ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система захисту об’єкту інформаційної діяльності від несанкціонованого доступу до каналів передачі конфіденційних даних»

на здобуття освітнього ступеня магістра
зі спеціальності __125__Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Нікіта СТРУК

Виконав: здобувач вищої освіти групи СЗДМ 62
Нікіта СТРУК

Керівник: Ігорь ІВАНЧЕНКО .
к.т.н., доцент (ПРІЗВИЩЕ, Ім’я)

Рецензент: _____
. *(ПРІЗВИЩЕ, Ім’я)*

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Технічних систем кіберзахисту
Ступінь вищої освіти магістр
Спеціальність Кібербезпека та захист інформації
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Струку Нікіті Олеговичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Система захисту об'єкту інформаційної діяльності від несанкціонованого доступу до каналів передачі конфіденційних даних»
керівник кваліфікаційної роботи Ігорь ІВАНЧЕНКО к.т.н., доцент .
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2025 р. №____

2. Строк подання кваліфікаційної роботи 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: об'єкті інформаційної діяльності, канали витоку інформації з обмеженим доступом на об'єкті інформаційної діяльності, системи та елементи фізичного та технічного захисту інформації на об'єкті інформаційної діяльності.
4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):
4.1. Захист інформації на об'єктах інформаційної діяльності
4.2. Огляд системи захисту інформації на об'єкті інформаційної діяльності
4.3. Розробка рекомендацій щодо удосконалення системи фізичного захисту інформації на об'єкті інформаційної діяльності

5. Перелік графічного матеріалу: Презентаційний матеріал на слайдах

6. Дата видачі завдання 15.10.2025

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Нікіта СТРУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Ігорь ІВАНЧЕНКО
(підпис) *(ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 82 сторінок, має 21 рисунки, 7 таблиці. Список використаних джерел містить 38 найменування і займає 4 сторінки.

Метою кваліфікаційної роботи є підвищення ефективності функціонування системи захисту об’єкту інформаційної діяльності від несанкціонованого доступу до каналів передачі конфіденційних даних.

В кваліфікаційній роботі визначено порядок розподілу інформації, проведено аналіз загроз інформаційній безпеці та аналіз технічних каналів витоку інформації на об’єкті інформаційної діяльності. Проведено огляд системи захисту інформації на об'єктах інформаційної діяльності. Досліджено шляхи та розроблено рекомендації щодо удосконалення системи фізичного захисту інформації на об'єктах інформаційної діяльності. Проведено огляд питань електромагнітного забруднення довкілля в межах проблем охорони природнього середовища.

Апробація:

Н.О. Струк, М.С. Максимчук, Ю.Л. Іванов, Структура, перелік та зміст конфіденційної інформації комерційної торговельної установи та канали її несанкціонованого доступу. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-комунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.36-37. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ, ТЕХНІЧНІ ПРИСТРОЇ ОХОРОНИ ТА ЗАХИСТУ ОБ’ЄКТУ.

ABSTRACT

The qualification work consists of an introduction, three sections, general conclusions, a list of sources used, the total volume of the work is 82 pages, has 21 figures, 7 tables. The list of sources used contains 38 names and takes up 4 pages.

The purpose of the qualification work is to increase the efficiency of the functioning of the system for protecting the object of information activity from unauthorized access to channels for transmitting confidential data.

The qualification work determines the procedure for distributing information, analyzes threats to information security and analyzes technical channels for information leakage at the object of information activity. A review of the information protection system at the objects of information activity is conducted. Ways are investigated and recommendations are developed for improving the system of physical protection of information at the objects of information activity. A review of the issues of electromagnetic pollution of the environment within the framework of environmental protection problems is conducted.

Approbation:

N.O. Struk, M.S. Maksymchuk, Yu.L. Ivanov, Structure, list and content of confidential information of a commercial trading institution and channels of its unauthorized access. All-Ukrainian scientific and practical conference: Current problems of information and communication systems security. Kyiv, November 5, 2025, Kyiv: RVC DUIKT. – 2025. P.36-37. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Keywords: INFORMATION PROTECTION SYSTEMS, OBJECT OF INFORMATION ACTIVITY, TECHNICAL CHANNELS OF INFORMATION LEAKAGE, TECHNICAL DEVICES OF PROTECTION AND PROTECTION OF THE OBJECT

.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ОІД	–	Об’єкт інформаційної діяльності
ІзОД	–	Інформація з обмеженим доступом
ТЗІ	–	Технічний захист інформації
ТКВІ	–	Технічні канали витоку інформації
ОТЗС	–	Об’єкт технічного захисту систем
ТЗО	–	Технічні засоби охорони
ТСО		Технічна система охорони
ТЗОС	–	Технічні засоби охоронної сигналізації
КПП	–	Контрольно-перепускний пункт
СКУД	–	Система контролю та управління доступом
ІЧЗВ	–	Інфрачервоні засоби виявлення руху
ЗВ	–	Засіб виявлення
ПІЧ-сповіщувачі	–	Пасивні інфрачервоні сповіщувачі
ППККП	–	Прилади приймально-контрольні й контрольні панелі
ППК	–	Прилад пожежного контролю
ВПОС	–	Виносний пристрій оптичної сигналізації

ВСТУП

На сучасному етапі суспільного розвитку однією з найсуттєвіших проблем, яка присутня як в Україні, так і в усьому світі, є захист інформації на об'єктах інформаційної діяльності. Важливість цієї теми визначається значущим характером інформації, яку вона містить, володіння якою має суттєвий вплив на вирішення питань державного, оборонного, економічного чи комерційного характеру. Одним з аспектів вирішення цього питання є здійснення фізичного захисту інформації на об'єктах інформаційної діяльності за наявності небезпеки та заборони. Це, у свою чергу, вимагає проведення відповідних досліджень та створення рекомендацій щодо впровадження системи фізичного захисту інформації в конкретному місці розташування стосовно об'єкта інформаційної діяльності, умов і наслідків, що характеризують його діяльність, а також потенційних небезпек зовнішнього доступу до інформації з обмеженим доступом у конкретному місці розташування.

Метою кваліфікаційної роботи підвищення ефективності функціонування системи захисту об’єкту інформаційної діяльності від несанкціонованого доступу до каналів передачі конфіденційних даних.

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

– Визначено порядок розподілу інформації на об’єкті інформаційної діяльності, проведено аналіз загроз інформаційній безпеці та аналіз технічних каналів витоку інформації на об’єкті інформаційної діяльності.

– Проведено огляд системи захисту інформації на об'єктах інформаційної діяльності.

– Досліджено шляхи та розроблено рекомендації щодо удосконалення системи фізичного захисту інформації на об'єктах інформаційної діяльності

Об’єкт дослідження. Процес захисту інформації на об’єкті інформаційної діяльності

Предмет дослідження. Система захисту інформації на об’єкті інформаційної діяльності.

Розділ 1
ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

1.1 Порядок розподілу інформації на об'єкті інформаційної діяльності

Інформація – будь-які розвідувальні дані або дані, які можна архівувати на фізичних носіях або відображати електронними засобами [1].

Залежно від теми, інформація поділяється на один із таких типів [1,2,3,4]:

– особисті дані особи;

– інформація, яка переважно базується на дослідженнях та має енциклопедичний характер;

– інформація про стан навколишнього середовища (екологічна інформація);

– відомості про продукт (роботу, процес);

– науково-технічні знання;

– податкові відомості;

– формальні правила;

– статистичні дані,

– соціальна інформація про соціологію.

Інші види знань [1].

Однак для практичного застосування більш важлива класифікація інформації за порядком доступу до неї. Далі йде інформація, яка є загальнодоступною або має обмежений доступ. 1.1) [2].

Відкритість – доступна будь-яка інформація, за винятком тієї, яка обмежена законодавством, це називається відкритістю. Основними характеристиками відкритої інформації є те, що вона доступна кожному, хто бажає отримати до неї доступ, і будь-які обмеження права на отримання відкритої інформації заборонені [1,2].

Методи забезпечення доступу до відкритої інформації [1,2,3,4]:

- систематичне поширення її в офіційних письмових виданнях (бюлетенях, збірниках);

- її передача через загальновживані засоби масової інформації;

– безпосереднє його розповсюдження серед зацікавлених сторін, зокрема державних органів та юридичних осіб [1, 2].

Рис.1.1 Режим доступу до інформації

ІзОД - До цієї категорії належить інформація, що вважається державною таємницею, або інша персональна інформація, що охороняється законом [1,5].

Секретна інформація - це вид розвідувальних даних, що стосується оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та правоохоронної діяльності, всі з яких вважаються таємними законом і підлягають державному захисту. Інформація, що вважається державною таємницею, поділяється на класи відповідно до Закону України "Про державну таємницю" [1,5].

Конфіденційна інформація - це інформація, яка перебуває у власності, використовується або знищується фізичними або юридичними особами та запитується ними відповідно до умов, визначених ними. Інформація, що є державною власністю та використовується органами державної влади або органами місцевого самоврядування, підприємствами, установами та організаціями всіх типів, для її збереження до неї може бути надано обмежений доступ законом - може бути досягнутий статус конфіденційності [1,5].

Відповідно до Закону «Про захист інформації в інформаційно-телекомунікаційних системах», до захисту в системі належить наступне:

- Інформація, яка є відкритою для держави та, згідно з визначенням Закону України «Про інформацію», є власністю держави та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також для опису діяльності конкретних органів, вся ця інформація оприлюднена в мережі Інтернет, інших глобальних інформаційних мережах та системах або передається через телекомунікаційні мережі (далі – відкрита інформація).

- Інформація, яка є конфіденційною та належить державі або підлягає захисту згідно із законом, включаючи персональні дані про особу (яку також називають конфіденційною інформацією).

Інформація, яка вважається таємною згідно із законом (або призначена для збереження в таємниці), називається інформацією, що становить державну або іншу таємницю.

Інформація повинна бути відкритою під час процесу обробки, це досягається шляхом захисту її від несанкціонованих змін, які можуть призвести до її випадкового або навмисного знищення чи модифікації. Усі користувачі повинні мати доступ до ознайомчих ресурсів, необхідних для розуміння відкритої інформації. Тільки ідентифіковані та уповноважені користувачі можуть змінювати або знищувати загальнодоступну інформацію.

Під час обробки конфіденційної та секретної інформації важливо забезпечити її захист від ознайомлення з нею осіб, які не уповноважені або не контролюються організацією, включаючи зміну, знищення або копіювання.

Усі дії, пов'язані зі зберіганням інформації з обмеженим доступом, здійснюються в інформаційних об'єктах, спеціально призначених для цієї мети. Згідно з визначенням, об'єктом інформації є будівля, фундамент, транспортні засоби або інші споруди, що мають функціональне призначення, що передбачає передачу інформації з обмеженим доступом. Інформаційна діяльність – це послідовність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб та держави [1,5].

Обробка інформації в інформаційних об'єктах, що перебувають у активному стані, забезпечує інформаційну безпеку, що досягається шляхом дотримання таких критеріїв інформаційної безпеки [1,2,3,4]:

Цілісність – властивість даних, яка повинна бути збережена від несанкціонованого знищення або зміни.

- секретність – властивість інформації, яка повинна бути захищена від несанкціонованого доступу;

- доступність – властивість інформації, яка повинна бути захищена від незаконного перешкоджання.

Для виконання інформаційних потреб державні органи, органи місцевого та регіонального самоврядування створюють інформаційні служби, системи, мережі, банки даних та бази даних. Процес їх створення, склад, права та обов'язки делегуються Кабінету Міністрів України або іншим державним посадовцям, а також органам місцевого та регіонального самоврядування [1,5].

Основними видами інформаційної діяльності є отримання, використання, зберігання та поширення інформації [1,5].

Отримання інформації – це документоване або публічно оголошене отримання інформації відповідно до чинного законодавства України фізичними, юридичними особами або державою.

Використання інформації – це задоволення інформаційних потреб громадян, юридичних осіб та держави. Поширення інформації – це передача, публікація та впровадження документованої або публічно оголошеної інформації [1,6].

Зберігання інформації має вирішальне значення для збереження інформації та її носіїв.

Отримання, використання, зберігання документованої інформації, яка публічно оголошена або задокументована, здійснюється відповідно до процедури, визначеної цим законом та іншими законами щодо інформації. Крім того, можна класифікувати діяльність, що стосується інформаційного забезпечення – отримання, оцінка, зберігання та обробка даних, усі з яких створюються з метою прийняття управлінських рішень. Це охоплює різноманітні види діяльності, включаючи виробництво та продаж, обслуговування та покращення технологічності продукції, а також якість виготовленої продукції, її вартість, рекламу та інформацію про різні продукти.[5,6].

Будь-яка форма інформаційної діяльності (включаючи інформаційний бізнес) не може відбуватися самостійно. Її учасники (контрагенти): продавець або покупець, роботодавець або працівник, діють у певному середовищі, яке впливає на їхнє становище, і називається середовищем підприємницької діяльності (або підприємництвом).[5,6]

Кожна компанія не може мати бюджету без плану підприємства. На основі розроблених бюджетів система управління керує різними видами бізнес-діяльності, спрямовує діяльність усіх своїх підрозділів, контролює та оцінює ефективність. На початку звітного періоду бюджет є планом, який формалізує очікувані продажі, витрати та інші фінансові операції на наступний період. Наприкінці звітного періоду бюджет функціонує як засіб вимірювання відхилення від запланованих значень, результати потім порівнюються із запланованими значеннями, і за необхідності проводяться додаткові заходи.

Якщо створення бюджетів та прогнозів базується на однакових вихідних даних та оцінках доходів, витрат, кількості запасів та обсягу ділової активності, то бюджети та прогнози будуть відповідати один одному та утворюватимуть залежну систему. Ефективне використання коштів сприятиме більш ефективному використанню технологій для підвищення ефективності підприємства, його стратегії розвитку та інформаційної безпеки всього підприємства, а також його матеріальних активів.

1.2. Аналіз загроз інформаційній безпеці на об’єкті інформаційної діяльності

Захист інформації є однією з найважливіших частин загального комплексу захисних заходів для технічної інформації (ТІ). Недозволений доступ до інформації з метою її подальшого використання можливий для хакерів [1.5,6].

Для незаконного вилучення даних використовуються різні технологічні засоби. Інформація про об'єкт поширюється серед зловмисника через різні фізичні носії. [6, 7].

Залежно від фізичної природи походження інформації, а також середовища, в якому вона поширюється, та способу її переривання, технічні канали витоку можна розділити на сім категорій:

- радіочастотні.
- електричні;
- акустичні;
- оптичні;
- матеріальні[7].

Фізична природа численних випромінювачів виявилася подібною: [6,7]:

- небезпечні сигнали викликаються елементами, вузлами та технічними засобами праці та виробництва, а також радіоелектронним обладнанням.

- кожне джерело небезпечного сигналу, яке відповідає певним умовам, може створити канал витоку технічної інформації.

- кожна електронна система, що складається з набору компонентів, вузлів та провідників, має численні шляхи витоку технічної інформації. Канали витоку інформації через радіо створюються в результаті:

- впливу мікрофона;

- магнітного поля;

- паразитичного потомства;

- через мережі електроживлення.

- на заземлювальних доріжках.

- внаслідок непрямого впливу;

- електромагнітного випромінювання;

- впливу радіочастотних перешкод;

- від оптичних волокон, що використовуються в зв'язку.

Загальна структура каналу витоку технічної інформації складається (рис. 1.2) з джерела або передавача сигналу, середовища поширення електричного струму або магнітних хвиль та приймача сигналу.

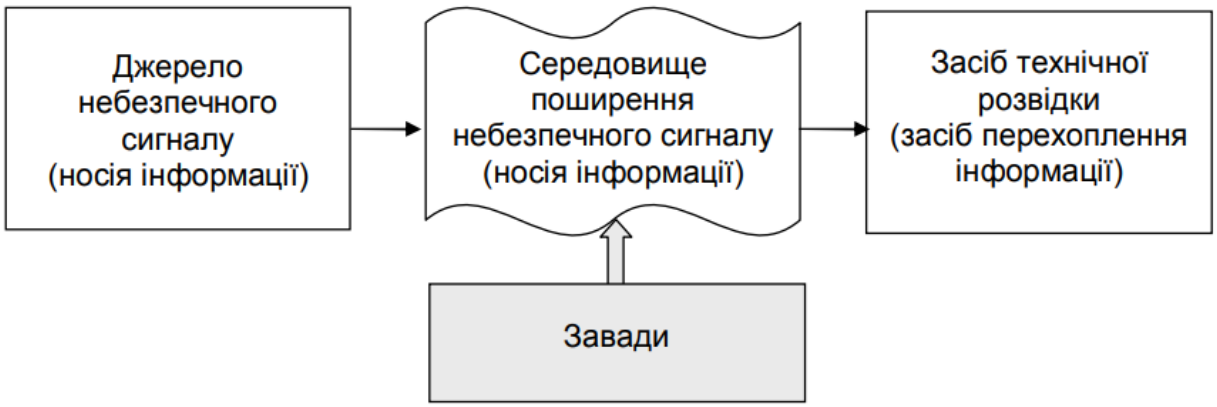


Рис. 1.2 Структура технічного каналу витоку інформації

1.3. Аналіз технічних каналів витоку інформації

Для категоризації вимог до захисту інформації та технічних каналів, через які відбувається її витік, інформацію було класифіковано за певними ознаками.

Зокрема, типи ТКВІ класифікуються за такими ознаками.

- за специфічною активністю інформації на ІЗО,

- за принципом (кінетичний ефект, процедура) створення шкідливого сигналу (інформаційне середовище),

- за середовищем передачі небезпечного повідомлення,

- за процесом переривання (видалення) небезпечного сигналу за допомогою технічних знань противника.

За типом інформаційної активності на ІЗО розрізняють такі типи ТКВІ:

- канали технічного характеру, тобто канали, що мають технічну складову,

- канали технічного характеру, що здійснюють витік інформації, що обробляється в ІЗО.

- візуальна інформація, що здійснює витік через технічні засоби,

- канали витоку інформації.

Рекомендується розглянути класифікацію ТКВІ за принципом (фізичним ефектом, процесом) створення небезпечного сигналу, середовищем, через яке передається сигнал, та методом його переривання (знищення).

Технічні способи отримання та поширення мовленнєвої інформації відповідно до цих властивостей поділяються на такі категорії:

Акустичні канали.

Канали акустичних коливань (віброакустичні).

- Акустооптичні (лазерні) канали.

Акустоелектричні канали.

- Відеоканали, що використовують звук.

- Канали, що використовуються для накладання радіочастот (для усунення інформації, пов'язаної з мовленням).

- Канали витоків інформації щодо мовлення, що базуються на вбудованих пристроях.

Технічні канали інформації, що обробляється в ОТЗС, поділяються на такі групи:

- Канали бокового випромінювання.

- Канали бокових електромагнітних перешкод.

- "Паразитичні" канали, що змінюють частоту радіочастотних сигналів від генераторів.

- Канали паразитної генерації радіочастотних підсилювачів потужності.

- Перехоплення (видалення) інформації з оптичних волокон.

- Перехоплення інформації через канали зв'язку.

- Канали радіочастотної потужності (для усунення обробки інформації в ОТЗС).

- Канали витоку в OTZS, що базуються на вбудованих пристроях.

Технічні канали витоку візуальної інформації поділяються на такі групи:

- Візуальні носії.

- Оптичні канали, що візуалізують.

- Канали, через які може витікати візуальна інформація на основі вбудованих пристроїв.

Витік інформації через матеріальні канали:

Вилучення інформації з несправних пристроїв ЕОТ.

Вилучення інформації з чернеток, виробничих відходів, видавничих відходів, офісних відходів тощо.

- Хімічні речовини, що проходять через канал.

- Наступні TCVI розрізняються за інформаційним змістом та принципом генерації небезпечного сигналу (7,8):

1. Канали витоку інформації через електромагнетизм, включаючи канали, що створюють побічне електронне випромінювання, канали, що підвищують

ВЧ-частоту генераторів, канали, що змінюють спосіб доступу до інформації через радіо (наприклад, через стільниковий або мобільний зв'язок), та інші канали;

2. Електричні канали витоку інформації, що включають канали, що мають побічний вплив на зв'язок, канали, що вилучають інформацію з дротового зв'язку, та інші канали;

3. Параметричні канали витоку інформації, що базуються на радіочастотах, включають канали, що мають «паразитичний» характер тощо.

За місцем розташування інформації, що перехоплюється технічною розвідкою противника, розрізняють такі різновиди ТСVI [7,8,9,10].

- методи збору (видалення) інформації поза зоною прямого зв'язку,

- методи прийому (видалення) інформації поза зоною прямого контакту з активним впливом на канал витоку технічної інформації (наприклад, радіочастотний канал),

- методи вилучення інформації за допомогою технічної розвідки, встановленої на об'єкті розвідки (наприклад, канали вилучення інформації за допомогою вбудованих технологій).

Запропонована класифікація технічних каналів витоку інформації дозволяє нам більш повно їх зрозуміти та розробити вимоги та методи запобігання викриттю інформації. Використання цих технічних каналів має бути обмежене за допомогою систем контролю витоку інформації.

1.4 Висновки по розділу

1. Описано процес поширення інформації в місці призначення інформаційної діяльності. Визначено спосіб класифікації та доступу до інформації. Перелічено методи та способи доступу до інформації. Визначено інформацію, що підлягає захисту, та встановлено правила інформаційної безпеки.

2. Проведено аналіз загроз та визначено шляхи витоку технічної інформації. Демонстровано склад технічного каналу розголошення інформації.

3. Проведено дослідження технічних каналів витоку інформації та зафіксовано результати. Це включає розмежування видів інформаційної діяльності, принцип формування небезпечного сигналу через середовище поширення небезпечного сигналу та метод захоплення (або видалення) небезпечного сигналу за допомогою технічної розвідки ворогів.

Розділ 2
ОГЛЯД СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

2.1. Технічні системи охорони та захисту інформації об’єкту інформаційної діяльності

2.1.1. Зміст та основні поняття у сфері технічних систем охорони та захисту інформації

Технічні засоби захисту – це фундаментальне поняття, яке описує обладнання (види обладнання), що входить до складу комплексів (систем) технічного захисту, призначених для захисту об'єктів (територій, будівель, приміщень) від несанкціонованого проникнення.

Історично склалося так, що для вирішення питання категоризації технічних ресурсів використовувалося кілька методів. У статті буде розглянуто метод, який вважається узагальнюваним, але не призводить до суперечок щодо більшої чи меншої точності конкретних підходів, оскільки відмінності випливають з конкретної мети класифікації, характерної для цього підходу. Деякі проблеми з розумінням можуть призводити до різної термінології, коли одне й те саме поняття виражається різними словами, наприклад: методи виявлення, датчики та сповіщувачі. Іноді у зв'язку з певним фізичним принципом дії як засіб виявлення використовується слово "сповіщувач". Усі ці терміни слід вважати синонімами, що позначають подібні поняття: компоненти технічної охоронної сигналізації (ТОС), яка функціонує як реакція на зовнішню дію. Наприклад, сейсмічна СЗ реагує на коливання в ґрунті, викликані рухом чогось (людини, тварини) або автомобіля, трактора чи іншого об'єкта. Кожен СЗ проектується з певною фізичною основою, основою якої є чутливий елемент (ЧЕ), що працює за допомогою електромагнітних, вібраційних, радіо, ємнісних, оптичних та інших методів.[7,11,12].

Таким чином:

– Пристрій виявлення – це пристрій, який автоматично генерує сигнал із певним набором параметрів (сигнал, що спрацьовує внаслідок тривоги, сигнал, що надсилається як сповіщення, або сигнал, що генерується автоматично). Це все приклади пристроїв виявлення.

– Чутливий елемент – це первинний перетворювач, на який впливає дія на нього (пряма чи непряма) об'єкта виявлення, і який сприймає зміну стану навколишнього середовища.

Під час проектування та впровадження ТЗО на об'єктах особлива увага приділяється забезпеченню захисту обладнання від його супротивників (обхід).

Виробники ТЗОС пропонують кілька підходів до виконання цього завдання: контроль відкриття блоків, автоматична перевірка функціональності методів виявлення та передача інформації. Всі ці речі детальніше розглядаються в розділах «безпека» та «конфіденційність» відповідно. Як правило, сучасні TZOS мають кілька рівнів захисту одночасно.

Як наслідок, одним із основних завдань проектування TZOS є створення механізмів для їх захисту від обходу зловмисником (порушником). Це складне завдання, яке включає кілька аспектів. Комплекс TZOS вважається сукупністю функціонально пов'язаних засобів, інформації, що збирається та обробляється, та додаткових систем, що використовуються для (тривожного) оповіщення, безпеки та інших цілей, а також завданням розпізнавання злодія [9].

2.1.2. Фізичні засоби захисту

Фізичні бар'єри складаються з різних пристроїв, конструкцій, апаратів та виробів, призначених для перешкоджання злочинцям.

Фізичні методи включають механічні, електромеханічні, електронні, електрооптичні, радіо- та радіотехнічні, а також інші пристрої для запобігання несанкціонованому доступу (входу, виходу), перенесенню (винесенню) предметів та іншій потенційній злочинній діяльності.

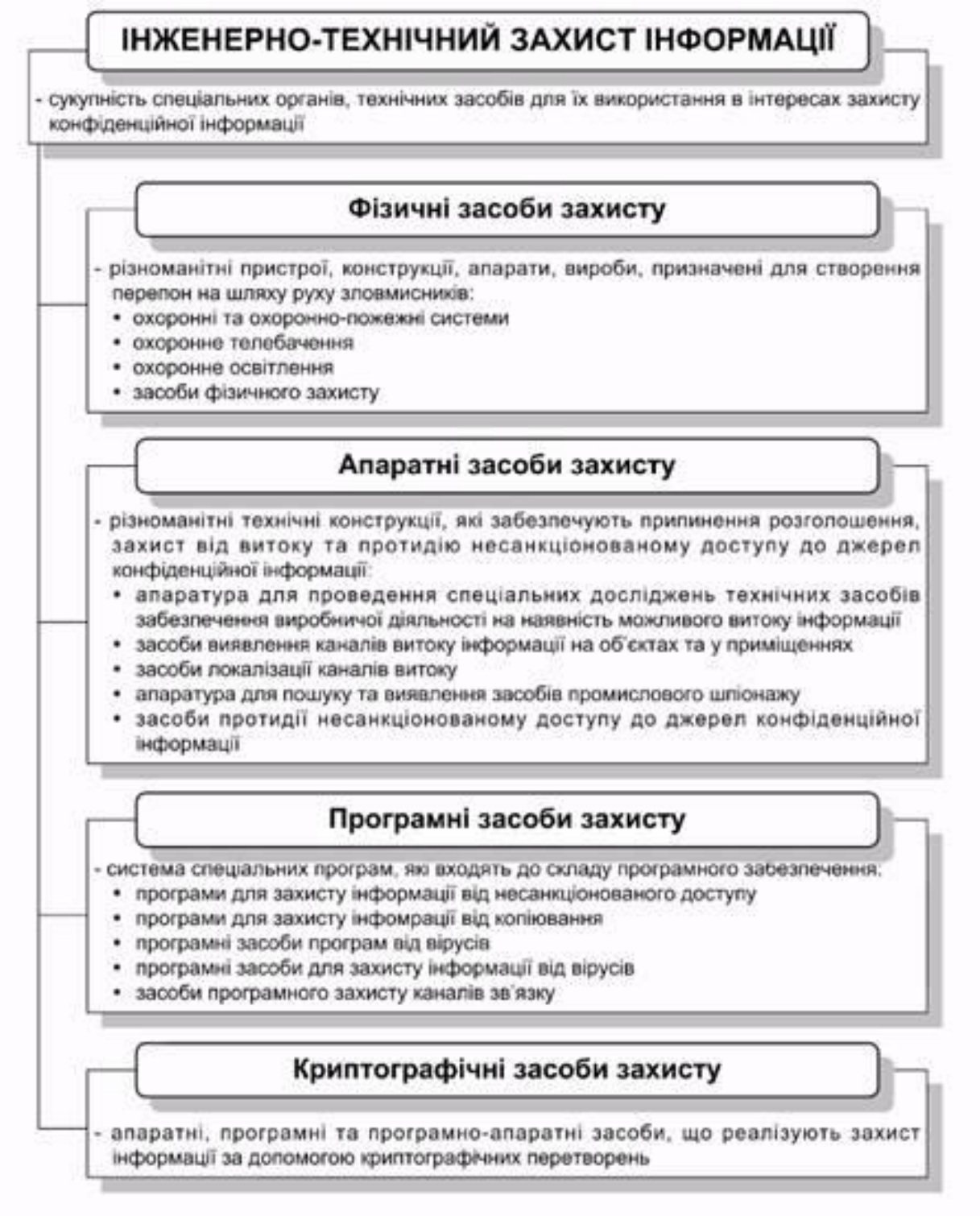


Рис. 2.1 Інженерно технічний захист інформації

Ці інструменти використовуються для вирішення наступних питань:

Захист території є відповідальністю підприємства, тому він і називається демікіанським.

• запобігання пошкодженню будівель, внутрішніх просторів та контроль над ними.

• захист обладнання, продукції, фінансів та знань;

Впровадження обмеженого доступу до будівель та просторів.

Усі фізичні методи захисту об'єктів можна класифікувати на три категорії: засоби виявлення, засоби запобігання та системи безпеки. Наприклад, охоронні сповіщення та охоронне телебачення відносяться до засобів виявлення; огорожі навколо об'єктів є засобами запобігання незаконному проникненню на територію, а посилені двері, стіни, стелі, ґрати на вікнах та інші елементи також служать захистом від незаконних атак (підслуховування, обстріл, кидання зброї тощо) [7,9,11,12]. Методи пожежогасіння – це системи, які намагаються усунути небезпеку.

Як правило, за фізичними характеристиками та функціональним призначенням усі методи цієї категорії можна розділити на три групи [11]:

• системи безпеки та пожежної безпеки;

• охоронне телебачення;

• Охоронне освітлення.

Методи фізичного захисту.

Системи безпеки та пристрої охоронної сигналізації призначені для розпізнавання різних видів небезпеки: спроб проникнення на об'єкт, що охороняється, в зони та приміщення, що охороняються, спроб заволодіння (або вилучення) зброєю, засобами промислового шпигунства, крадіжки матеріальних та фінансових цінностей та інших дій; оповіщення співробітників служби безпеки або іншого персоналу про наявність небезпек та необхідність розширення доступу до об'єкта, території, будівель та приміщень. [11,12,13].

Найважливішими компонентами систем безпеки є датчики, які розпізнають наявність загрози. Атрибути та принципи роботи датчиків визначають основні параметри та практичні обмеження систем безпеки.

Вже створено та широко використовується багато різних датчиків, як з метою виявлення фізичних полів, так і для стратегічних цілей.

Ефективність системи безпеки та сигналізації в першу чергу випливає з параметрів та принципів роботи датчиків. Сьогодні розрізняють такі типи датчиків: механічні вимикачі, дротові з вимикачем, притискні пластини, металева фольга, дротяна сітка, мікрохвильові датчики, ультразвукові датчики, інфрачервоні датчики, фотоелектричні датчики, акустичні датчики, датчики вібрацій, індуктивні датчики та ємнісні датчики.

Кожен тип датчика має певний тип безпеки: точковий захист, захист лінії, захист зони або об'ємний захист. Наприклад, механічні датчики призначені для захисту ліній, матові датчики пов'язані з точковим виявленням, а інфрачервоні датчики популярні в польових та об'ємних умовах.

Датчики пов'язані з контролером та приймальним пристроєм станції охорони (або поста), а також із засобами сповіщення, які сповіщають про наявність загрози, тими чи іншими засобами зв'язку.

Канали зв'язку в системах сигналізації, пов'язаних з безпекою, можуть бути виділеними дротовими або кабельними лініями, телефонними лініями, специфічними для об'єкта, трансляційними каналами, виділеними для об'єкта, або радіоканалами, призначеними для загального використання. Вибір каналів залежить від можливостей об'єкта.

Одним з найважливіших компонентів системи безпеки є засоби сповіщення про тривогу: дзвінки, ліхтарі, сирени та ліхтарики. Ці пристрої сигналізують про постійні або випадкові закономірності небезпеки.

Відповідно до мети тактичного підходу, системи безпеки поділяються на три типи: 11, 14 та 15.

Враховуються межі об'єктів.

• приміщення та шляхи до службових та складських приміщень;

• сейфи, інструменти, основні та вторинні технічні ресурси;

• транспортні засоби;

• споруди, включаючи камери відеоспостереження тощо. Фізичний захист включає:

Природні та штучні перешкоди (бар'єри);

• унікальні конструкції кордонів, проходів, вікон та дверей, сейфів, складських приміщень тощо;

• безпечні зони.

Природні та штучні бар'єри використовуються для запобігання незаконному проникненню на територію об'єкта. Однак основний захисний тягар все ще лежить на штучних кордонах, таких як паркани та інші типи огорож. Практика показує, що бар'єри, огорожі або стіни складної конструкції необхідні! Вони здатні утримувати порушника протягом достатнього часу. Сьогодні існує велика різноманітність таких інструментів: від простих сітчастих до складних комбінованих огорож, які мають значний стримуючий ефект на порушника [11,15].

Спеціальні конфігурації бордюрів, проходів, віконних сіток, приміщень, сейфів та сховищ є вкрай важливими для будь-яких організацій чи компаній з точки зору безпеки. Ці конструкції повинні витримувати будь-які фізичні впливи з боку злочинця, спрямовані на їх запобігання.

Механічна деформація, руйнування, спричинене свердлінням, термічне та механічне різання тощо;

• несанкціонований доступ за допомогою підроблених ключів, вгаданих кодів тощо.

Одним з основних технічних методів захисту проходів, входів, сейфів та складських приміщень є використання замків. Вони можуть бути простими (з ключами), кодовими (включаючи затримку відкриття на певний час) та мати програмне забезпечення, яке відкриває двері та сейфи у певний час.

Одним з важливих методів фізичного захисту є планування об'єкта, його будівель та приміщень відповідно до ступеня важливості різних частин об'єкта щодо заподіяння шкоди різним типам злочинців. Ідеальне розташування зон безпеки та розміщення ефективних технічних засобів для виявлення, відбиття

та ліквідації наслідків незаконної поведінки в цих зонах є основою концепції інженерно-технічного захисту навколо об'єкта.

Зони безпеки повинні розташовуватися на об'єкті послідовно, від периметральних огорож навколо території об'єкта до сховищ цінностей, це створює низку перешкод (рубежів), які зловмиснику доведеться подолати. Кількість часу, необхідна для проходження кожної зони, та ймовірність того, що пристрої виявлення в кожній зоні є складними та залежать від складності шляху та надійності перешкоди. Пости, датчики та камери, що виявляють вторгнення, подадуть сигнал про присутність злодія.

Основою планування та підготовки зон безпеки об'єкта є концепція рівності міцності меж цих зон. Загальна потужність зон безпеки визначатиметься їх найменшою складовою.[11,15].

Охоронне телебачення є одним з найпоширеніших методів запобігання. Одним з унікальних компонентів охоронного телебачення є здатність не тільки розпізнавати порушення протоколу безпеки об'єкта, але й спостерігати за навколишнім середовищем під час розвитку порушення, визначати ризик дій, вести приховане спостереження та записувати відеодані для подальшого аналізу правопорушення з метою його вивчення та притягнення злочинця до відповідальності.15].

Датчиками зображення (джерелом) у системах охоронного телебачення є відеокамери. Через вікно зображення порушника проектується на світлочутливий компонент камери, який потім перетворює проектоване зображення на електричний сигнал, що передається через спеціальний коаксіальний кабель на монітор і, за необхідності, на відеозаписний пристрій.

Відеокамера є центральним компонентом системи відеоспостереження, оскільки ефективність та працездатність усієї системи залежить від її можливостей. Сьогодні створено та виробляється безліч різних моделей, які відрізняються як дизайном і розміром, так і можливостями.

Другим за важливістю компонентом системи відеоспостереження є монітор. Він повинен відповідати характеристикам відеокамери. Часто один

монітор пов'язаний з кількома камерами, ці камери підключаються до нього за допомогою автоматичного перемикання на основі встановленого графіка.

Деякі системи телевізійного моніторингу мають можливість автоматично підключати камеру до зони спостереження за телебаченням. Якщо сталося порушення, ця інформація надається глядачеві. Також використовується більш складне обладнання, до цих інструментів належать програми автоматизації, пристрої, які одночасно відображають кілька зображень, та датчики руху, які сигналізують про тривогу, коли виявляються будь-які зміни зображення. [11, 14, 15].

Необхідним компонентом системи безпеки на будь-якому об'єкті є освітлення, пов'язане з безпекою. Доступні два види охоронного освітлення - чергове та сигналізаційне.

Аварійне освітлення призначене для тривалого використання у неробочий час, у вечірній та нічний час, як на території об'єкта, так і всередині будівлі [1,11].

Аварійне освітлення активується при отриманні сигналу від системи безпеки. Крім освітлення, використовуються також звукові пристрої (дзвінки, сирени тощо). Воно може активуватися сигналом, що запускає тривогу.

Сигналізація та аварійне освітлення повинні мати додаткове джерело живлення на випадок аварії або відключення електроенергії.

Останнім часом підвищена увага приділяється створенню систем фізичної безпеки, які поєднуються з сигналізацією. Це поширена електронна система моніторингу огородженої дротом території. Система складається з електронних датчиків та мікропроцесора, який керує процесом обробки даних. Бар'єри довжиною до 100 метрів можуть бути встановлені на відкритих майданчиках або розміщені на стінах, горищах та існуючих межах. [11,14,16].

Стійкі датчики розміщуються на опорах, кронштейнах. Дротяний бар'єр складається з 32 горизонтально натягнутих сталевих волокон, кожне з яких оснащене електромеханічним датчиком, що перетворює натяг струни на електричний сигнал.

Перевищення порогу напруги, запрограмованого на певну амплітуду на датчику коліна, призведе до спрацювання тривоги. Система підключена до центрального вузла та станції моніторингу через мультиплексор. Мікропроцесор автоматично контролює роботу апаратних та програмних компонентів у певний час і, якщо є відхилення, сигналізує про це відповідним чином.

Подібні системи фізичної безпеки та інші подібні пристрої можуть бути використані для охорони об'єктів по периметру з метою розпізнавання вторгнення на територію, на якій знаходиться об'єкт.

Використовуються системи з двох оптичних волокон, ці волокна призначені для передачі інфрачервоних сигналів на основі коду. Якщо сітка не пошкоджена, сигнали досягнуть місця призначення без спотворень. Спроби пошкодити сітку призводять до обриву або деформації кабелів, що призводить до чутного сигналу. Оптичні системи мають низьку ймовірність хибних тривог, спричинених впливом дрібних тварин, птахів, змінами погоди, та високу ймовірність розпізнавання спроби вторгнення.

Наступним рівнем фізичного захисту є захист компонентів будівель та просторів. Прийнятний фізичний захист віконних проміжків у приміщенні здійснюється за допомогою традиційних металевих ґрат, а також спеціальних віконних решіток на основі пластикових листів та сталевого дроту. Двері та вікна охоронюваних зон оснащені датчиками, які активуються при наявності скла або дверей, але інші вібрації, спричинені природними причинами, не активують датчики. Датчики активуються, що призводить до спрацьовування сигналу тривоги [15,16].

Серед заходів фізичної безпеки особливу увагу слід приділити засобам захисту ПК від крадіжки та проникнення в їхні внутрішні частини. Для цього використовуються металеві конструкції з основою, яка прилягає до столу, що забезпечує зусилля 250-2700 кг/см. Це виключає видалення або переміщення ПК без негативного впливу на цілісність поверхні столу. Перемістити ПК можна лише за допомогою спеціальних ключів та інструментів.

Інші спеціальні шафи та замкнені пристрої відіграють особливу роль у системах обмеження доступу, ці пристрої мають атрибути як фізичного бар'єру, так і засобу контролю доступу. Вони надзвичайно різноманітні та призначені для захисту документів, носіїв інформації, магнітних накопичувачів, фотокарт і навіть комп'ютерів чи інших технічних пристроїв: ПК, принтерів, копіювальних апаратів тощо.

Унікальні металеві скриньки призначені для зберігання ПК та інших комп'ютерів. Ці скриньки мають надійну систему подвійного замка: замок з ключем та кодовий замок, який дозволяє використовувати 3-5 комбінацій. Їх також можна використовувати як засіб блокування різноманітних об'єктів, ці об'єкти можна запрограмувати на відкриття за допомогою механічного або електронного годинника.

Пристрої контролю доступу. Доступ до приміщення визначається переважно шляхом процесу ідентифікації (верифікації) за допомогою засобів безпеки або технічної експертизи.

Контрольований доступ обмежений певною кількістю людей, яким дозволено вхід до певних зон, будівель, приміщень та транспортних засобів.

Критерієм допуску є певний метод ідентифікації та порівняння з еталонними параметрами системи. Існує дуже різноманітний спектр методів для розпізнавання уповноважених осіб щодо їхнього права доступу до будівель, приміщень та зон.

На основі зібраної інформації було прийнято рішення про допуск тих, хто мав на це право, або відмову тим, хто його не мав. Атрибути! Найбільш популярними є методи ідентифікації особи та посвідчення особи.

Атрибут – це наявність засобів автентифікації, таких як документи (паспорт, посвідчення особи тощо).), та жетони (картки з готівкою, фотокартки, картки з магнітами, електрикою та жетони). Інші компоненти включають індикатори, символи тощо. Важливо визнати, що ці методи в першу чергу вразливі до різних видів фальсифікації та крадіжки [15,16].

Персональні методи базуються на ідентифікації людини за її особистими маркерами: відбитками пальців, формою руки, рисами очей тощо. Особисті риси є переважно стаціонарними та також мають динамічний характер. До перших належать пульс, тиск, кардіограми, мовлення, почерк тощо.

Персональні підходи є найпопулярнішими. По-перше, вони детально описують кожну окрему Людину. По-друге, неможливо або надзвичайно важко імітувати індивідуальні риси.

Статичні методи передбачають аналіз фізичних властивостей, таких як відбитки пальців, риси форми руки тощо. Вони дуже надійні та мають низьку ймовірність помилок [15,16].

Динамічні методи характеризуються атрибутами, які розвиваються з часом.

Звички та навички, що залежать від практики та знань, не тільки легко імітувати, але й є найбільш практичними з усіх.

Методи ідентифікації, що включають будь-що, що можна запам'ятати (наприклад, коди, паролі або токени). Це корисно у випадках з найнижчим рівнем безпеки, оскільки ця інформація часто записується користувачами на різних носіях: папері, блокнотах та інших носіях, і якщо вони доступні іншим особам, ці носії можуть повністю звести нанівець усі зусилля безпеки. Крім того, існує реальна можливість шпигунства, підслуховування або отримання цієї інформації іншими способами (насильство, викрадення тощо) [15,16].

Процес ідентифікації особою (охоронцем, сторожем) не завжди є точним через наявність «людського фактору», який є результатом впливу багатьох зовнішніх факторів (втома, погане здоров'я, емоційний стрес, хабарництво тощо). І навпаки, зазвичай використовуються технологічні засоби ідентифікації, до яких належать посвідчення особи, розпізнавання голосу, почерку, відбитків пальців тощо.

Найпоширенішим і найпростішим методом ідентифікації є використання різних карток, які містять інформацію, що була кодована або оприлюднена, ця інформація стосується власника, його повноважень тощо.

Зазвичай це пластикові картки, які служать перепустками або жетонами. Картки вставляються у зчитувач щоразу, коли необхідно увійти або вийти з приміщення, що охороняється, або отримати доступ до чогось (наприклад).

Багато різних типів пристроїв особистої ідентифікації та розпізнавання використовують ці картки. Деякі з них оцінюють схожість фотографій та інших розпізнавальних ознак, інші ж використовують магнітні поля тощо.

Системи розпізнавання відбитків пальців. Принцип ідентифікації полягає в порівнянні відносного положення кінців та гілок ліній друку. Пошук зображень системою, який зараз здійснюється, спрямований на пошук контрольних елементів, які були визначені під час дослідження еталонного зразка. Щоб розпізнати когось конкретного, достатньо визначити розташування 12 точок [11,15,16].

Такі системи є досить складними. Їм радять щодо об'єктів, які потребують впевненого захисту.

Системи з голосовою активацією. Існує кілька методів розпізнавання спільних рис людського мовлення: аналіз коротких періодів часу, контроль аналізу та вибір статистичних властивостей. Важливо визнати, що теоретичні концепції ідентифікації голосу значно просунуті, але практичне виробництво цих систем все ще недостатньо розроблено [16,17].

Системи розпізнавання почерку вважаються найбільш практичними для користувачів. Основним правилом розпізнавання почерку є послідовний характер підпису кожної людини, незважаючи на відсутність точного збігу.

Розпізнавання геометрії руки. Для розпізнавання використовується комбінація ліній згину пальця та долоні, ліній, довжини та товщини пальців.

Технічно це досягається шляхом дотику до матриці фотодіодів. Підсвічування руки живиться від потужної лампи, а інформація про геометрію зберігається в сигналах від клітин.

Усі пристрої ідентифікації людини здатні функціонувати як окремо, так і в складі комплексу. Комплекс може бути вузькоспеціалізованим або

універсальним, система в ньому виконує функції безпеки, контролю, реєстрації та сигналізації. Такі системи вже є складними.

Складні системи мають наступний склад:

Картка може бути використана для входу на територію підприємства шляхом проходження через відповідні автомати.

• запобігання проходу, коли це не дозволено (прохід без перепустки, а потім проїзд до спеціальних підрозділів без перепустки).

Можливе запобігання порушенню графіка.

• надання вільного виходу для команд охоронця.

• перевірка кодів перепусток та утримання їх власників у визначеному місці за вказівкою оператора системи.

• фіксація часу проходження та зберігання його в базі даних комп'ютера;

• обробка отриманих даних та створення різних документів (табель обліку робочого часу, щоденний звіт, список працівників-порушників тощо), що дозволяє фіксувати інформацію про порушників трудового законодавства, кількість часу, витраченого на роботу, тощо;

Базу даних можна активувати, змінивши пароль.

• друк табелів обліку робочого часу для певної групи працівників (підприємство в цілому, структурний підрозділ або окремі особи);

• друк списків порушників встановленого графіка робочого дня з конкретною інформацією щодо порушення;

• поточний та історичний аналіз відвідувань відділів співробітниками, переміщення співробітників через контрольно-пропускні пункти, видача списку співробітників, присутніх або відсутніх у відділах або в компанії на певний момент часу (ведуться лише бази даних за минулі періоди);

• отримання інформації, корисної для операцій, шляхом відстеження абонентів локальної мережі! під час впровадження мережевої системи.

Фізичні бар'єри є першою перешкодою (бар'єром) для злодія під час спроби проникнення.

2.1.3 Апаратні засоби захисту

Інформація щодо апаратного захисту включає найрізноманітніші види технічного проектування, експлуатації та можливостей, призначених для запобігання розголошенню інформації, запобігання витоку та протидії несанкціонованому доступу до джерел конфіденційної інформації.

Апаратний захист інформації використовується для виконання таких завдань [11,15,16]:

проведення спеціальних розслідувань технічних методів захисту інформації під час виникнення потенційних витоків інформації;

• виявлення джерел витоку інформації в різних місцях та на різних об'єктах;

• запобігання витоку інформації в локальній зоні;

• пошук та розпізнавання промислових шпигунських пристроїв;

• запобігання несанкціонованому доступу до джерел секретної інформації та інших видів діяльності.

За функціональним призначенням апаратне забезпечення можна класифікувати на засоби виявлення, засоби пошуку та засоби вимірювання, які є активними або пасивними. Ці засоби використовуються для моніторингу, оцінки та вдосконалення процесів.

Крім того, відповідно до своїх характеристик, методи можуть бути застосовані до будь-якої ситуації, незалежно від ступеня фахівця. Непрофесіонали використовуватимуть ці методи для отримання першої (загальної) оцінки ситуації. Фахівці використовуватимуть ці методи для ретельного дослідження, виявлення та вимірювання всіх характеристик промислово розроблених засобів.

Перша категорія включає індикатори електромагнітного випромінювання, які можуть приймати різноманітні сигнали з відносно низьким порогом.

Друга група містить комплекси, призначені для виявлення та локалізації радіопередавачів, мікрофонів, телефонів та мережевих передавачів.

Обладнання, яке використовується для пошуку інформації, можна розділити на дві категорії: можна розглянути обладнання, призначене для пошуку способів збереження інформації та дослідження каналів, через які вона витікає.

Перший тип обладнання призначений для пошуку та локалізації методів несанкціонованого доступу, які вже використовуються злочинцями. Другий тип обладнання призначений для розпізнавання каналів втрати даних.

Подібно до інших галузей технологій, універсальність будь-якого обладнання зменшується, оскільки воно стає більш спеціалізованим.

І навпаки, існує велика кількість різних природних каналів розкриття інформації, а також фізичні принципи, що підтримують несанкціонований доступ до інформації. Ці фактори впливають на різноманітність пошукового обладнання, а його складність впливає на високу вартість кожного пристрою. У зв'язку з цим достатня кількість складного обладнання для пошуку може дозволити собі мати структури, які постійно виконують ефективні експертизи. Це або великі фірми безпеки, або спеціалізовані організації, що обслуговують треті сторони.

Певну групу можна ідентифікувати за допомогою апаратного захисту комп'ютерів та комунікаційних пристроїв на їх основі [15,16,18].

Пристрої захисту апаратного забезпечення використовуються як в окремих комп'ютерах, так і на різних рівнях та ділянках мереж у центральній частині комп'ютерів, в їх оперативній пам'яті (ОЗП), компонентах введення/виведення, зовнішніх сховищах, телефонах, таблицях тощо.

Для захисту центральних процесорів (ЦП) використовується надмірність коду - до формату машинних інструкцій додаються додаткові біти (біти секретності), а додаткові регістри резервуються для використання в ЦП. Крім того, доступні два різні режими роботи процесора, які відокремлюють допоміжні завдання від безпосереднього усунення неполадок користувача. Для цього використовується унікальна програма переривання, яка реалізується апаратно.

2.1.4. Програмні засоби захисту

Захист інформації за допомогою програмного забезпечення – це спеціальна система програм, пов’язаних із програмним забезпеченням та реалізуючих функції захисту інформації.

Визначено різні сфери використання програм для забезпечення безпеки конфіденційної інформації, до яких належать:

Захист інформації від несанкціонованого доступу;

Захист інформації від імітації;

• програмний захист від вірусів;

Захист інформації від вірусів;

Програми, що захищають канали зв’язку, називаються програмами захисту каналів.

Для кожної з вищезазначених сфер існує достатня кількість першокласних програмних продуктів, створених професійними організаціями та ефективно просуваних на ринку.

Засоби захисту програмного забезпечення мають додаткові спеціальні програми, унікальні для них [19,20]:

• процес перевірки ідентифікації обладнання, легітимності файлів та авторизації користувача;

Система повинна мати можливість реєструвати та регулювати поведінку обладнання та користувачів.

Підтримка режимів обробки інформації з обмеженим доступом.

Мета полягає в запобіганні знищенню операційних систем комп’ютера та програм, створених користувачем.

Знищення інформації на пристроях зберігання даних після їх використання є ще однією важливою причиною втрати даних.

Ознаки порушення використання ресурсів;

• додаткові програми різного призначення. Процес розпізнавання обладнання та файлів реалізується програмним забезпеченням, це робиться

шляхом аналізу реєстраційних номерів різних компонентів та об'єктів в інформаційній системі та їх зв'язку зі значеннями адрес та паролів у запам'ятовуючому пристрої системи.

2.1.5. Криптографічні засоби захисту

Криптографія — це форма дешифрування, яка спирається на використання ключа дешифрування, інформація потім приховується від зловмисника (наприклад,...).

Криптографія охоплює кілька частин сучасної математики, а також спеціалізовані галузі фізики, теорії інформації та інші суміжні галузі.

Як галузь науки, криптографія традиційно вважалася її основною метою захист державних та військових таємниць. Однак наразі методи та пристрої криптографії використовуються для забезпечення безпеки інформації не лише для держави, але й для приватних осіб та організацій. Акцент не обов'язково робиться на секретності. Багато різних типів інформації поширюються по всій планеті в цифровому вигляді. Крім того, ця інформація буквально «висить» над небезпекою несанкціонованого доступу, накопичення, підміни, фальсифікації тощо. Найефективнішими методами захисту від цих небезпек є криптографічні [8,11].

Для криптографічного перетворення інформації використовуються різні інструменти, які використовуються для шифрування документів, мови, телеграфії та даних, серед іншого.

Технологія комплексного шифрування. Початкове повідомлення, яке передається каналами зв'язку, часто називають незашифрованим... Повідомлення Р – розглядається передача розмовних повідомлень. Основним недоліком аналогових скремблерів є низький ступінь стабільності інформації. Крім того, вони вносять артефакти у реконструйований мовний сигнал, які називаються спотвореннями [17].

Останнім часом популярністю стали користуватися системи шифрування, які використовують цифрові методи кодування мовлення, що подаються у вигляді цифрових даних.

При аналого-цифровому перетворенні амплітуда сигналу записується через однакові інтервали часу, які називаються кроком дискретизації. Щоб отримати цифровий мовний сигнал, який не поступається телефонному сигналу, частота дискретизації не повинна перевищувати 160 мкс, а кількість рівнів амплітудного квантування мовного сигналу повинна бути не менше 128. У цьому випадку показання амплітуди кодуються 7-бітно; швидкість передачі перевищує 43 кбіт/с, а ширина спектру дискретного двійкового сигналу ідентична сумі смуг 14 стандартних телефонних каналів.

Рис. 2.2 Цифрове шифрування мовної інформації

2.2. Активні інфрачервоні засоби виявлення руху

Створення вітчизняних активних ІЧ-передавачів триває з початку 1960-х років. На ранніх етапах як джерела світла використовувалися лампи розжарювання. Частота випромінювання в цих виробах змінювалася за допомогою механічних перемикачів. Ці ІЧ-передавачів мали низьку

ефективність, великі габаритні розміри та споживали значну кількість енергії.[21,22].

Оптична система, пов'язана з джерелом випромінювання (ДВ), створює сфокусований вузький промінь інфрачервоного випромінювання. Як джерело ІЧ-випромінювання для оптичної системи використовуються напівпровідникові випромінювальні діоди з типовою робочою довжиною хвилі 0,94 мкм. Ці діоди розташовані у фокальній площині оптичної системи [21,22].

ІЧ-випромінювання концентрується оптичною системою ДВД поблизу чутливої області фотодіодів (фотодіодів). Імпульси струму, отримані від них, посилюються та надсилаються на пристрій, який обробляє їх для формування сигналів тривоги [22].

Залежно від кількості променів та їх положення (горизонтального чи вертикального), ІЧ-камери можуть брати участь у виконанні різних операційних завдань. Горизонтальне вирівнювання двох променів полегшує часову обробку інформації, що дозволяє визначити напрямок руху порушника. Вертикальне розташування променів в активних інфрачервоних (ІЧ) детекторах збільшує ймовірність блокування межі та периметра детектора порівняно з однопроменевими детекторами [22].

Конвективні перешкоди викликані рухом потоків рідини, такими як протяги, спричинені відкриттям вікна, тріснутими вікнами, а також побутовими опалювальними приладами – радіаторами та кондиціонерами. Потік повітря викликає випадкові, хаотичні зміни фонової температури, амплітуда та частота яких залежать від швидкості потоку повітря та властивостей фонової поверхні.

Електричні перешкоди є результатом будь-якого вимірюваного електричного або радіоджерела, телевізора, світла або електродвигуна, всі з яких враховуються. Також удари блискавки можуть створювати значну кількість перешкод [21,22].

Чутливість піроприймача надзвичайно висока – при підвищенні температури на 1 градус Цельсія вихідний сигнал безпосередньо виводиться з кристала та менший за 1 мікровольт, таким чином, додавання сигналу

перешкоди від джерела напругою кілька вольт на метр призведе до імпульсу перешкоди, який перевищує корисний сигнал. Однак більшість електричних перешкод має короткий період часу або крутий початок, що дозволяє відрізнити їх від корисного сигналу.

Власний звук піроприймача є найвищою межею чутливості для IRIR-діапазону та виглядає як білий шум. У цьому контексті методи фільтрації неефективні. Ступінь перешкоди зростає з кожним додатковим градусом підвищення температури кристала. Сучасні піродетектори мають рівень шуму, пов'язаний зі зміною температури на 0,05...0,15°C [21].

2.3 Технічні системи спостереження на об’єкті інформаційної діяльності

2.3.1 Системи відеоспостереження

Технологічна система відеоспостереження в інформаційній системі складається з апаратних та програмних компонентів (відеокамер, об'єктивів, моніторів, реєстраторів тощо), призначених для управління як локальними, так і віддаленими об'єктами. Функції спостереження включають не лише запобігання злочинцям, але й моніторинг співробітників та відвідувачів в офісі, на складі чи в магазині.

Рис.2.3 Активні інфрачервоні засоби виявлення

Сьогодні найпопулярніші відеокамери складаються з ПЗС-матриць. Зазвичай використовуються короткофокусні об'єктиви фіксованого типу, ці об'єктиви не потребують фокусування та експонуються автоматично.

Конструкція камери поділяється на три основні типи:

- модульна відеокамера - пристрій, який не має корпусу та складається з одношарової друкованої плати, призначеної для встановлення в термоконтейнери, сфери тощо;

- малі відеокамери - камери квадратної або сферичної конструкції,

зазвичай упаковані як готовий продукт для встановлення в приміщенні.

- натільна відеокамера - найпопулярніший вид пристрою,

також відомий як камера стандартної конфігурації або коробчаста камера;

- куполоподібна відеокамера, також звана купольною камерою, є частиною основи та кріпиться до неї.

- маніпульовані (поворотні або високошвидкісні камери) - комбінований пристрій,

що включає камеру, об'єктив, що збільшує масштаб, та нерухомий пристрій;

- гіростабілізовані відеокамери - камери, що використовуються на рухомих об'єктах для отримання чіткого зображення.

Рис.2.4. Купольна відеокамера

Сучасні цифрові відеореєстратори вважаються сучасними жорсткими дисками (HDD), які здійснюють запис. Одним із показників, за яким оцінюються цифрові відеореєстратори, є їхня стабільність, яка в першу чергу залежить від типу операційної системи. Автономні відеореєстратори, що використовують операційну систему Linux, сьогодні є найбільш стабільними в роботі (рис. 2.5) [14,15,23].

Рис.2.5 Відеореєстратор 16-канальний

В Цифрове зображення може мати кілька компонентів даних зображення.

- зазвичай 7*6 пікселів у режимі кадрів. Можливі й інші, менші значення (природно, швидкість передачі відеоінформації по мережі збільшується).

Обсяг зайнятого місця на жорсткому диску, необхідного для відеозапису, зменшується, але розпізнавання об'єктів на зображенні все ще неможливе через низьку роздільну здатність відеосистеми.

Ще одним компонентом оцінки відеореєстраторів є швидкість відеозапису (fps - field per second, тобто кількість кадрів за секунду) - цей параметр також називають частотою запису, швидкістю запису. Часто тут виникають непорозуміння, оскільки не визнається, що більшість відеореєстраторів використовують для запису не повну роздільну здатність відеосигналу, а замість цього відеополя (якщо це прямо зазначено). Ігноруючи цю інформацію, багато постачальників обладнання схильні вказувати значення

швидкості відеозапису терміном "кадри/с", що має на увазі значення слова "зображення" у значенні "кадр". Важливо визнати, що деякі зарубіжні виробники цифрових відеореєстраторів мають більш суворе позначення цього параметра, вони використовують термін pps (pictures per second - кількість зображень за секунду) для опису вимірювання [15,23].

Для відеореєстраторів, що мають кілька каналів, вказується або швидкість запису кожного каналу, або загальна швидкість усього пристрою. Наприклад, якщо в паспортах на 16-канальний відеореєстратор зазначено, що він має повну потужність 400 кадрів за секунду, це означає, що пристрій записує відео в режимі реального часу зі швидкістю 25 кадрів за секунду, якщо повна швидкість становить 25 кадрів за секунду, то швидкість кожного каналу дорівнює 1,56 кадру за секунду. У деяких відеореєстраторах швидкість запису відео та швидкість відображення «живого» зображення відрізняються, це необхідно враховувати при придбанні обладнання. [15,23].

Загалом, вибір цифрового відеореєстратора обов'язково пов'язаний з певною поступкою. Правда полягає в тому, що технічні ресурси відеореєстратора (як і будь-якого іншого пристрою) обмежені, тому розробнику системи відеоспостереження часто доводиться вибирати між записом відео в режимі «живого» з нижчою роздільною здатністю та записом, який відносно рідко оновлюється (в середньому кілька разів на секунду), з вищою роздільною здатністю.

Останній варіант передбачає припущення, що кожен випадок можна детально проаналізувати, роздрукувати, збільшити тощо. Звичайно, для живої демонстрації відеоінформації швидка швидкість оновлення інформації має першорядне значення (оператор менше втомлюється, ймовірність пропустити появу об'єкта нижча) [15.23].

Під час запису відео значення високої роздільної здатності більше, оскільки вона необхідна для розпізнавання людини, розпізнавання номерного знака автомобіля або інших ознак. Зрештою, це питання має вирішуватися на основі фактичних секторів відеокамер, розташованих на об'єкті. [15,23].

Високошвидкісний відеозапис передбачає запис більшої кількості інформації, тому пошук потрібного фрагмента має велике значення. Спробу знайти потрібне місце можна здійснити кількома способами [15,16,23]:

- за певною датою та часом;

- за номером відеозапису.

- за попередніми випадками запису тривоги або події.

- за місцем розташування диска (що є найпопулярнішим) [15,16].

Цифрові відеореєстратори використовують різні типи стиснення (Wavelet, MPEG-2, MPEG-4, H.263), кожен з яких має свої переваги та недоліки (такі як коефіцієнт стиснення, наявність артефактів, вимоги до передачі даних та ємність жорстких дисків). Наразі немає остаточної відповіді на питання, який тип стиснення є найефективнішим для використання в технології відеоспостереження. З точки зору споживача, тип стиснення не має першорядного значення - значущий результат, досягнутий у конкретному відеореєстраторі при використанні певного типу стиснення, становить 15,23.

Обсяг стисненого зображення (залежно від типу та ступеня стиснення) може становити від одиниць до десятків кілобайт, а час безперервного відеозапису цифрових відеореєстраторів зі швидкістю запису 25 кадрів/с може становити кілька годин.

Для зменшення обсягу дискового простору зазвичай використовується вибірковий запис за тривогою (коли датчик замикає свої контакти) або за рухом (коли виявляється активність).

Вбудовані датчики руху, як це зазвичай буває, мають 256 зон з програмованим порогом спрацьовування, хоча деякі пристрої мають понад 1000 таких зон. Крім того, існують вбудовані датчики руху, які мають різноманітні програмовані конфігурації, а також напрямки виявлення руху, які дозволені або заборонені.

Відстань між відеокамерами та станцією моніторингу повинна бути визначена для передачі відеосигналів на великі відстані. Кожне рішення, доступне розробнику, має свої переваги та недоліки.

Поширеним рішенням для передачі відеоінформації є використання коаксіального кабелю з хвильовим опором 75 Ом. Залежно від якості кабелю, зазвичай можна досягти прийнятної якості зображення, якщо відеокамеру розмістити на відстані не більше 200...400 метрів від станції спостереження. На більших відстанях рекомендується використовувати основні відеопідсилювачі для компенсації втрат кабелю. Оскільки вони є допоміжними пристроями, їх можна розміщувати на відстані від оператора, а для збільшення співвідношення сигнал/шум доцільно розмістити основний відеопідсилювач якомога ближче до відеокамери.

Переваги використання оптоволоконного кабелю задокументовані [12,18].

стійкість до електронних перешкод;

- Низькі втрати відеоінформації під час передачі на відстані до 50 кілометрів.

- вони екранують обладнання від гальванічного струму (не виникають петлі заземлення).

- можливість одночасно передавати відеоінформацію по одному дроту, аудіо та дані.

Недоліками волоконно-оптичного кабелю донедавна були:

- відносно висока вартість;

Низький обсяг виробництва [12,18].

Однак останнім часом метод роботи з волоконно-оптичними кабелями значно спростився, а ціни значно знизилися. При використанні волоконно-оптичних кабелів на стороні передачі та прийому розміщуються відповідні пристрої, вартість цього обладнання наразі є значною.

Слабкістю систем на основі волоконно-оптичного кабелю є їхня низька довговічність. Це проявляється у випадку випадкового або запланованого пошкодження цього кабелю, здатність організації його ремонтувати зазвичай втрачається [18,20].

Використання скруток у конструкції кабелю є проміжним між коаксіальним та волоконно-оптичним кабелями, їх вартість менша за вартість коаксіальних кабелів. Практика використання скруток кабельних пар дуже виправдана для систем відеоспостереження, які територіально розподілені, це особливо актуально в умовах несприятливих магнітних полів [12,18].

При проектуванні системи відеоспостереження висока якість зображення є надзвичайно важливою як вдень, так і вночі. Щоб отримати детальне зображення навіть у ситуаціях недостатнього освітлення, камери оснащені ІЧ-підсвічуванням, але цього може бути недостатньо. Саме тому присутні ІЧ-прожектори. Інфрачервоний прожектор покращить якість відеозапису в місцях з недостатнім освітленням, розширить діапазон видимості для відеокамери, а також зробить відеоспостереження більш непомітним.

ІЧ-підсвічування зазвичай складається з таких компонентів:

- кут сектора, що освітлюється;

- діапазон впливу;

- довжина спектру випромінювання світла;

- Споживана потужність наразі становить 11.

Конструктивно ІЧ-прожектори можуть бути побудовані двома способами: на основі галогенних ламп або світлодіодів.

ІЧ-прожектори, що використовують галогенні лампи (ІЧ-лампи) як джерело освітлення та мають інфрачервоний фільтр перед собою, мають такі властивості:

- широка зона впливу, яка може включати понад 100 метрів;

- значні витрати енергії (від 20 до 300 Вт, залежно від моделі).

- довжина хвилі 730...850 нм, що є видимою для людини областю світу. Це означає, що цей тип світла досить легко виявити.

- термін служби близько кількох місяців для галогенних ламп (зазвичай).

Твердотільні світлодіоди (ІЧ-світлодіоди), що використовують ІЧ-світлодіоди, мають додаткові відмінності:

- типова дальність дії, як зазвичай, не перевищує кількох сотень метрів;

- вони мають значно менше енергоспоживання;

- термін їх служби набагато довший;

- вони менші за розмірами та мають більшу вагу.

- Вони безпечніші; на них можна покластися.

В результаті система відеоспостереження має такі властивості: [14,21]:

- Спостереження за ситуацією на об'єкті, що охороняється, в режимі реального часу - ця інформація надається на пост моніторингу в режимі реального часу.

- запис відеоінформації в цифровому форматі, що дозволяє документувати виникнення подій на об'єкті.

- виконання функцій, пов'язаних з безпекою, за допомогою датчиків руху у відеокамерах або зовнішніх датчиків, пов'язаних з безпекою, та усвідомлення оператором системи наявності тривоги в цільовій зоні.

2.3.2. Пасивні інфрачервоні детектори.

Пасивні інфрачервоні детектори руху (також звані оптоелектронними) - це пристрої, які зазвичай використовуються для спостереження за рухом у заздалегідь запрограмованій зоні. Це зумовлено високим ступенем ефективності виявлення руху та низькою вартістю цих пристроїв. Ефективність детектора у розпізнаванні вторгнення в охоронювану зону, перш за все, випливає з того, що він дозволяє регулювати весь об'єм приміщення. Це вирішує проблему реєстрації вторгнення на додаток до найбільш вразливих зон, а також вирішує проблему реєстрації вторгнення практично через будь-який шлях: через вікна, двері, щілини в підлозі, стелі та стіни. Очевидно, що це набагато вигідніше, ніж спроби блокувати лише зовнішню частину об'єкта (наприклад, це не включає запобігання першій лінії оборони, що в більшості випадків дозволить вам отримати ранній сигнал тривоги та мати додатковий час для відповідного реагування [21,24].

Контроль загального об'єму приміщення не є виключною відповідальністю ІЧ-датчиків. Використовуючи змінні лінзи (оптичні системи),

ви можете ефективно контролювати невелику ділянку землі (наприклад, коридор) або створювати горизонтальний бар'єр (наприклад, для регулювання входу домашніх тварин у певні кімнати) або виявляти вертикальні загрози вздовж стін за допомогою вікон або дверей.

Сучасні ІЧ-датчики використовують цифрову обробку сигналів, вони постійно самоспостерігаються, розрізняють домашніх тварин та справжніх злочинців та мають більшу стійкість до впливу різних дестабілізуючих факторів (перешкоди від радіохвиль, сонячного світла тощо). Як наслідок, завдяки цим можливостям ці пристрої мають відносно низьку ціну, їх можна використовувати для охорони об'єктів з різними властивостями безпеки та необхідним ступенем безпеки [20,24].

Рис.2.6 Пасивні інфрачервоні засоби виявлення з фото фіксацією

2.3.3 Ультразвукові сенсори

Ультразвукові датчики в системі охоронної сигналізації призначені для захисту від вторгнення та подання сигналу, який має як тривожний, так і превентивний характер. Основою їхньої роботи є реєстрація зміни ультразвукового поля, спричиненої присутністю людини в приміщенні або виникненням пожежі. Вони мають високий ступінь чутливості, але також

високий рівень хибних спрацьовувань, наприклад, якщо зловмисник рухається з повільною швидкістю, він може обійти систему сигналізації. Крім того, деякі матеріали мають здатність поглинати звук, і якщо об'єкт, що охороняється, містить численні об'єкти такого типу або великогабаритні об'єкти, датчик буде обмежений мертвими зонами, що призведе до того, що датчик не реагуватиме на рух зловмисника, що, у свою чергу, призведе до проблем із використанням системи.

Заміна цих датчиків залежить від факторів навколишнього середовища, наприклад, потік повітря, що створюється кондиціонерами та опалювальними пристроями, також може призвести до хибного спрацьовування системи сигналізації. Як наслідок, ці датчики в основному використовуються для захисту об'єктів невеликого об'єму, наприклад, вітрин, музейних артефактів, салонів автомобілів тощо [17,24].

Рис.2.7. Ультразвукові засоби виявлення

2.3.4 Магнітоконтактний сповіщувач

Магнітний детектор контакту містить два основні компоненти. Перший компонент – це геркон, який складається з герметичної посудини, що містить пластини з низьким опором. Провідники з'єднані з пластинами для забезпечення зв'язку з Міжнародною космічною станцією. Для створення

пластин використовуються метали або сплави (наприклад, сталь), які ефективно керують ними за допомогою магнітного поля. Один із методів створення геркона – це використання пластин, намагнічених у протилежний бік. Поблизу магнітного поля від близького магніту контакти маніпулюють, щоб вони замикалися або розмикалися. Як правило, контакти змушені замикатися магнітним полем. Коли магнітне поле зникає, контакти розмикаються під дією сил пружності [21,24]. Контакти зазвичай покриті спеціальною сумішшю, наприклад, родієм, яка має низький опір і тривалий термін служби.

Рис.2.8. Магнітоконтактний сповіщувач

Наразі виробники випускають кілька різновидів ІКС, кожен з яких має свої унікальні характеристики: спосіб встановлення, місце використання, конструкцію, основні атрибути та інші особливості [21,24].

Стійкість до вібрацій та ударів є значним компонентом ймовірності помилкового спрацьовування. Це пояснюється тим, що короткочасний контакт можливий за наявності певних тригерів [21,24].

Типові параметри, пов'язані зі стабільністю ІКС: при діапазоні вібрацій 10...2000 Гц та межі прискорення 30 g тривалість контакту, що перевищує 20

мс, обмежена 11 мс; це також стосується ударного навантаження 100 g, яке має тривалість 11 мс.

2.3.5 Фотодіоди

Фотоелектричні датчики використовуються для запобігання порушенню внутрішніх та зовнішніх меж шляхом безконтактного блокування проходів, дверей, ліфтів, отворів, коридорів тощо. Конструктивно ці датчики мають передавач та приймач, розташовані вздовж лінії безпеки. Передавач виробляє інфрачервоний сигнал з довжиною хвилі близько 1 мкм, цей сигнал досягає приймача. Коли хтось намагається пройти через систему променя, датчик активується. Ці датчики мають високий ступінь надійності та стійкі до зовнішніх збурень. Однією з унікальних властивостей цих датчиків є їхня здатність працювати автономно, наприклад, завдяки наявності в їхній конструкції елементів на сонячній енергії [21,24].

Рис.2.9. Фотоелектричні сенсори

2.3.6 Вібросенсори

Датчики вібрації призначені для розпізнавання навмисного руйнування різних конструктивних елементів: стін і стель, цегли, дерев'яних (рам і дверей) елементів та покриття стелі, а також сейфів і металевих шаф.

Ці датчики поділяються на дві категорії: контактні вимикачі, що з'єднані послідовно або паралельно. Ці датчики розміщуються на стовпах або сітчастих огорожах і активуються поштовхами, тряскими або вібраціями. Основою їхньої роботи є п'єзоелектричний ефект або ефект електромагнітної індукції, коли постійний магніт рухається через котушку і тим самим індукує в ній змінний струм. Електричний сигнал, пропорційний рівню вібрацій, посилюється, а потім обробляється схемою детектора відповідно до певного алгоритму, який відрізняє руйнівний ефект від сигналу перешкоди. Як правило, у цих датчиках використовуються мікропроцесори для обробки електричних сигналів від контактних вимикачів та генерації тривоги. Ці датчики недорогі та мають високий рівень хибнопозитивних спрацьовувань. У літературі вітчизняного та зарубіжного походження технічна реалізація цих датчиків називається електромагнітним, магнітним резонансом [21,24].

Рис.2.10 Вібросенсор

2.3.7. Сповіщувачі розбиття скла

Акустичні детектори розбиття скла наразі є найпопулярнішими. Це пояснюється їхніми численними перевагами, включаючи відсутність компонентів на контрольованих скляних поверхнях, можливість керування кількома вікнами за допомогою одного детектора тощо. Як наслідок, слід детальніше обговорити специфіку коливань, що виникають при розбитті скла [21,24].

Як загальновідомо, при розбитті скла виникають коливання різних частот. Спочатку, коли скло розбивається, воно деформується. Це викривлення, або вигин скла, створює появу низькочастотних акустичних коливань (рис. 1а). Коли деформація досягає порогу, скло механічно руйнується. Останнє має високу частоту акустичних коливань. Крім того, щоб розпізнати наявність розбиття скла, необхідно враховувати той факт, що ці слухові коливання займають певний часовий інтервал [21,24].

Рис.2.11. Сповіщувач розбиття скла

Після зіткнення виникають коливання, спектр яких досягає частот приблизно 25 кГц. У цьому випадку низькочастотні компоненти розташовані переважно в діапазоні частот від десятків до сотень герц і пов'язані з деформацією скла під час удару. Ці компоненти мають найбільшу амплітуду протягом перших 200-300 мілісекунд, після чого з часом згасають [24].

Відразу після удару спостерігається широкосмуговий шум, спричинений механічним руйнуванням скла. Ці компоненти з високою частотою швидко згасають з часом [21,24].

Через кілька сотень мілісекунд знову з'являються високочастотні коливання зі спектром від 3 до 20 кГц. Ці компоненти пояснюються акустичними коливаннями, спричиненими падінням скла на підлогу та його подальшим руйнуванням [21], [24].

2.3.8 Комбінований інфрачервоний сповіщувач руху та розбиття скла

Датчик руху та розбиття скла призначені для відстеження руху людей у захищеному приміщенні та виявлення ударів та розбиття скла. Основний принцип роботи датчика руху полягає у виявленні інфрачервоного (ІЧ) випромінювання. Кожна жива істота має джерело інфрачервоного випромінювання. Щойно детектор виявляє ІЧ-енергію в охоронюваній зоні, він передає сигнал тривоги центральному компоненту системи безпеки. Датчик стійкий до тварин вагою від 25 до 1 метра, і спрацьовує лише тоді, коли людина рухається. Якщо в кімнату впаде предмет або повз пробіжить кішка, детектор не зможе функціонувати [21,24,25].

Рис.2.12 Комбінований інфрачервоний сповіщувач руху та розбиття скла

Вбудований електретний мікрофон здатний розпізнавати удари по склу та його розбиття. У цьому випадку використовується система, яка запобігає хибним спрацьовуванням. Вхідний звук вивчається поетапно. Для активації

сигналізації спочатку необхідно створити низькочастотні звуки (звук розбиття скла), після чого спрацьовують високочастотні звуки (звук удару скла). Нарешті, спрацьовує сигнал тривоги [21,25].

Комбінована система виявлення руху та скла використовується для захисту більшості об'єктів: заміських маєтків, котеджів, офісів, торгових центрів, квартир. Датчик руху є поширеним явищем у сигналізаціях, пов'язаних з безпекою.

2.4. Призначення, принцип дії та галузь застосування приймально-контрольних і контрольних панелей

Прийомно-розподільні пристрої керування та запису (ПКЗ) – це технологічні засоби для моніторингу та запису інформації. Вони призначені для збору інформації про стан сповіщувачів у системі сигналізації, оцінки тривожної ситуації на об'єкті, створення сповіщень про стан об'єкта на централізований пульт моніторингу та керування локальними світлозвуковими сповіщувачами та індикаторами. Крім того, пристрої забезпечують активацію та деактивацію об'єкта відповідно до визнаних методів, а в деяких випадках – живлення сповіщувачів.

ПКЗ є основними компонентами інформаційної системи та системи охоронної або пожежної сигналізації на об'єкті. Цей тип системи є автономним або централізованим. При автономній охороні пристрої розміщуються поблизу приміщення (пункту охорони) або в самому об'єкті. У централізованій охороні об'єктовий комплекс технологічних засобів, що складається з одного або кількох пристроїв, утворює підсистему безпеки, яка за допомогою системи передачі сповіщень передає інформацію про стан об'єкта на централізований пульт моніторингу, розташований у центрі прийому тривожної інформації (централізований пункт охорони). Інформація, що генерується пристроєм, як щодо автономної, так і централізованої безпеки, передається співробітникам спеціальних служб з метою забезпечення безпеки об'єкта, на яких покладається завдання реагування на тривожні повідомлення щодо об'єкта [21,24].

Для підвищення надійності інформації, отриманої під час використання технічних засобів для управління станом об'єкта, використовуються багатолінійні охоронні комплекси. Кожна з ліній сигналізації складається з низки технічних засобів охоронної сигналізації, які спільно керуються електричним колом (шлейфом сигналізації), що дозволяє передавати повідомлення про спробу проникнення в охоронювану територію (зони), незважаючи на інші технічні засоби, які не входять до ланцюга. Крім того, до кожної системи сигналізації вбудовані різні типи сповіщувачів [21,24].

Окрім постановки та зняття з охорони об'єкта (приміщення) відповідно до загальноприйнятої тактики, вони зазвичай забезпечують живлення сповіщувачів.

Приймально-керуючі пристрої поділяються на дві категорії згідно з [24, 26]:

– інформаційна ємність (кількість пристроїв, що беруть участь у циклі сигналізації)

на пристрої, що мають малу (до 5 СВС), середню (від 6 до 50 СВС) та велику (понад 50 СВС) інформаційну ємність;

- інформативність – можуть мати обмежену (до 2 типів повідомлень) або розширену

(3... 5 рівнів) та велику (понад 5 рівнів) інтелект.

Залежно від кількості напрямків передачі інформації, їх класифікують на системи.

з можливістю передачі інформації в обох напрямках (з наявністю зворотного шляху).

Залежно від способу відображення, інформація, доступна на централізованому пульті керування, є

Системи інформаційного моніторингу, що використовують світло та звук для передачі інформації, поділяються на системи, що мають індивідуальне або колективне відображення інформації у вигляді світла та звуку, при цьому інформація відображається на екрані за допомогою пристроїв обробки та зберігання даних.

Шлейф сигналізації – це електричне коло, що з'єднує вихідні кола датчиків, включаючи додаткові компоненти (діоди, резистори тощо), які підключені до коробок та проводів і призначені для видачі сповіщень про вторгнення, спробу вторгнення, пожежу, несправність, а в деяких випадках – для живлення сповіщувачів. В результаті створюється шлейф із сигналізацією для спостереження за станом певної зони, що охороняється [24,26,27].

Зона безпеки – це частина об'єкта, що охороняється, яка контролюється одним або кількома датчиками сигналізації.

Сьогодні сучасні багатофункціональні щити керування мають велику кількість опцій для організації системи безпеки, пожежної та охоронно-пожежної сигналізації. Розуміння цих можливостей допоможе вам вибрати відповідний пульт керування для вашого об'єкта, атрибути та параметри якого найбільше стосуються захисту конкретного об'єкта.

Пульт керування може працювати в різних режимах, включаючи: охоронний, спостереження (зняття з охорони), програмування [24,27].

Режим «Охорона».

Таким чином, пульт керування уважно стежить за своїми параметрами та станом шлейфів. Порушення циклів призводить до генерації звуків сигналізації. У цьому випадку можливі такі режими:

- повна охорона - панель керування контролює стан усіх циклів та себе.

- часткова охорона, що включає нагляд за частиною шлейфів та самою панеллю керування [24,27].

Процес встановлення та зняття об'єкта з охорони називається тактичними параметрами та складається з таких кроків:

- автоматичний вогонь.

- наявність запізнілого виходу.

- розгортання без затримки, пов'язаної з виходом [24,27]. Режим "Спостереження (охорона)".

У режимі «спостереження» панель керування деактивована, але вона все ще контролює всі цикли та себе.

Шлейф сигналізації є важливим для технічної системи безпеки. Практика показує, що однією з основних причин нестабільної поведінки пристроїв TSO на об'єкті є порушення роботи шлейфу сигналізації, це форма відмови, яка передбачає обрив або коротке замикання в шлейфі. Слід враховувати можливість навмисного електричного втручання в електричне коло шлейфу з метою переривання його природної функції (саботаж) [24,27].

Існує три методи керування циклом сигналізації:

- з живленням шлейфу сигналізації постійним струмом та використанням резистора як засобу для дистанційного керування елементом;

- з використанням послідовно з'єднаних резистора та напівпровідникового діода як навантаження, сигналізація вимкнеться при вимкненні живлення.

- з живленням шлейфу сигналізації імпульсною напругою та використанням конденсатора як дистанційного компонента.

Контроль пожежі та пристрої, що отримують сповіщення та інформацію про пожежу, призначені для живлення пожежних сповіщувачів через сигнальні петлі, що живляться від пожежі, генерації повідомлень "СПРОБУХА" та "НЕСПРАВНІСТЬ", проектування джерел живлення, здатних забезпечувати живлення для пожежогасіння та видалення диму, а також передачі цих повідомлень до централізованої системи моніторингу або інших пристроїв.

Основними характеристиками пожежних панелей, а також панелей безпеки, є їхня інформаційна ємність та ступінь їхньої інформативності [24,27].

Пристрої, що запускають сигнал, насправді є тими ж приймальними та керуючими пристроями, які доповнені здатністю генерувати сповіщення "Увага" при спрацьовуванні одного пожежного сповіщувача, сповіщення

"ПОЖЕЖА" при спрацьовуванні щонайменше двох пожежних сповіщувачів, затримкою запуску систем пожежогасіння, яку можна змінювати, та здатністю керувати системами пожежної сигналізації. Унікальною рисою панелі керування цього покоління пристроїв є променеподібна структура систем пожежної сигналізації та використання неінтуїтивних пожежних сповіщувачів на основі порогів, які самі визначають пожежу, щойно цікавий параметр перевищує дозволений діапазон [24,27].

Дистанційний оптичний сигналізатор (ДОПС) призначений для відображення оптичного сигналу пожежного сповіщувача, до цього пристрою важко отримати візуальний доступ, відсутність освітлення також є недоліком. Рекомендується використовувати ДОПС для ідентифікації сповіщувача, який надіслав повідомлення «ПОЖЕЖА», та встановлювати його в місці, до якого можна легко дістатися, наприклад, у коридорі над входом до приміщення, що охороняється.

Неадресовані, адресовані та аналогові системи пожежної сигналізації – це всі типи систем пожежної сигналізації, які поділяються на три класи.

Їхня основна відмінність полягає в методі, за допомогою якого система визначає, чи слід піднімати тривогу, тобто чи потрібно запобігти пожежі. У неадресованих та адресних системах це рішення приймається безпосередньо встановленими пожежними сповіщувачами. Потім тривожні сигнали передаються на приймальне та керуюче обладнання, сигнал від сповіщувача використовується для активації системи пожежогасіння.

Спроби розпізнати пожежу на ранній стадії шляхом зниження порогів точкового виявлення диму зазвичай призводять до спрацьовування хибних тривог та гасіння початку пожежі. Постійний пошук золотої середини між раннім виявленням та хибним запуском [27].

В аналогових системах, що є адресними, процес прийняття рішення про наявність пожежі відрізняється. Значення параметра, на який впливає сповіщувач (температура, наявність диму в приміщенні), передається на приймальне та додаткове обладнання. Основне обладнання завжди буде

обстежувати стан навколишнього середовища в кожній кімнаті будівлі та фіксувати зміну цих параметрів. На основі вищезазначеної інформації визначається не лише формування сигналу "ПОЖЕЖА", але й сигналу "ТРИВОГА". Тобто, адресна аналогова система пожежної сигналізації базується на рішенні про активацію не окремими датчиками, а обладнанням, яке приймає та контролює дані, що базується на прогресії змін даних від сповіщувачів. Адресовані аналогові системи, які постійно контролюють стан навколишнього середовища в приміщенні, негайно розпізнають зміну температури або наявність куріння та подадуть сигнал відповідальній особі [27].

Раннє виявлення кризової ситуації дозволяє своєчасно вивести людей з зони пожежі та активувати автоматичну систему пожежогасіння. Крім того, досягається кілька важливих цілей, наприклад, моніторинг ефективності сповіщувачів. Як результат, в адресованій аналоговій системі несправний сповіщувач, який не виявляється приймальним або керуючим пристроєм, не матиме можливості розрізнити сигнал від власного сигналу сповіщувача. оскільки останнє є специфічним для першого. Якщо додати до цього потужні можливості самооцінки самих сповіщувачів, автоматичну компенсацію запиленості та виявлення запилених димових сповіщувачів, то очевидно, що ці компоненти лише підвищують ефективність адресних аналогових систем.

Рис 2.11. Прилад приймально-контрольний охоронно пожежний

2.5 Висновки по розділу

1. Викладено фундаментальні принципи змісту та основні ідеї в технічній галузі інформаційної безпеки та захисту. Перераховано фундаментальні компоненти фізичної, апаратної, програмної та криптографічної системи захисту інформації.

2. Наведено опис та ілюстрації використання активних інфрачервоних методів руху.

3. Задокументовано склад та опис окремих компонентів системи технічного моніторингу в центрі інформаційної діяльності. Розглянуто процес встановлення систем відеоспостереження, пасивних інфрачервоних методів виявлення, ультразвукових датчиків, магнітних датчиків, фотоелектричних датчиків, датчиків вібрацій, датчиків розбиття скла та їх комбінації.

4. Розглянуто призначення, принцип роботи та сферу застосування приймальних та керованих панелей для безпеки, моніторингу та пожежної сигналізації.

Розділ 3
ДОСЛІДЖЕННЯ НАПРЯМКІВ УДОСКОНАЛЕННЯ СИСТЕМИ ФІЗИЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

3.1 Розробка рекомендацій щодо організації фізичного захисту об’єкту інформаційної діяльності

Методи фізичного захисту, що використовують механічні, електричні, електронні пристрої та системи, що є автономними. Ці пристрої та системи запобігають діяльності зовнішніх сил, спрямованих на отримання конфіденційної інформації.

Ці типи систем є периметральними, пасивними або активними, всі з яких дозволяють гарантувати фізичну безпеку платформи ІС, додаткового обладнання, постачальників інформації та методів передачі інформації. Основні тактики фізичного захисту спрямовані на запобігання пожежам, воді, пилу, корозії, радіації, вандалізму та запобігання несанкціонованому доступу до простору. Необхідні захисні бар'єри та місця розташування визначаються цінністю інформації, ризиком порушень безпеки та необхідністю дотримання існуючих захисних протоколів [13,15,16].

Спектр прийнятних заходів фізичної безпеки, призначених для запобігання катастрофам або порушенням. Кожен рівень фізичної безпеки має певні області, зони або приміщення, доступ до яких обмежений, в межах цих областей гарантується рівень безпеки. Для забезпечення захисту периметра встановлюються система безпеки та пожежної безпеки, система відеомоніторингу, система контролю та управління доступом (СКУД) тощо [13,15,16].

Ці пропозиції слід впроваджувати правильно:

Зони та простори, що стосуються інформації, що захищається.

Межі безпеки повинні бути чітко визначені.

Інше обладнання слід додавати до системи таким чином, щоб мінімізувати ймовірність несанкціонованого доступу до обмежених зон.

Фізичні стіни, за необхідності, повинні сягати стелі, щоб запобігти несанкціонованому доступу (NSD) до обмежених зон.

Інформація щодо обмежених зон не повинна розголошуватися особам, які не мають на це дозволу.

Забороняється займатися роботою самостійно без належного нагляду.

• ІС повинна розташовуватися у відведених місцях, окремо від обладнання, яке контролюється третьою стороною.

У періоди, окрім робочого часу, територія об'єкта повинна бути фізично неможливою для доступу та контролюватися охороною.

У межах обмежених зон не повинно використовуватися фото- та відеозапис.

Необхідний належний контроль доступу.

Для вжиття заходів контролю важливо [20,29,30]:

Відстежувати дату та час входу та виходу відвідувачів;

Позбавити звільнених працівників прав на доступ до обмежених зон.

дотримання режиму доступу та внутрішніх правил організації.

3.2 Розробка рекомендацій щодо порядку застосування засобів технічного захисту об’єкту інформаційної діяльності

Ефективними інструментами для запобігання зовнішнім атакам є технічні засоби захисту, що базуються на методах, що запобігають несанкціонованому доступу до інформації та зловмисному використанню зовнішніх пристроїв для доступу до неї.

Технічні методи використовуються шляхом комбінації різних пристроїв, вбудованих в апаратне забезпечення систем обробки інформації, або комбінації методів, призначених для запобігання доступу та захопленню інформації соціальними інженерами. Ці пристрої або обходять, або запобігають фізичному

доступу до інформації (Таблиця 3.1), включаючи маскування [20,21,24].

Таблиця 3.1

Основні методи і засоби несанкціонованого отримання інформації та її захисту

Типова ситуація	Канал витоку інформації	Методи і засоби	
		отримання інформації	захисту інформації
Розмова в приміщенні та на вулиці	Акустичний	Підслуховування (диктофон, мікрофон тощо)	Шумові генератори, пошук закладних пристроїв, захисні фільтри, обмеження доступу
	Віброакустичний	Стетоскоп, вібродатчик	
	Акустоелектронний	Спеціальні радіоприймачі	
Розмова по телефону:	Акустичний	Підслуховування (диктофон, мікрофон тощо)	Шумові генератори, пошук закладних пристроїв, захисні фільтри, обмеження доступу
– проводовому	Сигнал у лінії	Паралельний телефон, пряме підмикання, електромагнітний датчик, диктофон, телефонна закладка	Маскування, скремблювання, шифрування, спецтехніка
	Наведення	Спеціальні радіотехнічні пристрої	Спецтехніка
– радіотелефону	ВЧ-сигнал	Радіоприймачі	Маскування, скремблювання, шифрування, спецтехніка
Дії з документом на паперовому носії:	Безпосередньо сам документ	Крадіжка, прочитування, копіювання, фотографування	Обмеження доступу, спецтехніка
	Продавлення стрічки або паперу	Крадіжка, прочитування	Оргтехзаходи
– виготовлення	Акустичний шум принтера	Апаратура акустичного контролю	Пристрої шумозаглушування
	Паразитні сигнали, наведення	Спеціальні радіотехнічні засоби	Екранування
– поштове відправлення	Безпосередньо сам документ	Крадіжка, прочитування	Спеціальні методи
Документ на машинному носії:	Носій	Крадіжка, копіювання, прочитування	Контроль доступу, фізичний захист, криптозахист
– виготовлення	Відображення на дисплеї	Візуальний, копіювання, фотографування	Контроль доступу, фізичний захист, криптозахист
	Паразитні сигнали, наведення	Спеціальні радіотехнічні пристрої	Контроль доступу, криптозахист, пошук закладок, екранування
	Електричні та оптичні сигнали	Апаратні закладки	
	Програмний продукт	Програмні закладки	
– передавання документа по каналах зв'язку	Електричні та оптичні сигнали	Несанкціоноване підмикання, імітація зареєстрованого користувача	Криптозахист
Виробничий процес	Відходи, випромінювання тощо	Спецапаратура різного призначення	Оргтехзаходи, фізичний захист

Крім того, ми обговорюємо замки, віконні решітки, сигналізацію, генератори шуму, мережеві фільтри та скануючі радіоприймачі, призначені для запобігання витоку інформації через потенційні технічні засоби або для їх виявлення. Для захисту інформації на апаратному рівні використовуються апаратні ключі, системи сигналізації, блокування пристроїв та інтерфейси введення/виведення інформації [20,21,24].

Системи зв'язку використовують засоби захисту інформації, що базуються на мережі [18,19,20]:

• брандмауери – використовуються для запобігання атакам із зовнішнього світу, ці правила регулюють спосіб обробки мережевого трафіку. Часто вони розміщуються на вході мережі, щоб розрізняти внутрішні та зовнішні мережі (брандмауер Cisco PIX, брандмауер Symantec Enterprise FirewallTM, Contivity Secure Gateways та Alteon Switched Firewall від Nortel Networks).

• системи виявлення вторгнень – використовуються для захисту від NDS та забезпечення відсутності обслуговування, основою цих атак є використання механізмів, що запобігають шкідливій поведінці, це скорочує час після атаки та витрати на підтримку функціональності мережі (Cisco Secure IDS, Intruder Alert та NetProwler від Symantec).

• засоби створення віртуальних приватних мереж – ці засоби використовуються для створення безпечних каналів передачі даних у незахищеному середовищі, це дозволяє передавати інформацію без необхідності додаткового захисту (Symantec Enterprise VPN, Cisco IOS VPN та Cisco VPN concentrator).

• засоби безпеки корпоративної мережі та потенційних каналів інформаційних атак, це дає можливість запобігати атакам на корпоративну мережу, зменшувати витрати на захист інформації та спостерігати за поточним станом безпеки мережі (Symantec Enterprise Security Manager, Symantec NetRecon).

Технічні канали – зовнішнє електронне випромінювання та наведення акустичних та оптичних каналів. Захист інформації від впливу витоків технічних комунікацій гарантується [18,19,21]:

Використання екранованого кабелю, прокладання проводів та кабелів в екранованих конструкціях, а також конструкція самого екрану – все це приклади цього.

Встановлення потужних фільтрів;

• створення екранованих зон;

Використання екранованого обладнання.

Встановлення активних систем шумозаглушення.

1) витік через структурні коливання в стінах та стелях;

2) видалення інформації зі стрічки принтера, неправильно записаних дискет тощо;

3) стирання інформації за допомогою відеозакладок;

4) програмні та апаратні посібники в комп'ютерах.

5) радіозакладки в стінах та меблях;

6) знищення інформації з вентиляційної системи;

7) видалення акустичної інформації за допомогою лазера;

8) виробництво та створення технологічних відходів;

9) комп'ютерні віруси, логічні бомби тощо;

10) вилучення інформації за допомогою інструкцій та «авторитетів»:

11) дистанційний відеозапис;

12) захоплення акустичної інформації за допомогою диктофонів;

Потенційні шляхи витоку інформації та несанкціонованого доступу до обробленої інформації в типовій одноповерховій будівлі включають такі канали витоку [18,19,21]:

1) крадіжка передавачів інформації.

2) часто використовуваний канал у високотехнологічних побутових приладах.

3) захоплення інформації спрямованим мікрофоном;

4) канали внутрішнього витоку інформації;

5) несанкціоноване відтворення;

6) вихід випромінювання з боку терміналу;

7) захоплення інформації через «телефонне вухо».

8) захоплення клавіатури та принтера акустичним засобом;

9) захоплення дисплея електромагнітним шляхом;

10) візуальне враження від дисплея та принтера;

11) спроба зв'язку через лінії зв'язку та зовнішні канали;

12) витік даних через канали зв'язку;

13) витік води через систему заземлення;

14) витік даних через мережу, що передається;

15) витік даних через трансляційний канал та гучномовці.

16) спрацьовування систем безпеки та пожежної сигналізації;

17) втрата мережі електропостачання;

18) вихід з ладу системи опалення, газо- та водопостачання.

Склад засобів, що використовуються для забезпечення технічного захисту інформації, зокрема від атак соціального чи технологічного характеру, постачальники цих засобів, послуги з встановлення, монтажу, налаштування та обслуговування визначаються власниками, а потім утилізуються Організацією інформаційної безпеки самостійно або спільно з фахівцями в галузі технічного захисту інформації (ТЗІ) відповідно до чинного законодавства. Вибір здійснюється на основі властивостей пошкодженого або складного захисту інформації. Фрагментований захист забезпечує захист від конкретної небезпеки та складних небезпек [18,19,29,30].

TIP – це термін, що охоплює як автономні функції, так і функції, поєднані з TIP у вигляді окремих пристроїв чи компонентів. що вбудовані. Для визначення стану TIP, що обробляється та передається в ІС, комп'ютерних мережах та системах зв'язку. Для висновків, які використовуються для координації рішень, проводиться дослідження щодо стану справ у сфері TZI. Процес розрахунку та визначення зон інформаційної безпеки задокументовано

в нормативних документах щодо TZI та визнано ефективним у захисті інформації. Ці документи також визначають процедуру сертифікації відповідних технічних ресурсів.

Переваги методів TZI полягають у надійності, недоліки – у відсутності гнучкості, великій кількості та кількості використовуваних інструментів, а також у їхній високій вартості [21,26,29].

Основою програмних методів захисту інформації та запобігання зовнішнім атакам є спеціальні пакети або окремі програми, що інтегруються в програмне забезпечення процесорів даних. Ці підходи передбачають використання програмних засобів, які ідентифікують та автентифікують користувачів, контролюють доступ до інформації, шифрують її та видаляють нерелевантну інформацію, все це робиться для перевірки безпеки системи та її захисту, це здійснюється шляхом моніторингу, аудиту та захисту від вірусів.

Ці підходи використовуються для [18,19]:

Автентифікація та ідентифікація користувачів і співробітників.

- Обмеження доступу користувачів до інформації, комп'ютерів та Інтернету.

Автентичність інформації та конфігурація ІС.

Запис та документування дій користувачів називається реєстрацією.

• приховування інформації, що обробляється.

• реагування на санкціоновані спроби.

Для забезпечення їх ефективності необхідно застосовувати превентивні заходи. Одним із критичних компонентів безпеки, який часто ігнорується після впровадження системи чи послуги, є інтеграція в неї заходів безпеки та відсутність спеціальної допомоги. Ефективність заходів безпеки повинна зберігатися, а не як формальний факт.

Вкрай важливо спостерігати за середовищем, переглядати журнал та обробляти інциденти інформаційної безпеки, а також підтримувати стан інформаційної безпеки. Підтримка функціональності засобів має вирішальне значення для безпеки інформаційних технологій, які використовують заходи

безпеки та працюють автоматично, ці заходи підлягають частій перевірці протягом циклу розробки.

Важливо переконатися, що ці кроки виконано правильно. Будь-які інциденти або зміни в SIS повинні бути негайно розпізнані та вжиті відповідні заходи.

Зрештою, спостерігається тенденція до погіршення якості будь-яких послуг або механізмів, метою яких є покращення систем, виявлення проблем та вжиття коригувальних заходів. Це метод підтримки необхідної безпеки інформаційно-технологічної системи. Управління безпекою інформаційних технологій – це безперервний процес [20].

Підтримка функціональності систем та інформаційної безпеки повинна включати такі дії:

Підтримка захисту з метою забезпечення їхньої безперервної роботи.

• перевірка, яка гарантує, що захист достатній для виконання вимог методів.

• управління активами, небезпеками, вразливостями та запобіжними заходами, які призначені для запобігання виникненню небезпечних ситуацій.

• розслідування подій з метою забезпечення реагування на несприятливі події.

Тобто, підтримка здатності функціонувати – це складний процес, який включає багато аспектів, цей процес є тривалим і передбачає критичну оцінку попередніх рішень.

Допомога – заходи, спрямовані на сприяння правильній та доцільній поведінці цих методів під час їхньої експлуатації.

Графіки створюються заздалегідь і дотримуються за призначенням. В результаті витрати зменшуються.

Регулярні аудити необхідні для виявлення проблем. Пристрій, який є захисним, але не перевіряється, не має цінності, оскільки немає підстав вважати його надійним.

Технічне обслуговування. Захисні пристрої вимагають масштабного технічного обслуговування, включаючи нагляд, ми обговорюємо впровадження комплексної програми безпеки, яка включає організацію. Відповідність пристроїв - аудит безпеки пристроїв, оцінка безпеки. Щоб забезпечити ефективний захист рівня безпеки інформаційних технологій, вкрай важливо, щоб впровадження захисних пристроїв повністю відповідало проекту. Це зусилля має бути санкціоновано на кожному етапі проекту та системи, під час етапів проектування, інтеграції та експлуатації, або під час процесу переміщення. [6,20]

Тестування на відповідність слід планувати разом з іншими заходами. На практиці слід використовувати грубі перевірки, оскільки вони надають можливість оцінити співробітників на предмет дотримання вимог. Процеси інспекції важливі для забезпечення ефективного виконання захисних заходів, ці заходи повинні бути впроваджені правильно та перевірені належним чином.

Регулярна робота системи оцінюється щодня з метою використання захисних тактик. Інтерв'ю відіграють значну роль, коли дані є критично важливими під час процесу комунікації. Цей метод сприяє створенню контрольного списку та розробці відповідного стилю звіту, останній з яких містить загальну інформацію, яку потрібно визначити [6,20].

Фізичний захист повинен охоплювати як зовнішні, так і внутрішні аспекти. Обов'язки фізичного захисту включають розпізнавання потрапляння рідини або несправностей систем живлення тощо [6,20].

Перевірка того, що захист дотримано, є складним завданням, і для його виконання необхідні досвід та обізнаність. Ці дії здійснюються без урахування внутрішніх заходів моніторингу чи інспекції [6,20,21,31].

Управління змінами. Інформаційні технології та їх середовище постійно розвиваються. Зміни пов'язані з додаванням нових функцій чи послуг або розпізнаванням нових небезпек чи вразливостей. Ці зміни спричиняють появу нових небезпек та слабкостей [43].

Якщо ми обговорюємо заплановані зміни в системі, то важливо запобігти несправностям, які змінюють механізми захисту. Якщо система має пункт управління конфігурацією або іншу формальну структуру для роботи з технічними змінами в системі, тоді корисно призначити системного спеціаліста та його представника на цю посаду. Ці особи повинні будуть оцінити проблеми або зміни захисту системи та визначити, чи є вони порушенням. У разі змін, спричинених придбанням нового апаратного та програмного забезпечення, корисно провести дослідження, щоб визначити, як найкраще захистити себе. Багато змін у системі слід вважати незначними та не вимагати всебічного аналізу ситуації, яка вимагає змін. Навіть найменші зміни потребують аналізу, і обидва типи змін повинні враховувати переваги та недоліки. Якщо зміни незначні, ефективніше проводити їх неформально, під час зустрічей зі спеціалістами, але остаточне рішення керівництва має бути задокументовано.

Контроль. Важливим етапом циклу є контроль попередньо виконаних кроків. Якщо кроки правильні, адміністрація дізнається:

чи були досягнуті поставлені цілі;

чи є досягнення значними, питання дискусійне.

Контроль повинен включати процедури, що стосуються створення звітів для менеджера з безпеки інформаційних технологій, та постійного управління процесом ІС.

Сутність носія інформації та пов'язаний з ним контент, небезпеки та обмеження інформації призводять до перевірки інформації.

Активи вразливі до виявлення змін їхньої вартості або безпеки їхніх інформаційно-технологічних систем. Загрози та вразливості оцінюються, а зміни їхньої важливості виявляються. Коли виникає загроза або вразливість, її швидко усувають. Зміни в небезпеках та слабкостях призводять, щонайбільше, до зміни активів.

Коли в системі захисту інформації виявляються аномальні дані, проводиться розслідування, а результати повідомляються керівництву. Ці рішення приймаються, включаючи зміну політики безпеки інформаційно-

технологічної системи та проведення аналізу ризиків потенційних небезпек [20,31].

Якщо ми обговорюємо розкриття походження випадку, то доречно зібрати інформацію з журналів та представити її у вигляді єдиного звіту про випадок. Ці історії оцінюються для окремих випадків. Незважаючи на складність створення звіту про інциденти, Основна вимога полягає в категоризації зв'язків між різними журналами.

Керівництво повинно здійснювати щоденний нагляд, готуючи документацію, яка підтримує процедури операційної безпеки. Це корисно для подальшого використання. Документація описує дії, призначені для забезпечення належного рівня безпеки в системі та окремих службах, ці дії включають та призначені для управління системами або службами [20,31].

Документування процесу зміни поточної конфігурації безпеки, що включає зміну параметрів безпеки та модифікацію інформації про безпеку. Ці зміни відповідають процедурі управління конфігурацією системи. Важливо розпізнати процедуру виконання ручного обслуговування, щоб зібрати гарантії, якщо безпека не під загрозою. Розподіл процедури документується для кожного використовуваного компонента безпеки [20,31].

Слід визначити частоту та умови аналізу журналів безпеки, включити опис необхідних методів статистичного аналізу та їх застосування.

Керівництво повинно схвалити інструкції щодо організації аудитів, які перевищують початкову точку.

Управління інцидентами використовується з метою уникнення інцидентів, пов'язаних з безпекою, це неможливо.

Для точної оцінки та визначення ступеня серйозності, для всебічного розуміння ризиків та способів їх успішного усунення, необхідне повне розуміння застосованих заходів безпеки. Варто зібрати інформацію та оцінити її практичні переваги.

Аналіз небезпечних інцидентів має значний вплив, оскільки він поєднує

зусилля компанії щодо роботи з базою даних та її організаційні зусилля щодо запобігання інцидентам.

3.3. Рекомендації по розробці та втіленню системи контролю та управління доступом

Приміщення, важливі для підприємства, повинні мати систему безпеки та контролю доступу (СКД) [15,32].

Встановлення системи безпеки та системи управління є критично важливим для структури організації. Функціональність системи автоматизує виробництво товарів, регулює доступ на територію підприємства та до його будівель, ідентифікує та керує користувачами, запобігає несанкціонованому доступу та дозволяє впроваджувати різні правила щодо доступу до приміщень. Це стало можливим завдяки використанню інформаційних технологій, які швидко розвиваються, що забезпечує нову форму безпеки та контролю як об'єктів, так і інформації про підприємство. Сьогодні існує безліч способів використання системи контролю та управління доступом, залежно від ступеня секретності компанії, її потреб та можливостей. [15,32-34].

Система контролю та управління доступом – це поєднання апаратного та програмного забезпечення, що встановлює засоби безпеки, призначені для: обмеження входу та виходу об'єктів (людей, транспортних засобів) з певної території шляхом створення «точок проходу»: дверей, воріт, контрольно-пропускних пунктів.

Сучасні системи контролю доступу мають такі компоненти:

1. Ідентифікатор – це пристрій, який ідентифікує особу. Сьогодні в цій якості зазвичай використовуються популярні безконтактні картки, контактні картки (з чорною магнітною смугою) та електронні брелоки. Ще однією відмінною рисою може бути спеціальний код, який людина використовує під час входу в обмежену зону, або біометричні дані, що включають відбитки пальців або долонь, або розпізнавання голосу тощо.

2. Зчитувач – це пристрій, який розпізнає інформацію та передає її контролеру.

3. Контролер – це «мозок» системи. Він функціонує як особа, що приймає рішення щодо необхідності доступу до приміщення стосовно певного ідентифікатора. Якщо доступ дозволено, сигнал надсилається на електронний замок (турнікет, шлагбаум або двері). У мережевих системах контролю доступу комп'ютер підключений до контролера разом із блоком керування.

Основне призначення ACS [15,32,33]:

• контроль доступу до певної території, включаючи також доступ до певної території, особи, яка має доступ до певної території, а також облік відпрацьованих годин.

Процес розрахунку заробітної плати в поєднанні з бухгалтерським програмним забезпеченням є трудомістким і схильним до помилок.

Ведення бази даних персоналу та відвідувачів;

• поєднання з усіма системами безпеки.

Використання системи відеоспостереження для об'єднання файлів подій системи, надсилання сповіщень до системи про необхідність початку запису та спрямування камери на результати зафіксованої підозрілої події.

За допомогою системи охоронної сигналізації (SOS) доступ до будівлі може бути обмежений або автоматично знятий з охорони та знову підключений.

Система з пожежною сигналізацією (FAS) використовується для отримання інформації про стан пожежних сповіщувачів, автоматичного розблокування евакуаційних дверей та закриття протипожежних дверей у разі пожежної тривоги.

На об'єктах, спеціально призначених для цієї мети, мережа пристроїв ACS фізично ізольована від інших інформаційних мереж.

Зчитувачі розташовані в точках доступу до об'єкта, ці точки зчитують код, пов'язаний з електронними картками доступу, та передають його менеджерам СКУД.

Потім контролер приймає рішення на основі внутрішньої бази даних користувачів або комп'ютеризованої бази даних, і, дотримуючись запрограмованих алгоритмів керування, контролер керує виконавчими механізмами СКУД.

Кожному користувачеві СКУД, внутрішньому чи зовнішньому, видається пластикова картка, яка електронно зареєстрована в точці керування.

Кожна електронна картка доступу пов'язана з певним користувачем системи, який має права на об'єкт, що контролюється.

Вся відповідна інформація про користувача також зберігається на комп'ютері менеджера системи в базі даних СКУД.

Під час проектування мережі для СКУД враховуються чотири різні рівні взаємодії між мережами.

1. Перший (найвищий) рівень - це клієнт-серверна комп'ютерна мережа, яка базується на протоколі ETHERNET, з протоколом обміну TCP/IP та використовує операційні системи Windows NT або Unix. Цей рівень сприяє зв'язку між сервером та комп'ютерами підсистем, що використовуються для роботи.

2. Другий рівень – це зв'язок між системними контролерами та комп'ютерами-компонентами. На цьому етапі використовується протокол RS 232.

3. Третій рівень – це зв'язок між контролерами та пристроями-слухачами. Тут використовується інтерфейс RS 485, який вже є поширеним, або зчитувач, який використовує магнітну властивість картки.

4. Четвертий рівень – це склад системи пожежної сигналізації та її схем керування – як збалансованих, так і незбалансованих, останні включають радіальний розподіл адрес та пропорційно-інтегральний контролер. Тут використовуються нестандартизовані спеціалізовані інтерфейси та протоколи передачі інформації.

Автоматизовані системи контролю доступу поділяються на два типи: автономні та мережеві [32, 33, 34].

Автономні системи контролю доступу (СКД) складаються з систем, розташованих в одному приміщенні. Їхнє основне призначення — заборонити доступ до об'єктів з обмеженим доступом.

Ці СКД використовуються в організаціях, які мають кілька способів дістатися до об'єкта.

До цієї СКД можна підключити різні компоненти: шлагбауми, турнікети, електромагнітні замки та RFID-зчитувачі. RFID (радіочастотна ідентифікація) — це технологія, яка автоматично ідентифікує об'єкти шляхом запису інформації, що зберігається в RFID, та зчитування цієї інформації за допомогою радіочастотних пристроїв.

Мережеві СКД складаються з систем, які сприяють контролю відвідуваності співробітників на робочих місцях, отриманню різних звітів про відвідуваність у різні періоди часу для кожного співробітника та всього підрозділу в цілому. Ці системи також мають обмежений доступ до контрольованих ресурсів за часом доби. Створіть зони доступу, розподілені по офісах, поверхах, будівлях та інших компонентах, розробіть програмне забезпечення, яке створюватиме особисту картку для кожного співробітника, що містить фотографію, особисту інформацію, марку автомобіля та інші характеристики.[15,32,33,34]

Категоризація ACS наведена в таблиці 3.2.

Однією з найважливіших характеристик ACS є ступінь доступності: обмежена, середня, висока та дуже висока. ACS зазвичай складається з

чотирьох класів з різними рівнями доступу. Залежно від характеру об'єкта, конфігурації ACS та виробника, набір можливостей у кожному класі може відрізнятися та доповнюватися можливостями з інших класів [33,34].

ACS класу 1 складається з автономних систем з низькими зусиллями та низькою потужністю, які забезпечують:

• доступ до зони, що охороняється, для всіх осіб, які мають відповідне посвідчення особи.

• внутрішнє освітлення та звук, що вказує на режим роботи;

• керування (автоматичне або ручне) відкриттям та закриттям шлагбаума (дверей).

Ці системи використовуються, коли клієнт бажає контролювати певний процес.

Таблиця 3.2

Класифікація СКУД

За технічними характеристиками і функціональними можливостями	• рівень ідентифікації; • кількість контрольованих місць; • пропускна здатність; • кількість користувачів; • умови експлуатації
За рівнем ідентифікації доступу	• однорівневі (ідентифікація здійснюється за однією ознакою, наприклад, з зчитування коду картки); • багаторівневі (ідентифікація здійснюється за кількома ознаками, наприклад, з зчитування коду картки і біометричних даних);
За кількістю контрольованих місць	• малої місткості (до 16 місць); • середньої місткості (від 16 до 64 місць); • великої місткості (понад 64 місць);
За умовами експлуатації	• у закритих приміщеннях; • у закритих неопалюваних приміщеннях; • під навісом на вулиці в умовах помірно-холодного клімату; • на вулиці в умовах помірно-холодного клімату; • в особливих умовах (підвищена вологість, запиленість, вібрації і т. п.)

За основними функціональними можливостями	• можливість оперативного перепрограмування; • схемно-технічний та програмний захист від вандалізму і саботажу; • високий рівень секретності; • автоматична ідентифікація; • розмежування повноважень співробітників і відвідувачів з доступу в приміщення і на об’єкт у цілому; • надійне механічне замикання контрольованих місць з можливістю аварійного ручного відкриття; • автоматичний збір і аналіз даних; • вибіркова роздруківка даних. [3]

3.4 Розробка системи фізичного захисту інформації на об'єкті інформаційної діяльності

3.4.1 Опис опорного об’єкта інформаційної діяльності

Кімната з обмеженим доступом розташована на першому поверсі будівлі організації та використовується як приміщення для зустрічей. Вона займає площу 13,5 квадратних метрів (довжина кімнати – 5 метрів, ширина – 2,7 метра).

Вікно кімнати, що охоронятиметься, покрите захисним покриттям зсередини та має ґрати зовні. Висота стелі – 2,7 метра, додаткових стель немає.

Стіни побудовані з цегли, а основа конструкції – з бетону. Електропостачання централізоване. Підлоги – з бетону. Кімната обладнана звуковою системою та обігрівачем, останній заземлений. Немає каналізаційних ліній та резервуарів для води, внутрішніх телефонних ліній, шнурів та зайвого дроту.

Доступ до зони обмеженого доступу мають лише особи, які обіймають керівні посади в компанії та мають засоби для ідентифікації особи та доступу до кімнати. У приміщенні є відеокамери, які спостерігають за територією, система безпеки, яка генерує електроенергію, комплект генераторів, що створюють шум, а двері оснащені механічним замком.

У системі опалення розміщуються діелектричні втулки, їх називають нагрівальними батареями.

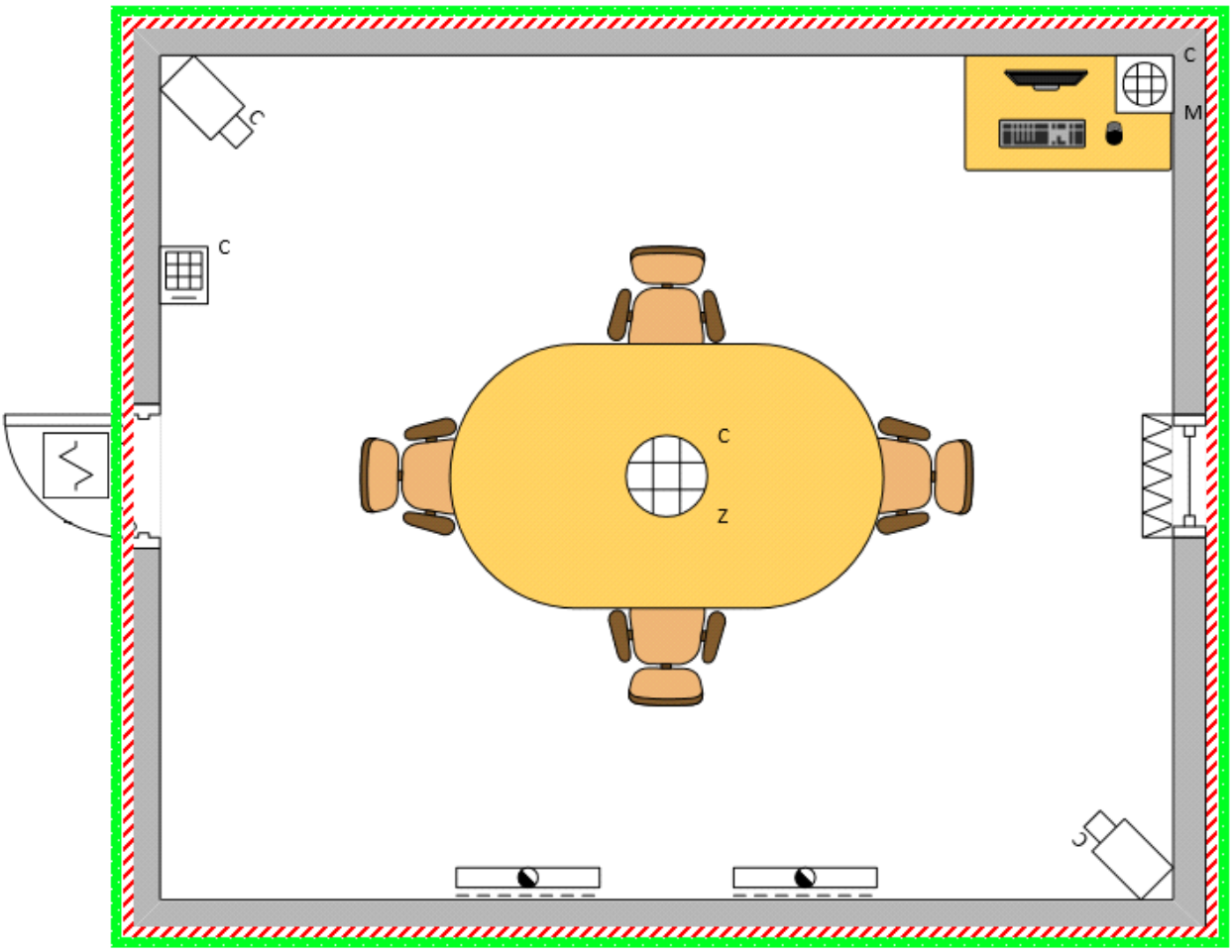
Після того, як гість покидає приміщення, двері герметизуються, всі прилади та інструменти гаснуть, а кімната програмується на спрацювання сигналізації.

Організація працює з 9:00 до 18:00, з перервою на обід, яка починається о 12:00 та закінчується о 13:00.

Повний план приміщення з обмеженим доступом проілюстровано на рис. 3.1.

3.4.2 Підбір та обґрунтування вибору обладнання

Під час побудови системи захисту інформації в обмеженому просторі постає питання, яке обладнання та технічні пристрої гарантуватимуть безпеку інформації в обмеженій зоні. Будуть розглянуті можливі пристрої, які будуть використані під час побудови системи.



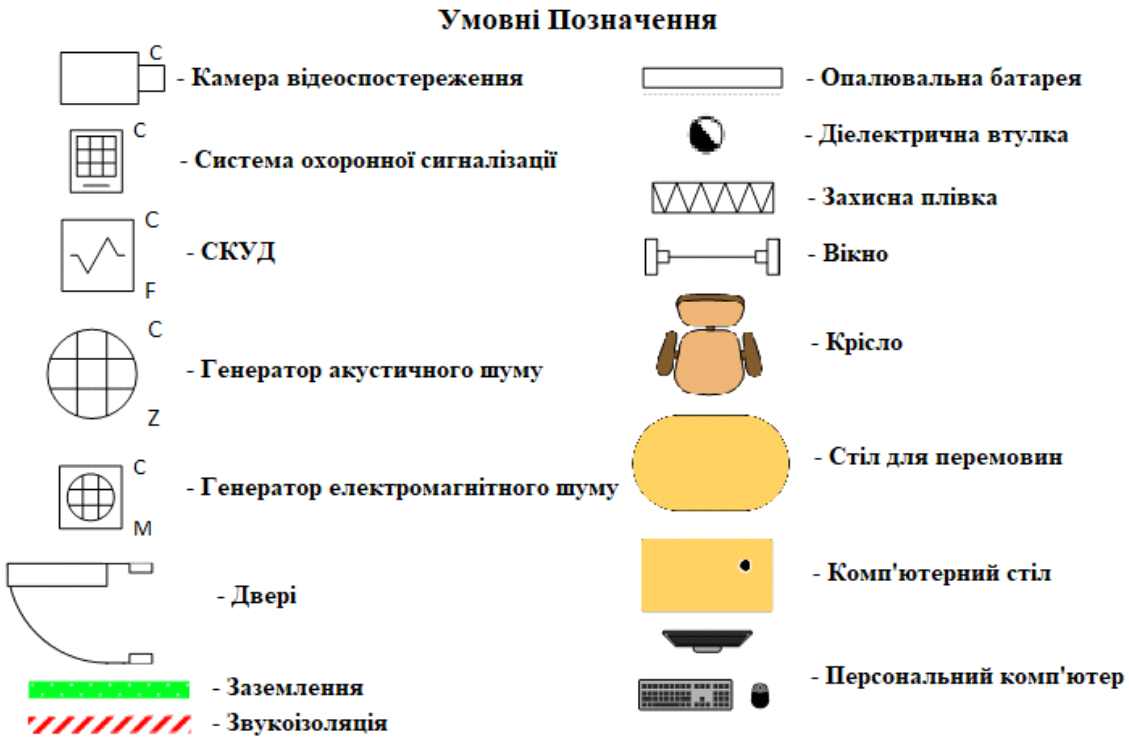


Рис.3.1 Генеральний план приміщення з обмеженим доступом

Вибір камери

На рис.3.2 зображено IP-камери, що були використані для порівняння [22,23].

Рис.3.2 IP-камери

Далі Буде представлено таблицю порівняння найважливіших характеристик IP-камер, і буде обрано найефективніший варіант (Таблиця 3.3) [22,23].

Розглянуті вище характеристики призводять до висновку, що найефективнішим варіантом для системи безпеки приміщення з обмеженим доступом є камера Dahua DHK-IPC-T1B30P.

Такий вибір пояснюється такими перевагами обраної камери порівняно з іншими конкурентами:

наявність 16-кратного цифрового зуму;

низька вартість;

Здатність протистояти вандалізму за протоколом IK08;

• запобігання потраплянню пилу та вологи за протоколом IP67.

низьке енергоспоживання;

Таблиця 3.3

Порівняння характеристик IP-камер

Характеристики	Камера Hikvision DS-2CD1121-I	Камера Dahua DH-IPC-T1B20P	Камера Dahua DH-IPC-HFW1230SP-S2	Камера Dahua DH-SD22204T-GN	Камера Hikvision DS-2CD2543G0-IWS
Ціна, грн	1800	1800	2100	4060	4844
Роздільна здатність камери	2 Мп	2 Мп	2 Мп	2 Мп	4 Мп
Інфрачервоне підсвічування	До 30 м	до 30 м	до 30 м	до 300 м	—
Кут повороту	360°	360°	360°	360°	-30°-+30°
Цифровий зум	—	16x	16x	—	—
Роздільна здатність зображення	1920x¶ 1080	1920x¶ 1080	1920x1080	1920×1080	2688x1520
Споживана потужність	5.5 Вт	4.8 Вт	4,9 Вт	10 Вт	8,5 Вт
Вандалозахищеність	—	+	—	+	+

Крім того, обрана камера має такі можливості:

• інфрачервоне підсвічування, спричинене ICR-фільтром.

висока якість зображення;

• дальність виявлення - 43 м?

• розпізнавач руху;

наявність системи шумозаглушення 3D-DNR;

вибір системи контролю та управління доступом (СКД).

Необхідність використання СКД у нашій системі безпеки очевидна, коли йдеться про контроль входу. Використання біометричних СКД є найефективнішим методом забезпечення безпечного доступу до об'єкта. Обрані СКД зображені на рис. 3.3 [23,35].

Рис.3.3 Елементи СКУД

Вивчивши атрибути, найефективнішим вибором для СКУД є Hikvision DS-K1CT5011SF.

Серед переваг цієї СКУД:

Простий у використанні інтерфейс;

Відзначається наявність камери.

• міцний та щільний матеріал корпусу, який є довговічним та високоякісним;

• низька вартість;

• захист від пилу та вологи;

Додатково, обрана СКУД має низку атрибутів:

• максимальна кількість рукописних цифр - 5001;

• підтримка подвійного аудіопотоку;

• функція захоплення зображення, вбудована в камеру (опція 2 МП);

Кілька режимів автентифікації включають: QR-код, відбиток пальця, картку, відбиток пальця + пароль тощо;

• Максимальна кількість карток - 50 000, Максимальна кількість записів контролю доступу - 200 000 000

• Виявлення недозволеного доступу, розблокування на основі понаднормового часу, перевірка неправильної картки на момент спрацьовування тривоги, виявлення на основі насильства тощо.[37]

Таблиця 3.4

Порівняння характеристик СКУД

Характе-ристики	Hikvision DS-K1T605M	Hikvision DS-K1T501SF	ZKTECO F11	ROSSLARE AY-B1660	ROSSLARE AYC-B7661
Ціна, грн	14 400	6 400	6520	6667	6718
Матеріал корпусу	Метал	Метал	Пластик	пластик	Пластик
Тип системи	Розпізнавання обличчя + безконтакт на картка	відбиток пальця + безконтактна картка	відбиток пальця + безконтактна картка	відбиток пальця + безконтактна картка	відбиток пальця + безконтактна картка
Живлення	12В	12В	12В	5 - 16В	10 - 16В
Інтерфейс	Wiegand 26/34, RS-485	Wiegand 26/34, RS-485	Wiegand 26	Wiegand 26	Wiegand 26
Пило-вологозахищеність	—	+	—	—	—
Наявність камери	+	+	—	—	—

Вибір генератора шуму, який створює звук в акустичній області.

Генератор акустичного шуму призначений для захисту об'єктів від витоку секретної інформації за допомогою віброакустичних та акустичних засобів. Це досягається шляхом генерації маскованого шумового сигналу. Генератори шуму, що створюють акустичний шум, порівнюються на рис. 3.4.[23,36]

Розглянувши властивості генераторів шуму, що створюють акустичний шум, ми обрали модель RIAS-2GS як остаточний вибір.

Цей генератор має такі переваги:

Конкурентна ціна;

Широкий діапазон роботи;

Здатність працювати від батарейок.

Вихідна потужність підсилювача повинна бути не менше 10 Вт;

Voice Noice 4M2

Топаз ГША-4

РІАС-2ГС

DNG-2300

Рис.3.4 Генератор акустичного шуму

Таблиця 3.5

Порівняння характеристик генераторів акустичного шуму

Характеристики	Voice Noice 4M2	Топаз ГША-4	PIAC-2ГС	DNG-2300
Ціна, грн	3600	9864	7800	20540
Діапазон робочих частот	50…8000 Гц	170--5700 Гц	180 Гц до 5,6 кГц	250—6500 Гц
Електроживлення	7...9 В	220±22 В	220 ± 22 В	220В
Вихідна потужність підсилювача	не менше 2.5 Вт	не менше 6 Вт	не менше 10 Вт	не менше 8 Вт
Мінімальний опір навантаження	2 Ом	4 Ом	4 Ом	3 Ом
Можливість роботи від акумулятора	+	—	+	—

Крім того, RIAS-21GS має низку інших переваг:

Глибина регулювання рівня шуму в робочому діапазоні частот не менше 20 дБ.;

Генератор ефективний у діапазоні температур: +10 ÷ +40 С°;

Час технічної готовності не більше 1 секунди.;

Середній максимальний звуковий тиск у робочому діапазоні частот з похибкою встановлення не більше 6 дБ на відстані 1 метра від випромінювача відносно нульового значення 2х105 Па (для звукового тиску) - не менше 70 дБ.

Генератор входить до переліку засобів загального захисту, дозволених законодавством України, яке формується Адміністрацією спеціального зв'язку України.[21,31]

Вибір генератора шуму, що використовує електроенергію.

Генератор електромагнітного шуму призначений для маскування пристроїв збору інформації, лабораторій, персональних комп'ютерів та обчислювальної техніки шумовим сигналом, що є надокучливим та поширеним за частотою, який потім проектується в навколишній простір, схеми та засоби зв'язку. Різні типи генераторів електромагнітного шуму, що порівнюються, зображено на рис. 3.5 [23,36]

Салют 2000 Б

Гном-3

Старкад-32

РІАС-1ГМ

Рис.3.5 Генератори електромагнітного шуму

Беручи до уваги вищезазначені характеристики, найефективнішим генератором шуму буде генератор електромагнітного шуму RIAS-21GMI.

Переваги цього генератора:

Система автоматичного керування функціями генератора розташована як у пульті дистанційного керування, так і в генераторі. Ця система є автоматичною, а її функцію індикують світлові та звукові сигнали. Система може бути розташована на робочому місці користувача або в центральному центрі управління. Панель управління також дозволяє дистанційно активувати/деактивувати генератор.

Таблиця 3.6

Генератори електромагнітного шуму

Характеристики	Салют-2000-Б	Гном-3	Старкад-32	РІАС-1ГМ
Ціна, грн	6500	10500	8300	9200
Регулювання рівня сигналу, що підводиться до випромінюючих систем	—	—	+	+
Наявність сигналізації (види оброблюваних тривог і аварій)	—	+	+	+
Максимальна споживана потужність	10 Вт	не більше 20 Вт	12.95 Вт	не більше 20 Вт
Діапазон частот	10 кГц – 400 МГц	10 кГц – 2.5 ГГц	10 кГц – 400 МГц	10 кГц – 2 ГГц
Коефіцієнт якості шуму	Не менше 0.9	Не менше 0.8	Не менше 0.9	Не менше 0.8
Електроживлення	220В±10%, 50 Гц	220В,50Гц	220В, 50Гц	220±22 В, 50 (±1) Гц
Можливість роботи від акумулятора	—	—	—	+

Максимальна сумарна вихідна потужність становить 5 Вт, і повинна бути більше 3,3 Вт.

Величина коефіцієнта міжспектральної кореляції повинна бути не менше 2,0.

Генератор входить до списку засобів загального захисту, дозволених законодавством України, яке формується Адміністрацією спеціального зв'язку України.[31]

Вибір системи охоронної сигналізації

Охоронні сповіщення призначені для розпізнавання спроб проникнення на об'єкт, що охороняється, це робиться для того, щоб забезпечити обробку, зберігання, представлення та передачу інформації щодо спроби проникнення. (Рис. 3.6) [22, 23,36]

Рис.3.6 Системи охоронної сигналізації

Максимальна сумарна вихідна потужність становить 5 Вт, і повинна бути більше 3,3 Вт.

Величина коефіцієнта міжспектральної кореляції повинна бути не менше 2,0.

Генератор входить до списку засобів загального захисту, дозволених законодавством України, яке формується Адміністрацією спеціального зв'язку України.[31]

Вибір системи охоронної сигналізації

Охоронні сповіщення призначені для розпізнавання спроб проникнення на об'єкт, що охороняється, це робиться для того, щоб забезпечити обробку, зберігання, представлення та передачу інформації щодо спроби проникнення. (Рис. 3.6) [22, 23,36]

Таблиця 3.7.

Системи охоронної сигналізації

Характеристики	Tecsar Alert Ward	DSC WP-8010-Kit	Ajax StarterKit
Ціна, грн	2 900	10 414	5 799
Особливості	-Підтримує до 99 безпровідних датчиків; -Канал зв'язку GSM; -Робоча радіочастота 433 МГц; -Робоча відстань між датчиками і централлю до 30/100 метрів (закрите приміщення / відкритий простір); -Управляється за допомогою мобільного додатку; -При тривозі: дзвінок з голосовим повідомленням, відправка SMS і push повідомлення; -Оснащений вбудованою сиреною (80 дБ), працює з сиренами.	-Кількість розділів: 3; -Кількість бездротових пристроїв PowerG: 30; -Кількість бездротових клавіатур: 8; -Кількість виходів: 1 на платі +5; -Кількість дротяних зон на платі: 1; -Вбудована сирена: +; -Вбудована клавіатура: +; -Кількість користувачів: 8; -Мобільний додаток: Android, iOS.	-Проста інсталяція завдяки кріпленням SmartBracket; -Система працює на Ethernet з підключенням GSM в якості резервного каналу зв'язку; -Двосторонній зв'язок з пристроями; -Бездротова технологія Jeweller дозволяє розкинути мережу на відстані до 2000 метрів на відкритому просторі або на декількох поверхах; -Час роботи на резервному живленні сягає 7 годин.

Інше обладнання

Слід використовувати інше обладнання, яке допоможе захистити приміщення від сонячних променів, а також захисне металеве покриття на вікні кімнати, яке служитиме для його екранування. Через численні шари металу, що входять до складу конструкції, та інформацію, що витікає через віброакустичні та електромагнітні канали, захисна плівка не може запобігти витоку інформації через ці канали. У нашій системі безпеки ми використовуватимемо покриття Ultra Vision R Silver (рис. 3.7).[37]

Властивості плівки Ultra Vision R Silver наведено в таблиці 3.8.

Ще одним необхідним доповненням для захисту приміщення з обмеженим доступом є серія діелектричних втулок, що встановлюються на нагрівальних елементах (радіаторах). Діелектричні втулки - це компоненти, які не мають провідності та встановлюються замість роз'ємного з'єднання між

компонентами трубопроводу. Основне призначення діелектричних втулок - екранувати себе від розсіяного електричного поля.

Таблиця 3.8

Характеристики плівки Ultra Vision R Silver

Ціна, грн (за рулон)	300
Тип плівки	Металізована, тонуюча
Проникність світла	50%
Товщина	2 мм
Кількість шарів	3
Коефіцієнт затемнення	0.28

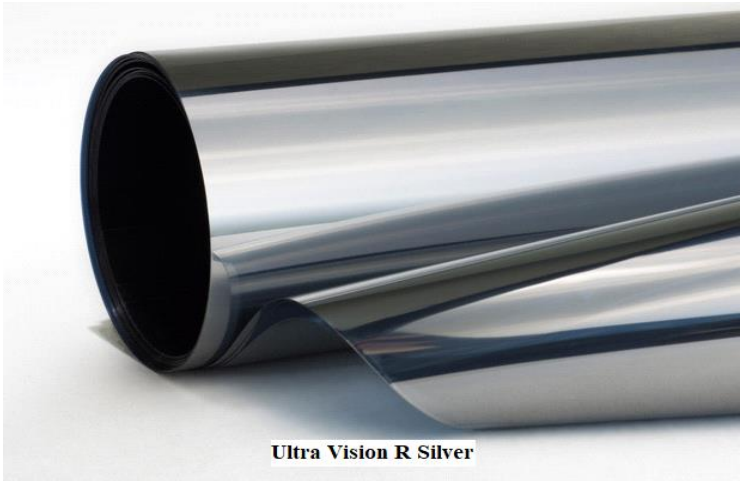


Рис.3.7 Захисна металізована плівка

Для максимального ступеня захисту приміщення буде звукоізольоване. Для звукоізоляції будуть використані акустичні панелі ECOSOUND PYRAMID GAIN BLACK, які мають більший спектр звукопоглинання, ніж їхні аналоги, завдяки спеціальній конструкції, яка посилює пористу природу конструкції. Така конструкція дозволяє краще поглинати звукові хвилі пористою природою конструкції. Надзвичайно прості в установці та переміщенні, не схильні до механічних пошкоджень завдяки еластичності використаного матеріалу [17,38].

Визначимо кількість акустичних панелей, необхідних для звукоізоляції [17,38]:

Висота стелі = 2,7 м.

Довжина кімнати - 5 метрів.

Площа кімнати = 13,5 квадратних метрів;

Довжина кімнати = 2,7 м

Таким чином, загальна площа бічних стін становить 4,1 квадратних метра, або 41,58 квадратних метрів, при довжині 5 метрів та ширині 2,7 метра.

Площа підлоги та площа стелі: 2×(5 м×2,7 м) = 27 кв.м.

Загальна площа кімнати становить 41,58 кв.м + 27 кв.м = 69 кв.м.

3.5 Висновки по розділу

1. Сформульовано рекомендації щодо організації фізичного захисту об'єкта інформаційної діяльності. Задокументовано використання механічних, електричних, електронних пристроїв та систем, які є автономними та запобігають зовнішньому втручанню з метою доступу до секретної інформації.

2. Встановлено рекомендовані практики щодо процесу застосування методів технічного захисту до об'єкта інформаційної діяльності. Ці пропозиції включають технічний захист, інформацію щодо апаратного забезпечення, захисту мережі та захисту програмного забезпечення. Для підтримки ефективності та належної роботи системи технічного захисту було зроблено кілька пропоицій щодо її технічного забезпечення.

3. Створено рекомендовані практики для сприяння розробці та впровадженню системи контролю доступу та управління нею. Задокументовано склад системи контролю доступу та її зв'язок з іншими системами технічного захисту та

4. Створено систему фізичного захисту інформації за місцем проведення інформаційної діяльності. Склад обладнання вже відомий, а його вибір є правомірним.

ВИСНОВКИ

У процесі підготовки кваліфікаційного завдання було виконано такі дії:

- Визначено процес поширення інформації в об'єкті інформаційної діяльності, проведено аналіз загроз щодо інформаційної безпеки та технічний аналіз витоку інформації в об'єкті інформаційної діяльності.

- Проведено дослідження системи захисту інформації на об'єктах інформаційної діяльності.

- Досліджено шляхи та надано пропозиції щодо вдосконалення системи фізичного захисту інформації на об'єктах інформаційної діяльності.

1. У першій частині кваліфікації описано метод поширення інформації в об'єкті інформаційної діяльності. Визначено метод класифікації інформації за змістом та способи доступу до неї. Обговорено методи та способи доступу до інформації. Визначено інформацію, що підлягає захисту, та описано правила інформаційної безпеки.

Проведено аналіз загроз та визначено інформацію з технічних питань. Продемонстровано склад каналу витоку технічної інформації.

Проведено дослідження технічних каналів витоку інформації та представлено класифікацію результатів. Зокрема: розподіл інформації за видами діяльності, принцип створення небезпечного сигналу, середовище поширення небезпечного сигналу та метод захоплення (або видалення) небезпечного сигналу за допомогою технічного інтелекту супротивника.

2. У другій частині процесу кваліфікації розкриваються фундаментальні принципи та концепції, пов'язані з технічними системами захисту та інформаційної безпеки. Перераховуються фундаментальні компоненти фізичної, апаратної, програмної та криптографічної системи захисту інформації. Надається опис та розгорнутий вигляд активних інфрачервоних методів транспортування. Документується склад та опис окремих компонентів системи технічного моніторингу у фокусі інформаційної діяльності. Розглядається процес застосування систем відеоспостереження, пасивних

інфрачервоних методів виявлення, ультразвукових датчиків, магнітних датчиків, фотоелектричних датчиків та інших датчиків, призначення, принцип та сфера застосування цих пристроїв, а також їх комбінованих систем.

3. У третій частині кваліфікаційного завдання надано пропозиції щодо організації фізичного захисту об'єкта інформації. Задокументовано використання механічних, електричних, електронних пристроїв та систем, які є автономними та запобігають зовнішньому втручанню з метою доступу до секретної інформації. Встановлено рекомендовані практики щодо процедури застосування методів технічного захисту до об'єкта інформаційної діяльності. Ці пропозиції включають технічний захист, інформацію щодо апаратного забезпечення, захисту мережі та захисту програмного забезпечення. Для підтримки ефективності та належної роботи системи технічного захисту було зроблено кілька пропозицій щодо її технічного забезпечення.

Створено рекомендації щодо створення та впровадження системи контролю доступу та системи управління. Задокументовано склад системи контролю доступу та її зв'язок з іншими системами технічного захисту та мережевою взаємодією.

Створено систему фізичного захисту інформації на інформаційному об'єкті. Склад обладнання вже відомий, а його вибір є правомірним.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Головань С.М. Нормативне забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко, Д.В. Чирков, Л.М. Щербак / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 533 с.

2. Садердинов А.А., Трайнёв В.А., Федулов А.А. Информационная безопасность предприятия/ ИТК Дашков и К. –М., 2005. ––336 с.

3. www.ik.3dscorpion.com.ua

4. www.factor-ltd.by

5. Інформаційно-психологічна протидія в Національній гвардії України (психологічний аспект) [Текст] : монографія / І. В. Воробйова, Я. В. Мацегора, І. І. Приходько та ін.; за заг. ред. проф. І.І. Приходька; 2-ге вид. – Х.: Національна акад. НГУ, 2016. – 265 с.

6. Кормич Б.А. Інформаційна безпека: організаційно-правові основи [Текст] : навч. посібник для студ. вищих навч. закл. / Б.А. Кормич. –К.: Кондор, 2004. – 384 с.

7. Термінологічний довідник з питань технічного захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.

8. Каторин Ю.Ф. Большая энциклопедия промышленного шпионажа / Ю.Ф.Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко. – СПб.: ООО «Издательство Полигон», 2000. – 896 с.

9. Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013. – [Second edition 2013-10-01]. – Geneva, 2013. – P. 23.

10. Information technology. Security techniques. Information security risk management: ISO/IEC 27005:2011. – [Second edition 2011-06-01]. – Geneva, 2011. – P. 68.

11. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. В 2-х томах. Том I. Несанкционированное получение

информации – К.: Арий, 2008. - 464 с.

12. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г Защита информации в телекоммуникационных системах.. — К.: МК-Пресс, 2005. — 288 с, ил.

13. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии Учебное пособие. – М.: Академия, 2009. – 416 с.

14. Кашкаров А.П. Системы видеонаблюдения. Практикум. Ростов-на-Дону: Феникс, 2014. — 120 с.: ил. — ISBN: 978-5-222-22579-0.

15. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. –М.: Горячая линия – Телеком, 2013. – 272 с.

16. Гришина Н.В. Организация комплексной системы защиты информации. М.: Гелиос АРВ, 2007. — 256 с, ил.

17. Хорев А.А. Технические каналы утечки акустической (речевой) информации – М.: Специальная Техника, №№4, 5, 6 - 2004 год. 37 с.

18. Андрончик А.Н., Богданов В.В. Домуховский Н.А. и др. Защита информации в компьютерных сетях. Практический курс/ А.Н. Андрончик, В.В. Богданов, Н.А. Домуховский, А.С. Коллеров, Н.И. Синадский, Д.А. Хорьков, М. Ю. Щербаков. – Екатеринбург: УГТУ-УПИ, 2008. – 248 с. — ISBN: 978-5-321-01219-2

19. Мохор В. В. Наставления по кибербезопасности (ISO/IEC 27032:2013) / В. В. Мохор, А. М. Богданов, А. С. Килевой. К.: ООО «Три-К», 2013. — 129 с.

20. Домарєв В.В. Організація захисту інформації на об’єктах державної та підприємницької діяльності /Домарєв В.В., Скворцов С.О./ Навч. Посібник. – К.: Вид-во Європейського університету, 2006. – 102с.

21. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами, Учебное пособие. – СПб.: НИУ ИТМО, 2012. – 416 с.

22. https://worldvision.com.ua/ua/datchiki-dvizheniya-tekhnologicheskie-osobennosti/

23. http://www.sirius.kiev.ua/images/documents/instrukcii

24. Груба И.И. Системы охранной сигнализации. Технические средства обнаружения / И.И Груба — М.: Солон-Пресс, 2012. — 220 с.

25. https://secur.ua/kombinirovannyj-datchik-dvizhenija-i-razbitija-satel-navy.html

26. ДСТУ EN 54-1:2003 Системи пожежної сигналізації. Частина 1. Вступ (EN 54-1:1996, IDT)

27. https://secur.ua/ua/articles/ua_ogljad-zasobiv-ohoroni-i-bezpeki.html

28. Горніцька Д. А. Система социотехнических атак в информационной среде / Д. А. Горніцька, О. Г. Корченко, В. П. Харченко // Проблемы экономики и управления на железнодорожном транспорте. Материалы второй международной научно-практической конференции. − .: ЭКУЖТ, 2007. − С. 137-138.

29. Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект) // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - К., 2000. - С 50-52.

30. Кормич Б.А. Інформаційна безпека: організаційно-правові основи [Текст] : навч. посібник для студ. вищих навч. закл. / Б.А. Кормич. – К. : Кондор, 2004. – 384 с. – (Юридична книга).

31. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. 2000, 37 с.

32. Гинце А. А. Особенности СКУД систем доступа крупных распределенных объектов / А. А. Гинце. ААМ Систем, 2005.

33. Волхонский В.В. Системы контроля и управления доступом - СПб: Университет ИТМО, 2015.

34. О. К. Юдін, О. М. Весельська. Аналіз та класифікація систем контролю та управління доступом на підприємстві. Наукоємні технології, 2(38), 2018. С. 220-225

35. https://valtek.com.ua/ua/system-integration/security-control-system/access-control/access-control-review.

36. https://tzi.com.ua/zagalnij-oglyad-sistem-vbroakustichnogo-zashumlennya.html.

37. https://plenka.market/ua/ultra_vision_r_silver_20_1524_m/

38. https://ecosound.kiev.ua/akucticheckie-paneli

ДОДАТОК А

Оформлення слайдів та роздаткового матеріалу

Система захисту об’єкту інформаційної діяльності від несанкціонованого доступу до каналів передачі конфіденційних даних

Кваліфікаційна робота магістра

Здобувач: Нікіта СТРУК
Керівник: Михайло РІЗАК

Актуальність теми

- захист інформації на об’єктах інформаційної діяльності є критично важливим для державної,
- оборонної, економічної та комерційної сфер;
- наявність каналів передавання конфіденційних даних створює ризики несанкціонованого доступу,
- витоку та порушення цілісності інформації;
- ефективний фізичний та технічний захист потребує комплексного поєднання організаційних,
- інженерних, апаратних і програмних заходів;
- для конкретного ОІД потрібні рекомендації з урахуванням умов функціонування, загроз і технічної
- інфраструктури.

Мета, об’єкт і предмет дослідження

Мета	Об’єкт	Предмет
підвищення ефективності функціонування системи захисту ОІД від НСД до каналів передачі конфіденційних даних.	процес захисту інформації на об’єкті інформаційної діяльності.	система захисту інформації на об’єкті інформаційної діяльності.

Основні задачі

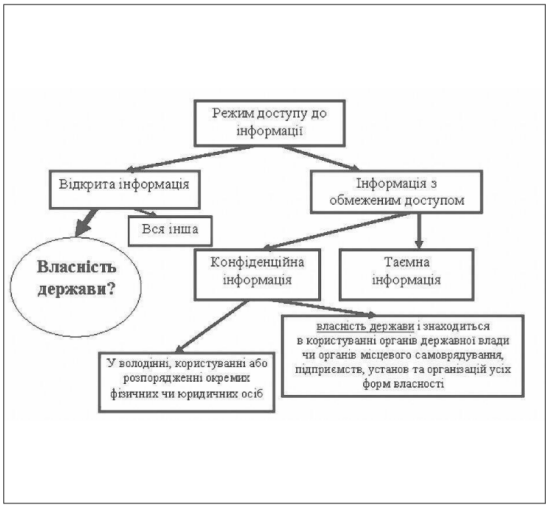
- визначити порядок розподілу інформації на ОІД та провести аналіз загроз;
- проаналізувати технічні канали витоку інформації;
- дослідити засоби фізичного, технічного та організаційного захисту;
- розробити рекомендації щодо удосконалення системи фізичного захисту.

Структура кваліфікаційної роботи

Розділ 1	Розділ 2	Розділ 3
Захист інформації на об’єктах інформаційної діяльності	Огляд системи захисту інформації на ОІД	Дослідження напрямків удосконалення системи фізичного захисту

Робота охоплює аналіз інформаційних загроз, класифікацію каналів витоку, огляд технічних засобів охорони та формування практичних рекомендацій для посилення фізичного захисту об’єкта.

Режим доступу до інформації на ОІД



- відкрита інформація - доступна кожному, крім випадків
- обмеження законом;
- інформація з обмеженим доступом - конфіденційна, таємна
- або службова;
- захист має забезпечувати цілісність, секретність і доступність;
- доступ до ІзОД повинен надаватися лише ідентифікованим та
- уповноваженим користувачам.

Загрози інформаційній безпеці та канали витоку

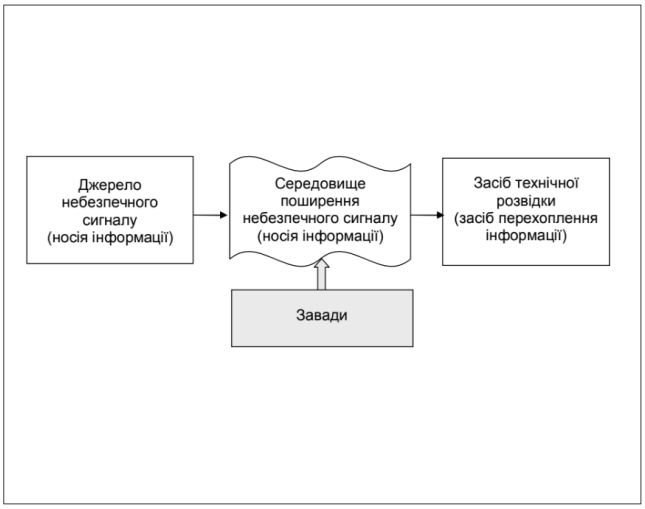
Основні категорії технічних каналів

радіочастотні	побічне випромінювання
електричні	мережі живлення
акустичні	заземлювальні кола
оптичні	мікрофонний ефект
матеріальні	вбудовані пристрої

Висновок

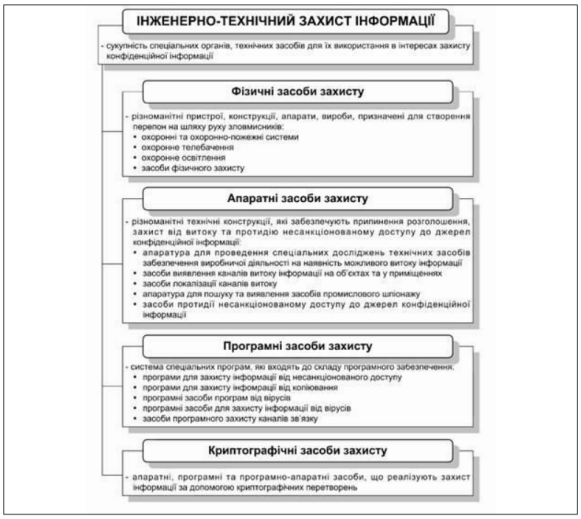
Кожне джерело небезпечного сигналу за певних умов може утворити канал витоку технічної інформації, тому система захисту повинна бути багаторівневою та контрольованою.

Структура технічного каналу витоку інформації



- джерело небезпечного сигналу є носієм інформації;
- середовище поширення може бути електричним,
- магнітним, акустичним, оптичним або матеріальним;
- засіб технічної розвідки здійснює прийом та
- перетворення сигналу;
- завади впливають на можливість перехоплення, але не
- усувають ризик витоку.

Інженерно-технічний захист інформації



- фізичні засоби формують перешкоди для руху порушника;
- апаратні засоби спрямовані на запобігання витоку та НСД до
- джерел інформації;
- програмні засоби забезпечують захист від копіювання, вірусів
- та НСД;
- криптографічні засоби реалізують захист через криптографічні
- перетворення.

Фізичні засоби захисту ОІД

Засоби виявлення	датчики, сповіщувачі, охоронне телебачення, контроль периметра
Засоби перешкоджання	огорожі, укріплені двері, решітки, шлюзи, сейфи, замки
Системи реагування	тривожна сигналізація, пожежна сигналізація, оповіщення, контрольні пости

Фізичний захист має будуватися як послідовність рубежів, що ускладнюють проникнення, забезпечують раннє виявлення порушника та створюють час для реагування служби безпеки.

Технічні системи спостереження та охоронної сигналізації

Компоненти системи

- відеокамери спостереження
- приймально-контрольні панелі
- активні та пасивні ІЧ-засоби
- магнітоконтактні та фотоелектричні сенсори
- вібраційні та акустичні сповіщувачі

Призначення

- контроль периметра та зон обмеженого доступу
- фіксація спроб проникнення або пошкодження
- автоматичне формування тривожного повідомлення
- підтримка доказової бази та журналювання подій

Засоби виявлення порушення режиму безпеки

- активні інфрачервоні засоби - створюють контрольований промінь або бар’єр;
- пасивні інфрачервоні сповіщувачі - реагують на теплові зміни у зоні контролю;
- ультразвукові сенсори - аналізують зміну параметрів акустичного поля;
- магнітоконтактні сповіщувачі - контролюють стан дверей, вікон і люків;
- вібросенсори та сповіщувачі розбиття скла - виявляють механічний вплив на конструкції.

Оптимальна конфігурація має поєднувати різні типи сенсорів для зменшення ймовірності обходу системи та підвищення достовірності тривожних подій.

СКУД і приймально-контрольне обладнання

Функції СКУД

- ідентифікація користувачів та розмежування прав
- доступу;
- керування проходами, дверима, турнікетами та
- електромагнітними замками;
- реєстрація подій доступу та формування журналів;
- інтеграція з відеоспостереженням та охоронною
- сигналізацією.

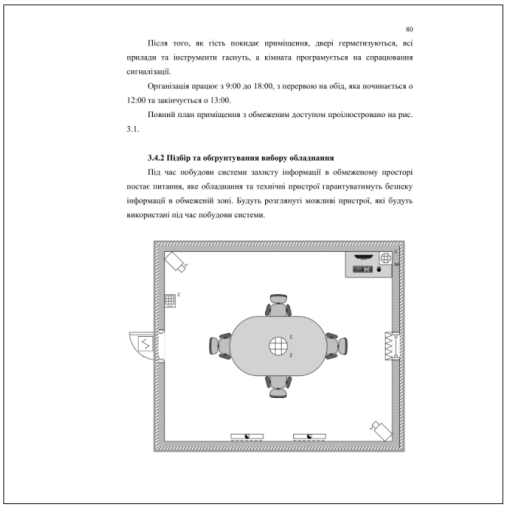
Контрольні панелі

- збір сигналів від сповіщувачів;
- обробка тривожних станів;
- передавання повідомлень на пост охорони;
- контроль працездатності шлейфів і ліній зв’язку.

Рекомендації щодо організації фізичного захисту

1. визначити межі контрольованих зон та рівні доступу;
2. забезпечити інженерні бар’єри на периметрі та у критичних приміщеннях;
3. розмістити засоби виявлення за принципом послідовних рубежів;
4. інтегрувати відеоспостереження, СКУД і тривожну сигналізацію;
5. організувати перевірку працездатності системи та регламент технічного обслуговування.

Підбір обладнання та побудова системи захисту



80

Після того, як гість покидає приміщення, двері герметизуються, всі прилади та інструменти гаснуть, а кімната програмується на спрацювання сигналізації.

Організація працює з 9:00 до 18:00, з перервою на обід, яка починається о 12:00 та закінчується о 13:00.

Повний план приміщення з обмеженим доступом проілюстровано на рис. 3.1.

3.4.2 Підбір та обґрунтування вибору обладнання

Під час побудови системи захисту інформації в обмеженому просторі постає питання, яке обладнання та технічні пристрої гарантуватимуть безпеку інформації в обмеженій зоні. Будуть розглянуті можливі пристрої, які будуть використані під час побудови системи.

- обладнання має відповідати зоні контролю, режиму доступу та
- очікуваному сценарію загроз;
- для об’єкта доцільне поєднання охоронної сигналізації,
- відеоспостереження, СКУД та інженерних перешкод;
- приймально-контрольні прилади повинні забезпечувати
- централізований контроль стану рубежів;
- система має підтримувати масштабування та технічне обслуговування
- без втрати захисних властивостей.

Основні результати роботи

- систематизовано порядок розподілу інформації на об’єкті інформаційної діяльності;
- проаналізовано загрози інформаційній безпеці та технічні канали витоку;
- проведено огляд фізичних, апаратних, програмних і криптографічних засобів захисту;
- обґрунтовано застосування технічних систем охорони, відеоспостереження та контролю доступу;
- запропоновано рекомендації щодо удосконалення системи фізичного захисту інформації на ОІД.

Практичне значення: підвищення стійкості ОІД до НСД і витоку конфіденційних даних