримані таблиці, креслення та результати тривимірного моделювання можуть бути легко перенесені в Word, Excel, OpenOffice, Visio та інші офісні програми.

Вбудована база даних, що оновлюється, за популярними моделями відеокамер (понад 3000 моделей).

Програма спеціально розроблена для людей що, встановлюють системи відеоспостереження, яким часто не вистачає часу, щоб вирішувати розрахункові завдання, виїжджати на об'єкт і ставити досліди на місці.

Програма проста в користуванні і при цьому має всі основні функції для планування та проектування відеоспостереження. Кінцевим замовникам програма буде корисною як для створення грамотного технічного завдання на проектування системи відеоспостереження та ескізного проекту, так і для самостійного проектування. Для вказаних параметрів установки програма показує модельоване зображення з телевізійної камери, і відображає на кресленні за допомогою різних кольорів зони огляду, в яких можливе детектування, огляд, розпізнавання або ідентифікація людини.

На першій вкладці програми «Креслення установки камери» рис.2.11 розташовано вигляд камери збоку та згори.

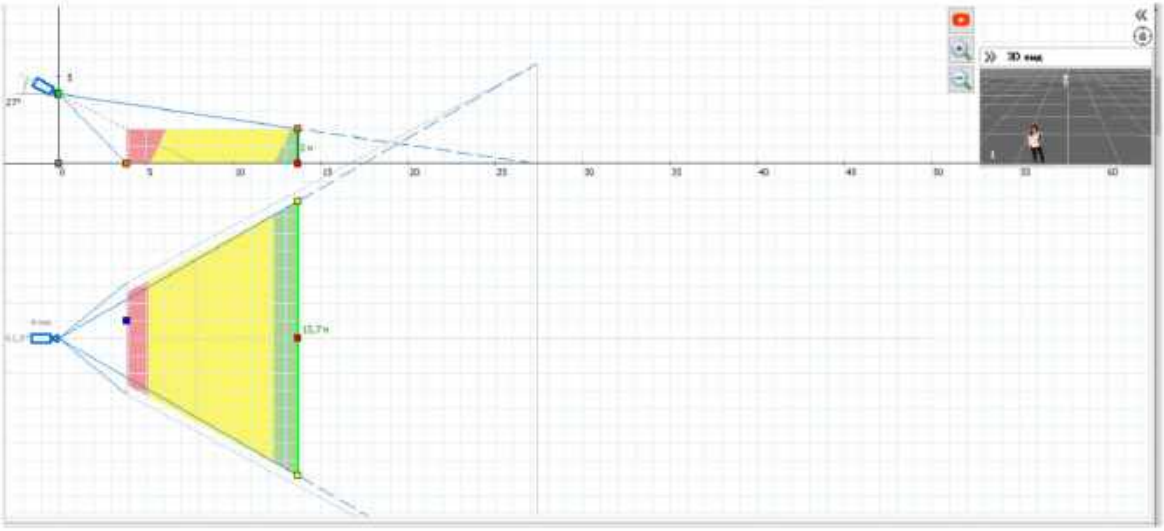

Рисунок 2.11 – вкладка «Креслення установки камери»

Користувач може змінювати висоту встановлення камери, відстань від камери до об'єкта і ширину зони огляду камери.

Під параметром зони огляду камери розташоване вікно «3D вигляд камери» рис. 2.12. Це вікно показує, що буде бачити камера. За замовчуванням у вікні розташовані два об'єкти чоловік і жінка. Ці 3D моделі показують границі зони огляду відеокамери.

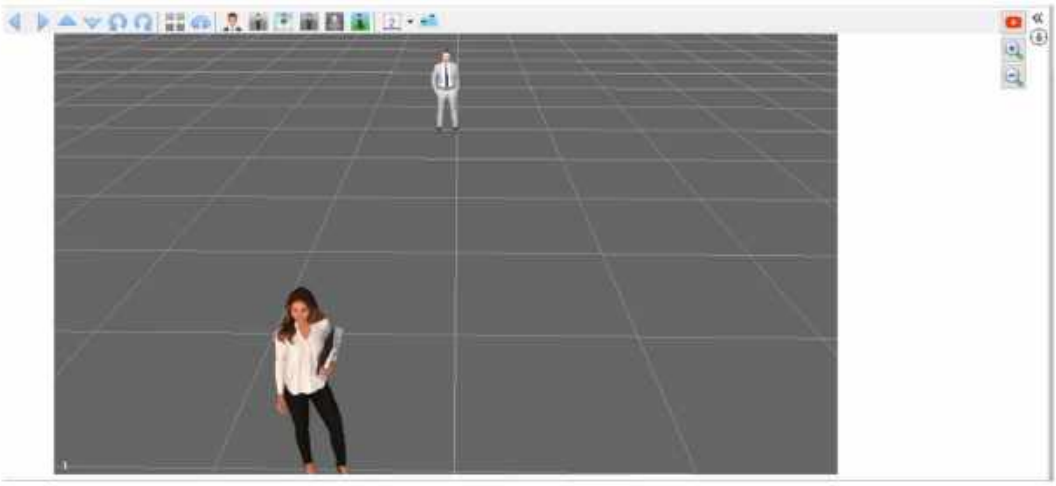

Рисунок 2.12 – вікно «3D вигляд з камери»

Тестовий чоловік розташований в кінці зони огляду камери на вказаній відстані. На вигляді збоку, прямо над камерою видно «мертву зону» камери рис. 2.13.

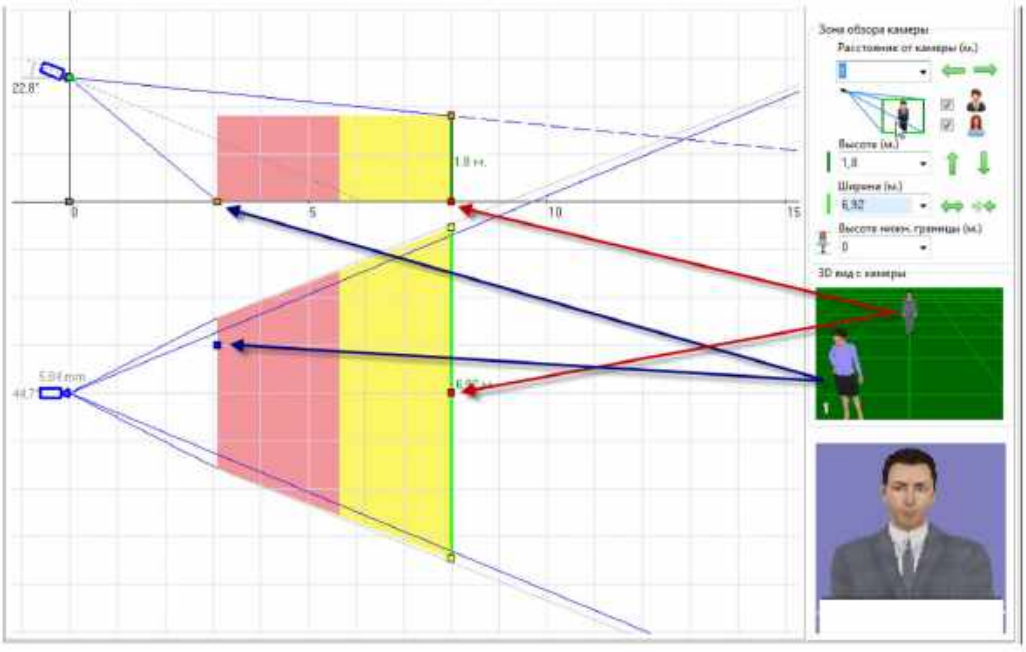

Рисунок 2.13 – зони огляду камери та «мертва зона»

Висновки до другого розділу

Даний набір пристроїв призначений тільки для одного конкретного приміщення, щоб система кіберзахисту могла забезпечити повну безпеку.

Система кібербезпеки досить складна в обладнанні, адже в ній є маса датчиків, контролерів та сенсорів, які завжди передають інформацію на керуючий пристрій, котрий в подальшому після обробки інформації передає кінцеві команди на пристрої. Система може працювати в автоматичному режимі, але завжди є інформація, яку потрібно повідомити користувачеві. Для цього використовують панель керування, або контрольну панель, використання якої дозволить користувачеві вручну керувати різними пристроями.

Будь-яка система комплексного кібербезпеки складається з різних компонентів, кожен з яких виконує властиві йому функції. В теперішній час ринок послуг кіберзахисту надає широкий спектр, як і самих технічних засобів, так і їх моделей, що мають різні технічні характеристики. В таких умовах вибір оптимальних захисних пристроїв є непростим завданням. Для вирішення якої пропонується використовувати комплексний метод визначення рівня якості, який дозволяє за чисельним значенням технічних характеристик різних моделей одного й того ж виду технічного засобу захисту, визначати у відносних одиницях їх рівень якості та порівнювати моделі між собою. Отримані результати дозволяють рекомендувати вище зазначені пристрої для проектування комплексної системи кіберзахисту.

3. ПРОЕКТУВАННЯ СИСТЕМИ КОМПЛЕКСНОЇ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА НА ОСНОВІ СТАНДАРТІВ ЄС

При побудові системи комплексної кібербезпеки необхідно керуватися наступними принципами адекватності, зональності, рівноміцності та адаптивності.

- адекватність означає відповідність прийнятим моделям загроз, в тому числі моделям порушників;
- зональність означає організацію і створення зон обмеженого доступу;
- рівноміцність означає забезпечення необхідного рівня ефективності відповідно до принципів адекватності;
- адаптивність це не що інше, як адаптованість до технологічних особливостей роботи підприємства, в тому числі в надзвичайних ситуаціях.

Принципи побудови систем комплексної кібербезпеки слугують для забезпечення ефективності захисту підприємств, тобто здатність технічних підсистем протистояти нештатним ситуаціям.

Функціонування системи кібербезпеки залежить від структури підприємства, зоною що охороняється:

- одним шлейфом охоронної сигналізації;
- одним шлейфом пожежної сигналізації;
- одним шлейфом охоронно-пожежної сигналізації;
- сукупністю шлейфів охоронної і пожежної сигналізації.

Шлейф сигналізації це – ланцюг (електричний, бездротовий, оптоволоконний) який з'єднує вихідні вузли датчиків, включаючи допоміжні(виносні) елементи та з'єднувальні лінії і призначені для передачі на приймально-контрольний пристрій від датчиків про контрольовані ними параметри, а в деяких випадках для подачі електроживлення на датчики.

Кордон охоронної сигналізації це – шлейф, або сукупність шлейфів, що контролюють охоронні зони підприємства. Під кордоном охоронної

сигналізації розуміють сукупність зон, що охороняються, котрі контролює кордон охорони.

При організації зонування об'єкту повинно забезпечуватися підсилення захисту від периферії до центру, тобто до критичних елементів, що визначають категорію підприємства. При недостатній ефективності системи кібербезпеки організовуються додаткові кордони захисту в середині існуючих зон. Властивість адаптивності систем кібербезпеки дозволяє своєчасно та гнучко враховувати динаміку потенційних та реальних загроз та небезпек для підприємства.

3.1. Обрання способу побудови системи

Враховуючи характеристики та площу приміщення, а також проаналізувавши норми та стандарти ЄС потрібно створити систему, яка буде спостерігати, швидко попереджувати та реагувати на різні загрози безпеці. Система розпізнавати конкретні ситуації, що відбуваються в приміщенні та відповідним чином на них реагувати [18].

Приміщення знаходиться в будівлі на другому поверсі «Л» корпусу Національного університету «Полтавська політехніка імені Юрія Кондратюка». Система повинна бути постійною та надійною, так як від неї залежить безпека людей та майнові втрати.

Система повинна задовольняти наступні вимоги:

- цінова доступність;
- модульність;
- нарощування (можливість додавання обладнання для розширення функціоналу системи);
- інтуїтивно зрозумілий інтерфейс, що адаптується під користувача;
- адаптованість системи (можливість підстроювання не тільки інтерфейсу, але й функціоналу системи під вимоги і особливості конкретних користувачів);
- підтримка обладнання різних виробників;

- використання відкритого програмного забезпечення;
- підтримка різних протоколів взаємодії компонентів системи;
- розвинена технічна підтримка.

Система комплексного кіберзахисту буде мати наступну класифікацію:

1. Бездротовий спосіб передачі сигналів забезпечить високу надійність всієї системи та швидку реакцію на події. Це дозволить скоротити кількість дротів, а також час та вартість на інсталяцію системи. Такий спосіб дозволяє монтувати систему в приміщеннях з готовим ремонтом і класичною проводкою [18].
2. Змішана система керування найбільш застосовувана на сьогоднішній день. Роль центрального керування виконує контролер (HUB), але інші пристрої мають вбудовані модулі керування, таким чином при виході з ладу центрального контролера всі компоненти системи переходять на ручне керування. Вона включає в себе всі переваги децентралізованої та централізованої системи, при відносно не високій вартості.
3. Протокол зв'язку Jeweller – це розроблений компанією Ajax System протокол радіозв'язку, що гарантує безперебійну взаємодію хабу та інших пристроїв системи. Працює в оптимальному для охоронного обладнання діапазоні 868,0–868,6 МГц або 868,7–869,2 МГц.

Комплексна система кібербезпеки включає в себе наступні основні елементи:

1. Підсистему відеоспостереження в рамках комплексної системи кібербезпеки, забезпечує постійний відео контроль за територією приміщення, реалізована на базі цифрових технологій. Місця встановлення відеокамер вибрані згідно завдання та з урахування наступних вимог [19]:

- оптимальність кутів огляду підконтрольних зон;
- недосяжність камер для зовнішнього втручання сторонніми особами;
- можливість здійснювати візуальний контроль приміщення.

Підсистема працює цілодобово та автоматично проводить відеозйомку контрольованої зони. Запис з частотою в діапазоні 8-25 к/с.

Централізована та має розподілену базу даних налаштувань користувачів, подій та тривоги. Є можливість пошуку матеріалів в архіві за критеріями: час, дата, подія, ескізний пошук та пошук по поміткам оператора. При розробці підсистеми відеоспостереження використали можливість підключені до мережі інтернет, що дає можливість переглядати відео з різних приладів. Кожен кадр, який записується має час і дату. Доступна можливість перегляду відео в реальному часі та експорту на відеоматеріалів обраного періоду часу на зовнішні носії, а також передачу по мережі [19].

2. Охоронна сигналізацію виконує завдання своєчасного сповіщення про факт несанкціонованого доступу до приміщення або спробі проникнення, з фіксацією дати, місця та часу. Одним із основних аспектів системи є автономність, важливо забезпечити захист в умовах відсутності основного джерела живлення. Захист від заглушення та перехвату є ще одним важливим критерієм безпечної роботи сигналізації. Зручність роботи на зрозумілий інтерфейс для всіх користувачів, систему треба вмикати і вимикати кожен день. Масштабованість та функціональність важливо розглянути ці варіанти у випадку необхідності.
3. Пожежна сигналізація, необхідно вибрати таку систему, що буде швидко сповіщати про пожежу, або задимлення приміщення при перших ознаках займання. Проаналізувавши поставлене завдання, визначено, що буде використано адресно-аналогові системи пожежної безпеки. Адресно-аналогові системи постійно контролюючи стан середовища в приміщенні, негайно виявляють зміну температури або задимленості і подають попереджувальний сигнал.

   Таким чином, застосування адресно-аналогових систем сигналізації при менших витратах на монтаж та експлуатацію дозволяють збільшити надійність контролю за пожежною ситуацією в приміщенні, а також зменшити фактичний час виявлення пожежі та пришвидшити початок її ліквідації. Це дозволяє суттєво знизити шкоду від пожежі та її гасіння.

Шлейф сигналізації – це ланцюг(електричний, бездротовий, оптоволоконний) з'єднує вихідні вузли датчиків, включаючи в себе допоміжні (виносні) елементи та з'єднувальні лінії і призначена для передачі на приймально-контрольні прилади або об'єктовий пристрій системи передачі повідомлень від датчиків про контрольовані ними параметри, а в деяких випадках, для подачі живлення на датчики [19].

Рубіж охоронної сигналізації – це шлейф або сукупність шлейфів, що контролюють зони, що охороняються системою. Під рубежом розуміють сукупність зон, що контролює система кібербезпеки.

Розробка комплексної системи кібербезпеки передбачає ретельне відпрацювання кожного елемента.

У проекті буде використане наступне обладнання:

1. HUB.
2. Пульт керування.
3. Датчики диму.
4. Датчики температури.
5. Датчик відкриття вікон та дверей.
6. Датчики руху.
7. Відеокамери.

3.2. Принцип роботи та функціональна схема системи комплексної кібербезпеки

За результатами досліджень визначено, що система повинна бути побудована на наступних принципах:

1. Наявність центрального контролера з частковою автономністю периферійних пристроїв.
2. Бездротовий інтерфейс передачі даних з можливістю підключення дротових периферійних пристроїв.
3. Проста розширюваність і підтримка багатьох виробників.

Функціональна схема системи комплексної кібербезпеки інфокомунікаційної мережі приведена на рис. 3.1.

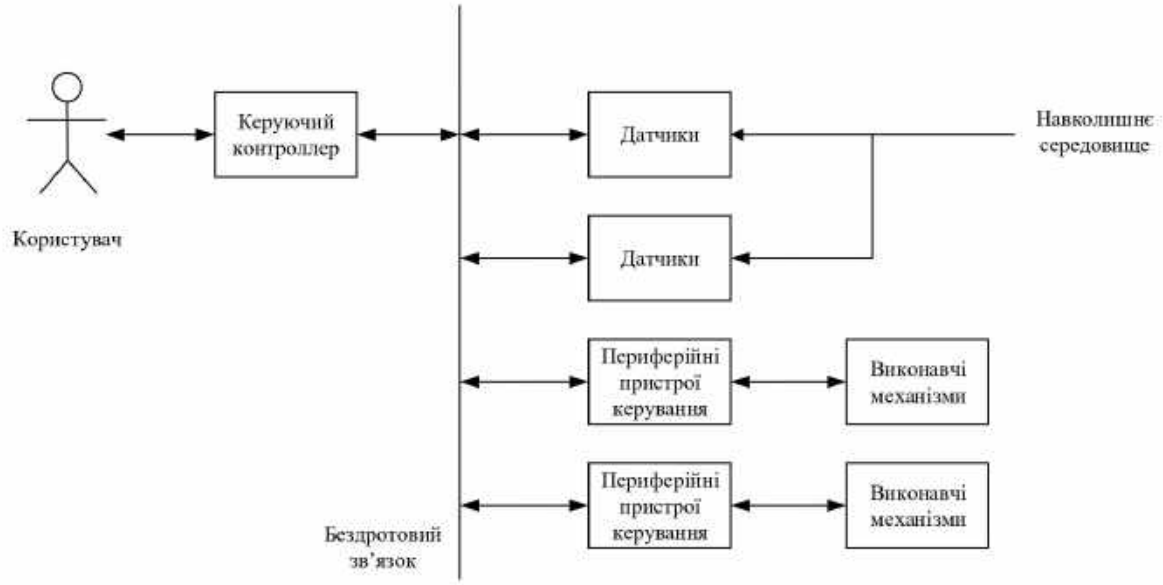

Рисунок 3.1 – Функціональна схема системи комплексної кібербезпеки

Система повинна складатися із центрального контролера та периферійних пристроїв, включаючи датчики та виконавчі механізми. Об'єднання всіх приладів в мережу повинно виконуватися за допомогою промислового інтерфейсу, так як це дає стабільність роботи та хорошу завадостійкість.

Центральний прилад системи комплексної кібербезпеки приймає тривожні та службові сигнали з датчиків, пульта керування, виконавчих блоків. Володіє можливістю передавати інформацію на пульт охоронного підприємства, або безпосередньо власнику приміщення. Контрольна панель під'єднується до електричної мережі, додатково має джерело резервного живлення – акумулятор, якого вистачає на 4-8 годин роботи.

Самотестування датчиків системи, для цього датчики мають 10 радіочастотних каналів передачі, автоматично вибір резервного каналу передачі (вільного від завад). Висока завадостійкість системи. Всі ці показники збільшують надійність системи кібербезпеки.

Приймальні пристрої здійснюють автоматичний контроль стану обладнання, допускають встановлення додаткових програм для розширення

існуючих можливостей. У випадку виявлення несправності окремих вузлів системи, пристрої подають сповіщення, що дозволяє підтримувати встановлене обладнання в робочому стані.

В стандартній дротовій системі кібербезпеки до кожного пристрою необхідно прокласти сигнальний кабель, який забезпечує передачу сигналу тривоги і опитування датчика. Окрім цього, датчикам і модулям потрібно забезпечити живлення, як правило це 12 вольт. Отже на один датчик задіяно від 3 до 4 ізольованих жил провідника [20].

В бездротових системах сигнали між датчиками, різноманітними блоками передаються по радіоканалу, а живлення забезпечується через батарейки чи акумулятор. Перед встановленням слід звернути увагу на частотний діапазон мережевого обладнання, від цього може залежати стабільність роботи та дальність зв'язку.

Проникнення сигналів радіозв'язку в значній мірі залежать від перепон, що трапляються на їх шляху. Різний тип матеріалів по різному знижує рівень сигналу. В таблиці 3.1 приведено залежність виду перепон на рівень якості зв'язку.

Таблиця 3.1 – Залежність виду перепон на якість радіосигналу

Вид матеріалу	Зниження дальності радіосигналу
Дерево, скло, вапно	0-10%
Цегла	5-35%
Залізобетон	10-90%
Метал	відбиває радіохвилі

Тому не варту сприймати вказану виробником дальність зв'язку, як абсолютну величину. Вона буде сильно залежати від архітектурних особливостей об'єкту, типів матеріалів, товщини стін.

Бездротова система кібербезпеки є одним з затребуваних видів систем безпеки. Такі системи необхідні в тих місцях, де немає можливості прокласти кабель, протягнути дроти над землею. Бездротова система може самостійно

слідкувати за своїм станом та своєчасно повідомляти про наявність запилення, або інших причин збоїв в роботі [20].

3.3. План розміщення обладнання системи

Розрахунок параметрів і місця розташування відеокамер проведений у програмі «IP Video System Design Tool», яка дозволяє знайти оптимальне місце розташування камер відеоспостереження, виконати розрахунок системи, визначити зони огляду, розташувати камери на плані приміщення.

Після створення плану приміщення в програмі «IP Video System Design Tool» в потрібних місцях були розташовані відеокамери. На основі цих вимог було проведено аналіз по пошуку оптимального відношення параметрів камери до зони покриття та якості сигналу [19].

Реальне проектування системи комплексної кібербезпеки слід починати з вибору кількості відеокамер і місць їх розташування. Варіантів розв'язання цього завдання може бути досить багато, вони відрізняються і обсягом устаткування, що використовується, і ціною. Зазвичай у цьому випадку говорять про необхідну достатність, оскільки з одного боку кількість відеокамер однозначно впливає на вартість системи, а з іншого боку, їхня кількість повинна бути не меншою за ту, яка необхідна для забезпечення заданого рівня безпеки об'єкта.

У відповідності до вимог, що висуваються системам кібербезпеки був розроблений план розміщення обладнання. При цьому враховувались технічні характеристики обладнання, конструктивні особливості будівлі.

Таблиця 3.2 – Умовні позначення обладнання

	Датчик відчинення
	Датчик руху
	Пожежний датчик
	Клавіатура
	Відеокамера
	Централь радіоканальна

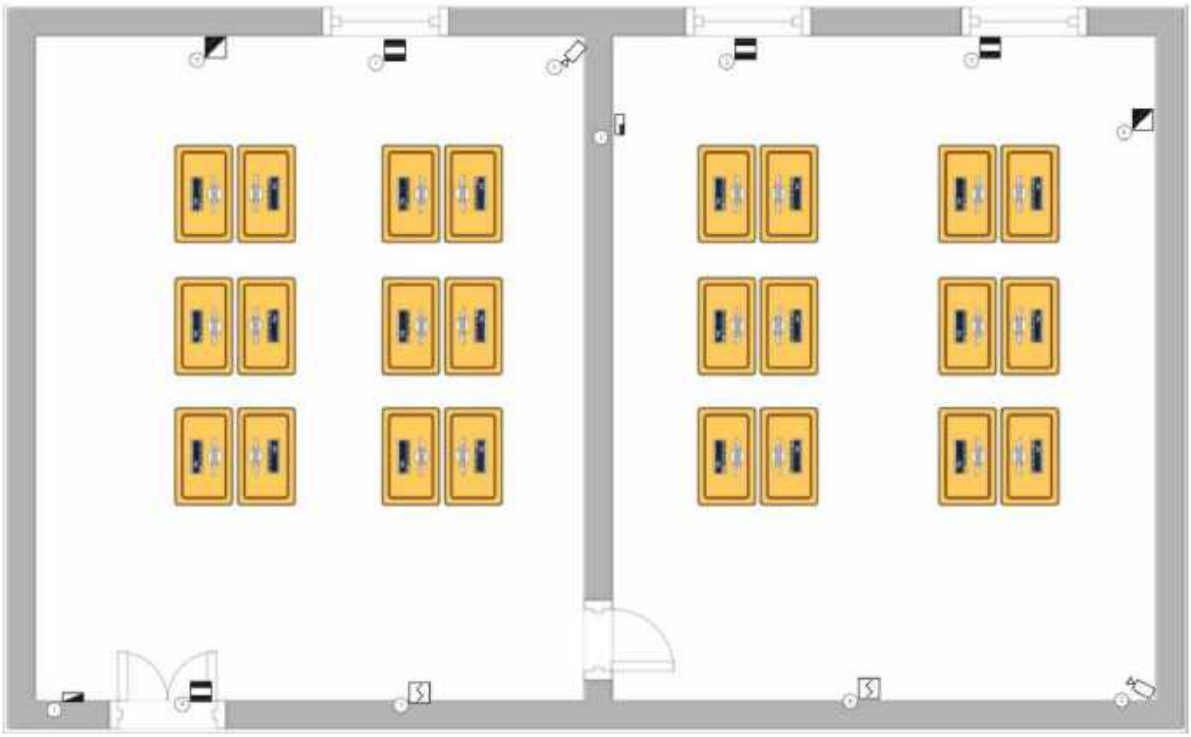

Рисунок 3.3. – План розташування обладнання комплексної системи кібербезпеки

На основі вимог того, що потрібно бачити вибираються відповідні зони відеоспостереження. Бажано щоб в поле зору камер потрапляло найбільша кількість дверей, коридорів, сходів, щоб відстежити будь-яку траєкторію руху. Для моніторингу обстановки в контрольованій зоні розмір зображення людини по вертикалі не повинен перевищувати 5% від висоти екрану, для чіткого

розпізнавання людини розмір повинен бути 10%, для впізнавання людини розмір повинен бути 50% . Далі вибираються найбільш зручні місця кріплення відеокамер це визначає ракурси відеоспостереження. При виборі місць розміщення відеокамер варто спрогнозувати вплив можливих перепон. Варто виключити потрапляння в об'єктив камери прямих джерел світла, а також відображень від утворюючих відблиски поверхонь [19].

Точка розташування відеокамери і підлягаючі відеоспостереження об'єкти утворюють сектор нагляду. Визначення оптимальної кількості таких секторів є багато варіативним завданням. Недостатня кількість відеокамер приводить до так званих «мертвих зон». Через мірна кількість відеокамер приводить до невиправданого повторення схожих зображень. Отже це веде до зростання вартості обладнання, ускладнення обладнання обробки відеосигналу, а значить до подорожчання системи.

Технічними засобами охоронно-пожежної сигналізації повинні бути обладнані всі приміщення з постійними чи тимчасовим зберіганням матеріальних цінностей, а також всі вразливі місця, через які можливий несанкціонований доступ до приміщень підприємства.

В кожному приміщенні повинно встановити не менше одного пожежного датчика, так як висота приміщення не перевищує 6 метрів максимальна відстань між датчиками не більше 9 метрів, відстань між датчиком і стіною не більше 5 метрів. Пожежні датчики рекомендується застосовувати, для оперативного локального оповіщення про місце пожежі в приміщеннях [20].

Кількість пожежних датчиків в одному приміщенні може бути будь-якою та не обмежена ніякими правилами. Однак якщо площа приміщення перевищує 10 кв.м., рекомендують встановлювати два і більше датчиків, щоб вони могли охопити як можна більшу по площі територію. Місця розміщення пожежних датчиків вибираються таким чином, щоб повітряні потоки, що проходять в приміщенні обов'язково потрапляли в зону їх дії. Ось чому зазвичай їх монтують біля вентиляційних виходів.

3.4. Розрахунок споживаної потужності та вартості системи

Розробники устаткування для систем кібербезпеки постійно вдосконалюють можливості і потенціал пристроїв та систем. Тому в якості джерела безперебійного живлення можна використовувати не лише знайомі багатьом ДБЖ, а й більш сучасні портативні джерела живлення з літієвим акумулятором чи системи накопичення енергії, здатні підтримати усю систему в робочому стані багато днів поспіль [21].

Для початку потрібно підрахувати максимальну кількість пристроїв, які будуть підключені до мережі, а також максимальну сумарну їх потужність. На підставі цих підрахунків можна визначити необхідну потужність пристрою резервування живлення – вона має бути вищою як мінімум, на 10% від підрахованої.

Сумарна споживна потужність складається з потужності яка споживається кожним окремим пристроєм, що входить до системи кібербезпеки. При чому потужність, що споживається всією системою, можна розділити на дві категорії потужність в режимі очікування і потужність в активному режимі [21].

Потужність, що споживає один датчик P_i визначається за формулою:

$$P_i = U_{\text{жив}} \cdot I_{\text{жив}} \tag{3.1}$$

де, $I_{\text{жив}}$ – струм, споживаний датчиком, А.

$U_{\text{жив}}$– величина напруги живлення, В.

Маємо для датчика руху CombiProtect

$$P_{\text{ч}} = 0{,}010 \cdot 3 = 0{,}030 \text{ Вт в режимі очікування;}$$

$$P_{\text{а}} = 0{,}012 \cdot 3 = 0{,}036 \text{ Вт в активному режимі.}$$

Маємо для датчика відчинення DoorProtect

$$P_{\text{ч}} = 0{,}008 \cdot 3 = 0{,}024 \text{ Вт в режимі очікування;}$$

$$P_{\text{а}} = 0{,}010 \cdot 3 = 0{,}030 \text{ Вт в активному режимі.}$$

Маємо для клавіатура бездротова Keypad

$$P_{\text{ч}} = 0{,}008 \cdot 3 = 0{,}024 \text{ Вт в режимі очікування;}$$

$$P_{\text{а}} = 0{,}010 \cdot 3 = 0{,}030 \text{ Вт в активному режимі.}$$

Маємо для пожежного датчика FireProtect

$$P_{\text{ч}} = 0{,}010 \cdot 3 = 0{,}030 \text{ Вт в режимі очікування;}$$

$$P_{\text{а}} = 0{,}012 \cdot 3 = 0{,}036 \text{ Вт в активному режимі.}$$

Маємо для WiFi відеокамери Dahua

$$P_{\text{а}} = 1 \cdot 5 = 5 \text{ Вт в активному режимі.}$$

Маємо для контролера HUB Ajax

$$P_{\text{ч}} = 1 \cdot 12 = 12 \text{ Вт в режимі очікування;}$$

$$P_{\text{а}} = 2 \cdot 12 = 24 \text{ Вт в активному режимі.}$$

Результати розрахунків зведені в таблицю 3.3.

Таблиця 3.3 – Потужність споживана обладнанням

Поз.	Обладнання	Режим очікування	Активний режим
		Споживана потужність, Вт	Споживана потужність, Вт
1	датчик руху	0,030	0,036
2	датчик вдічинення	0,024	0,030
3	клавіатура бездротова	0,024	0,030
4	пожежний датчик	0,030	0,036
5	WiFi відеокамера	5	
6	контролер HUB Ajax	12	24

Загальна споживана потужність розраховується за формулою:

$$P_{\Sigma} = \Sigma P_i \tag{3.2}$$

де P_{Σ} – загальна споживана потужність, Вт;

P_i – потужність споживана і-тим пристроєм, Вт.

Споживана потужність в режимі очікування дорівнює 17,108.

Споживана потужність в активному режимі дорівнює 20,132.

Визначивши максимальну потужність, можна попередньо розрахувати витрати енергії. За добу максимальні витрати в наведеному прикладі дорівнюватимуть:

$24 \cdot 17{,}108 = 410{,}592$ Ват/годин для режиму очікування

$24 \cdot 20{,}132 = 483{,}168$ Ват/годин для активного режиму

У цьому випадку варто взяти до уваги те, що реальні витрати за добу зазвичай менші, адже підсвітка камер вмикається лише при зниженні освітлення (вечір-ранок). Час роботи підсвітки також буде залежати від пори року, чим довший сонячний день – тим менші витрати енергії.

Отже, обираючи портативне джерело живлення для цієї системи відеоспостереження, нам слід звернути увагу на такі показники:

Ємність акумулятора має бути більше за 365 Вт (з деяким запасом на втрати в інверторі приладу). Задаємося ємністю не менше ніж 500 Ват/год. Номінальна потужність усіх ПДЖ значно більша ніж 91 Вт, тобто, основним критерієм вибору буде ємність АКБ та ціна пристрою.

Розрахунок вартості обладнання будемо проводити розрахунково-аналітичним методом калькулювання, який отримав найбільше поширення. Його сутність зводиться до того, що прямі витрати визначаються шляхом нормативного розрахунку, а непрямі пропорційно до прийнятої ознаки.

Ціна придбання обладнання визначається за поточними довідковими матеріалами на момент виконання кваліфікаційної роботи магістра: даними

договорів, цінами офіційного сайту виробника, та ін. Результати розрахунків приведені в таблиці 3.4.

Таблиця 3.4 – Вартість обладнання та комплектуючі системи кібербезпеки

Поз.	Назва	Кількість, *шт*	Вартість за одиницю, грн	Вартість, грн
1	Контролер	1	6 599	6 599
2	Датчик руху	2	2 299	4 598
3	Датчик відчинення	4	1 099	4 396
4	Клавіатура бездротова	1	2 299	2 299
5	Пожежний датчик	2	1 999	2 998
6	WiFi камера	2	3 936	7 872
Загальна вартість:				28 762

До переліку витрат також входять проведення монтажних робіт та доставка обладнання. Вартість монтажу враховує встановлення і налаштування системи та складає від 5 до 15 відсотків від вартості пристроїв, тобто приблизно 3000 грн.

Висновки до третього розділу

Кожне підприємство, на якому проектується система кібербезпеки є унікальним, тому кожна проектована система є продукцією одиничного виробництва, що створюється наново для кожного конкретного підприємства. Процес проектування при розробленні системи відіграє найважливішу роль, саме на цьому етапі закладаються усі необхідні якісні характеристики системи.

При проектуванні важливим питанням залишається вибір технічних засобів, з яких створюється система.

Прийняте технічне рішення ґрунтується на комплексному підході до захисту підприємства. Було розроблено структурну схему та запропоновано та обґрунтовано обладнання для її реалізації.

Спроектована охоронна система забезпечує захист від несанкціонованого проникнення об'єкт. Система включає датчики руху, датчики відкривання дверей і датчики розбиття скла, пожежний датчик. Було проведено розрахунок сигнальних рівнів та споживаної потужності. Розглянуто систему передачі сповіщень, розраховано основні параметри сигналу. Запропоновано заходи щодо збільшення перешкодозахищеності системи. Усі підсистеми взаємодіють один з одним і можуть використовувати загальні датчики.

В будь-якому випадку система є складним технічним проектом і при її створенні потрібно використовувати різне обладнання, як по функціональному призначенню, так і обладнання від різних виробників.

ВИСНОВОК

В рамках кваліфікаційної роботи магістра було розроблено систему комплексної кібербезпеки інфокомунікаційної мережі підприємства, що включає в себе підсистему відеоспостереження, охоронну та пожежну сигналізації. Викладено теоретичні та правові основи розробки систем кібербезпеки. Проведено огляд сучасних архітектур систем кібербезпеки. Розглянуто програмне та технічне забезпечення типового підприємства.

Основною метою було створення системи, яка здатна відповідати достатньому рівню захищеності матеріальних та інформаційних цінностей. Система повинна розроблятися для кожного підприємства індивідуально на основі правил, які передбачені законодавством та нормативними документами і враховувати відповідні правила монтажу та ДСТУ.

В результаті аналізу апаратного та програмного забезпечення, що представлене на ринку інформаційних технологій, розроблений оптимальний варіант системи комплексної кібербезпеки. Були розглянуто готові програмно-апаратні рішення, але ні одне з них не задовольняє вимоги. Частіше всього подібні системи орієнтовані на вирішення одної задачі, або мають достатньо високу вартість. Упор був зроблений на функції що дозволяють керувати системою дистанційно.

При виборі варіантів технічного забезпечення особлива увага приділялася їх функціональним характеристикам і технічною сумісністю пристроїв один з одним.

В результаті проектування була розроблена система комплексної кібербезпеки, яка дозволяє:

- спостерігати за робочим процесом в приміщенні;
- попереджувати про несанкціонований доступ до будівлі;
- сигналізувати про виникнення пожежі чи задимлення в приміщенні.

Система може бути легко встановлена за 30-60 хвилин. Бездротові датчики легко перенести з одного місця в інше, так як немає з'єднувальних ліній між датчиками. Отже економія в монтажі цієї системи у порівнянні з дротовою складає 30% від вартості всього обладнання. Кожен датчик або контролер енергонезалежний від інших приладів і не зв'язаний в одну загальну мережу електроживлення. Дроти ніколи не обірвуться, не потрібно шукати місце обриву шлейфа.

Виконано аналіз загроз безпеки, сформовані вимоги до розроблюваної системи, проведено порівняння особливостей, переваг та недоліків існуючих систем кібербезпеки.

В майбутньому можливий подальший розвиток системи, з метою її вдосконалення та масштабування. Такий підхід дозволить вирішити, як загальні завдання, так і задачі поставлені від конкретного користувача.

Підводячи підсумок проведеної розробки можна стверджувати, що застосування запропонованих технічних засобів дозволить підвищити безпеку інфокомунікаційної мережі підприємства та знизить ризик несанкціонованого доступу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мінін Д.С. Підходи до визначення поняття «кібербезпека» / Д.С. Мінін [Електронний ресурс]. – Режим доступу: http://istfak.org.ua/tendentsii-rozvytku-suchasnoi-systemy-mizhnarodnykh-vidnosyn-ta-svitovoho-politychnoho-protsesu/185-heopolitychna-dumka-ta-heostratehichni-protsesy-v-khkhi-st/971-pidkhody-do-vyznachennya-ponyattya-kiberbezpeka.
2. Аналогові системи відеоспостереження. – Режим доступу: https://profbez.pro/blog/analogovoe-videonabludenie/
3. Ліпкан В.А. Поняття системи забезпечення наці-ональної безпеки України / В.А. Ліпкан // Право і Без-пека. – 2003. – Т. 2. – No 4. – С. 57–60.
4. Аналогове відеоспостереження. – Режим доступу: https://crazyworldmen.livejournal.com/23917.html
5. Приймально-контрольні прилади охоронно-пожежної сигналізації. – Режим доступу: https://um.co.ua/11/11-4/11-4579.html
6. Правила улаштування електроустановок. ПУЕ.– Харків.: «Форт» – 2011 – 736 с.
7. Курок Р.О., Національна академія Служби безпеки України, ІНФОРМАЦІЙНА БЕЗПЕКА В ДІЯЛЬНОСТІ СБ УКРАЇНИ: СУЧАСНІ ПРОБЛЕМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ, [Текст]
8. Коваль З.В. Динаміка світової управлінської реакції на кіберзагрози: уроки для України / З.В. Коваль // Демократичне врядування. – 2014. – Вип. 14 [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/DeVr_2014_14_5.
9. Україні буде створена Національна система кібербезпеки, 27 січня 2016 [Електронний ресурс]. – Режим доступу: http://zaxid.net/news/showNews.do?v_ukrayini_bude_stvorena_natsionalna_sistema_kiberbezpeki&objectId=1380648.

10. Двинських В.І. Аналіз вразливостей систем охорони. Оцінки показників вразливості. Офіційний сайт охоронно-інформаціного аганства Каскад-сервіс, м.Харків. URL: http://www.tehbezpeka.com.ua/papers/papers103.php
11. Кругль Герман, Професійний відеоспостереження. Практика і технології аналогового і цифрового CCTV, 2-ге вид.: Переклад з англ. М.: Security Focus, 2010. – 640 с.
12. Гвоздек М. Довідник по техніці для відеоспостереження. Планування проектування, монтаж по технике для видеонаблюдения. [Текст] / М. Гвоздек – Техносфера, 2010. - 552 с.
13. Грайворонський М.В. Сучасні підходи до забезпечення кібернетичної безпеки/ Матеріали XVII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», НТУУ «КПІ», 2015 р., [Текст]
14. Ajax systems офіційний сайт. – Режим доступу: https://ajax.systems/ua/
15. Відеоспостереження і охоронні системи.[Електронний ресурс]. – Режим доступу: URL: http://www.install.in.ua
16. Партнер Ajax systems. – Режим доступу: https://alarm.bezpeka.systems/ua/
17. Конструктор комерційних пропозицій. – Режим доступу: https://s-p.zone/uk/
18. Відеоспостереження і охоронні системи.[Електронний ресурс]. – Режим доступу: URL: http://www.install.in.ua.
19. Загальний підхід до проектування систем відеоспостереження // Режим доступу: http://skaz.com.ua/jurnalistika/11745/index.html
20. Правила улаштування електроустановок. ПУЕ.– Харків.: «Форт» – 2017 – 736 с.
21. Як забезпечити безперебійне живлення. – Режим доступу: https://greenvision.ua/ua/blog/articles/kak-obespechit-bespereboynoye-pitaniye-dlya-videonablyudeniya

ДОДАТОК А

Специфікація обладнання

Поз.	Найменування та технічні характеристики	Код обладнання, виробу, матеріалу	Тип, марка позначення документу	Завод виробник	Одиниця виміру	Кількість
1.	Інтелектуальна централь	HUB	Контроллер	Ajax	*шт*	1
2.	Датчик руху	Combi protect	Кінцевий пристрій	Ajax	*шт*	2
3.	Датчик відчинення	Door protect	Кінцевий пристрій	Ajax	*шт*	4
4	Клавіатура бездротова	KeyPad	Кінцевий пристрій	Ajax	*шт*	1
5.	Пожежний датчик	Fire protect	Кінцевий пристрій	Ajax	*шт*	2
6.	Відеокамера	IPC-D42P IMOU	Кінцевий пристрій	Dahua	*шт*	2

ДОДАТОК Б

2. JUSTIFICATION OF THE CHOICE OF SOFTWARE AND HARDWARE

An adequate and effective level of cyber security can be provided only with the help of a comprehensive approach, which involves the targeted application of traditional organizational and technical rules for providing security on a single conceptual basis with the simultaneous search and in-depth study of new methods and means of protection.

These provisions are relevant to one degree or another for every developed country that strives to maintain internal and external security. Only the methods and means used in different states to achieve the optimal level of cyber protection differ.

Choosing an option for a complex cyber security system for any room should begin with its examination. Having determined the general characteristics of the object, it is worth analyzing the main vulnerable places along the perimeter of the object, the blocking of which, as a rule, is the first line of defense.

The selection of technical means of implementing the system was carried out on the basis of the analysis of structural and building characteristics and the purpose of the premises, taking into account the task, normative documents and EU standards, tactical and technical characteristics and the cost of equipment.

When choosing the technical means of implementing the system, the equipment and installation methods that are best suited to solving the system's tasks are taken into account.

Consideration of the interaction of equipment, the environment and potential violators is important for the correct selection of technical means necessary for the implementation of the system. The operation of the sensors is affected by the structure of the building and the premises, as well as other equipment that will be installed in the premises.

It is usually possible to identify and select appliances that will operate in given conditions, as these room conditions are defined and controlled.

Many cybersecurity devices have their own apps that allow you to control their basic functions. Other devices are more general in nature and use popular standards such as Zigbee and Z-Wave (Bluetooth wireless protocols for communicating with hubs) to control devices through an app on your phone or computer. Some devices fall into both categories: you can use both apps and a larger cybersecurity platform. However, some platforms limit the user in what devices can be connected to them. With such a large number of devices from different manufacturers, creating a system can seem like a difficult task, but like any other task, it can be simplified by breaking it down into simpler tasks. You can start with a few devices and then scale the system and add new gadgets.

Today there are many companies that manufacture equipment for cyber defense systems. Ajax Systems has been producing professional security systems for office premises and homes in Kyiv since 2011. The company's success lies in the harmonious combination of innovative solutions and technological design [A].

Their products combine engineering innovations, their own know-how and technological design. The creators of high-tech systems note that they believe in the Internet of Things and intelligent security as its basis. The company has offices not only in Ukraine, but also in the USA and Great Britain. [A]

The Ajax logo can now be found on a multi-million dollar yacht in Great Britain, on a cell tower in Bangladesh, on a railway in Switzerland, on a mushroom farm in Turkey, in museums in Denmark and South Africa, in a 19th century castle in Germany, in a hospital in the UAE and even on research station in Antarctica.

The company conquered not only the most remote corners of the planet, but also the best professionals. The Ajax Systems team already has almost 2,000 people. Among them are talented engineers and developers, strong managers with experience in global corporations. The company has formed local teams in Great Britain, Italy, France, Iberia, South Africa and is ready to conquer new heights.

They direct the main vector of their developments to remote security in Ukraine. The mentality formed in the 90s is characteristic of all post-Soviet countries, including Ukrainians – in the event of an emergency, people want

someone to come to them urgently. There is a certain element of mistrust. At home, people store and accumulate many valuable and valuable things. In our country, there are many private security companies, the state security service. If in 2019, Ajax Systems had only 20 security companies as partners, today there are more than 50-60 private companies, as well as state security police, who are Ajax partners across the country.

Ajax Systems is a rare example of a rapidly developing Ukrainian hardware company. It develops components for the cyber protection system, recognized by experts in the security industry as the best in Europe. The production of the equipment is located in Kyiv - production productivity has already reached 100,000 devices per month.

Ajax systems are completely independent, as they work on Jeweler's proprietary radio protocol. The peak communication range is 200 meters, which guarantees the normal operation of the system even in large rooms. If this is not enough, the manufacturer's arsenal includes repeaters that can always be added. With a repeater, the line-of-sight range increases to 3,800 meters. The manufacturer claims about 35 square kilometers of possible coverage - this is the maximum area that can be protected by one system.

2.1. Analysis of finished project solutions

Personal safety of people and their homes is one of the most urgent problems today. More and more people are installing various security and fire protection systems at work and at home in order to protect themselves and their property.

The concept of security is very voluminous and multifaceted, one of its priority aspects is the establishment of complex cyber security systems. Security departments of enterprises and organizations solve a wide range of problems, using various information technologies. The most common include:

- access control and management systems;
- video surveillance and video analytics systems;
- security and fire alarm systems.

Recently, these systems are often combined into a single complex, which is called a comprehensive cyber security system. In addition to the above, software and information systems are also often used to collect, analyze and process information necessary to solve the tasks facing the security unit.

Every year, more and more objects are created in the ideology of the intellectual house. In which all low-current systems are connected to each other and the operator has the opportunity to see the status of security and fire alarms, access control, heat and water supply, ventilation, lighting, etc. on the floor plans.

In Europe and America, 30% of homes use cyber security systems. Philips Lighting, Honeywell, Belkin, Nest, Ecobee, MyFox, Sonos, Canary, Netatmo and D-Link occupy the largest share of supplies in the analyzed market.

We present a number of systems developed by European companies:

- Dahua Technology comprehensive cyber security system;
- Axis Communications comprehensive cyber security system;
- Motorola Solutions comprehensive cyber security system;
- Tiandy Technologies comprehensive cyber security system.

We will conduct a brief description of systems based on materials provided by manufacturers and developers. Each of the presented comprehensive cyber security systems has its own features, pros and cons in application.

The Dahua Technology system is designed for the collection, processing, transmission, display and registration of notifications about the status of security, fire, and alarm loops, access control and management, control of the enterprise's fire automation, video monitoring devices, and engineering systems of the premises.

Computers for which the company has developed more than 20 types of software are connected to organize fully functional monitoring of large territorially distributed systems and to implement advanced control functionality of systems built on the basis of Dahua Technology. At the same time, the connection of the internal control logic of controllers and network control from a single center allows to create the necessary balance of centralization and decentralization of the cyber security system, which ensures the optimal ratio of the given functionality with the possibility

of uninterrupted operation of the system in case of failure of the central control device.

Dahua Technology's comprehensive cyber security system allows for flexible programming of security and fire alarm subsystems. A distinct advantage of the complex is the use of a wide range of proprietary equipment and sensors. However, hard hardware binding does not allow the use of devices from other manufacturers. The closed protocol does not allow the connection of other devices.

The Axis Communications comprehensive cyber security system is a set of a central controller, a motion, smoke, leak, window and door opening sensor and a plug-in module for controlling devices. This kit is a starter kit with the possibility of expansion. Modules communicate using a radio channel. In addition, it is possible to include in the system sensors of temperature, illumination, as well as other modules for controlling electrical appliances.

The complex from the manufacturer Motorola Solutions is built on the principle of an addressable distributed microprocessor system with hardware and software integration. The complex allows you to combine the security and fire alarm subsystem, video surveillance and access control. The role of the central microprocessor unit is performed by the controller. The system is very reliable, but such a system is tied to the equipment, a closed protocol makes it impossible to connect devices from other manufacturers.

The manufacturer Tiandy Technologies presented its modern multifunctional system for comprehensive cyber security of enterprises. It has an optimal composition and structure, has a wide range of software and hardware capabilities. The modular construction of the system, flexible software settings, a small inventory of equipment and its versatility provide excellent conditions for creating a system of various types of complexity and requirements of enterprises, taking into account all the features.

2.2. Security alarm

Combi Protect motion sensor fig. 2.1 [A] wireless combined motion and break sensor. Helps to protect the premises from intrusion through doors and windows, additionally controls the integrity of the glass. It combines the functions of two sensors - movement and breakdown. Detects movement in the room at a distance of up to 12 m and detects glass breakage at a distance of up to 9 m from the window.

Figure 2.1 – Combi protect motion sensor

Detects motion even in hot climates thanks to the temperature compensation method. Filters out false alarms about crashes caused by the sound of a thunderstorm, a dog barking, or the sound of a truck passing nearby. Connects to the hub in one click in the mobile application. Installs in a few minutes thanks to the SmartBracket [A].

Thanks to a special microphone, the sensor detects and registers specific low-frequency and high-frequency sounds that occur when glass is broken. If the glass is broken in the protected room, the sensor detects these sounds and sends an alarm signal via radio to the central alarm unit. Using a unique multi-stage analysis, the sensor reacts exclusively to the sound of broken glass, ignoring other loud sounds. The sensor can be used to detect broken glass in apartments, houses, shops, office buildings, hotels, restaurants, banks, schools, studios, warehouses, etc.

Table 2.1 – Technical parameters of the Combi protect motion sensor

Classification	Electro-optical combined radio channel security detector
Type of detector	Wireless
Installation method	Indoors
Compatibility	Operates with all Ajax hubs, range extenders, ocBridge Plus, uartBridge
Sensing element	PIR sensor, electret microphone
Alarm signal delivery time	0.15 s
Motion detection distance	Up to 12 m
Detection angles	Horizontal — 88.5° Vertical — 80°
Time for motion detection	From 0.3 to 2 m/s
Recommended installation height	2.4 m
Break detection distance	Up to 9 m
Detection angle	180°
Sensitivity	Adjustable, 3 levels
Frequency range	Radio frequency bands: 866.0 – 866.5 MHz 868.0 – 868.6 MHz 868.7 – 869.2 MHz 905.0 – 926.5 MHz 915.85 – 926.5 MHz 921.0 – 922.0 MHz
Protection class	2
Compliance with fire standards of EU countries	EN 50131-1:2006 / A1:2009 / A2:2017 EN 50131-2-6:2008 EN 50131-5-3:2017 PD 6662:2017

DoorProtect opening sensor Fig. 2.2 [A] wireless opening sensor reports the first signs of intrusion into the premises due to a broken door or window. It is installed on all types of doors, including those with a metal base.

Figure 2.2 – DoorProtect wireless opening sensor

The Ajax DoorProtect wireless door/window opening sensor is designed to detect the opening of doors, windows, etc. The sensor is equipped with a terminal block for connecting additional conductive sensors, including conductive opening sensors intended for installation on metal gates and hatches [A].

Detects the opening of a window or door with the help of a British hi-end reed switch, which is affected by a magnetic field. Can work in transmitter mode, sending a signal from a wired sensor to the hub. It consists of two modules - a sensor and a magnet. There are two magnets in the set: the large one is installed at a distance of up to 2 cm, the small one - up to 1 cm.

This wireless opening sensor can be used to protect any objects: apartments, private houses, cottages, offices, shops, warehouses, industrial premises, etc. The advantage of the sensor is its convenient and extremely easy independent installation with the help of a smart mount, for installation the user does not need to disassemble the sensor itself [A].

Table 2.2 - Technical parameters of the DoorProtect opening sensor

Classification	Point magnetic and contact radio channel security detector
Type of detector	Wireless
Installation method	Indoors
Compatibility	Operates with all Ajax hubs, range extenders, ocBridge Plus, uartBridge
Sensing element	Reed switch
Alarm signal delivery time	0.15 s
Activation threshold	Small magnet — 1 cm Big magnet — 2 cm
Sensor resource	2,000,000 openings
Frequency range	Radio frequency bands: 866.0 – 866.5 MHz 868.0 – 868.6 MHz 868.7 – 869.2 MHz 905.0 – 926.5 MHz 915.85 – 926.5 MHz 921.0 – 922.0 MHz
Temperature sensor	Available
Anti-sabotage	Protection against fraud Jamming detection Tamper-resistant
Dimensions	Diameter: 20 mm Height: 90 mm
Protection class	2
Compliance with fire standards of EU countries	EN 50131-1:2006 / A1:2009 / A2:2017 EN 50131-2-6:2008 EN 50131-5-3:2017

KeyPad fig. 2.3. [A] – wireless touchpad is used to change the protection mode of the Ajax security system. Installed indoors near the front door for quick access to the keyboard.

Figure 2.3 - wireless touch keyboard KeyPad

Controls security modes when entering a numeric code on the keypad. The indication informs about the status of protection, problems with sensors or loss of communication with the hub. There is an alarm button. Notifies of each attempt to pick up a code and automatically blocks if the permissible number of entries is exceeded.

Continuation of table 2.3 - Technical parameters of the KeyPad wireless touch keyboard

Table 2.3 – Technical parameters of the wireless touch keyboard

Classification	Radio channel touch keypad
Type of detector	Wireless, touch
Installation method	Indoors
Compatibility	Operates with all Ajax hubs, range extenders, ocBridge Plus, uartBridge
Duress code	Yes
User Passcode	Yes
Protection against code guessing	Yes

Arming/disarming indication	Yes
Frequency range	Radio frequency bands: 866.0 – 866.5 MHz 868.0 – 868.6 MHz 868.7 – 869.2 MHz 905.0 – 926.5 MHz 915.85 – 926.5 MHz 921.0 – 922.0 MHz
Temperature sensor	Yes
Anti-sabotage	Protection against fraud Jamming detection Tamper-resistant
Dimensions	Diameter: 20 mm Height: 90 mm
Protection class Remote setting and testing	Yes
Compliance with fire standards of EU countries	EN 50131-1:2006 / A1:2009 / A2:2017 EN 50131-2-6:2008 EN 50131-5-3:2017 PD 6662:2017 BS EN 50131

2.3. Fire alarm

FireProtect fire detector Fig. 2.4 [A] wireless fire detector with a temperature sensor monitors indoor safety 24 hours a day and instantly reports the appearance of smoke and sudden temperature spikes.

Figure 2.4 – FireProtect wireless fire sensor

Detects smoke using a camera with a photoelectric sensor. If the combustion occurs without the release of smoke, an additional sensor detects the increase in temperature in the room. Can work autonomously from the hub, notifying of a fire alarm with the help of a built-in siren. Several sensors signal an alarm synchronously. Ready to work out of the box: the battery is already installed, so there is no need to disassemble the sensor. Connects to the hub in one click in the mobile application. Installs in a few minutes thanks to the SmartBracket [A].

Ajax FireProtect wireless smoke detection sensor is designed to detect fire in a protected room. The sensor detects smoke using an infrared emitter and a photoreceptor. The elements are mounted in a special smoke chamber. When smoke particles enter the camera, the photo receiver detects the distortion of the infrared beam. If there is a lot of smoke, the beam distortion becomes strong, the sensor sends a wireless fire alarm signal to the smart center and the siren [A] is activated.

The sensor is used to detect smoke in a house, shop, hotel, restaurant, office building, school, bank, library, warehouse, etc.

Table 2.4 - Technical parameters of the FireProtect fire sensor

Classification	Radio channel smoke detector with temperature sensor and built-in siren
Type of detector	Wireless
Installation method	Indoors

Compatibility	Operates with all Ajax hubs, range extenders, ocBridge Plus, uartBridge
Sensing element	Photoelectric and temperature sensors
Activation threshold	+59°C ±2°C
Type of notification	Sound/light
Volume of built-in siren	85 dB
Alarm signal delivery time	+
False alarm filter	+
Frequency range	Radio frequency bands: 866.0 – 866.5 MHz 868.0 – 868.6 MHz 868.7 – 869.2 MHz 905.0 – 926.5 MHz 915.85 – 926.5 MHz 921.0 – 922.0 MHz
Anti-sabotage	Protection against fraud Jamming detection Tamper-resistant
Compliance with fire standards of EU countries	EN 14604:2005/AC:2008

2.4. Video surveillance subsystem

Indoor dome video camera 4 IMOU Dome Lite (Dahua IPC-D42P) thanks to its compact size and attractive design will be appropriate almost everywhere where security control is needed: in apartments and private houses, offices and salons, banks and shops. Excellent functionality and shooting quality make this IMOU camera model one of the most popular among consumers [A].

Figure 2.5 – Wi-Fi video camera

The possibility of using individual types of storage. Video footage captured with the Dahua IPC-D42P can be stored (and used for later viewing) on a microSD memory card up to 128 GB, Dahua network (NVR) and hybrid (XVR) digital video recorders, as well as cloud storage. The feature of this IMOU model can be considered the possibility of simultaneously recording data in three types of storage at once. Connection features. In addition to Wi-Fi connection, you can connect the Dahua IPC-D42P to a personal computer using a twisted pair via an Ethernet RJ-45 interface. Video viewing in real time is possible using a special program. Attractive design. The compact size and dome shape of the case give the 4 MP IMOU Dome Lite visual lightness and the ability to fit very harmoniously into any interior. In addition, this form is practically invulnerable to quick dismantling of the video camera, which increases its practicality.

Table 2.5 – Technical parameters of the Dahua WiFi video camera

Matrix	1/3″ Progressive CMOS
Resolution	4 Mpx (2560×1440)
The focal length	2.8 mm
Ethernet port	1×100 Mbit/c
Viewing angles	H: 97 °; V: 52 °; D: 115 °
Wi-Fi	IEEE802.11b/g/n
The frame rate	25 fps
Video compression	H.265 / H.264
IR illumination	up to 20 meters
Power supply	12 B DC, 1A
Power consumption	5 W
Weight	195 g
Compliance with the standards of EU security systems	EN 50131-1:2006 / A1:2009 / A2:2017 EN 50131-3:2009 EN 50131-6:2017 EN 50131-5-3:2017 EN 50131-10:2014 EN 50136-2:2013 EN 50136-1:2016 PD 6662:2017 BS EN 50131

2.5. Network equipment

HUB Ajax Fig. 2.7 [A] is an intelligent device, a key element of a complex cyber protection system, designed for indoor use. The device monitors the operation of all sensors and instantly sends a signal to the control panel. Collects information about the operation of sensors in an encrypted form, analyzes the data in the event

of an alarm, instantly notifies the system owner of the danger and directly to the control panel.

Figure 2.7 – HUB Ajax controller

Uses Jeweler technology to monitor the operation of sensors and quickly react to danger. Transfers the entire system to clean frequencies during jamming is protected from viruses at the software level. Configured using a mobile application, sensors are added in one click. HUB requires access to the Internet, to connect to a cloud server - for configuration, management from anywhere in the world, transmission of event notifications and software updates. Personal data and detailed logs of system operation are stored under multi-level protection, information exchange with the hub takes place around the clock through an encrypted channel [A].

Up to 100 Ajax devices can be connected to the hub. The secure Jeweler protocol is used for communication between devices with a range of up to 2 km in the absence of interference. It has a light indication of the status and physical connectors for connecting Fig. 2.8 [A].

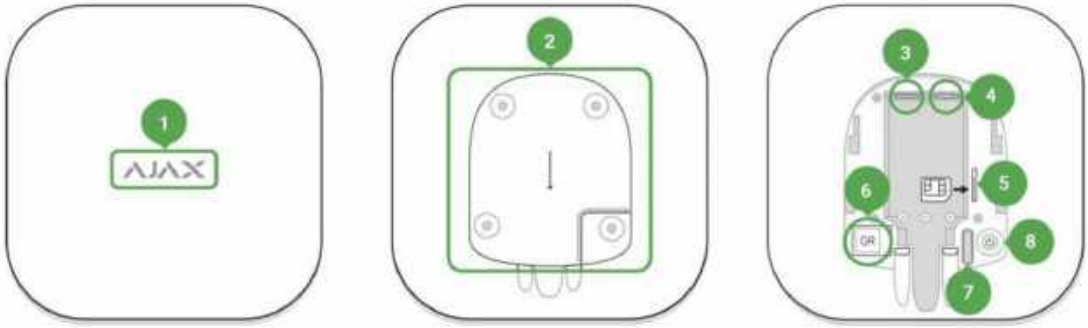

Figure 2.8 - connectors and indication of the HUB Ajax controller

1. Logo with a light indicator

2. SmartBracket mounting panel. The perforated part is necessary for triggering the tamper when trying to tear the hub from the surface.

3. Power cable connection connector

4. Ethernet cable connection connector

5. Slot for installing a cellular operator card (Micro-SIM format)

6. QR code

7. Tamper button

8. On / off button

Table 2.6 – Technical parameters of HUB Ajax

Classification	The radio channel central unit with GSM and Ethernet modules
Installation	Indoors
Connected device	100
Users	50
Communication channels	Ethernet, GSM (850/900/1800/1900 MHz)
Processor	ARM
Power supply	110-250 V from mains or 12 V Built-in back-up battery: Li-Ion 2 A·h
Frequency range	Radio frequency bands:

	866.0 – 866.5 MHz 868.0 – 868.6 MHz 868.7 – 869.2 MHz 905.0 – 926.5 MHz 915.85 – 926.5 MHz 921.0 – 922.0 MHz
Anti-sabotage	Protection against fraud Jamming detection Tamper-resistant
Video surveillance	Up to 10 cameras or DVRs
Compliance with the standards of EU security systems	EN 50131-1:2006 / A1:2009 / A2:2017 EN 50131-3:2009 EN 50131-6:2017 EN 50131-5-3:2017 EN 50131-10:2014 EN 50136-2:2013 EN 50136-1:2016 PD 6662:2017 BS EN 50131

2.6. Design software

SecurityProject Zone is a unique online solution designed to optimize the work of trade and installation organizations in the process of preparing commercial offers in the field of security and electrical systems:

- video surveillance;
- access control and management systems;
- security alarm system;
- cable networks;
- electricity;

- lighting equipment.

A convenient tool for creating an object plan and placing on it video surveillance equipment, access control and management systems, security alarms, electricity, lighting, cable routes [Z].

Online access from anywhere on the planet where the Internet is available, there is no need to install a designer program on your computer - SecurityProject Zone works online in any browser (Windows | Mac OS X | Linux). And all created projects and documents are securely stored in the cloud server.

Equipment from leading suppliers in the SecurityProject Zone catalog always has up-to-date information on availability and prices, well-known brands, proven quality. A presentable commercial offer of the project (including an estimate, your contact details and a logo) is generated by the system automatically in Excel-document format according to the equipment placement plan, it remains only to print it and hand it to the Customer or send it by e-mail. Equipment specification and connection specification automatically generated documentation will simplify the installation process.

The design service is a functional graphic editor, which consists of a design field in Fig. 2.9 and a toolbar in Fig. 2.10.

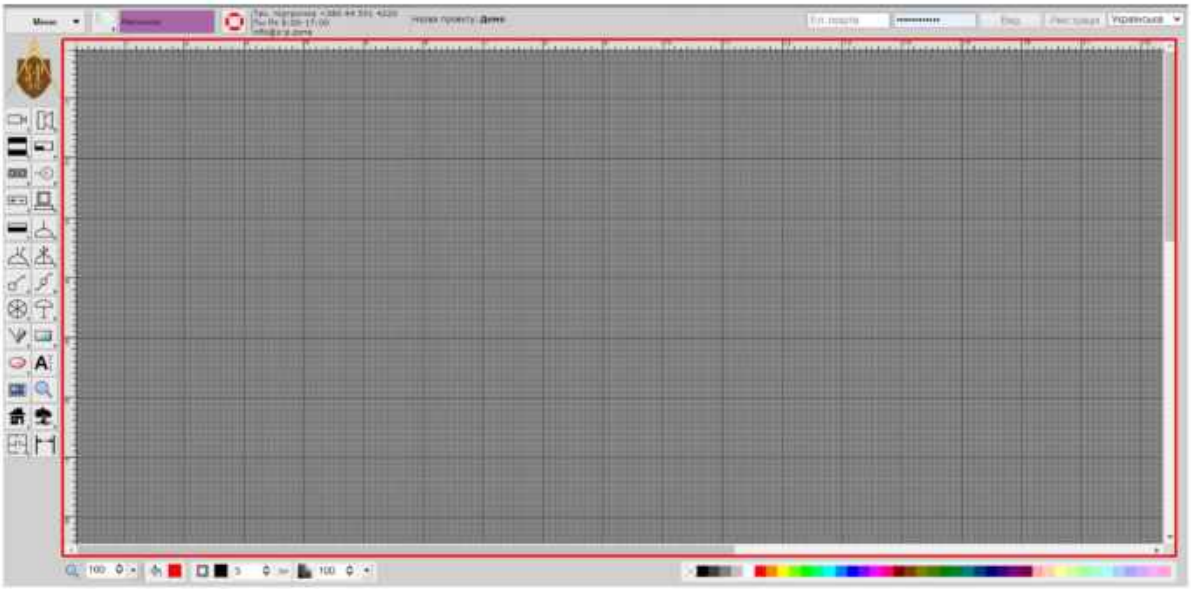

Figure 2.9 – field for designing the SecurityProject Zone service

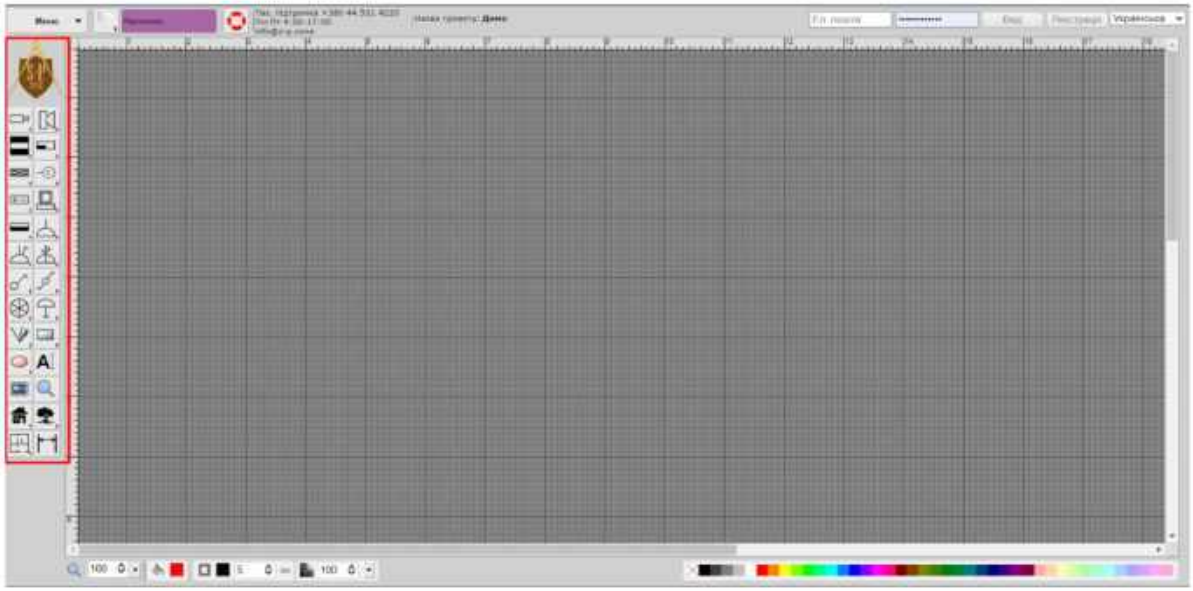

Figure 2.10 – SecurityProject Zone service toolbar

For convenient scaling, there is a ruler on the upper and left side of the design field, and the field itself is divided by a grid that is attached to the ruler.

Using the toolbar and built-in graphic elements, you can independently design a comprehensive cyber security system at scale.

IP Video System Design Tool – software for designing subsystems of modern video surveillance. With its help, you can adjust the layout of video cameras.

The program allows you to model the viewing areas of the cameras, calculate the viewing angles and focal length of the lenses, and determine how well the surveillance objects will be visible. On the premises/location plan, the zones of monitoring, detection, recognition and identification of people are highlighted, taking into account the lenses used, the maximum resolution of the cameras and their location in space. In addition to traditional video surveillance cameras, the program supports modern network IP cameras, including megapixel cameras.

The program allows you to quickly assess the network bandwidth requirements and calculate the volume of the video archive.

Advantages of using IP Video System Design Tool:

- increasing the effectiveness of the video surveillance system through optimal placement of cameras.

- reducing the risk of errors due to quick and visual calculation of visibility areas, viewing angles and focal lengths of surveillance camera lenses.

- the ability to instantly evaluate various options for selecting and installing cameras with the display on the floor plan of the areas of detection, recognition and identification of people.

- the ability to download room plans or area maps in JPEG, PDF, PNG, TIFF formats.

Creating impressive project documentation - the program allows you to print projects, export them to PDF. The obtained tables, drawings and results of three-dimensional modeling can be easily transferred to Word, Excel, OpenOffice, Visio and other office programs.

Built-in, updated database of popular video camera models (over 3000 models).

The program is specially designed for people who install video surveillance systems, who often do not have enough time to solve calculation tasks, go to the object and conduct experiments on site.

The program is easy to use and at the same time has all the basic functions for planning and designing video surveillance. The program will be useful to end customers both for creating a competent technical task for the design of a video surveillance system and a sketch project, as well as for independent design. For the specified installation parameters, the program shows a simulated image from a television camera, and displays on the drawing with the help of different colors the viewing area, in which detection, inspection, recognition or identification of a person is possible.

On the first tab of the "Camera Installation Drawing" program, Fig. 2.11 shows the side and top view of the camera.

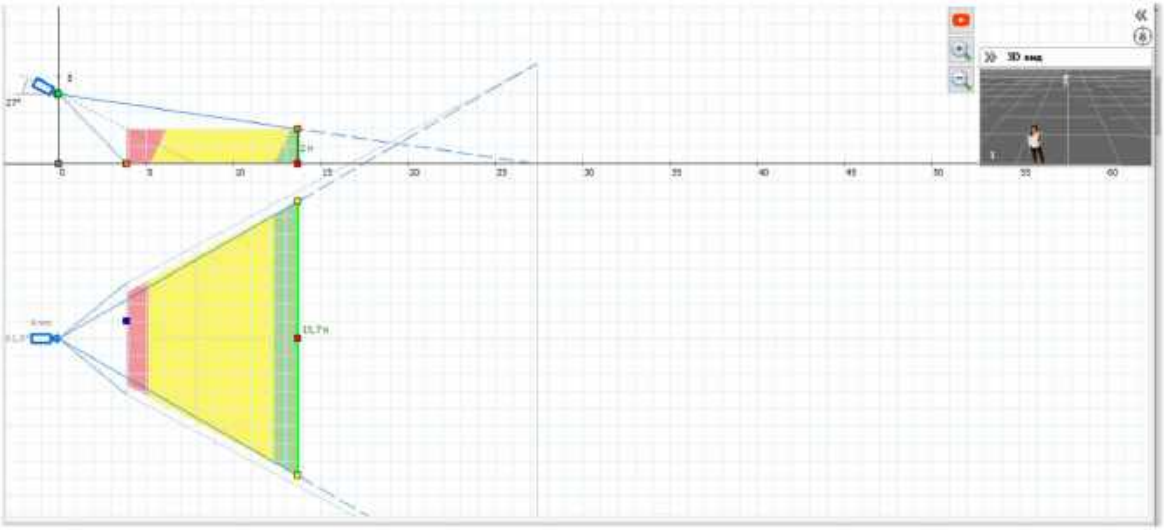

Figure 2.11 – "Camera installation drawing" tab

The user can change the height of the camera installation, the distance from the camera to the object, and the width of the camera's field of view.

Under the parameter of the camera viewing area, there is a window "3D view of the camera" Fig. 2.12. This window shows what the camera will see. By default, the window contains two objects, a man and a woman. These 3D models show the boundaries of the video camera's field of view.

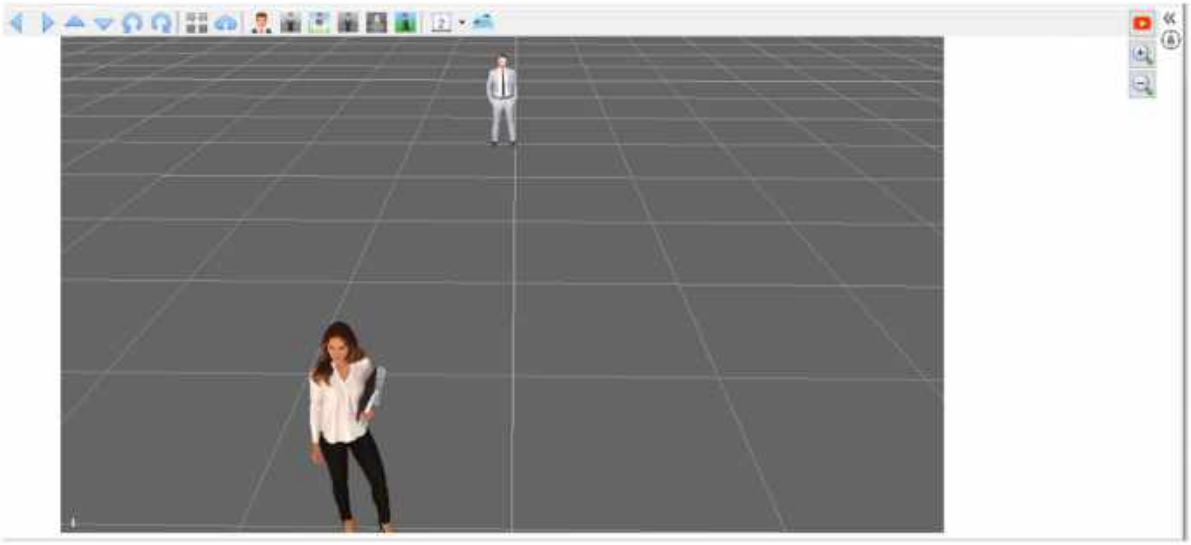

Figure 2.12 – "3D view from the camera" window

The test man is located at the end of the viewing area of the camera at the indicated distance. On the side view, directly above the camera, you can see the "dead zone" of the camera, Fig. 2.13. The female test model is located at the end of the "dead zone" and at the very beginning of the camera's visibility zone.

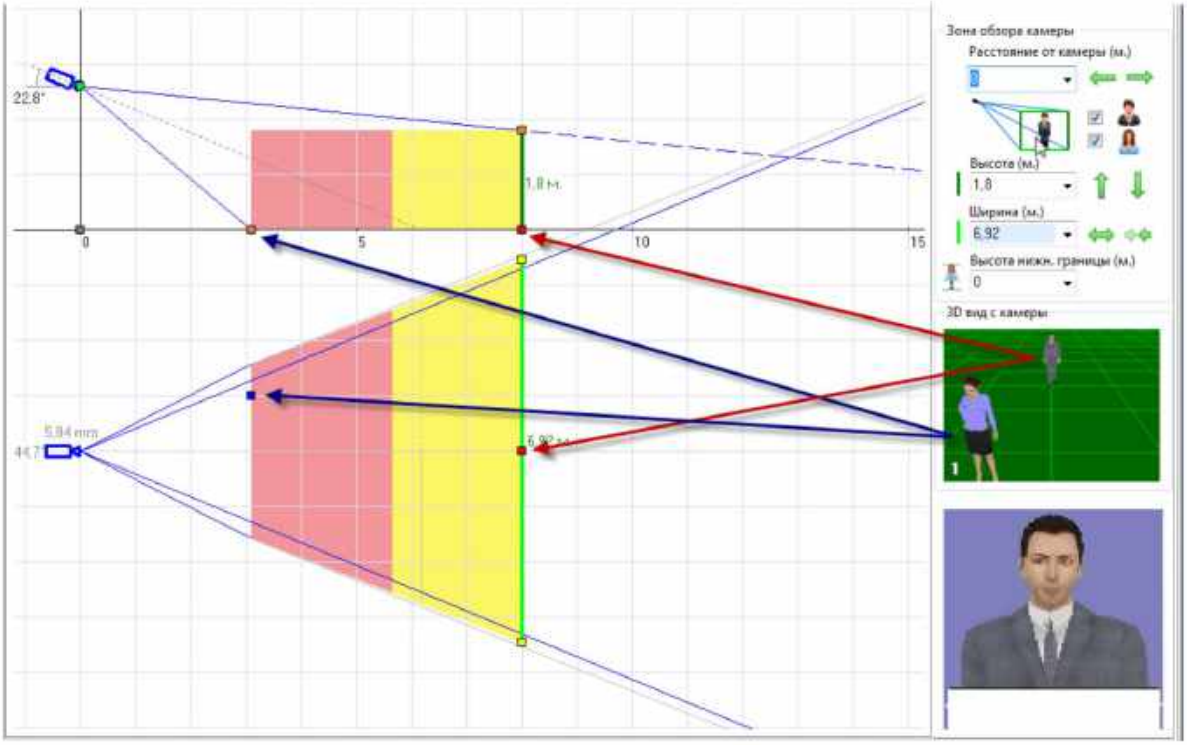

Figure 2.13 – camera viewing areas and "dead zone"

Conclusions to the second chapter

This set of devices is intended only for one specific room, so that the cyber protection system can provide complete security.

The cyber security system is quite complex in terms of equipment, because it has a lot of sensors, controllers and sensors that always transmit information to the control device, which, after processing the information, transmits the final commands to the device. The system can work in automatic mode, but there is always information that needs to be communicated to the user. For this, a control panel or control panel is used, the use of which will allow the user to manually control various devices.

Any system of comprehensive cyber security consists of various components, each of which performs its own functions. Currently, the market of cyber protection services provides a wide range of both the technical means themselves and their models with different technical characteristics. In such conditions, the choice of optimal protective devices is a difficult task. To solve it, it is proposed to use a complex method of determining the level of quality, which allows, based on the

numerical value of the technical characteristics of different models of the same type of technical means of protection, to determine their quality level in relative units and to compare the models with each other. The obtained results allow us to recommend the above-mentioned devices for the design of a comprehensive cyber protection system.

ДОДАТОК В

АПРОБАЦІЇ ТА ПУБЛІКАЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами VIII Всеукраїнської науково-практичної конференції

«ЕЛЕКТРОННІ ТА МЕХАТРОННІ СИСТЕМИ:
ТЕОРІЯ, ІННОВАЦІЇ, ПРАКТИКА»

04 листопада 2022 року

Полтава 2022

УДК 004.89 + 681.51

Збірник наукових праць за матеріалами VIII Всеукраїнської науково-практичної конференції «Електронні та мехатронні системи: теорія, інновації, практика», 4 листопада, 2022 р. / Національний університет «Полтавська політехніка імені Юрія Кондратюка».

Редколегія: О.В. Шефер (головний редактор) та ін. – Полтава: НУ «Полтавська політехніка імені Юрія Кондратюка», 2022. – 100 с.

У збірнику представлені результати наукових досліджень та розробок в області сучасних електромеханічних систем та автоматизації, електричних машини і апаратів, моделювання та методів оптимізації, енергозбереження в електромеханічних системах, управління складними технічними системами, проблем аварійності та діагностики в електромеханічних системах та електричних машинах, інформаційно-комунікаційних технологіях та засобах управління. Призначений для наукових й інженерно-технічних працівників, аспірантів і магістрів.

Матеріали відтворено з авторських оригіналів та рекомендовано до друку VII Всеукраїнської науково-практичної конференції «Електронні та мехатронні системи: теорія, інновації, практика». Редакція не обов'язково поділяє думку автора і не відповідає за фактичні помилки, яких він припустився.

Відповідальний за випуск - д.т.н., професор О.В. Шефер.

Редакційна колегія:

О.В. Шефер – головний редактор, доктор технічних наук, професор, завідувач кафедри автоматики, електроніки та телекомунікацій Національного університету «Полтавська політехніка імені Юрія Кондратюка»;

Н.В. Єрмілова – кандидат технічних наук, доцент кафедри автоматики, електроніки та телекомунікацій Національного університету «Полтавська політехніка імені Юрія Кондратюка»;

С.Г. Кислиця – кандидат технічних наук, доцент кафедри автоматики, електроніки та телекомунікацій Національного університету «Полтавська політехніка імені Юрія Кондратюка»

Б.Р. Боряк – кандидат технічних наук, доцент кафедри автоматики, електроніки та телекомунікацій Національного університету «Полтавська політехніка імені Юрія Кондратюка».

ЗМІСТ

УДК 621.391

***Г.В. Сокол**, к.т.н., доцент,*
***А.С. Міщенко**, магістрант*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

АНАЛІЗ НОРМАТИВНО-ПРАВОВИХ ТА ОРГАНІЗАЦІЙНИХ ОСНОВ СИСТЕМ КІБЕРБЕЗПЕКИ КРАЇН ЄС

Проаналізувавши системи кібербезпеки провідних країн світу можна зробити висновок, що на сьогоднішній день не існує уніфікованої моделі побудови національної системи кібербезпеки. Наприклад, відповідно до прийнятого 25 листопада 2002 року комплексного нормативно-правового акту у сфері безпеки – закону «Про внутрішню безпеку» (Homeland Security Act of 2002) – урядові структури, які займались забезпеченням комп'ютерної безпеки, перейшли під контроль цього новоствореного відомства. Даний закон, також посилив відповідальність за комп'ютерні злочини (включаючи кримінальну відповідальність), зобов'язав інтернет-провайдерів надавати інформацію про клієнтів за вимогою правоохоронних органів, розширив права останніх щодо можливості перехоплення інформації (прослуховування телефонних переговорів і перлюстрацію електронних повідомлень) без дозволу суду, визначив основні напрями діяльності федеральних органів з підвищення ефективності захисту критичної інфраструктури США від кібератак, у тому числі об'єктів стратегічного значення, що перебувають у приватній власності [1].

Одним з перших сучасних правових актів, що регламентують діяльність європейських країн по підтримці та підвищенню рівня кібербезпеки є Директива про безпеку мережевих та інформаційних систем прийнята Європейським парламентом 6 червня 2016 року [2].

Директива висуває вимоги до всіх 28 членів Євросоюзу. Уряд кожної країни буде зобов'язаний дотримуватись зазначених у ній вимог і створити власний центр реагування на інциденти, пов'язані з комп'ютерною безпекою (CERT), а також центр дотримання директиви в кожній державі.

Даний нормативно-правовий документ визначає стратегію розвитку кібербезпеки, зобов'язує країни члени Євросоюзу приймати заходи по інформаційно технічному забезпеченню національних органів кібербезпеки, їх своєчасному реагуванню за кіберзагрози та кіберінциденти.

Влада Європейського союзу приділяє значну увагу координації діяльності в різноманітних напрямках кібербезпеки. Для вивчення, аналізу та оцінки досвіду протидії кіберзагрозам, вирішення кіберінцидентів створена спеціалізована комплексна плафторма [3].

Стандарт TS 103645 був анонсований Технічним комітетом з кібербезпеки Європейського інституту телекомунікаційних стандартів. Стандарт встановлює базовий рівень захисту для пристроїв, підключених до інтернету, чи то пристрої системи кібербезпеки, чи мобільні гаджети. Крім того, на основі TS 103645

розробники планують впровадити схеми сертифікації, які допоможуть захистити особисті дані користувачів [4].

Таким чином, приходимо до висновку що, розробка стандартів кібербезпеки – важливий крок на шляху до правової нормалізації всієї сфери інтернету речей. На сьогоднішній день персональні дані користувачів IoT-пристроїв залишаються незахищеними, тоді як сама сфера застосування подібних пристроїв зростає. Інша проблема – початкова непристосованість продуктів до "розумного" використання, коли пристрої мають конструктивні особливості, що не дозволяють використовувати стандарти захисту.

ЛІТЕРАТУРА:

1. Council of Europe (2001). Budapest Convention on Cybercrime, ETS No 185, open for signature 23 November, entry into force 1 July 2004. Available at: https://www.coe.int/en/web/conventions/fulllist//conventions/rms/0900001680081561 (accessed 20 April 2020).

2. Gov.UK (2016). National Cyber Security Strategy 2016–2021. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (accessed 9 March 2020).

3. Harrison Dinniss A. (2018) The Threat of Cyber Terrorism and What International Law Should (Try To) Do About It. Georgetown Journal of International Affairs, vol. 19, pp. 43–50. Available at: https://doi.org/10.1353/ gia.2018.0006.

4. International Telecommunications Union (ITU) (2008). Overview of Cybersecurity, Recommendation ITU– T X.1205. Available at: https://www.itu.int/rec/T-REC-X.1205-200804-I (accessed 22 April 2020).

ANALYSIS OF THE NORMATIVE-LEGAL AND ORGANIZATIONAL FOUNDATIONS OF THE CYBERSECURITY SYSTEM OF THE EU COUNTRY

***G. Sokol**, Ph.D., Associate professor,*
***A. Mishchenko**, Master's Student*
National University «Yuri Kondratyuk Poltava Polytechnic»

УДК 621.313

***Г.М. Кожушко**, д.т.н., професор,*
***С.Г. Кислиця**, к.т.н., доцент,*
***В.С. Дорошенко**, магістрант*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

СИНТЕЗ ЦИФРОВОГО РЕГУЛЯТОРА ВАГИ В ЕЛЕКТРОМЕХАНІЧНІЙ СИСТЕМІ

Автоматичні системи дозування сипких матеріалів широко застосовуються в будівельних, харчових і фармацевтичних галузях промисловості для

ДОДАТОК Г

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»
НАВЧАЛЬНО НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА РОБОТОТЕХНІКИ
КАФЕДРА ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

172 Телекомунікації та радіотехніка

НА ТЕМУ: Розроблення системи комплексної кібербезпеки інфокомунікаційної мережі підприємства, на основі стандартів ЄС

Виконав: студент 6 курсу, групи 601-ТТ
Міщенко Артем Сергійович
Керівник: к.т.н., доцент
Сокол Галина Вікторівна

Полтава 2022

Рисунок Г.1 – слайд № 1

2

Вступ

Об'єкт дослідження: система комплексної кібербезпеки інфокомунікаційної мережі підприємства.

Предмет дослідження: технології та стандарти ЄС для розробки системи комплексної кібербезпеки інфокомунікаційної мережі підприємства

Метою кваліфікаційної роботи магістра є: на основі аналізу методів та технологій країн ЄС розробити та спроектувати систему комплексної кібербезпеки, яка буде захищати інфокомунікаційну мережу підприємства.

Призначення системи комплексної кібербезпеки. Автоматизує процес збору та обробки інформації від систем та обладнання технічних засобів охорони підприємства, взаємоузгодженого функціонування цих засобів та систем.

Рисунок Г.2 – слайд № 2

Рисунок Г.3 – слайд № 3

Рисунок Г.4 – слайд № 4

Рисунок Г.5 – слайд № 5

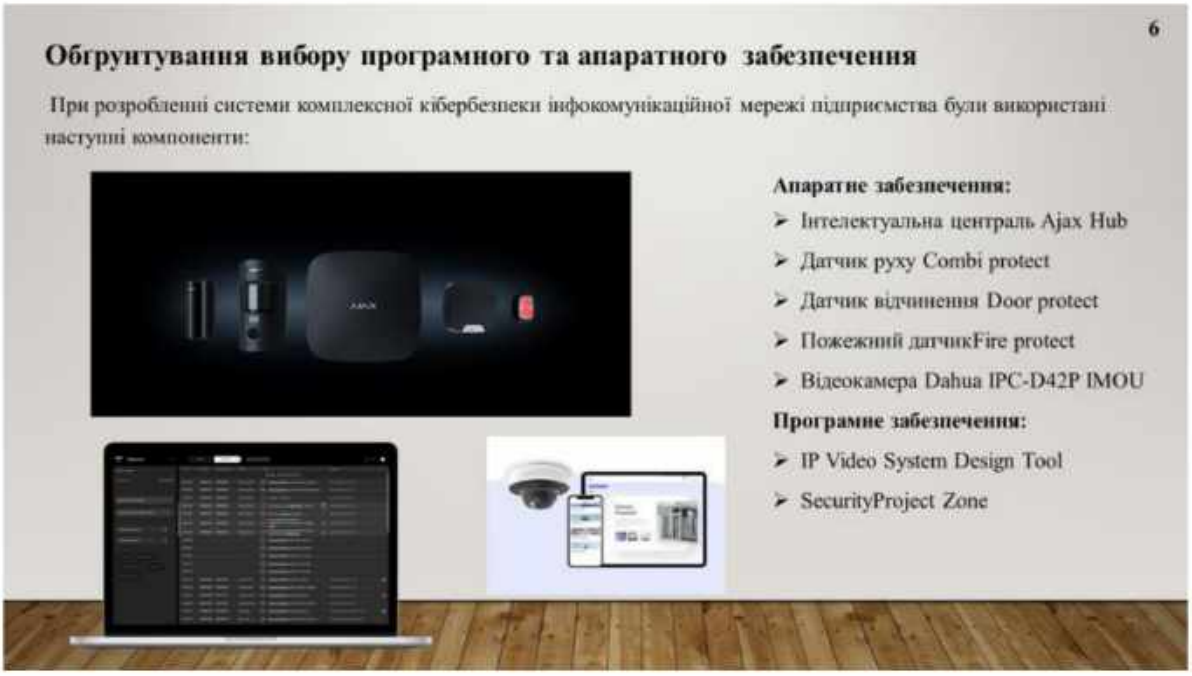

Рисунок Г.6 – слайд № 6

7

Обрання способу побудови системи

Враховуючи характеристики та площу приміщення, а також проаналізувавши норми та стандарти ЄС потрібно створити систему, яка буде спостерігати, швидко попереджувати та реагувати на різні загрози безпеці. Приміщення знаходиться в будівлі на другому поверсі «Л» корпусу Національного університету «Полтавська політехніка імені Юрія Кондратюка».

Система повинна задовольняти наступні вимоги:

- цінова доступність;
- модульність;
- нарощування (можливість додавання обладнання для розширення функціоналу системи);
- інтуїтивно зрозумілий інтерфейс, що адаптується під користувача;
- адаптованість системи (можливість підстроювання не тільки інтерфейсу, але й функціоналу системи під вимоги і особливості конкретних користувачів);
- розвинена технічна підтримка.

Рисунок Г.7 – слайд № 7

8

Принцип роботи та функціональна схема системи

Система повинна складатися із центрального контролера та периферійних пристроїв, включаючи датчики та виконавчі механізми.

За результатами досліджень визначено, що система повинна бути побудована на наступних принципах:

- Наявність центрального контролера з частковою автономністю периферійних пристроїв.
- Бездротовий інтерфейс передачі даних з можливістю підключення дротових периферійних пристроїв.
- Проста розширюваність і підтримка багатьох виробників.

Рисунок Г.8 – слайд № 8

Рисунок Г.9 – слайд № 9

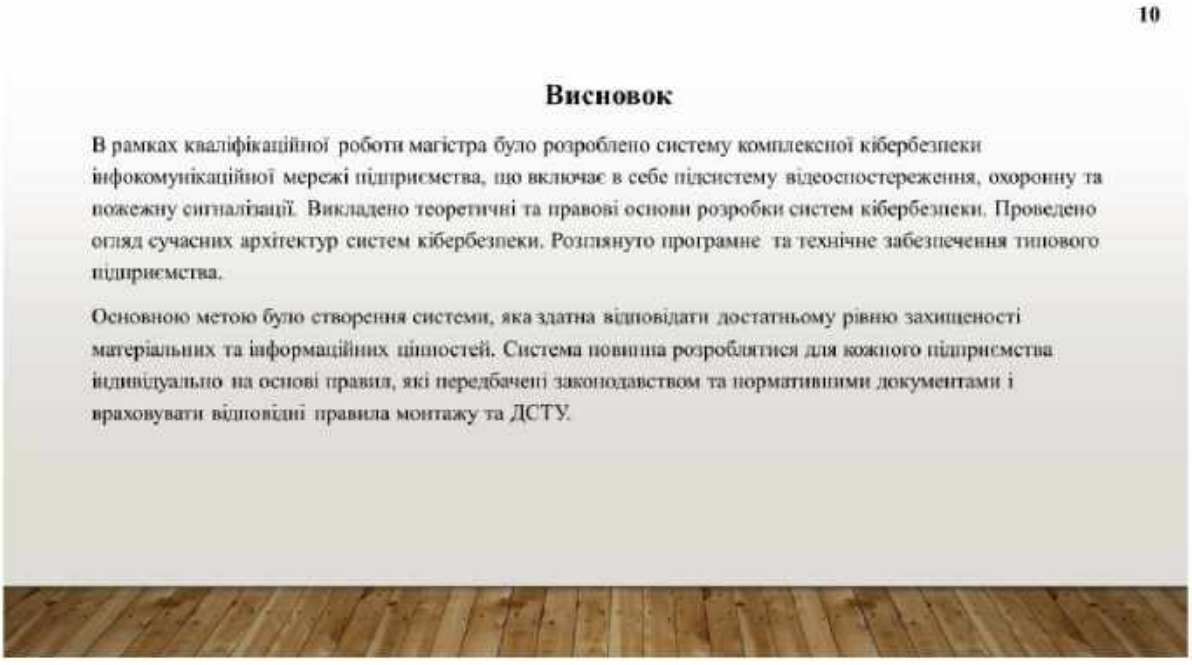

Рисунок Г.10 – слайд № 10