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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Комплексна система захисту об'єкту інформаційної діяльності від витоку інформації технічними каналами передачі 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

_____ Єгор СЕРДЮК

Виконав: здобувач вищої освіти групи СЗДМ 61
Єгор СЕРДЮК

Керівник: _____ТУРОВСЬКИЙ Олександр___
д.т.н. , професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2025

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

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___125-Кібербезпека та захист інформації_____
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСК
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Сердюку Єгору Романовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Комплексна система захисту об'єкту інформаційної діяльності від витоку інформації технічними каналами передачі даних»
керівник кваліфікаційної роботи ТУРОВСЬКИЙ Олександр, д.т.н., професор

затверджені наказом Державного університету інформаційно-комунікаційних технологій
від « 15 » жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи 20.12.2024 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 розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Огляд процесів обробки та захисту конфіденційних даних на об'єктах інформаційної діяльності
4.2. Аналіз системи запобігання несанкціонованого доступу до конфіденційних даних на об'єкті інформаційної діяльності
4.3. Розробка рекомендацій щодо удосконалення система захисту об'єкту інформаційної діяльності від витоку конфіденційних даних технічними каналами

5. Перелік графічного матеріалу: ___Презентаційний матеріал на слайдах.

6. Дата видачі завдання _____20.10.2024 ___ _____

КАЛЕНДАРНИЙ ПЛАН

/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
	Підбір науково-технічної літератури		
	Написання першого розділу роботи		
	Написання другого розділу роботи		
	Написання третього розділу роботи		
	Написання висновків по роботі		
	Підготовка демонстраційних матеріалів		
	Підготовка доповіді		

Здобувач вищої освіти _____ Єгор СЕРДЮК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Олександр ТУРОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 90 сторінок, має 21 рисунки, 7 таблиці. Список використаних джерел містить 38 найменування і займає 4 сторінки.

Метою кваліфікаційної роботи є удосконалення системи захисту об’єкту інформаційної діяльності від витоку конфіденційних даних технічними каналами.

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 процесів обробки та захисту інформації на об'єктах інформаційної діяльності. Проаналізовано порядок функціонування системи запобігання несанкціонованого доступу до конфіденційних даних на об’єкті інформаційної діяльності. Досліджено шляхи та розроблено рекомендації щодо удосконалення система захисту об’єкту інформаційної діяльності від витоку конфіденційних даних технічними каналами.

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

Предмет дослідження. Система захисту інформації від несанкціонованого витоку технічними каналами на об’єкті інформаційної діяльності.

Апробація:

Є.Р. Сердюк, Р. С. Марчук, О. В. Рожков. Напрямки удосконалення єдиної моделі комплексної системи захисту від витоку інформації технічними каналами. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.92-93. https://duikt.edu.ua/uploads/p_2661_93669247.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 90 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 improve the system of physical protection of information at the objects of information activity.

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 processes of processing and protecting information at the objects of information activity is conducted. The procedure for the functioning of the system for preventing unauthorized access to confidential data at the object of information activity is analyzed. Ways are investigated and recommendations are developed for improving the system for protecting the object of information activity from the leakage of confidential data through technical channels.

Object of research. The process of protecting information at the object of information activity

Subject of research. Information protection system at the object of information activity.

Approbation:

E.R. Serdyuk, R. S. Marchuk, O. V. Rozhkov. Directions for improving a single model of a comprehensive system of protection against information leakage through technical channels. All-Ukrainian scientific and practical conference: Current problems of information and telecommunication systems security. Kyiv, November 3, 2024, Kyiv: RVC DUIKT. - 024. P.92-93.
https://duikt.edu.ua/uploads/p_2661_93669247.pdf

Keywords: INFORMATION PROTECTION SYSTEMS, OBJECT OF INFORMATION ACTIVITY, TECHNICAL CHANNELS OF INFORMATION OUTPUT, 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 розвитку суспільства, однією з найактуальніших проблем, яка є не тільки в Україні, а й в світі, полягає в захисту інформації на об’єктах інформаційної діяльності. Актуальність цього питання визначається великим значенням інформації різного характеру, володіння якою чинить великий вплив при вирішенні питання державного, оборонного, економічного чи комерційного характеру. Одним з аспектів вирішення вказаного питання є організація та здійснення фізичного захисту інформації на об'єктах інформаційної діяльності в умовах загроз і обмежень. Це, в свою чергу, вимагає проведення відповідних досліджень та розробки рекомендацій щодо втілення системи фізичного захисту інформації на визначеному об'єктах інформаційної діяльності відповідно умов та впливів, що характеризують його діяльність та можливі загрози зовнішнього доступу до інформації з обмеженим доступом на вказаному об’єкті.

Метою кваліфікаційної роботи є удосконалення системи захисту об’єкту інформаційної діяльності від витоку конфіденційних даних технічними каналами і.

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

- проведено огляд процесів обробки та захисту конфіденційних даних на об’єктах інформаційної діяльності;

- проаналізовано систему запобігання несанкціонованого доступу до конфіденційних даних на об’єкті інформаційної діяльності;

- розроблено рекомендацій щодо удосконалення система захисту об’єкту інформаційної діяльності від витоку конфіденційних даних технічними каналами.

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

Предмет дослідження. Система захисту інформації від несанкціонованого витоку технічними каналами на об’єкті інформаційної діяльності.

Розділ 1.
ОБРОБКА ТА ЗАХИСТ КОНФІДЕНЦІЙНИХ ДАНИХ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

1.1 Порядок розподілу інформації на об'єкті інформаційної діяльності

Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [1].

За своїм змістом інформація поділяється на такі види [1,2,3,4]:

– інформація про фізичну особу;
– інформація довідково-енциклопедичного характеру;
– інформація про стан довкілля (екологічна інформація);
– інформація про товар (роботу, послугу);
– науково-технічна інформація;
– податкова інформація;
– правова інформація;
– статистична інформація;
– соціологічна інформація;
– інші види інформації [1].

Втім для практичного використання більш важливою є класифікація інформації за порядком доступу до неї. У відповідності до цього інформація поділяється на: відкриту та з обмеженим доступом (Рис. 1.1) [2].

Відкрита - будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. Основними ознаками відкритої інформації є те, що доступ до неї надається будь-яким зацікавленим особам, а будь-яке обмеження права на одержання відкритої інформації забороняється [1,2].

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

– систематична публікація її в офіційних друкованих виданнях (бюлетенях, збірниках);

– поширення її засобами масової комунікації;

– безпосереднє надання її зацікавленим громадянам, державним органам та юридичним особам [1,2].

Рис.1.1 Режим доступу до інформації

ІзОД - інформація, що становить державну або іншу передбачену законом таємницю, а також конфіденційна інформація, що є власністю держави або вимога щодо захисту якої встановлена законом [1,5].

Таємна інформація - вид інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані, у порядку встановленому Законом, державною таємницею і підлягають охороні державою. Інформація, що становить державну таємницю, в свою чергу, поділяється на категорії відповідно до Закону України “Про державну таємницю” [1,5].

Конфіденційна інформація - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб

поширюються за їх бажанням відповідно до передбачених ними умов. Стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ - надано статус конфіденційної [1,5].

У відповідності до Закону "Про захист інформації в інформаційно-телекомунікаційних системах" захисту в системі підлягає [1,5]:

- відкрита інформація, яка є власністю держави і у визначенні Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація);
- конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу (далі - конфіденційна інформація);
- інформація, що становить державну або іншу передбачену законом таємницю (таємна інформація).

Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення [1,5].

Усі дії, що пов’язані з обробкою інформації з обмеженим доступом виконуються на об’єктах інформаційної діяльності. Відповідно до визначення об'єкт інформаційної діяльності – будівлі, приміщення, транспортні засоби чи інші інженерно-технічні споруди функціональне призначення яких передбачає обіг інформації з обмеженим доступом [1,5]. Інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави [1,5].

Обробка ІзОД на об’єктах інформаційної діяльності дозволяє забезпечити безпеку інформації, яка полягає в збереженні наступних критеріїв інформаційної безпеки [1,2,3,4]:

- цілісність - властивість інформації бути захищеною від несанкціонованого знищення, модифікації;
- конфіденційність - властивість інформації бути захищеною від несанкціонованого ознайомлення;
- доступність - властивість інформації бути захищеною від несанкціонованого блокування.

З метою задоволення інформаційних потреб, органи державної влади, місцевого й регіонального самоврядування створюють інформаційні служби, системи, мережі, бази й банки даних. Порядок їх формування, структура, права і обов'язки визначаються Кабінетом Міністрів України або іншими органами державної влади, а також органами місцевого й регіонального самоврядування [1,5].

Основними видами інформаційної діяльності є одержання, використання, поширення й зберігання інформації [1,5].

Одержання інформації – це придбання й накопичення відповідно до чинного законодавства України документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою [1,5].

Використання інформації – це задоволення інформаційних потреб громадян, юридичних осіб і держави. Поширення інформації – це розповсюдження, обнародування, реалізація у встановленому законом порядку

документованої або публічно оголошуваної інформації [1,6].

Зберігання інформації – це забезпечення належного стану інформації і її матеріальних носіїв [5,6].

Одержання, використання, поширення і зберігання документованої або публічно оголошуваної інформації здійснюється у порядку, передбаченому цим Законом та іншими законодавчими актами в галузі інформації. Крім того, можна виділити діяльність, пов'язану з інформаційним забезпеченням –одержання, оцінки, зберігання та переробки даних, створена з метою вироблення управлінських рішень. Це стосується різних видів діяльності, наприклад виробничої і збутової, сервісного обслуговування, включаючи підвищення технологічності виробництва, якості вироблюваної продукції, зниження її собівартості, рекламу, інформацію про асортимент продукції, ціни, форми організації сервісу тощо [5,6].

Будь який вид інформаційної діяльності (включно інформаційний бізнес) не може здійснюватися в умовах ізоляції. Його учасники (контрагенти), тобто продавець чи покупець, роботодавець чи найманий робітник функціонують у певному середовищі, яке визначає їх позиції і називається середовищем підприємницької діяльності (підприємництва) [5,6].

Кожне підприємство не може існувати без бюджету. На основі розроблених бюджетів у системі управління здійснюється координація різних видів діяльності підприємства, узгодження діяльності всіх його підрозділів, контроль і оцінка ефективності. На початку звітного періоду бюджет являє собою план чи стандарт, що формалізує сподівання менеджерів щодо продажів, витрат й інших фінансових операцій у наступному періоді. Наприкінці звітного періоду бюджет відіграє роль вимірника, що дозволяє менеджерам управляти за відхиленнями: порівнювати отримані результати з запланованими величинами і коректувати подальшу діяльність. Якщо розробка бюджетів і прогнозів заснована на тому самому комплексі вихідних даних і припущеннях про надходження, виплати, величину товарно-матеріальних запасів, рівні ділової активності, то вони будуть відповідати один одному, і утворять взаємозалежну

систему. Раціональне використання коштів дозволить більш ефективно застосовувати технології щодо покращення роботи підприємства, стратегії його розвитку та інформаційної захищеності підприємства в цілому та його матеріальних активів [5,6].

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

Захист інформації є одним із найважливіших у загальному комплексі заходів технічного захисту інформації (ТЗІ). Несанкціоноване ознайомлення із інформацією з метою її подальшого використання є можливим шляхом перехоплення її зловмисниками [1.5,6].

Для нелегального знімання інформації використовуються різні технічні засоби. Інформація з об'єкта надходить зловмисникові по різним фізичним каналам [6,7].

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх поширення і способів перехоплення повідомлення, технічні канали витоку можна розділити на [7,8]:

- радіоканал;
- електричний;
- акустичний;
- оптичний;
- матеріально-речовий [7].

Аналіз фізичної природи численних випромінювачів показує, що [6,7]:

- джерелами небезпечного сигналу є елементи, вузли і провідники технічних засобів забезпечення виробничої та трудової діяльності, а також радіоелектронна апаратура;
- кожне джерело небезпечного сигналу за певних умов може утворити технічний канал витоку інформації;

- кожна електронна система, що містить в собі сукупність елементів, вузлів і провідників, володіє безліччю технічних каналів витоку інформації. Радіоканали витоку інформації утворюються за рахунок:
- мікрофонного ефекту;
- магнітного поля;
- паразитної генерації;
- по ланцюгах живлення;
- по ланцюгам заземлення;
- за рахунок взаємного впливу;
- електромагнітного випромінювання;
- ВЧ нав'язування;
- із волоконно-оптичних систем зв'язку.

Структура технічного каналу витоку інформації в загальному випадку включає (Рис. 1.2) джерело сигналу або передавач, середу поширення електричного струму або електромагнітної хвилі і приймач сигналу [7].

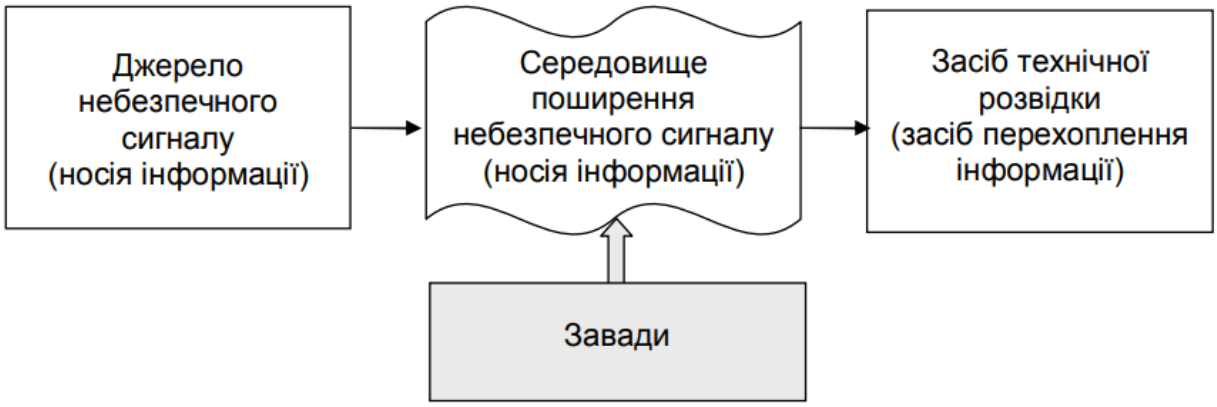


Рис. 1.2 Структура технічного каналу витоку інформації

1.3. Аналіз технічних каналів витоку інформації

Для встановлення вимог та організації захисту інформації від витоку технічними каналами здійснена їх класифікація за певними ознаками.

Зокрема відокремлені типи ТКВІ за такими ознаками [6,7]:

- за видом інформаційної діяльності на ОІД,
- за принципом (фізичним ефектом, процесом) формування небезпечного сигналу (носія інформації),
- за середовищем поширення небезпечного сигналу,
- за способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника.

За видом інформаційної діяльності на ОІД відокремлюються такі типи ТКВІ:

- технічні канали витоку мовної інформації,
- технічні канали витоку інформації, що обробляється в ОТЗС,
- технічні канали витоку візуальної інформації,
- матеріально-речовинні канали витоку інформації.

Класифікацію ТКВІ за принципом (фізичним ефектом, процесом) формування небезпечного сигналу, середовищем поширення небезпечного сигналу та способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника доцільно розглянути у межах визначених вище типів ТКВІ.

Технічні канали витоку мовної інформації за цими ознаками поділяються на такі [7,8]:

- Акустичні канали.
- Акустовібраційні (віброакустичні) канали.
- Акустооптоелектронні (лазерні акустичні) канали.
- Акустоелектричні канали.
- Відеоакустичні канали.
- Канали ВЧ нав’язування (для зняття мовної інформації).
- Канали витоку мовної інформації на основі закладних пристроїв.

Технічні канали витоку інформації, що обробляється в ОТЗС, поділяються на такі [7,8]:

- Канали побічних електромагнітних випромінювань.

- Канали побічних електромагнітних наведень.
- Канали “паразитної” модуляції сигналів ВЧ генераторів.
- Канали “паразитної” ВЧ генерації підсилювачів.
- Канали перехоплення (зняття) інформації з волоконно-оптичних ліній передачі даних.
- Канали перехоплення (зняття) інформації з каналів зв’язку.
- Канали ВЧ нав’язування (для зняття інформації, що обробляється в ОТЗС).
- Канали витоку інформації, що обробляється в ОТЗС, на основі закладних пристроїв.

Технічні канали витоку візуальної інформації поділяються на Такі [7,8]:

- Візуальні канали.
- Візуально оптичні канали.
- Канали витоку візуальної інформації на основі закладних пристроїв.

Матеріально-речовинні канали витоку інформації [7,8,9,10]:

- Добування інформації з магнітних та інших носіїв інформації засобів ЕОТ, що вийшли з ладу.
- Добування інформації з чернеток документів, з відходів виробництва, видавницької діяльності, діловодства тощо.
- Хімічні канали.
- За носієм інформації та принципом формування небезпечного сигналу відокремлюються такі ТКВІ [7,8]:

1. Електромагнітні канали витоку інформації, до яких відносяться канали побічних електромагнітних випромінювань, канали “паразитної” ВЧ генерації підсилювачів, канали “паразитної” модуляції ВЧ генераторів, канали перехоплення інформації з ліній радіо- (радіорелейного, стільникового, мобільного) зв’язку та тому подібні;
2. Електричні канали витоку інформації, до яких відносяться канали побічних електромагнітних наведень на комунікації, канали зняття інформації з ліній провідного зв’язку та тому подібні;

3. Параметричні канали витоку інформації, до яких відносяться, канали ВЧ нав’язування, канали “паразитної” модуляції та тому подібні.

За місцем перехоплення інформації засобами технічної розвідки противника відокремлюються такі типи ТКВІ [7,8,9,10]:

- канали перехоплення (зняття) інформації за межами КЗ,
- канали перехоплення (зняття) інформації за межами КЗ з активним впливом на параметри технічного каналу витоку інформації (наприклад, канал ВЧ нав’язування),
- канали зняття інформації засобами технічної розвідки, встановленими на ОІД (наприклад, технічні канали витоку інформації закладними пристроями).

Розглянута класифікація технічних каналів витоку інформації дозволяє систематизувати уявлення про них та встановити вимоги і заходи щодо захисту інформації від витоку відповідними ТКВІ.

1.4 Висновки по розділу

1. Подано порядок розподілу інформації на об’єкті інформаційної діяльності. Визначено класифікацію інформації за змістом та порядком доступу. Подано способи та режими доступу до інформації. Визначено інформацію, яка підлягає захисту та подано критерії інформаційної безпеки.

2. Проведено аналіз загроз та визначено канали витоку технічної інформації. Показана структура технічного каналу витоку інформації.

3. Здійснено аналіз технічних каналів витоку інформації та подана їх класифікація. Яка включає розподіл за видом інформаційної діяльності, принципом формування небезпечного сигналу, за середовищем поширення небезпечного сигналу, за способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника.

Розділ 2.
СИСТЕМА ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО КОНФІДЕНЦІЙНИХ ДАНИХ НА ОБ'ЄКТІ 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

Технічний засіб охорони – це базове поняття, що позначає апаратуру (вид техніки), яка використовується у складі комплексів (систем) технічних засобів призначених для охорони об'єктів (територій, будівель, приміщень) від несанкціонованого проникнення [7.11].

Історично склалося декілька підходів до вирішення проблем класифікації ТЗО. В роботі буде розглянутий підхід, який можна характеризувати як узагальнений, не провокуючий полеміки на предмет більшої або меншої коректності тих або інших підходів, бо їх відмінності виникають з відмінностей цілком певної мети класифікації. Деякі незручності для розуміння можуть створювати відмінності в термінології, коли близькі поняття позначаються різними словами, як то: засіб виявлення, датчик, сповіщувач. Іноді стосовно конкретних фізичних принципів дії застосовується слово "детектор,, як різновид сповіщувача. По суті до всіх цих термінів слід відноситися як до синонімів, що позначають близькі поняття - елементи апаратури технічних засобів охоронної сигналізації (ТЗОС), виконуючих функцію реагування на зовнішню дію. Наприклад, сейсмічний ЗВ реагує на коливання ґрунту, викликане рухом якого-небудь (людини, тварини) або чого-небудь (автомобіля, трактора і ін..). Кожний ЗВ будується на певному фізичному принципі, на основі якого діє його чутливий елемент (ЧЕ) (наприклад, електромагнітний, вібраційний, радіотехнічний, ємкісний, оптичний і ін.) [7,11,12].

Таким чином:

– засіб виявлення - це пристрій, призначений для автоматичного формування сигналу із заданими параметрами (сигналу тривоги, сигналу спрацьовування або сповіщення) унаслідок вторгнення або подолання об'єктом виявлення чутливої зони (говорять також – зони виявлення) даного пристрою.

– чутливий елемент - це первинний перетворювач, що реагує на дію на нього (пряме або непряме) об’єкта виявлення і сприймає зміну стану навколишнього середовища [9].

При виборі і впровадженні ТЗОС на об'єктах приділяється особлива увага досягненню високої захищеності апаратури від її подолання (обходу).

Виробники ТЗОС пропонують різні способи реалізації цього завдання: контроль відкриття блоків, автоматична перевірка справності засобів виявлення і каналів передачі інформації, захист доступу до управління апаратурою за допомогою кодів (паролів), архівація всіх виникаючих подій, захист інформаційних потоків між складовими частинами ТЗОС методами маскування і шифрування і ін. Як правило, сучасні ТЗОС мають одночасно декілька ступенів захисту [10,12].

Таким чином, одним з головних завдань при проектуванні ТЗОС є створення засобів захисту від обходу їх зловмисником (порушником) і це є складним багатоплановим завданням [7,11].

Під комплексом ТЗОС розуміється сукупність функціонально зв'язаних засобів виявлення, системи збору і обробки інформації і допоміжних засобів і систем (системи тривожного сповіщення, системи охорони периметра і ін..), об'єднаних завданням по виявленню порушника [9].

2.1.2. Фізичні засоби захисту

Фізичні засоби захисту— це різноманітні пристрої, конструкції, апарати, вироби, призначені для створення перепон на шляху руху зловмисників.

До фізичних засобів відносяться механічні, електромеханічні, електронні, електронно-оптичні, радіо- і радіотехнічні та інші пристрої для заборони

несанкціонованого доступу (входу, виходу), пронесення (винесення) засобів і матеріалів та інших можливих видів злочинних дій.

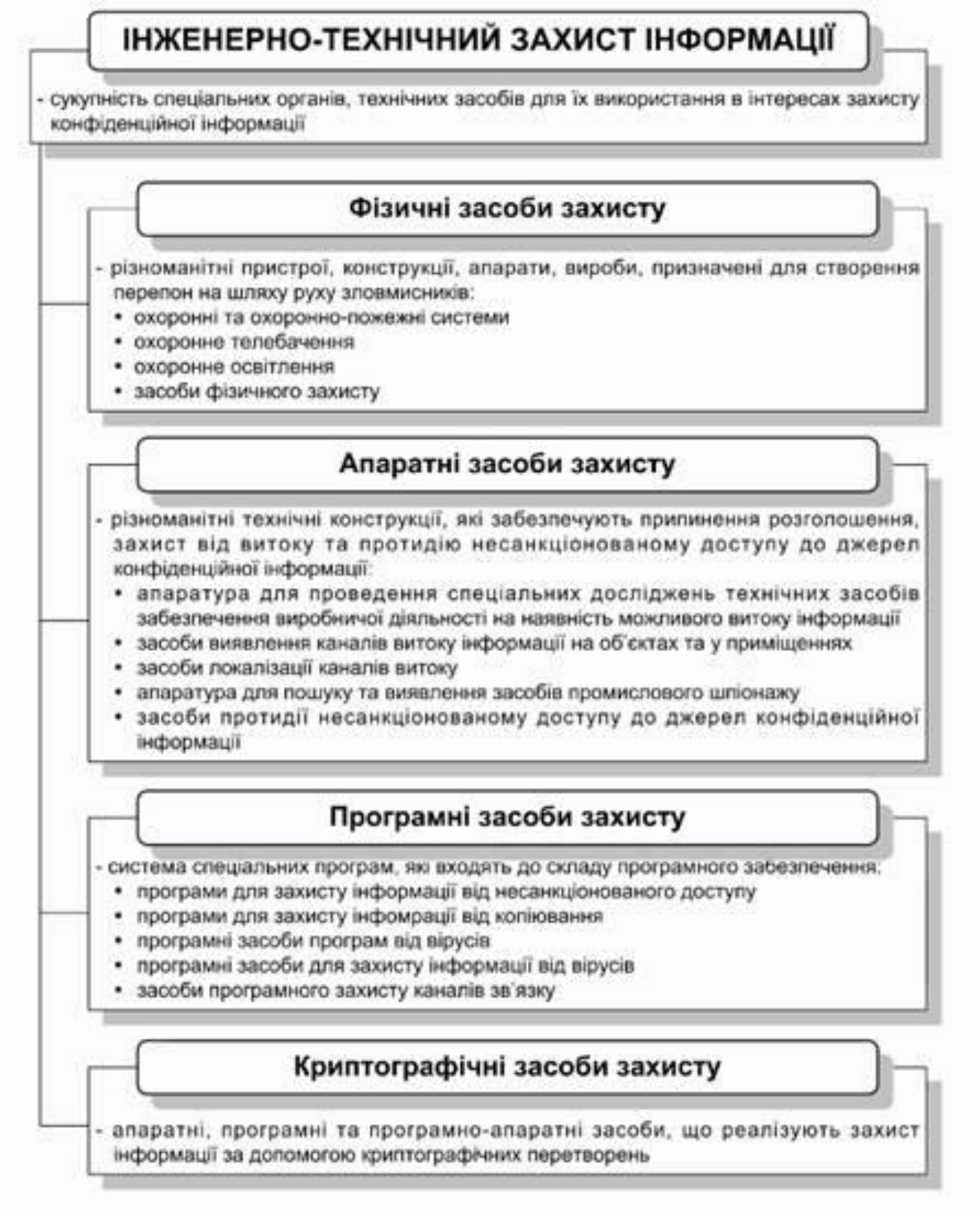


Рис. 2.1 Інженерно технічний захист інформації

Ці засоби застосовуються для вирішення наступних завдань [11]:

• охорона території підприємства на спостереження за нею;

• охорона будівель, внутрішніх приміщень та контроль за ними;

• охорона обладнання, продукції, фінансів та інформації;

• здійснення контрольованого доступу до будівель та приміщень.

Усі фізичні засоби захисту об'єктів можна розділити на три категорії: засоби попередження, засоби виявлення та системи ліквідації загроз. Охоронна сигналізація та охоронне телебачення, наприклад, відносяться до засобів виявлення загроз; загорож;! навколо об'єктів — це засоби попередження

несанкціонованого проникнення на територію, а підсилені двері, стіни, стелі, грати на вікнах та інші заходи служать захистом також; і від проникнення, і від інших злочинних дій (підслуховування, обстрілу, кидання гранат і т.ін.) [7,9,11,12]. Засоби пожежогасіння відносяться до систем ліквідації загроз.

У загальному випадку за фізичною природою та функціональним призначенням усі засоби цієї категорії можна поділити на наступні групи [11]:

• охоронні та охоронно-пожежні системи;

• охоронне телебачення;

• охоронне освітлення;

• засоби фізичного захисту.

Охороні системи та засоби охоронної сигналізації призначені для виявлення різноманітних видів загроз: спроб проникнення на об'єкт захисту, в зони та приміщення, які охороняються, спроб пронесення (винесення) зброї, засобів промислового шпіонажу, викрадення матеріальних та фінансових цінностей та інших дій; оповіщення співробітників охорони або персоналу об'єкта про появу загроз та необхідність підсилення контролю доступу на об'єкт, територію, в будівлі та приміщення [11,12,13].

Найважливішими елементами охоронних систем є датчики, які виявляють появу загрози. Характеристики та принципи роботи датчиків визначають основні параметри та практичні можливості охоронних систем.

Уже розроблені та широко використовується значна кількість різноманітних датчиків як за принципами виявлення різноманітних фізичних полів, так і за тактичним призначенням.

Ефективність роботи системи охорони та охоронної сигналізації, в основному, визначається параметрами та принципом роботи датчиків. На сьогодні відомі датчики наступних типів: механічні вимикачі, дріт із вимикачем, килимки тиску, металева фольга, дротова сітка, мікрохвильові датчики, ультрахвильові датчики, інфрачервоні датчики, фотоелектричні датчики, акустичні датчики, вібраційні датчики, індуктивні датчики, ємнісні датчики і т.ін.

Кожний тип датчика реалізує певний вид захисту: точковий захист, захист по лінії, захист по площі або захист по об'єму. Наприклад, механічні датчики орієнтовані на захист лінії, килимки – на точкове виявлення, а інфрачервоні знаходять широке застосування на площі і в об'ємі.

Датчики через ці чи інші канали зв'язку з'єднані з контрольно-приймальним пристроєм пункту (або поста) охорони і засобів тривожного оповіщення.

Каналами зв'язку в системах охоронної сигналізації можуть бути спеціально прокладені проводові або кабельні лінії, телефонні лінії об'єкта, лінії зв'язку трансляції, системи оповіщення або радіоканали. Вибір каналів визначається можливостями об'єкта.

Важливим об'єктом охоронної системи є засоби тривожного оповіщення: дзвінки, лампочки, сирени, які подають постійні або перервні сигнали про появу загрози.

За тактичним призначенням охоронні системи поділяються на системи охорони [11,14,15]:

• периметрів об'єктів;

• приміщень та проходів до службових та складських будівель;

• сейфів, обладнання, основних та допоміжних технічних засобів;

• автотранспорту;

• персоналу, у тому числі й особового складу охорони, і т.ін. До засобів фізичного захисту відносяться:

• природні та штучні перепони (бар'єри);

• особливі конструкції периметрів, проходів, віконних та дверних плетінь, приміщень, сейфів, сховищ і т.ін.;

• зони безпеки.

Природні та штучні бар'єри призначені для протидії незаконному проникненню на територію об'єкта. Проте основне захисне навантаження лягає все-таки на штучні бар'єри — такі як паркани та інші види огорож;. Практика показує, що огорож;! складної конфігурації здатні затримати зловмисника на

достатньо тривалий час. На сьогодні нараховується значний арсенал таких засобів: від простих сітчастих до складних комбінованих огорож, які здійснюють певний відлякуючий вплив на порушника [11,15].

Особливі конструкції периметрів, проходів, віконних сплетінь, приміщень, сейфів, сховищ є обов'язковими з точки зору безпеки для будь-яких організацій та підприємств. Ці конструкції повинні протистояти будь-яким способам фізичного впливу зі сторони кримінальних елементів [11,15]:

• механічним деформаціям, руйнуванню свердлінням, термічному та механічному різанню тощо;

• несанкціонованому доступу шляхом підробки ключів, відгадування коду тощо.

Одним із головних технічних засобів захисту проходів, приміщень, сейфів та сховищ є замки. Вони бувають простими (з ключами) кодовими (у тому числі з часовою затримкою на відкривання) і з програмним пристроями, що відкривають двері та сейфи в певний час.

Важливим засобом фізичного захисту є планування об'єкта, його будівель та приміщень за зонами безпеки, які враховують міру важливості різних частин об'єкта з точки зору нанесення збитків від різного виду загроз. Оптимальне розташування зон безпеки та розташування в них ефективних технічних засобів виявлення, відбиття та ліквідації наслідків протиправних дій складає основу концепції інженерно-технічного захисту об'єкта.

Зони безпеки повинні розташовуватися на об'єкті послідовно, від огорож;! навкруг території об'єкта до сховищ цінностей, створюючи ланцюг перешкод (рубежів), які доведеться долати зловмисникові. Від складності та надійності перепони на його шляху залежить відрізок часу, необхідного на подолання кожної зони, та ймовірність того, що розташовані в кожній зоні засоби виявлення (охороні пости, охоронна сигналізація та охоронне телебачення) виявлять наявність порушника та подадуть сигнал тривоги.

Основу планування та обладнання зон безпеки об'єкта складає принцип рівноміцності границь зон безпеки. Сумарна міцність зон безпеки буде оцінюватися найменшою з них [11,15].

Охоронне телебачення є одним із розповсюджених засобів охорони. Особливістю охоронного телебачення є можливість не тільки відзначити порушення режиму охорони об'єкта, але й контролювати обстановку навкруги нього в динаміці її розвитку, визначати небезпеку дій, вести приховане спостереження та здійснювати відеозапис для наступного аналізу правопорушення як із метою вивчення, так і з метою притягнення до відповідальності порушника [11,14. 15].

Джерелами зображення (датчиками) в системах охоронного телебачення є відеокамери. Через об'єктив зображення зловмисника попадає на світлочутливий елемент камери, в якому воно перетворюється в електричний сигнал, який подається спеціальним коаксіальним кабелем на монітор і при необхідності — на відеомагнітофон.

Відеокамера є центральним елементом системи охоронного телебачення, так як від її характеристик залежить ефективність та результативність всієї системи контролю та спостереження. На сьогоднішній день розроблені та випускаються найрізноманітніші моделі, які відрізняються як за конструкцією та габаритами, так і за можливостями.

Другим за значення елементом системи охоронного телебачення є монітор. Він повинен підходити за параметрами з відеокамерою. Часто використовують один монітор із декількома камерами, які приєднуються до нього почергово засобами автоматичного переключання за певним регламентом.

У деяких системах телевізійного спостереження передбачається автоматичне приєднання камери, в зоні огляду якої виникло порушення. Використовується й більш складне обладнання, яке включає засоби автоматизації, пристрої одночасного виведення декількох зображень, детектори руху для подавання сигналу тривоги при виявленні будь-яких змін у зображенні [11,14,15].

Обов'язковою складовою частиною системи захисту будь-якого об'єкта є охоронне освітлення. Розрізняють два види охоронного освітлення — чергове та тривожне.

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

Тривожне освітлення вмикається при надходженні сигналу тривоги від засобів охоронної сигналізації. Окрім того, за сигналом тривоги на додаток до освітлення можуть включатися і звукові прилади (дзвінки, сирени і т.ін.).

Сигналізація та чергове освітлення повинні мати резервне електроживлення на випадок аварії або вимкненні електромереж.

Останніми роками велика увага надається створенню систем фізичного захисту, сполучених із системами сигналізації. Так відома електронна система сигналізації для використання з дротовим загородженням. Система складається з електронних датчиків та мікропроцесора, який керує блоком оброблення даних. Загородження довжиною до 100 м може встановлюватися на відкритій місцевості або розташовуватися на стінах, горищах та на наявних огорожах [11,14,16].

Стійкі до впливу навколишнього середовища датчики монтуються на стійках, кронштейнах. Дротове загородження складається з 32 горизонтально натягнутих стальних ниток, у середній частині кожної з яких кріпиться електромеханічний датчик, який перетворює зміну натягу ниток в електричний сигнал.

Перевищення граничної величини напруги, яке програмується за амплітудою для коленого датчика окремо, викликає сигнал тривоги. Зв'язок системи з центральним пунктом управління та контролю здійснюється за допомогою мультиплексора. Мікропроцесор автоматично через певні інтервали часу перевіряє роботу компонентів апаратури та програмних засобів і, у випадку встановлення відхилень, подає відповідний сигнал.

Подібні і ряд інших аналогічних систем фізичного захисту можуть використовуватися для захисту об'єктів по периметру з метою виявлення вторгнення на територію об'єкта.

Використовуються системи з двох волоконно-оптичних кабелів, по яких передаються кодовані сигнали інфрачервоного діапазону. Якщо в сітці нема пошкоджень, то сигнали поступають на приймальний пристрій без спотворень. Спроби пошкодження сітки призводить до обривів або деформації кабелів, що викликає сигнал тривоги. Оптичні системи відрізняються низьким рівнем помилкових тривог, викликаних впливом на неї дрібних тварин, птахів, зміною погодних умов та високою ймовірністю виявлення спроб вторгнення .

Наступним видом фізичного захисту є захист елементів будівель та приміщень. Прийнятний фізичний захист віконних прорізів приміщень забезпечують традиційні металеві решітки, а також спеціальне оскляніння на основі пластичних мас, армованих стальним дротом. Двері та вікна приміщення, що охороняється, обладнують датчиками, що спрацьовують при руйнуванні скла, дверей, але не реагують на їхні коливання, викликані іншими причинами. Спрацьовування датчиків викликає сигнал тривоги [15,16].

Серед засобів фізичного захисту особливо слід відзначити засоби захисту ПЕОМ від викрадення та проникнення до їхніх внутрішніх компонентів. Для цього використовуються металеві конструкції з клейкою підставкою, яка забезпечує зчеплення з поверхнею столу з силою 250-2700 кг/см. Це виключає вилучення або переміщення ПЕОМ без порушення цілісності поверхні столу. Переміщення ПЕОМ можливе тільки з використанням спеціальних ключів та інструментів [16,17].

Замикаючі пристрої та спеціальні шафи займають особливе місце в системах обмеження доступу, оскільки вони несуть у собі ознаки як системи фізичного захисту, так і пристроїв контролю доступу. Вони надзвичайно різноманітні та призначені для захисту документів, матеріалів, магнітних носіїв, фотоносіїв і навіть технічних засобів: ПЕОМ, принтерів, ксероксів і т.ін.

Випускаються спеціальні металеві шафи для зберігання ПЕОМ та іншої техніки. Такі шафи забезпечуються надійною подвійною системою замикання: замком ключового типу та комбінованим на 3-5 комбінацій. Можуть застосовуватися також; замки з програмованим часом відкривання за допомогою механічного або електронного годинника.

Системи контролю доступу. Регулювання доступу в приміщення здійснюється насамперед через упізнавання (автентифікацію) службою охорони або технічними засобами [15,16].

Контрольований доступ передбачає обмеження кола осіб, які допускаються в певні захищені зони, будівлі, приміщення, і контроль за переміщенням цих осіб у середині них.

Основою для допуску служить певний метод для впізнавання і порівняння з еталонними параметрами системи. Існує вельми широкий спектр методів упізнавання уповноважених осіб на право їхнього доступу в приміщення, будівлі, зони.

На основі впізнавання приймається рішення про допуск осіб, які мають на це право, або заборону — для тих, хто не має цього права. Найбільше розповсюдження одержали атрибути! та персональні методи впізнавання.

До атрибутних засобів відносяться засоби підтвердження повноважень, такі, зокрема, як документи (паспорт, посвідчення і т.ін.), картки (фотокартки, картки з магнітними, електричними, механічними ідентифікаторами і т.ін.) та інші засоби (ключі, сигнальні елементи і т.ін.). Слід відзначити, що ці засоби в значній мірі піддаються різного виду підробкам та шахрайству [15,16].

Персональні методи — це методи визначення особи за його незалежними показниками: відбитками пальців, геометрією рук, особливостями очей і т.ін. Персональні характеристики бувають статичні та динамічні. До останніх відноситься пульс, тиск, кардіограми, мова, почерк і т.ін.

Персональні способи є найбільш привабливими. По-перше, вони повно описують кожну окрему людину. По-друге, неможливо або вкрай важко підробити індивідуальні характеристики.

Статичні способи включають аналіз фізичних характеристик — таких, як відбитки пальців, особливості геометрії рук і т.ін. Вони достатньо достовірні та мають малу ймовірність помилок [15,16].

Динамічні ж способи використовують характеристики, що змінюються у часі.

Характеристики, які залежать від звичок та навичок, є не тільки найбільш простими для підробки, але й найбільш дешевими з точки зору практичної реалізації.

Способи впізнавання, засновані на будь-чому, що запам'ятовується (код, пароль і т.ін.), можуть застосовуватися у випадках найбільш низьких вимог до безпеки, так як часто ця інформація записується користувачами на різноманітних носіях: аркушах бумаги, в записних книжках та інших носіях, що при їх доступності іншим може звести нанівець усі зусилля з безпеки. Крім того, існує реальна можливість підглянути, підслухати або одержати цю інформацію іншим шляхом (насильство, викрадення і т.ін.) [15,16].

Спосіб упізнавання людиною (вахтер, вартовий) не завжди надійний із-за так званого "людського фактору", який полягає в тому, що людина піддається впливові багатьох зовнішніх умов (утома, погане самопочуття, емоційний стрес, підкуп і т.ін.). На противагу цьому знаходять широке застосування технічних засобів упізнавання, таких, наприклад, як ідентифікаційні картки, впізнавання за голосом, почерком, відбитками пальців і т.ін.

Найпростіший та найбільш розповсюджений метод ідентифікації використовує різноманітні картки, на яких розташовується кодована або відкрита інформація про власника, його повноваження і т.ін.

Звичайно це пластикові картки типу перепусток або жетонів. Картки вводяться з читаючий пристрій кожний раз, коли необхідно увійти або вийти з приміщення, що охороняється, або одержати доступ до чого-небудь (сейфа, камери, термінала і т.ін.).

Існує багато різновидів пристроїв упізнавання та ідентифікації особистості, які використовують подібні картки. Одні з них звіряють фотографії та інші ідентифікаційні елементи, інші – магнітні поля і т.ін.

Системи впізнавання за відбитками пальців. В основу ідентифікації лежить порівняння відносного положення закінчень та розгалужень ліній відбитка. Пошукова система шукає на поточному зображенні контрольні елементи, визначені при дослідженні еталонного зразка. Для ідентифікації однієї людини вважається достатнім визначити координати 12 точок [11,15,16].

Такі системи достатньо складні. Вони рекомендуються до використання на об'єктах, які потребують надійного захисту.

Системи впізнавання за голосом. Існує декілька способів виділення характерних ознак мови людини: аналіз короткочасних сегментів, контрольний аналіз, виділення статистичних характеристик. Слід відзначити, що теоретичні питання ідентифікації за голосом розроблені достатньо повно, але промислове виробництво таких систем поки відстає [16,17].

Системи впізнавання за почерком вважаються найбільш зручними для користувача. Основним принципом ідентифікації за почерком є постійність підпису кожної особистості, хоча абсолютного збігу не буває [16].

Система впізнавання за геометрією рук. Для ідентифікації застосовують аналіз комбінацій ліній згинів пальців та долоні, ліній складок, довжина та товщина пальців [16].

Технічно це реалізується шляхом накладення руки на матрицю фотокомірок. Рука освітлюється потужною лампою, здійснюється реєстрація сигналів із комірок, які несуть інформацію про геометрію.

Усі пристрої ідентифікації людини можуть працювати як окремо, так і в комплексі. Комплекс може бути вузькоспеціальним або багатоцільовим, при якому система виконує функції охорони, контролю, реєстрації та сигналізації. Такі системи є вже комплексними.

Комплексні системи забезпечують [15,16]:

• допуск на територію підприємства за карткою (перепусткою), яка містить індивідуальний машинний код;

• блокування проходу при спробах несанкціонованого проходу (прохід без перепустки, прохід до спеціальних підрозділів співробітників, які не мають перепустки);

• можливість блокування проходу для порушників графіка роботи (запізнення на роботу, передчасне залишення робочого місця і т.ін.);

• відкриття зони проходу для вільного виходу за командою вахтера;

• перевірка кодів перепусток та затримання їх пред'явників на КПП за вказівкою оператора системи;

• реєстрацію часу перетинання прохідної та збереження його в базі даних ПЕОМ;

• оброблення одержаних даних та формування різноманітних документів (табель робочого часу, рапорт за добу, відомість порушників трудової дисципліни і т.ін.), що дозволяє мати оперативну інформацію про порушників трудової дисципліни, відпрацьованих кожним час і т.ін.;

• оперативне коригування бази даних із доступом за паролем;

• роздруківка табелів робочого часу за довільною групою співробітників (підприємство в цілому, структурний підрозділ, окремо вибрані співробітники);

• роздруківка списків порушників графіка робочого часу з конкретними даними про порушення;

• поточний та ретроспективний аналіз відвідування співробітниками підрозділів, пересування співробітників через КПП, видача списку присутніх або відсутніх у підрозділах або на підприємстві для довільно вибраного моменту часу (при умові збереження баз даних за минулі періоди);

• одержання оперативної інформації абонентами локальної мереж;! на випадок мережної реалізації системи.

Фізичні засоби є першою перешкодою (бар'єром для зловмисника при реалізації ним заходових методів доступу.

2.1.3 Апаратні засоби захисту

До апаратний засобів захисту інформації відносяться найрізноманітніші за принципом дії, побудовою та можливостями технічні конструкції, які забезпечують припинення розголошення, захист від витоку та протидію несанкціонованому доступові до джерел конфіденційної інформації.

Апаратні засоби захисту інформації застосовуються для виконання наступних завдань [11,15,16]:

• проведення спеціальних досліджень технічних засобів забезпечення виробничої діяльності на наявність можливих каналів витоку інформації;

• виявлення каналів витоку інформації на різних об'єктах та в приміщеннях;

• локалізація каналів витоку інформації;

• пошук та виявлення засобів промислового шпіонажу;

• протидія несанкціонованому доступові до джерел конфіденційної інформації та іншим діям.

За функціональним призначенням апаратні засоби можуть поділятися на засоби виявлення, засоби пошуку та детальних вимірювань, засоби активної та пасивної протидії [11,15,16].

При цьому за своїми характеристиками засоби можуть бути загального застосування, розраховані на використання непрофесіоналами з метою одержання попередніх (загальних) оцінок, і професійні комплекси, які дозволяють здійснювати ретельний пошук, виявлення та прецизійне вимірювання всіх характеристик засобів промислового шпіонажу.

До першої групи можна віднести індикатори електромагнітних випромінювань, які можуть приймати широкий спектр сигналів із достатньо низькою чутливістю.

До другої групи можна віднести комплекси для виявлення та пеленгування радіозакладок, призначені для автоматичного виявлення та виявлення місцезнаходження радіопередавачів, радіомікрофонів, телефонних закладок та мережних радіопередавачів.

Пошукову апаратуру можна розділити на апаратуру пошуку засобів знімання інформації та дослідження каналів її витоку.

Апаратура першого типу спрямована на пошук та локалізацію вже впроваджених зловмисниками засобів несанкціонованого доступу. Апаратура другого типу призначена для виявлення каналів витоку інформації.

Як і в будь-якій галузі техніки, універсальність будь-якої апаратури призводить до зниження її параметрів із кожної окремої характеристики.

З іншої сторони, існує велика кількість різних за природою каналів витоку інформації, а також; фізичних принципів, на основі яких працюють системи несанкціонованого доступу. Ці фактори зумовлюють різноманіття пошукової апаратури, а її складність визначає високу вартість кожного приладу. У зв'язку з цим достатній комплекс пошукового обладнання можуть дозволити собі мати структури, які постійно проводять відповідні обстеження. Це або великі служби безпеки, або спеціалізовані фірми, які надають послуги стороннім організаціям.

До особливої групи можна віднести апаратні засоби захисту ЕОМ та комунікаційних систем на їхній основі [15,16,18].

Апаратні засоби захисту застосовуються як в окремих ПЕОМ, так і на різних рівнях та ділянках мереж в центральних процесорах ЕОМ, в їхніх оперативних запам'ятовуючих пристроях (ОЗУ), контролерах вводу – виводу, зовнішніх запам'ятовуючих пристроях, терміналах і т.ін.

Для захисту центральних процесорів (ЦП) застосовується кодове резервування — створення додаткових бітів у форматах машинних команд (розрядів секретності) і резервних регістрів (у пристроях ЦП). одночасно передбачаються два можливих режими роботи процесора, які відділяють допоміжні операції від операцій безпосереднього вирішення задач користувача. Для цього служить спеціальна програма переривань, яка реалізується апаратними засобами [12,18].

2.1.4. Програмні засоби захисту

Програмний захист інформації – це система спеціальних програм, які входять до складу програмного забезпечення та реалізують функції захисту інформації.

Виділяють наступні напрями використання програм для забезпечення безпеки конфіденційної інформації, зокрема, такі [18,19,20]:

• захист інформації від несанкціонованого доступу;

• захист інформації від копіювання;

• захист програм від вірусів;

• захист інформації від вірусів;

• програмний захист каналів зв'язку.

За кожним із вказаних напрямів існує достатня кількість якісних, розроблених професіональними організаціями програмних продуктів, представлених на інформаційному ринку.

Програмні засоби захисту мають наступні різновиди спеціальних програм [19,20]:

• ідентифікації технічних засобів, файлів та автентифікації користувачів;

• реєстрації та контролю роботи технічних засобів та користувачів;

• обслуговування режимів обробки інформації з обмеженим доступом;

• захисту операційних систем ЕОМ та прикладних програм користувачів;

• знищення інформації у запам'ятовуючих пристроях після використання;

• сигналізації порушень використання ресурсів;

• допоміжні програми захисту різноманітного призначення. Ідентифікація технічних засобів і файлів, яка здійснюється програмне, реалізується на основі аналізу реєстраційних номерів різних компонентів та об'єктів інформаційної системи та співставлення їх із значеннями адресів і паролів, що зберігаються в запам'ятовуючому пристрої системи управління.

2.1.5. Криптографічні засоби захисту

Криптографія — спосіб тайнопису, заснований на використанні шифру, де під шифром звичайно розуміють сукупність обернених перетворень тексту повідомлень, які виконуються з метою схову від зловмисника (противника) інформації, яка знаходиться у повідомленні.

Криптографія включає декілька розділів сучасної математики, а також; спеціальні галузі фізики, теорії інформації та зв'язку і деяких інших суміжних дисциплін [8,11].

Як наука про шифри, криптографія довгий час була засекречена, так як застосовувалася, в основному, для захисту державних і воєнних секретів. Проте, на теперішній час методи та засоби криптографії використовуються для забезпечення інформаційної безпеки не тільки держави, але й приватних осіб та організацій. Справа тут зовсім не обов'язково в секретах. Дуже багато різноманітних відомостей циркулює по всьому світу в цифровому вигляді. І над цими відомостями буквально "висять" загрози несанкціонованого ознайомлення, нагромадження, підміни, фальсифікації і т.ін. Найбільш надійні методи захисту від таких загроз дає саме криптографія [8,11].

Для криптографічного перетворення інформації використовуються різноманітні шифрувальні засоби — такі, як засоби шифрування документів, засоби шифрування мови, засоби шифрування телеграфних повідомлень та передачі даних.

Загальна технологія шифрування. Вихідна інформація, яка передається каналами зв'язку, може представляти собою мову, дані, відеосигнали, називається незашифрованим повідомленням *Р–пе*редавання мовних повідомлень. Основний недолік аналогових скремблерів — відносно низька стійкість закриття інформації. Крім того, вони вносять спотворення у відновлений мовний сигнал [17].

Останнім часом знайшли широке розповсюдження системи шифрування, у яких застосовується цифрове шифрування мовної інформації, яка представлена у цифровій формі [17].

При аналого-цифровому перетворенні амплітуда сигналу вимірюється через рівні проміжки часу, що називаються кроком дискретизації. Для того щоб цифровий мовний сигнал мав якість не гіршу телефонного, крок дискретизації не повинен перевищувати 160 мкс, а кількість рівнів квантування амплітуди мовного сигналу — не менше 128. В цьому випадку відлік амплітуди кодується 7 бітами, швидкість передавання перевищує 43 кбіт/с, а ширина спектра дискретного двійкового сигналу дорівнює сумі смуг 14 стандартних телефонних каналів [17].

Рис. 2.2 Цифрове шифрування мовної інформації

2.2. Активні інфрачервоні засоби виявлення руху

Розробка вітчизняних активних ІЧЗВ ведеться з початку 60-х рр. У перших розробках як джерела випромінювання використовувалися лампи розжарювання. Модуляція випромінювання в цих виробах здійснювалася за допомогою механічних модуляторів. Такі ІЧЗВ мали низьку ефективність, великі габаритні розміри і значні струми споживання [21,22].

Оптична система джерела випромінювання (скорочено передавача - ПРД) створює вузьконаправлений промінь ІЧ-випромінювання. Як джерело ІЧ-випромінювання використовують напівпровідникові випромінюючі діоди з робочою довжиною хвилі 0,94 мкм, які розташовують у фокусі оптичної системи [21,22].

ІЧ-випромінювання фокусується оптичною системою ПРМ на чутливий майданчик фотоприймачів (фотодіодів). Отримувані з них імпульси фотоструму посилюються і поступають на пристрої обробки для формування сигналів тривоги [22].

Залежно від кількості променів і їх розташування (горизонтальне або вертикальне) ІЧЗВ можуть виконувати різні тактичні завдання. Горизонтальне розташування двох променів дозволяє за рахунок тимчасової обробки сигналів визначати напрям руху порушника. Вертикальне розташування променів в активних ІЧЗВ підвищує надійність блокування рубежів і периметрів в порівнянні з однопроменевими ЗВ [22].

Конвективні завади обумовлені дією потоків повітря, що переміщаються, наприклад протягів при відкритій кватирці, щілин у вікні, а також побутових опалювальних приладів – радіаторів і кондиціонерів. Потоки повітря викликають хаотичну флуктуаційну зміну температури фону, амплітуда і частотний діапазон якого залежать від швидкості потоку повітря і характеристик фонової поверхні [20,21,22].

Електричні завади виникають при включенні будь-яких джерел електро-і радіовипромінювання, вимірювальної і побутової апаратури, освітлення, електродвигунів, радіопередавальних пристроїв, а також при коливаннях струму в кабельній мережі і лініях електропередач. Значний рівень перешкод створюють також розряди блискавок [21,22].

Чутливість піроприймача дуже висока – при зміні температури на 1°С вихідний сигнал безпосередньо з кристала складає долі мікровольта, тому наведення від джерел завад в декілька вольт на метр можуть викликати завадовий імпульс, в тисячі разів більший за корисний сигнал. Проте велика частина електричних завад має малу тривалість або крутий фронт, що дозволяє відрізнити їх від корисного сигналу [21].

Власні шуми піроприймача визначають найвищу межу чутливості ІЧЗВ і мають вигляд білого шуму. У зв'язку з цим методи фільтрації тут не можуть бути використані. Інтенсивність завади збільшується при підвищенні температури

кристала приблизно в два рази на кожні десять градусів. Сучасні піроприймачі мають рівень власних шумів, що відповідають зміні температури на 0,05...0,15°С [21].

2.3 Технічні системи спостереження на об’єкті інформаційної діяльності

2.3.1 Системи відеоспостереження

Технічна система відеоспостереження на об’єкті інформаційної діяльності - це програмно-апаратний комплекс (відеокамери, об'єктиви, монітори, реєстратори та ін. обладнання), призначений для організації контролю як на локальних, так і на територіально-розподілених об'єктах. До функцій спостереження відноситься не тільки захист від злочинців, а й спостереження за працівниками, відвідувачами в офісі, на складі або в магазині [14,15].

Рис.2.3 Активні інфрачервоні засоби виявлення

На даний час найбільше застосування отримали відеокамери на основі ПЗЗ-матриць. У більшості випадків використовуються короткофокусні об'єктиви типу фікс-фокус, які не потребують фокусування, і автоматичне керування експозицією [14,15].

За конструктивними особливостями камери можна розділити на наступні

типи:

- модульна відеокамера - безкорпусний пристрій у вигляді одношарової друкованої плати, найбільш поширений розмір 32 × 32 мм, призначена для установки в термокожухи, півсфери і т. п.;

- мініВідеокамера - відеокамери в квадратних або циліндричних корпусах,

зазвичай застосовуються як готовий виріб для установки всередині приміщень;

- корпусні відеокамера - найбільш поширений форм-фактор пристроїв,

званий також камера стандартного дизайну або Box camera;

- купольна відеокамера, також відома як Dome camera - корпус являє собою півсферу або кулю, прикріплений до основи;

- керовані (поворотні або швидкісні відеокамери) - комбінований пристрій,

що складається з камери, трансфокатора і поворотного пристрою;

- гіростабілізовані відеокамери - відеокамери, які використовуються на рухомих об'єктах з метою отримання стабілізованого зображення [14,15,23].

Рис.2.4. Купольна відеокамера

Цифрові реєстратори - сучасні пристрої запису на жорсткий диск (HDD).

Одним з параметрів, за якими оцінюють роботу цифрових відеореєстраторів, є стабільність їх роботи, яка багато в чому визначається типом операційної системи. Автономні відеореєстратори, що використовують операційну систему Linux, в даний час є найбільш стабільними в роботі (Рис. 2.5) [14,15,23].

Рис.2.5 Відеореєстратор 16-канальний

Відцифроване зображення може мати різну кількість елементів зображення

- найчастіше 720*576 пікселів в режимі кадру. Можливі й менші значення (при цьому, природно, збільшується швидкість передачі відеоінформації по мережі,

зменшується займаний простір жорсткого диска, яке необхідне для відеозапису), проте ідентифікація об'єктів на такому зображенні може виявитися не реалізованою в силу низької роздільної здатності відеосистеми [8].

Іншим параметром, що служить для оцінки відеореєстраторів, є швидкість відеозапису (fps - field per second, тобто кількість полів в секунду) - цей параметр також називають частотою запису, темпом запису. Нерідко тут виникають непорозуміння, оскільки не враховується, що більшість відеореєстраторів для запису використовує не повні кадри відеосигналу, а відеополя (якщо це не вказується додатково). Ігноруючи цей факт, багато постачальників обладнання вказують значення швидкості відеозапису з розмірністю «кадрів/с», вкладаючи в значення «кадр» сенс слова «зображення». Треба відзначити, що деякі зарубіжні виробники цифрових відеореєстраторів більш суворо ставляться до

позначення даного параметра, використовуючи для вказівки розмірності позначення pps (pictures per second - кількість зображень в секунду) [15,23].

Для багатоканальних відеореєстраторів вказується або швидкість запису по кожному каналу, або сумарна швидкість в розрахунку на всі канали, наприклад, якщо в паспорті для 16-канального відеореєстратора вказана повна швидкість запису 400 полів / с, то це означає, що відеореєстратор здійснює відеозапис по кожному каналу в режимі реального часу 25 полів / с, а якщо повна швидкість 25 полів / с, то в перерахунку на кожен канал швидкість буде дорівнює 1,56 поля / с. у деяких відеореєстраторів швидкість відеозапису і швидкість відображення «живого» зображення різні, і при виборі обладнання це треба мати на увазі [15,23].

Загалом вибір цифрового відеореєстратора неминуче пов'язаний з певним компромісом. Справа в тому, що технічні ресурси відеореєстратора (як і будь-якого приладу) обмежені, тому перед проектувальником системи охоронного телебачення нерідко стоїть дилема, що краще: мати «живий» відеозапис, але з меншою роздільною здатністю, або відеозапис, що складається з порівняно рідко оновлюваних зображень (кілька разів на секунду), але з високою роздільною здатністю [15,23].

Останній варіант передбачає, що в разі будь-якого інциденту кожне поле відеозапису можна буде детально проаналізувати, роздрукувати, збільшити і т.п. Звісно ж, що для «живого» відображення відеоінформації більш важливим є висока швидкість оновлення інформації (оператор менше втомлюється, менше ймовірність того, що він пропустить появу будь-якого об'єкта, - тут важлива швидкість виявлення) [15.23].

При здійсненні відеозапису важливішою є висока роздільна здатність, оскільки вона є передумовою для надійної ідентифікації людини, розпізнавання номера автомобіля та ін. В будь-якому випадку це питання має вирішуватися виходячи з реальних секторів огляду відеокамер, встановлених на об'єкті [15,23].

Висока швидкість відеозапису тягне за собою збільшення архіву, тому дуже важливим є пошук потрібного фрагмента. Пошук необхідного місця може

здійснюватися різними способами [15,16,23]:

- за часом і датою;
- за номером відеокамери;
- за попереднім записом сигналів тривоги або події;
- за місцем на диску (що є найбільш оперативним) [15,16].

У цифрових відеореєстраторах використовуються різні види компресії (Wavelet, MPEG-2, MPEG-4, H.263), кожен з яких має свої переваги і недоліки щодо ступеня стиснення, якості зображення (наявності артефактів), вимог до каналу передачі даних і обсягом жорсткого диска. В даний час немає однозначної відповіді на питання, який з видів компресії кращий для використання в системах охоронного телебачення. З споживчої точки зору вид компресії не грає вирішального значення - важливий результат, досягнутий в конкретному відеореєстраторі при використанні того чи іншого виду компресії [15,23].

Обсяг стисненого зображення (в залежності від виду та рівня компресії) може становити від одиниць до десятків кілобайт, а час безперервної відеозапису цифрових відеореєстраторів при швидкості запису 25 полів / с може становити кілька годин [23].

Для скорочення дискового простору широко застосовується вибірковий запис по тривозі (реакція на замикання контактів охоронних датчиків), або по руху (спрацьовування детектора руху або активності) [23].

Вбудовані детектори руху, як правило, мають 256 зон з програмованої чутливістю, хоча в деяких приладах детектор руху має понад 1000 таких зон. Крім того, існують вбудовані детектори руху з програмованими розмірами і швидкістю контрольованих об'єктів, а також з дозволеним / забороненим напрямком руху [23].

Відстань місця розташування відеокамер від поста спостереження вимагає рішення задачі передачі відеосигналів на значні відстані. Кожне з наявних у розпорядженні розробника рішень має свої переваги і недоліки [15,23].

Стандартним рішенням передачі відеосигналу є використання коаксіального кабелю з хвильовим опором 75 Ом. Залежно від якості кабелю, як

правило, прийнятну якість зображення може бути досягнуто, якщо відеокамера віддалена від поста спостереження на відстань не більше 200 ... 400 м При великих відстанях для компенсації втрат в кабелі рекомендується використовувати магістральні відеопідсилювачі. Будучи допоміжними приладами, вони можуть бути розміщені на відстані від оператора, причому, для підвищення відношення сигнал / шум магістральні відеопідсилювачі бажано розташовувати якомога ближче до відеокамери [15,23].

Переваги використання волоконно-оптичних кабелів загальновідомі [12,18]:

- несприйнятливість до електромагнітних завад;
- низькі втрати при передачі відеосигналу (до 50 км);
- вони забезпечують гальванічну розв'язку обладнання (не виникають так звані «земельні петлі»);
- можливість передачі по одному кабелю одночасно відеосигнали, аудіосигнали та дані.

До недоліків волоконно-оптичних кабелів до недавнього часу ставилися:

- порівняно висока вартість;
- невисока технологічність [12,18].

Однак за останній час технологія роботи з волоконно-оптичними кабелями значно спростилася, а ціни поступово знижуються. При використанні волоконно-оптичних кабелів узгоджувальні пристрої встановлюються на передавальній і приймальній стороні, і вартість такого обладнання в даний час значна [12,18].

Слабким місцем систем з волоконно-оптичними кабелями є їх низька живучість. Це виражається в тому, що при випадковому або навмисному пошкодженні такого кабелю відновлення його силами експлуатуючої організації, як правило, неможливо [18,20].

Використання кабелів витої пари займають проміжне положення між коаксіальними і волоконно-оптичними кабелями, а їх вартість набагато нижча за вартість коаксіальних кабелів. Застосування кабелів витої пари вельми

виправдано для територіально-розподілених систем охоронного телебачення, особливо в умовах несприятливої електромагнітної обстановки. [12,18].

При побудові системи відеоспостереження потрібне якісне зображення як вдень так і вночі. Для отримання чіткої картинки, навіть в умовах недостатньої освітленості, камери оснащені ІЧ-освітленням, але її може бути не достатньо. Для цього й існують ІЧ-прожектори. ІЧ-прожектор дозволить поліпшити якість відеозйомки при недостатньому освітленні, збільшити дальність видимості відеокамери, а також зробити відеоспостереження більш непомітним [20].

ІЧ-освітлення характеризуються [21,23]:

- кутом освітленого сектору;
- радіусом дії;
- довжиною хвилі випромінюваного світла;
- струмом (потужністю) споживання [11].

Конструктивно ІЧ-освітлювачі можуть бути виконані двояко: на основі галогенних ламп або світодіодів [18,23].

ІЧ-освітлювачі на основі галогенних ламп (IR-Lamps) з встановленими перед ними ІЧ-фільтрами характеризуються такими особливостями:

- великим радіусом дії, який може досягати більше 100 м;
- значною споживаної потужністю (в залежності від моделі від 20 до 300 Вт);
- довжиною хвилі 730 ... 850 нм, що відповідає області видимого людиною світу, тому подібний ІЧ-освітлювач досить легко може бути виявлений;
- порівняно невеликим терміном служби галогенних ламп (порядку декількох місяців).

Твердотільні освітлювачі (IR-LEDs) з використанням світлодіодів ІЧ-діапазону мають наступні відмінності:

- радіус дії, як правило, не перевищує кількох десятків метрів;
- вони мають суттєво меншу споживану потужність;
- у них набагато вище термін служби;

- у них менші габарити і маса;
- вони більш безпечні при експлуатації.

Таким чином, система відеоспостереження забезпечує [14,21]:

- візуальний контроль ситуації на об'єкті, що охороняється - надання інформації на пост спостереження в режимі реального часу;
- запис відеоінформації на цифровий відеореєстратор, що дозволяє документувати події, які відбуваються на об'єкті;
- виконання функцій охоронної сигналізації через детектори руху відеокамер або зовнішніх охоронних датчиків і інформованість оператора системи про виникнення тривоги в контрольованій зоні.

2.3.2. Пасивні інфрачервоні засоби виявлення

Пасивні інфрачервоні сповіщувачі руху (сповіщувачі), відомі також за назвою оптико-електронні, є пристроями, які найчастіше використовуються для виявлення руху в контрольованій зоні. Це обумовлено досить високою ефективністю виявлення руху та низькою вартістю цих пристроїв. Ефективність виявлення проникнення в зону, що охороняється, визначається насамперед тим, що пасивні інфрачервоні сповіщувачі дозволяють контролювати весь об’єм приміщення. Тим самим вирішується задача реєстрації вторгнення не тільки через найбільш уразливі місця, але практично при будь-якому шляху проникнення: через вікна, двері, проломи підлоги, стелі, стіни. Очевидно, що це значно ефективніше, ніж блокування тільки периметра об'єкта (вікон, дверей і тому подібних конструктивних елементів об'єкта). Це не виключає блокування першого рубежу охорони, що дозволяє в більшості випадків отримати ранній сигнал тривоги і мати більше часу на відповідну реакцію [21,24].

Контроль об’єму всього приміщення – це не єдина задача, яку розв'язують ПІЧ-сповіщувачі. Використовуючи змінні лінзи (оптичні системи), можна ефективно контролювати вузьку смугу (наприклад, коридор) чи створити горизонтальну фіранку (наприклад, для контролю приміщень, у яких знаходяться домашні тварини) чи формувати вертикальну зону виявлення

уздовж стін з вікнами чи дверима [20,24].

Сучасні ПІЧ-сповіщувачі використовують цифрову обробку сигналів, здійснюють постійний самоконтроль, розрізняють сигнали від домашніх тварин реальних порушників, мають підвищену стійкість до впливу різних дестабілізуючих факторів (радіозавад, сонячного світла і т.п.). З огляду на те, що при таких можливостях ці пристрої мають цілком прийнятні ціни, вони можуть використовуватися для охорони найрізноманітніших по тактиці охорони і необхідному рівню безпеки об'єктів [20,24].

Рис.2.6 Пасивні інфрачервоні засоби виявлення з фото фіксацією

2.3.3 Ультразвукові сенсори

Сенсори ультразвукової системи охоронної сигналізації призначені для охорони закритих приміщень і видають сигнал тривоги як у разі появи порушника, так і у разі виникненні пожежі. Принцип їхньої дії заснований на реєстрації зміни ультразвукового поля, викликаного появою в приміщенні людини або виникненні пожежі. Вони характеризуються високою чутливістю, але і високим рівнем хибних спрацювань, наприклад, якщо порушник дуже повільно переміщується, то він може обійти систему сигналізації. Окрім цього, деякі матеріали поглинають звук і, якщо об'єкт, що охороняється, містить багато предметів, виготовлених з такого матеріалу, або великогабаритні предмети, то вони обмежують дію такого сенсора, створюючи ділянки екранування ("мертві

зони"), в яких сенсор не реагує на рух порушника, а це, своєю чергою, створить труднощі у використанні системи [17,21,24].

Налаштування таких сенсорів залежить від зміни навколишнього середовища, наприклад, повітряні потоки, що створюються кондиціонерами і опалювальними приладами, також можуть призвести до помилкового спрацьовування системи сигналізації. Тому ці сенсори здебільшого використовують для охорони об’єктів, малих за об’ємом, наприклад, вітрин, музейних цінностей, салону автомобіля тощо [17,24].

Рис.2.7. Ультразвукові засоби виявлення

2.3.4 Магнітоконтактний сповіщувач

Магнітоконтактний сповіщувач містить у собі два основних елементи. Перший елемент – це геркон, що складається з герметичної колби, у якій знаходяться пластини з контактами, які мають малий опір. До пластин під’єднані провідники, що забезпечують підключення МКС. Для виготовлення пластин використовуються метали або сплави (наприклад, сталь), які забезпечують ефективне керування пластинами магнітним полем. Один з варіантів побудови геркона – використання протилежно намагнічених пластин. Під впливом магнітного поля від розташованого поруч магніту відбувається замикання чи розмикання контактів. У більшості випадків під впливом магнітного поля контакти нормально замкнуті. При знятті магнітного поля під дією пружних сил відбувається розмикання контактів [21,24].

Контакти звичайно покриваються спеціальним сплавом, наприклад,

родієвим, що забезпечує малий опір і тривалий термін служби [21,24].

Рис.2.8. Магнітоконтактний сповіщувач

На цей час фірми-виробники випускають різноманітні типи МКС, які розрізняються за: способом встановлення, місцем використання, конструктивним виконанням, основними параметрам і іншими ознаками [21,24].

Стійкість до вібрацій і ударних навантажень – це досить важливий параметр, що впливає на імовірність помилкового спрацьовування. Він пояснюється тим, що при деяких впливах можливі короткочасні розмикання контактів [21,24].

Типові параметри, що характеризують стійкість МКС: при вібрації в діапазоні 10...2000 Гц і прискоренні до 30 g тривалість замикання чи розмикання контактів не перевищує 20 мс; те ж саме буде і при ударних навантаженнях 100 g тривалістю 11 мс [24].

2.3.5 Фотоелектричні сенсори

Фотоелектричні сенсори використовуються для захисту внутрішнього та зовнішнього периметра, шляхом безконтактного блокування прольотів, дверей, ліфтів, отворів, коридорів тощо. Конструктивно такі сенсори складаються з передавача та приймача, які розміщують вздовж лінії охорони. Передавач випромінює інфрачервоний сигнал з довжиною хвилі близько 1 мкм, який надходить до приймача сигналу. Під час спроби перетнути систему променів

сенсор спрацьовує. Такі сенсори характеризуються високим рівнем надійності та стійкості роботи до впливу зовнішніх чинників. Однією з характерних ознак таких сенсорів є можливість їхньої автономної роботи, за рахунок, наприклад, їхнього оснащення сонячними елементами підзарядки [21,24].

Рис.2.9. Фотоелектричні сенсори

2.3.6 Вібросенсори

Вібросенсори призначені для виявлення навмисного пошкодження різних будівельних конструкцій: бетонних стін і перекриттів, цегляних стін, дерев'яних (рами і двері) і стельових покриттів, а також сейфів і металевих шаф.

Сенсори цього типу є контактними вимикачами різних видів, які сполучені або послідовно, або паралельно. Такі сенсори кріпляться на стовпах або сітках огорож і спрацьовують від гойдань, струсів або вібрацій. Принцип їхньої дії заснований на п'єзоефекті або ефекті електромагнітної індукції, коли постійний магніт переміщається уздовж обмотки котушки і тим самим наводить в ній змінний струм. Електричний сигнал, пропорційний до рівня вібрації, підсилюють і опрацьовують схемою сповіщувача за певним алгоритмом, щоб відокремити руйнівну дію від сигналу завади. Як правило, у таких сенсорах використовують мікропроцесори для опрацювання сигналів від контактних вимикачів та формування сигналу тривоги. Відрізняються такі сенсори низькою вартістю і високим рівнем помилкових спрацьовувань. У вітчизняній і

зарубіжній літературі залежно від технічної реалізації такі сенсори називають електромагнітними, магніторезонансними [21,24].

Рис.2.10 Вібросенсор

2.3.7. Сповіщувачі розбиття скла

Акустичні сповіщувачі розбиття скла є найбільш розповсюдженими на цей час. Це викликано рядом їхніх переваг, таких як відсутність якихось елементів на контрольованих поверхнях скла, можливість контролювати кілька вікон одним сповіщувачем та ін. Тому зупинимося докладніше на особливостях акустичних коливань, що виникають при розбитті скла [21,24].

Як відомо, при руйнуванні скла виникають акустичні коливання різних частот. У перший момент при ударі по склу воно деформується. Ця деформація, тобто вигин скла, викликає появу акустичних коливань низьких частот (рис. 1*а*). Коли величина деформації досягає граничного значення, відбувається механічне руйнування скла. Останнє супроводжується акустичними коливаннями високих частот. Причому для виявлення факту розбиття скла потрібно враховувати і те, що ці звукові коливання з’являються у визначеному часовому інтервалі [21,24].

Рис.2.11. Сповіщувач розбиття скла

Після удару виникають коливання, спектр яких поширюється до частот близько 25 кГц. При цьому низькочастотні складові зосереджені головним чином області частот десятків і сотень герц і пов'язані з деформацією скла в момент удару. Ці складові мають максимальну амплітуду в перші 200-300 мс і потім поступово загасають у часі [24].

Практично відразу після удару виникає широкополосне коливання, що обумовлене механічним руйнуванням скла. Ці високочастотні складові досить швидко загасають у часі [21,24].

Через декілька сот мілісекунд знову виникають високочастотні коливання зі спектральними складовими в області 3-20 кГц. Ці складові викликані акустичними коливаннями, що виникають при падінні осколків скла на підлогу і їхньому подальшому руйнуванні [21,24].

2.3.8 Комбінований інфрачервоний сповіщувач руху та розбиття скла

Датчик руху та розбиття скла призначений для відстеження руху людини в приміщенні, що охороняється і детектування ударів по склу та розбиття скла. Принцип дії сенсора руху заснований на визначенні інфрачервоного (ІЧ) випромінювання. Кожна жива істота - джерело ІЧ випромінювання. Як тільки

сповіщувач починає ІЧ-випромінювання в межах охоронної зони, він відсилає сигнал тривоги на центральний блок охоронної сигналізації. У датчику реалізований імунітет від тварин вагою до 25 кг і висотою до 1 м, спрацювання генерується тільки при русі людини. Якщо в приміщенні впаде який-небудь предмет, пробіжить кішка сповіщувач не спрацює [21,24,25].

Рис.2.12 Комбінований інфрачервоний сповіщувач руху та розбиття скла

Вбудований електретний мікрофон дозволяє виявити удари по склу та розбиття скла. При цьому використовується захист від помилкових спрацьовувань. Вхідний звук аналізується поетапно. Для включення тривоги спочатку повинні бути зроблені низькочастотні звуки (удар по склу), а потім - високочастотні (звук скла, що розбивається), тільки після цього відправиться сигнал тривоги [21,25].

Комбінований сповіщувач руху та розбиття скла використовується для охорони практично всіх об'єктів: заміських будинків, дач, офісів, торгових залів, квартир. Сповіщувач руху - один з найпоширеніших елементів охоронних сигналізацій [25].

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

Прилади приймально-контрольні й контрольні панелі (ППККП) відносяться до технічних засобів контролю і реєстрації інформації. Вони призначені для безперервного збору інформації від сповіщувачів, включених в

шлейф сигналізації, аналізу тривожної ситуації на об'єкті, формування та передачі сповіщень про стан об'єкта на пульт централізованого спостереження, а також управління місцевими світловими і звуковими сповіщувачами і індикаторами. Крім того, прилади забезпечують здачу і зняття об'єкта з охорони за прийнятою тактикою, а в ряді випадків - електроживлення сповіщувачів.

Прилади ППККП є основними елементами, що формують на об'єкті інформаційно-аналітичну систему охоронної або охоронно-пожежної сигналізації. Така система може бути автономною або централізованою. При автономної охорони прилади встановлюються в приміщенні (пункті) охорони, який розміщується на об'єкті або в безпосередній близькості від нього. При централізованій охороні об'єктовий комплекс технічних засобів, що формується одним або декількома приладами, утворює об'єктову підсистему охоронно-пожежної сигналізації, яка за допомогою системи передачі сповіщень передає в заданому вигляді інформацію про стан об'єкта на пульт централізованого спостереження, що розміщується в центрі прийому сповіщень про тривогу (пункті централізованої охорони). Інформація, яка формується приладом, як при автономної, так і централізованої охорони передається співробітникам спеціальних служб забезпечення охорони об'єкта, на яких покладено функції реагування на тривожні повідомлення, що надходять з об'єкта [21,24].

З метою підвищення достовірності одержуваної інформації при організації контролю стану об'єкта за допомогою технічних засобів застосовують багаторубежеві комплекси охоронної сигналізації. Кожен з рубежів сигналізації являє собою сукупність послідовно об'єднаних електричним колом (шлейфом сигналізації) спільно діючих технічних засобів охоронної сигналізації, що дозволяє видати повідомлення про проникнення (спробі проникнення) в зону, що охороняється (зони) незалежно від інших технічних засобів, який не входять в даний ланцюг. При цьому в кожен рубіж сигналізації включають сповіщувачі,засновані на різних принципах дії [21,24].

Крім здачі під охорону і зняття об'єкта (приміщення) з охорони за прийнятою тактикою, зазвичай забезпечують електроживлення сповіщувачів.

Прилади приймально-контрольні класифікуються за [24,26]:

– інформаційної ємності (кількість контрольованих шлейфом сигналізації) на прилади малої (до 5 ШС), середньої (від 6 до 50 ШС) і великий (понад 50 ШС) інформаційної ємності;

– інформативності - можуть бути малої (до 2 видів повідомлень), середньої (3 ... 5 видів) і великий (понад 5 видів) інформативності.

За кількістю напрямків передачі інформації вони поділяються на системи з одно- і двобічної передачею інформації (з наявністю зворотного каналу).

За способом відображення надходить на пульт централізованого спостереження інформації системи передачі сповіщень підрозділяються на системи з індивідуальним або груповим відображенням інформації у вигляді світлових і звукових сигналів, з відображенням інформації на дисплеї з застосуванням пристроїв обробки та накопичення бази даних [24,26].

Шлейф сигналізації - це електричний ланцюг, що з'єднує вихідні ланцюги сповіщувачів, що включає в себе допоміжні елементи (діоди, резистори і т.п.), з'єднувальні дроти і коробки та призначена для видачі сповіщень про проникнення, спробу проникнення, пожежі, несправності, а в деяких випадках і для подачі електроживлення на сповіщувачі. Таким чином, шлейф сигналізації призначений для контролю стану деякої зони, що охороняється [24,26,27].

Зона охорони - це частина об'єкту, що охороняється, контрольована одним або декількома шлейфами сигналізації [9].

Сучасні багатофункціональні КП мають широкі можливості по організації систем охоронної, пожежної та охоронно-пожежної сигналізації. Знання цих можливостей дозволить зробити правильний вибір КП, характеристики і параметри якої найбільш повно задовольняють вирішення поставлених завдань з охорони конкретного об'єкта [27].

Робота КП може здійснюватися в різних режимах, а саме: охорона, спостереження (зняття з охорони), програмування [24,27].

Режим "охорона".

У цьому режимі КП контролює свої параметри і стан шлейфів [24,27]. Порушення шлейфів призводить до формування сигналів тривоги. При цьому можливі наступні різновиди режиму:

- повна охорона - КП контролює стан всіх шлейфів і самого себе.
- часткова охорона з контролем частини шлейфів і самій КП [24,27].

Процедура взяття об'єкта під охорону і зняття з охорони відноситься до тактичних параметрах і може розділятися на такі різновиди:

- автоматична постановка під охорону.
- постановка на охорону з затримкою на вихід.
- постановка на охорону без затримки на вихід [24,27]. Режим "спостереження (знято з охорони)".

У режимі «спостереження» КП знятий з охорони, але продовжує контролювати всі шлейфи і самого себе [24,27].

Шлейф сигналізації є однією з необхідних складових частин технічної системи охорони. Практика показує, що однією з основних причин нестійкої роботи приладів ТСО на об'єкті є порушення шлейфу сигналізації, які представляють собою відмову у вигляді обриву або короткого замикання в шлейфі. Не повинна виключатися також можливість умисного втручання в електричний ланцюг шлейфу з метою порушення його правильного функціонування (саботаж) [24,27].

Існують три методи контролю шлейфу сигналізації:

- з живленням шлейфу сигналізації постійним струмом і використанням у якості виносного елементу резистора;
- з живленням шлейфу сигналізації знакозмінною імпульсною напругою і використанням якості навантаження послідовно з'єднаних резистора та напівпровідникового діода;
- з живленням шлейфу сигналізації імпульсною напругою і використанням

у якості виносного елементу конденсатора.

Прилади й пульти приймально-контрольні пожежні призначені для

живлення пожежних сповіщувачів по шлейфах пожежної сигналізації, прийому тривожних сповіщень від пожежних сповіщувачів, контролю пожежних шлейфів на обрив і коротке замикання, формування повідомлень «Пожежа» і «Несправність», формування сигналів включення систем пожежогасіння та димовидалення , а також для передачі цих повідомлень на пульт централізованого спостереження або інші ППК [24,27].

Основними характеристиками пожежних ППК, також як і охоронних, є інформаційна ємність і інформативність [24,27].

Сигнально-пускові пристрої - це, по суті, ті ж прилади приймально-контрольні, які доповнені можливістю формування сповіщення «Увага» при спрацьовуванні одного пожежного сповіщувача, сповіщення «Пожежа» при спрацьовуванні не менше двох пожежних сповіщувачів, регульованою затримкою сигналу пуску систем пожежогасіння, можливістю управління системами оповіщення про пожежу. Відмінною особливістю ППК даного покоління приладів є променева структура побудови систем пожежної сигналізації та використання неадресних, порогових пожежних сповіщувачів, які самі приймають рішення про пожежу, як тільки контрольований ними параметр виходить за рамки допустимого значення [24,27].

Виносний пристрій оптичної сигналізації (ВПОС) призначений для дублювання оптичного сигналу спрацьовування пожежних сповіщувачів, візуальний оперативний доступ до яких утруднений. ВПОС рекомендується використовувати для визначення сповіщувача, який подав повідомлення «Пожежа», і встановлювати в доступному для огляду місці, наприклад в коридорі над дверима приміщення, що охороняється [26,27].

Системи пожежної сигналізації діляться на три класи: неадресні системи, адресні і адресно-аналогові пожежні системи [24,27].

Головна їхня відмінність це метод, за яким система приймає рішення про тривожну ситуацію, тобто про пожежу. У неадресних і адресних системах це рішення приймається безпосередньо самими встановленими пожежними сповіщувачами і потім тривожний сигнал передається на приймально-

контрольоване обладнання і на підставі цього сигналу з сповіщувача включається система пожежогасіння [27].

Спроби виявити загоряння на ранній стадії шляхом зниження порогів чутливості точкових димових сповіщувачів зазвичай призводять до помилкових спрацьовувань пожежної сигналізації і хибним пусків систем пожежогасіння. Постійний пошук компромісу між раннім виявленням і хибним пуском [27].

В адресно-аналогових системах принцип прийняття рішення про виникнення пожежі зовсім інший. На приймально-контрольне обладнання передається значення контрольованого сповіщувачем параметра (температура, задимленість в приміщенні). Головне обладнання постійно відстежує стан навколишнього середовища в усіх приміщеннях будівлі і відстежує динаміку зміни зазначених параметрів. На підставі цих даних приймає рішення не тільки про формування сигналу «Пожежа», а й сигналу «Попередження». Тобто адресно-аналогова система пожежної сигналізації побудована на ухваленні рішення про тривогу не окремими пожежними датчиками, а приймально-контрольним обладнанням на основі динаміки зміни даних, що надходять з сповіщувачів. Адресно-аналогові системи, постійно контролюючи стан середовища в приміщенні, негайно виявляють зміну температури або задимленість і видають черговому попереджуючий сигнал [27].

Раннє виявлення спалаху дозволяє своєчасно евакуювати людей ще на початковій стадії пожежі і провести запуск автоматичної установки пожежогасіння. Одночасно вирішується так само ряд важливих завдань, наприклад, контроль працездатності сповіщувачів. Так, в адресно-аналогової системі в принципі не може бути несправного сповіщувача, що не виявленого приймально-контрольним приладом, так як весь час сповіщувач повинен передавати певний сигнал. Якщо до цього додати потужну самодіагностику самих сповіщувачів, автоматичну компенсацію запиленості та виявлення запилених димових сповіщувачів, то стає очевидним, що ці чинники тільки підвищують ефективність адресно-аналогових систем [27].

Рис 2.11. Прилад приймально-контрольний охоронно пожежний

2.5 Висновки по розділу

1. Розкрито сутність змісту та основні поняття у сфері технічних систем охорони та захисту інформації. Розглянуто основи застосування фізичних, апаратних, програмних та криптографічних засобів захисту інформації.

2. Подано опис та можливості застосування активних інфрачервоних засобів руху.

3. Подано склад та опис окремих елементів технічна системи спостереження на об’єкті інформаційної діяльності. Розглянуто порядок застосування систем відео спостереження, пасивних інфрачервоних засобів виявлення, ультразвукових сенсорів, магніто контактних сповіщувачів, фотоелектричних сенсорів, вібросенсорів, сповіщувачів розбиття скла та їх комбінованих систем.

4. Розглянуто призначення, принцип дії та галузь застосування приймально-контрольних і контрольних панелей, призначених для охорони, спостереження 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

Фізичними методами захисту, які ґрунтуються на застосуванні механічних, електричних, електронних пристроїв та систем, котрі функціонують автономно, перешкоджаючи діяльності зовнішніх впливів, направлених на доступ до конфіденційної інформації [12,13,28].

Такими системами можуть бути периметрові, пропускні на базі технологій smart-card, touch-memory, які дають можливість забезпечити фізичну безпеку приміщень ІС, додаткового обладнання, носіїв інформації та каналів передачі інформації. Основними заходами для фізичного захисту мають мету – захистити від вогню, води, пилу, корозійних газів, електромагнітного випромінювання, вандалізму та захисту від несанкціонованого доступу до приміщень. Вимогами до захисних бар’єрів та місця розташування, які визначаються цінністю інформації, ризиком порушення безпеки та необхідністю дотримання чинних захисних заходів [13,15,16].

Діапазон засобів фізичного захисту, який вважається прийнятним для запобігання катастрофам чи порушенням. Кожен рівень фізичного захисту має визначені режимні території, зони чи приміщення, у межах забезпечення рівню захисту. Для здійснення захисту периметру створюється система охоронної та пожежної сигналізації, система відео спостереження, система контролю та управління доступом (СКУД) та інше [13,15,16].

Коректно керуватись наступними рекомендаціями [13,15,28,29]:

- Території та приміщення, які відповідають цінностям інформації, які підлягають захисту;

- Периметр безпеки має точно визначений;
- Додаткове обладнання має розміщуватися таким чином, щоб мінімізувати ризик НСД до ІзОД;
- Фізичні бар'єри мають за потреби діставати стелі, для запобігання несанкціонованого доступу (НСД) до режимних приміщень;
- Стороннім особам не можна надавати інформацію про дії на режимних територіях;
- Заборона виконувати роботу наодинці без належного контролю;
- ІС необхідно розміщувати у спеціально визначених місцях, окремо від обладнання, контрольованого будь-якими сторонніми підрозділами;
- У неробочий час територія об'єкту має бути фізично недоступні та перевірятися охороною;
- У межах режимних територій, не має застосовуватися фото та відео фіксація;
- Необхідно забезпечити належний контроль доступу.

Для реалізації заходів щодо контролю необхідно [20,29,30]:

- Вести облік дати та часу входу і виходу відвідувачів;
- Вилучати права доступу до режимних територій у звільнених співробітників;
- Дотримання пропускного режиму та правил внутрішнього розпорядку, установленого в організації.

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

Потужними інструментами захисту від зовнішніх атак є технічний захист, основний на методах, які мають на меті запобігти несанкціонованому отриманню інформації, та зловмисного використання зовнішнього обладнання для доступу до неї [20,21,29,30].

Технічні методи реалізуються за допомогою інтеграції різних пристроїв,

котрі інтегруються в апаратне забезпечення систем обробки інформації чи поєднання захисту ресурсів від вторгнення соціотехніків. Дані пристрої чи перешкоджають фізичному проникненню, чи проникнення до доступу до інформації (табл. 3.1), у тому числі 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, приймач підімкнення, 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 підімкнення, імітація зареєстрованого користувача	Криптозахист
Виробничий процес	Відходи, випромінювання тощо	Спецапаратура різного призначення	Оргтехзаходи, фізичний захист

Разом з тим, говоримо і про замки, ґрати на вікнах, сигналізацію, генератори шуму, мережні фільтри, скануючі радіоприймачі, які дозволяють запобігти витоку інформації через можливі технічні канали, чи надають змогу їх виявити. Для захисту інформації на рівні апаратного забезпечення застосовуються апаратні ключі, системи сигналізації, засоби блокування пристроїв та інтерфейси вводу-виводу інформації [20,21,24].

У комунікаційних системах використовуються засоби мережного захисту інформації [18,19,20]:

- міжмережеві екрани – використовуються для блокування атак із зовнішнього середовища, які управляють проходженням мережного трафіку згідно з правилами безпеки. Найчастіше їх встановлюються на вході мережі, аби розмежувати внутрішні і зовнішні мережі (Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway і Alteon Switched Firewall від компанії Nortel Networks).
- системи виявлення вторгнень – використовуються для захисту від НСД та атак типу «відмова в обслуговуванні», ґрунтуються на застосуванні механізмів, які здатні запобігати шкідливим діям, знижуючи час простою після атаки та витрати на підтримку роботоздатності мережі (Cisco Secure IDS, Intruder Alert і NetProwler від компанії Symantec).
- засоби створення віртуальних приватних мереж – використовується для організації захищених каналів при передачі даних через незахищене середовище, завдяки ним забезпечується прозоре з’єднання локальних мереж, зберігаючи конфіденційність та цілісність інформації (Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator).
- засоби аналізу захищеності корпоративної мережі та виявлення потенційних каналів реалізації загроз інформації, надаючи можливість запобігти потенційним атакам на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі (Symantec Enterprise Security Manager, Symantec NetRecon).

Технічні канали – сторонні електромагнітні випромінювання та наведення

акустичних та оптичних каналів.

Захист інформації від її витоку технічними каналами зв'язку забезпечується завдяки [18,19,21]:

- застосування екранованого кабелю, прокладання проводів та кабелю екранованих конструкцій;
- встановлення високочастотних фільтрів;
- побудова екранованих приміщень;
- застосування екранованого устаткування;
- встановлення активних систем зашумлення.

1) витік за рахунок структурного звуку в стінах і перекриттях;

2) знімання інформації зі стрічки принтера, погано стертих дискет і т. ін.;

3) знімання інформації з використанням відеозакладок;

4) програмно-апаратні закладки в ПЕОМ;

5) радіозакладки в стінах і меблях;

6) знімання інформації із системи вентиляції;

7) лазерне знімання акустичної інформації з вікон;

8) виробничі й технологічні відходи;

9) комп'ютерні віруси, логічні бомби тощо;

10) знімання інформації за рахунок наведень і «нав'язування»;

11) дистанційне знімання відеоінформації;

12) знімання акустичної інформації з використанням диктофонів;

Схема потенційних каналів витоку та несанкціонованого доступу до інформації, котра обробляється у звичайному одноповерховому приміщенні, включає наступні канали витоку[18,19,21]:

1) розкрадання носіїв інформації;

2) високочастотний канал витоку в побутовій техніці;

3) знімання інформації спрямованим мікрофоном;

4) внутрішні канали витоку інформації;

5) несанкціоноване копіювання;

6) витік за рахунок побічного випромінювання термінала;

7) знімання інформації за рахунок використання «телефонного вуха»;

8) знімання з клавіатури та принтера акустичним каналом;

9) знімання з дисплея по електромагнітному каналу;

10) візуальне знімання з дисплея та принтера;

11) наведення на лінії комунікацій і сторонні провідники;

12) витік через лінії зв'язку;

13) витік мережею заземлення;

14) витік мережею часофікації;

15) витік трансляційною мережею та гучномовним зв'язком;

16) витік охоронно-пожежною сигналізацією;

17) витік мережею електроживлення;

18) витік мережею опалення, газо- і водопостачання.

Склад засобів забезпечення технічного захисту інформації, у тому числі від соціотехнічних атак, постачальників даних засобів, послуг зі встановлення, монтажу, налаштування та обслуговування визначаються власники та розпоряджаються ІзОД самостійно чи за рекомендаціями фахівців у сфері технічного захисту інформації (ТЗІ), згідно чинного законодавства. Вибір зумовлений особливостями фрагментарного чи комплексного захисту інформації. Фрагментарний захист забезпечує протидію певній загрозі, та комплексні загрози [18,19,29,30].

Засоби ТЗІ функціонують автономно чи спільного з ТЗІ у вигляді самостійних пристроїв чи вбудованих у складові елементів. Для оцінки стану засобів ТЗІ, котра обробляється та циркулює в ІС, комп'ютерних мережах та системах зв'язку. Для підготовки висновків, застосовуються з метою погодження рішень, здійснюється експертиза щодо стану справ у сфері ТЗІ. Порядок розрахунку та визначення зон безпеки інформації, які направлені на ТЗІ, визнаючи ефективність даного захисту та порядку атестації відповідних технічний засобів, що регламентується нормативними документами з ТЗІ [25].

Перевагами методів ТЗІ є надійність, Недоліками – недостатня гнучкість, великі обсяги та велика кількість використовуваної апаратури та її високу

вартість [21,26,29].

Основою для програмних методів захисту інформації та захисту від зовнышных атак, ґрунтується на спеціальних прикладних пакетах чи окремі програми, які входять до складу ПЗ систем обробки даних. Дані методи передбачають застосування програм для ідентифікації та автентифікації користувачів, контролю та розмежування доступу до інформації, шифрування та вилучення зайвої інформації, тестового контролю системи захисту, її аудиту, моніторингу та антивірусного захисту [19].

Вказані методи застосовують для [18,19]:

- ідентифікації та автентифікації користувачів та співробітників;
- розмежування доступу користувачів до інформації, та засобів обчислювальної техніки та ТЗІ;
- цілісності інформації та конфігурації ІС;
- реєстрація та облік дій користувачів;
- маскування оброблюваної інформації;
- реагування на спроби несанкціонованих дій.

Засоби захисту мають застосовуватися, щоб функціонували у належний спосіб. Важливим аспектом безпеки, якій не приділяється належна увага, вже після впровадження системи чи служби, є інтеграція засобів захисту для неї і без особливої підтримки. Можливі втрати ефективності засобів захисту мають запобігатися, а не констатуватися як факт [20].

Необхідно здійснювати контроль за оточенням, переглядом записів у журналі та здійснювати обробку інцидентів та гарантувати стан захищеності інформації. Підтримання робото здатності засобів є важливим механізмом безпеки інформаційних технологій, які реалізовують засоби захисту та працюють безперервно, так як підлягають систематичній перевірці у циклі активності [6,16,20].

Варто бути впевненим, що дані засоби застосовуються коректно, і будь-які інциденти та зміни у СЗІ, необхідно негайно виявити та вжити відповідних заходів [6,16,20].

З часом, з’явилась тенденція щодо погіршення роботи будь-яких служб чи механізмів, де доопрацьовуючи системи для виявлення проблем та ініціювання коригувальних дій. Такий спосіб для підтримки необхідного рівня засобів захисту системи інформаційних технологій. Керування безпекою інформаційних технологій – процес є неперервним [20].

Підтримання роботоздатності систем та засобів захисту інформації повинно включати такі дії [6,16,20]:

- обслуговування засобів захисту для забезпечення їх неперервної роботи;
- перевірка, котра гарантує засоби захисту для задоволення вимог, котрі передбачаються методиками;
- контроль активів, загроз, вразливості та засобів захисту, котрі мають на меті запобігти виникненню ризикованих ситуацій;
- дослідження інцидентів для гарантування реакції на небажані події.

Тобто, підтримання роботоздантності – багатогранний досить довгий процес, який спонукає до критичного перегляду рішень, які ухвалені раніше [20].

Супроводження – події з боку керівництва, направлено на забезпечення правильного та відповідного функціонування даних засобів в процесі їх діяльності. Події плануються зараніш та реалізовуються згідно графіку. Таким чином, витрати можуть бути зменшені [20].

Для виявлення несправностей необхідна регулярна перевірка. Захисним засобом, який не зазнає перевірки, не представляє цінності, так як підстав, що він заслуговує на довіру [6,16,20].

- Обслуговування. Засоби захисту вимагають висококваліфікованого обслуговування, у тому числі і керування, тоді як мова йде про реалізацію повноцінної програми безпеки організації.

Відповідність засобів захисту – перевірка засобів захисту на відповідність, аудиту захисту. Для гарантії, що рівень безпеки інформаційних технологій дійсно ефективний, то важливо для впровадження засобів захисту залежить повною мірою відповідати проекту. Даний проект, необхідно затвердити на всіх

етапах проходження проектів та систем, у процесі проектування та інтеграції, процес експлуатації та модифікації чи переміщення [6,20].

Перевірку на відповідність варто планувати в поєднанні з іншими заходами. Вибіркові перевірки варто застосовувати на практиці, так як це дає можливість перевірити персонал на дотримання вимог. Процедури перевірки необхідні для забезпечення надійного функціонування засобів захисту, у тому числі, правильного їх впровадження та випробування [6,16,20].

Нормальний режим функціонування системи перевіряють щодня, на застосування засобів захисту. Співбесіди можуть бути корисними у випадку критичного ставлення до отриманих даних у процесі спілкування. Даний підхід допомагає скласти контрольний список та розробити доцільну форму звіту, де контрольні списки включають загальну ідентифікаційну інформацію [6,20].

Тоді як фізичний захист має стосуватися як деяких аспектів: зовнішніх та внутрішніх. Задачами фізичного захисту – своєчасне виявлення потраплянь рідин, несправності систем живлення та інше [6,20].

Перевірка на відповідність захисту – складна задача, тоді як для розв’язання необхідна наявність практичного досвіду та поінформованості. Дані дії здійснюються незалежно від заходів щодо внутрішнього огляду чи контролю [6,20,21,31].

Керування змінами. Системи інформаційних технологій, та їх оточення, де здійснюється функціонування, постійно змінюються. Зміни розглядаються як результат появи нових особливостей та служб чи виявлення нових загроз та вразливостей. Дані зміни, призводять до виникнення нових загроз та вразливостей [43].

Якщо мова йде про заплановані зміни в системі, то слід запобігати порушенням, які викликають зміни в механізмах захисту. Система має пункт з управління конфігурацією чи іншої організаційної структури з управління технічними змінами системи, то варто призначити системного фахівця та представників на пункті, зобов’язуючи їх робити висновки про виклики чи зміни захисту, які виявляються порушення. У випадку змін, які спричинені

придбанням нового апаратного та ПЗ, варто здійснити аналіз, для встановлення нових вимог захисту. Більшість змін, які внесені у систему, варто розглядати як незначні, такі котрі не вимагають поглибленого аналізу ситуації, який потребує змін. Певного аналізу вимагають навіть найменші зміни, для обох типів змін варто оцінити переваги та недоліки. Якщо зміни незначні, то краще зробити неофіційно, у процесі зустрічей з фахівцями, однак остаточне рішення керівництва має бути задокументовано [6,20,31].

Контроль. Вирішальною стадією циклу для захисту інформаційних технологій є контроль виконаних раніше кроків, у випадку здійснення коректних дій, то адміністрація з'ясовує [6,20,31]:

- чи вдалося досягти поставлених цілей;
- чи достатньо переконливі здобуті досягнення.

Контроль має охоплювати процедури, які пов'язані зі створенням звітності контролеру безпеки інформаційних технологій, управлінням на постійній основі процесу із забезпечення ІБ [21,31].

Перевірці підлягають матеріальні носії інформації та їх зміст, загрози та вразливості інформації, засобів, які підстраховують інформацію [6,20,31].

Активи підлягають для виявлення змін їх вартості та цілей безпеки системи інформаційних технологій [6,20,31].

Загрози та вразливості контролюють, виявлення змін їх важливості та вчасної фіксації для появи інших загроз та вразливостей. До змін загроз та вразливостей призводити, як мінімум до зміни активів [20].

При знаходженні аномалій у системі захисту інформації, здійснюється розслідування та повідомляються обставини керівництву, котре ухвалює відповідні рішення, у тому числі перегляду політики безпеки системи інформаційних технологій та ініціації аналізу можливих ризиків [20,31].

Якщо мова йде про розкриття походження випадку, то варто зібрати інформацію з журналів, які подають їх у вигляді єдиного звіту про випадок. Дані звіти, щодо випадків аналізують. Хоча, складання звіту випадків досить складна задача, при цьому основною умовою визначення взаємозв'язків у записах з

різних журналів [20,31].

Менеджмент здійснюючи щоденний моніторинг мають зосередитись на підготовці документації, яка супроводжує оперативні процедури захисту, для подальшого застосування. Документація описує дії, які направлені на гарантію відповідного рівня захисту системи та окремих служб у тому числі, та управляти системами чи службами [20,31].

Документування процедури з модифікації поточної конфігурації захисту, котра охоплює скориговані параметри захисту та будь-яких змін у інформації з управління захистом. Вказані зміни узгоджуються з процесом управління конфігурацією системи. Варто, виявити процедури виконання ручного супроводження, для складання гарантій, за умови, якщо захист не зазнає загроз. Розподіл процедур описується для кожного використовуваного компоненту захисту [20,31].

Слід виявити умови та періодичність аналізу журналів безпеки, з описом необхідних методів статистичного аналізу та їх застосування.

Керівництво має затвердити інструкції для організації аудиту різних оперативних станів за порогом базового.

Обробка інцидентів реалізується з метою уникнення інцидентів у сфері захисту, хоча це є неможливим.

Для коректної оцінки та визначення ступеню його серйозності, котра реалізує кожен із них. Для детального аналізу ризиків та успішного їх усунення, необхідна повна інформація щодо заходів із захисту. Варто зібрати інформацію, та проаналізувати, котру практичну користь з неї можна отримати.

Аналіз небезпечних інцидентів надає високий ефект, котрий йдеться про об’єднання бази даних та організаційних зусиль кількох компаній у боротьбі з інцидентами [31].

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

Приміщення, в якому має оброблятися цінна для підприємства інформація має бути обладнане системою контролю та управління доступом (СКУД) [15,32].

Установка системи контролю та управління доступом є однією з найбільш важливих і необхідних систем в структурі будь-якого підприємства. Функціонал системи автоматизує виробничі процеси, контролює доступ на територію підприємства і до його споруд, ідентифікує і управляє користувачами, запобігає несанкціонованому доступу, дозволяє зонувати приміщення з різними правилами організації доступу. Все це стало можливим завдяки використанню інформаційних технологій, які стрімко розвиваються, і цим самим надають нові можливості для посилення контролю і безпеки не тільки до об'єктів, а і до інформації підприємства. На сьогодні існує без-ліч варіантів використання СУКД залежно від режиму таємності підприємства та від його потреб та можливостей [15,32-34].

Системою контролю та управління доступу називають сукупність програмно-апаратних технічних засобів безпеки, що мають на меті: обмеження і реєстрацію входу-виходу об'єктів (людей, транспорту) на заданій території через «точки проходу»: двері, ворота, контрольно- пропускні пункти [15,32].

Сучасні СКУД складаються з таких елементів [15,32,33]:

1. *Ідентифікатор* — пристрій, який дозволяє системі розпізнати людину. На цій посаді часто використовуються популярні зараз безконтактні карти, контактні карти (з чорної магнітної смужкою), електронні брелоки. Ще в ролі ідентифікатора може виступати спеціальний код, який вводить людина під час входу в зону, що охороняється або біометричні дані — відбитки пальців або долоні, відбиток сітківки очей, розпізнавання голосу і т. д.

2. *Зчитувач* — пристрій для розпізнавання і передачі даних на керуючий блок.

3. *Керуючий блок*— «мозок» системи. Виконує функцію прийняття

рішень щодо можливості визначити, чи потрібен доступ до приміщення для власника конкретного ідентифікатора. Якщо доступ дозволяється — надсилається сигнал на відкриття електронного замка (турнікета, шлагбаума, двері). У мережевих СКУД додатково до керуючого блоку підключається комп'ютер [32].

Основним завданням СКУД є [15,32,33]:

- управління доступом на задану територію, включаючи також обмеження доступу на задану територію, ідентифікація особи, яка має доступ на задану територію, а також облік робочого часу;
- розрахунок заробітної плати (при інтеграції з системами бухгалтерського обліку);
- ведення бази персоналу/відвідувачів;
- інтеграція зі всіма системами безпеки:
  - з системою відеоспостереження для суміщення архівів подій систем, передачі системі відеоспостереження повідомлень про необхідність стартувати запис, повернути камеру для запису наслідків зафіксованого підозрілого події;
  - з системою охоронної сигналізації (СОС) для обмеження доступу в приміщення, або для автоматичного зняття і постановки приміщень на охорону;
  - з системою пожежної сигналізації (СПС) для отримання інформації про стан пожежних сповіщувачів, автоматичного розблокування евакуаційних виходів і закривання протипожежних дверей в разі пожежної тривоги [4].

На особливо відповідальних об’єктах мережа пристроїв СКУД виконується фізично незв’язаної з іншими інформаційними мережами.

У точках доступу на об’єкт монтуються зчитувачі, які зчитують код електронних карт доступу і передають його в контролери СКУД.

Далі контролер приймає рішення на підставі внутрішньої бази даних користувачів або отриманої з комп’ютерної бази даних, і відповідно до запрограмованих алгоритмам контролю, управляє виконавчими пристроями СКУД.

Кожен користувач СКУД, будь то працівник підприємства або відвідувач,

отримує електронну пластикову карту доступу, яка видається після реєстрації на пункті контролю.

Кожній електронній карті доступу відповідає конкретний користувач системи зі своїми правами доступу на контрольований об’єкт.

Уся необхідна інформація про користувача також заноситься на комп’ютер диспетчера системи в базу даних СКУД.

При побудові мережевих СКУД використовуються чотири рівні мережевої взаємодії [33,34]:

1. Перший (вищий) рівень являє собою комп’ютерну мережу типу клієнт/сервер на основі мережі ETHERNET, з протоколом обміну TCP/IP і з використанням мережевих операційних систем Windows NT або Unix. Цей рівень забезпечує зв’язок між сервером і робочими комп’ютерами підсистем.
2. Другий рівень — зв’язок між контролерами і комп’ютерами підсистем. На цьому рівні використовується інтерфейс RS 232.
3. Третій рівень — зв’язок між контролерами і зчитувачами пристроями. Тут застосовується інтерфейс RS 485 або, що стали вже стандартом, інтерфейси зчитувачів або магнітних карт.
4. Четвертий рівень — рівень сповіщувачів пожежної сигналізації і ланцюгів управління — збалансовані і незбалансовані радіальні і адресні шлейфи, релейні вихідні ланцюга управління. Тут застосовуються нестандартні спеціалізовані інтерфейси і протоколи обміну інформацією.

Системи автоматизованого контролю доступу можна поділити на два типа: *автономні і мережеві системи* [32,33,34].

До *автономних* СКУД належать системи, що розташовані у одному приміщені. Їх головна функція — обмеження доступу до об’єктів, що контролюються.

Такі СКУД використовують для невеликих підприємств з декількома пунктами пропуску на об’єкт.

До таких СКУД можливо підключити різні пристрої: шлагбауми, турнікети, електромагнітні замки та зчитувачі RFID. RFID (Radio Frequency

Identification) — метод, що автоматично ідентифікує об’єкти за допомогою запису даних, що зберігаються в так званих RFID-мітках і зчитує ці данні за допомогою радіопристроїв.

До *мережевих* СКУД відносять системи, що дають можливість контролювати присутність працівників на робочих місцях, отримувати різноманітні звіти про присутність за різні відрізки часу по кожному працівнику і по підрозділу в цілому, обмежувати доступ до контрольованих об’єктів за часом доби, розподіляти зони доступу по кабінетах, поверхах, корпусах і т.п., розробити програмне забезпечення для складання особистої карточки для кожного працівника з фотографією, особистими даними, маркою автомобілю та ін. [15,32,33,34]

Класифікація СКУД Подана в Таблиці 3.2.

Важливою характеристикою СКУД є ступінь доступу: недостатній, середній, високий і дуже високий. СКУД умовно поділяють на чотири класи з різним рівнем доступу. Залежно від особливостей об’єкта, конфігурації СКУД, фірми виробника набір функцій у кожному класі може змінюватися і доповнюватися функціями з інших класів [33,34].

До СКУД 1-го класу відносять малофункціональні системи малої місткості, що працюють в автономному режимі і забезпечують:

- допуск до зони, яка знаходиться під охороною всіх осіб, які мають відповідний ідентифікатор;
- вбудовану світлову/звукову індикацію режимів роботи;
- управління (автоматичне або ручне) відкриттям/закриттям пристроїв загородження (наприклад, двері).

Такі системи застосовують тоді, коли замовнику необхідно забезпечити контрольований процесс [33,34].

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

Приміщення з обмеженим доступом розташоване у будові організації на 1 поверсі та використовується як кімната для перемовин. Займає площу 13.5 кв.м (довжина кімнати складає 5 м, ширина – 2.7 м).

Вікно приміщення, що підлягає захисту обладнане захисною плівкою із внутрішньої та гратами з зовнішньої сторони. Висота стелі складає 2.7м, підвісні стелі відсутні.

Стіни – цегляні, фундамент будови - залізобетонний. Електроживлення - централізоване. Поли виконані з бетону. Приміщення звукоізольовано та заземлено, присутня система теплопостачання. Труби каналізації та систем водопостачання, лінії внутрішнього телефонного зв'язку, кабелі і незадіяні проводи відсутні.

Доступ до контрольованої зони мають лише особи, що займають керівні посади організації та мають ідентифікатори до СКУД, що встановлено задля контролювання доступу до приміщення. Об'єкт обладнано камерами відеоспостереження, системою охоронної сигналізації, електромагнітним та акустичним генераторами шуму а двері обладнані електромеханічним замком.

У систему опалення, а саме опалювальні батареї встановлено діелектричні втулки.

Після закінчення перебування на об'єкті двері зачиняються, всі пристрої та обладнання вимикаються, а приміщення ставиться на сигналізацію.

Організація працює з 9-00 до 18-00 з перервою на обід з 12-00 до 13-00.

Генеральний план приміщення з обмеженим доступом, що підлягає захисту зображено на рис.3.1.

3.4.2 Підбір та обґрунтування вибору обладнання

На етапі побудови системи захисту інформації у приміщенні з обмеженим доступом постає питання вибору обладнання та технічних пристроїв, що будуть забезпечувати захист інформації у контрольованій зоні. Буде розглянуто можливі варіанти обладнання, що буде використано при побудові системи.

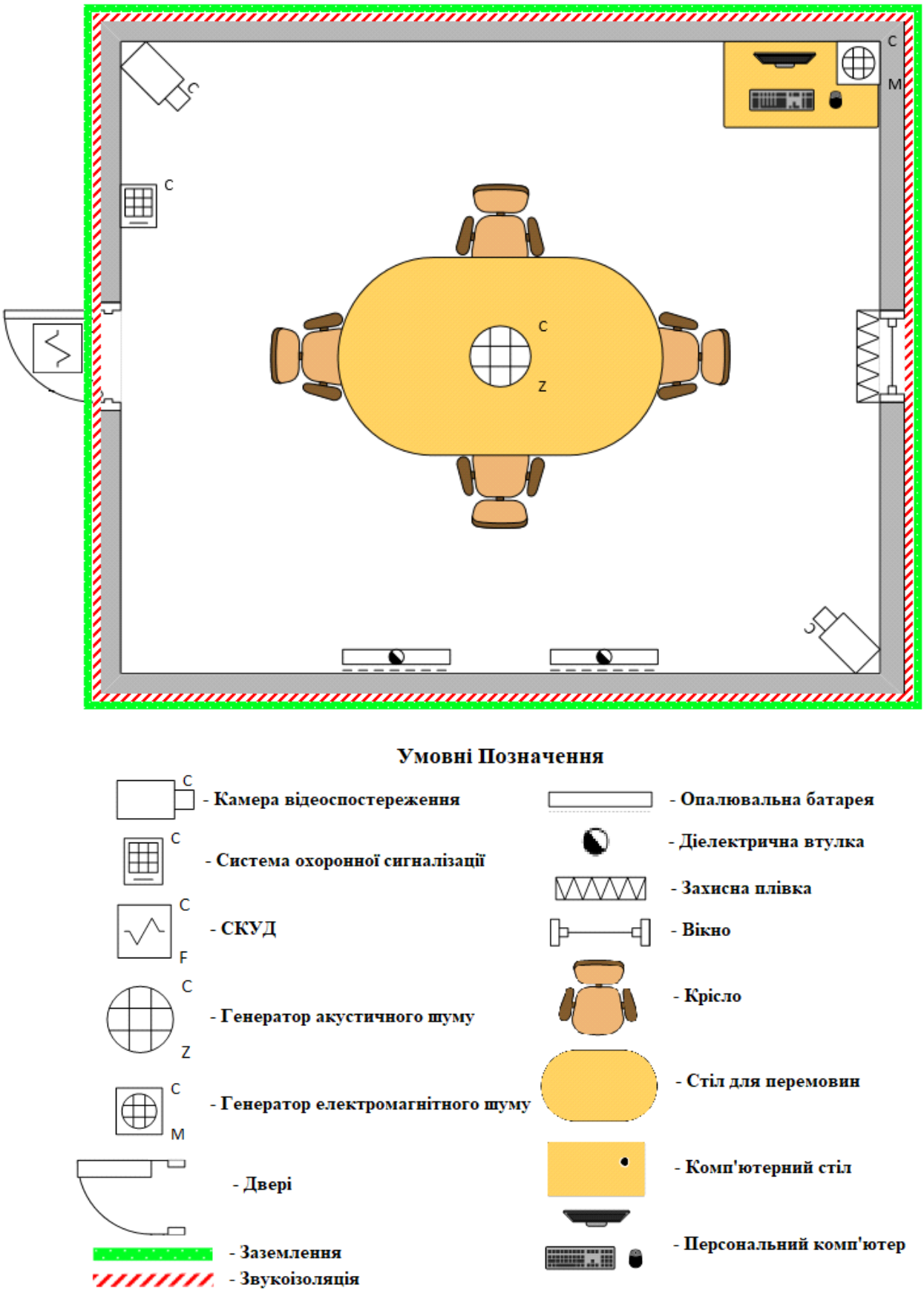


Рис.3.1 Генеральний план приміщення з обмеженим доступом

Вибір камери

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

Рис.3.2 IP-камери

Далі буде представлена таблиця порівняння найважливіших характеристик IP-камер та буде обрано найдоцільніший варіант (табл.3.3) [22,23].

Виходячи із розглянутих вище характеристик можна зробити висновок, що найдоцільнішим варіантом для використання у системі захисту приміщення з обмеженим доступом для забезпечення фіксування подій, що будуть відбуватися на об’єкті є камера **Dahua DH-IPC-T1B20P.**

Такий вибір обґрунтований наступними перевагами обраної камери в порівнянні з конкурентами:

- наявність цифрового зуму 16х;
- невелика ціна;
- вандалозахищеність за стандартом IK08;
- захист від пилу та вологи за стандартом IP67.

- низька споживана потужність;

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	—	+	—	+	+

Окрім цього, обрана камера надає наступний функціонал:

- інфрачервоне підсвічування за рахунок ICR фильтру.
- висока якість зображення;
- дистанція виявлення - 43м;
- детектор руху;
- наявність системи шумозаглушення **3D-DNR**;

Вибір системи контролю та управління доступом (СКУД).

Використання СКУД у нашій системі захисту необхідно задля контролювання доступу до приміщення. Застосування біометричних СКУД є оптимальним варіантом гарантування безпеки доступу до об’єкту. СКУД, що були обранні для порівняння зображено на Рис. 3.3 [23,35].

Рис.3.3 Елементи СКУД

Проаналізувавши характеристики, найоптимальнішим варіантом СКУД є **Hikvision DS-K1T501SF**.

Серед переваг даної СКУД можна назвати:

- зручний інтерфейс;
- наявність камери.
- міцний та якісний матеріал корпусу;
- не велика ціна;
- наявність пило-вологозахищенність;

В додаток, обрана СКУД характеризується низкою особливостей:

- Максимальна кількість відбитків пальців – 5000;
- Підтримка двостороннього звуку;
- функція захоплення зображення, вбудована в камеру (опція 2 МП);
- Кілька режимів автентифікації: QR-код, відбиток пальця, карта, відбиток пальця + пароль, карта + пароль, карта + пароль, карта + відбиток пальця + пароль і т.д.;

- Максимальна кількість карт - 50 000, максимальна кількість записів контролю доступу - 200 000;
- Виявлення несанкціонованого доступу, розблокування аварійного сигналу овертайму, недійсна перевірка карти по часу тривоги, сигнал тривоги з примусу і т.д.[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	Розпізнаван-ня обличчя + безконтакт-на картка	відбиток пальця + безкон-тактна картка	відбиток пальця + безкон-тактна картка	відбиток пальця + безкон-тактна картка	відбиток пальця + безкон-тактна 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 акустичного шуму

Генератор акустичного шуму призначений для захисту об'єктів від витоку конфіденційної інформації віброакустичними і акустичними каналами за допомогою генерації маскуючого шумового сигналу. Генератори акустичного шуму, що були обрані для порівняння зображено на Рис. 3.4. [23,36]

Розглянувши характеристики генераторів акустичного шуму, зупиняємо наш вибір на генераторі **РІАС-2ГС**.

Цей генератор володіє наступними перевагами:

- конкурентна ціна;
- широкий діапазон роботи;
- можливість роботи від акумулятора.

- вихідна потужність підсилювача не менше 10 Вт;

Voice Noice 4M2

Топаз ГША-4

PIAC-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	20 540
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	+	—	+	—

Окрім цього, PIAC-2ГС має низку інших переваг:

- глибина регулювання рівня шумового сигналу в робочому діапазоні частот не менше 20 дБ.;
- генератор зберігає працездатність в діапазоні температур: +10 ÷ +40 С°;

- час технічної готовності - не більше 1 сек.;
- Усереднений максимальний рівень вихідного акустичного сигналу в діапазоні робочих частот з похибкою установки не більше 6 дБ на відстані 1 м від випромінювача щодо нульового значення 2х105 Па (для звукового тиску) - не менше 70 дБ.
- Генератор включено до Переліку засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України, формується Адміністрацією Держспецзв'язку України.[21,31]

Вибір генератора електромагнітного шуму

Генератор електромагнітного шуму призначений для маскування інформативних ПЕВ, робочих станцій, персональних комп'ютерів, обчислювальної техніки шляхом випромінювання і формування в навколишній простір, в ланцюги і інженерні комунікації шумового сигналу в широкому діапазоні частот. Генератори електромагнітного шуму, що були обрані для п порівняння зображено на Рис.3.5 [23,36]

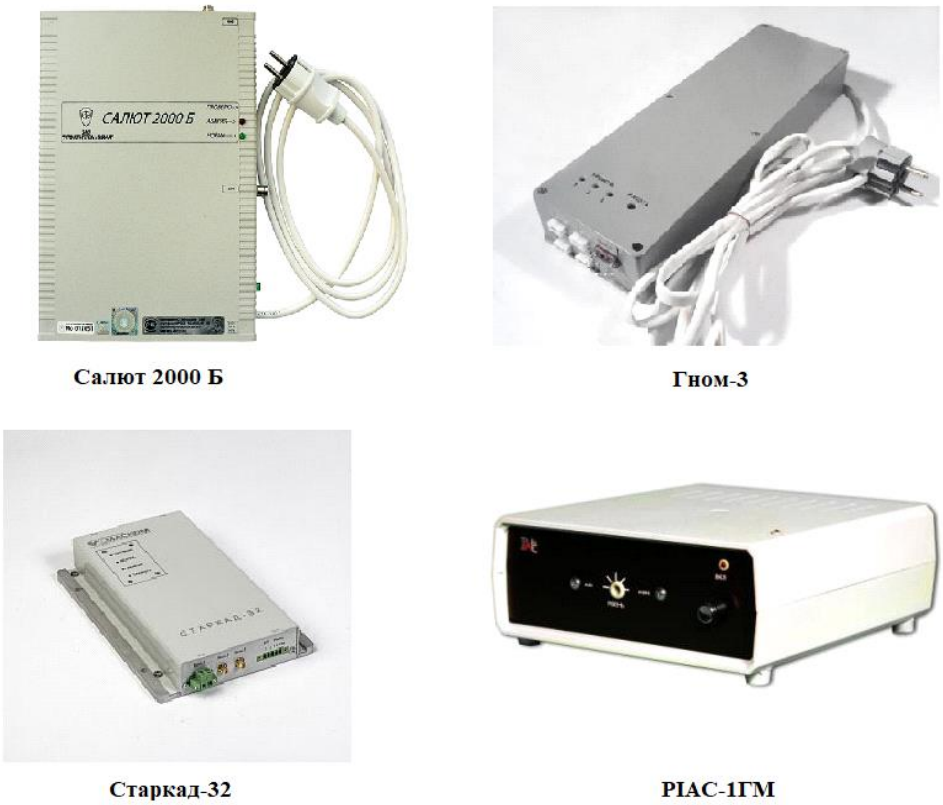


Рис.3.5 Генератори електромагнітного шуму

Виходячи із розглянутих вище характеристик, найдоцільнішим буде використання генератору електромагнітного шуму **РІАС-1ГМ**.

До переваг даного генератора можна віднести:

- Генератор має вбудовану систему автоматичного контролю функціонування, світлову та звукову індикацію контролю функціонування, що знаходяться як на виносному пульті, так і в генераторі, який може знаходитися на робочому місці користувача або в центрі контролю і управління. Пульт також забезпечує дистанційне включення / вимикання генератора;

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	—	—	—	+

- Максимальне інтегральне значення вихідної потужності - не менше ніж 5 Вт;
- коефіцієнт міжспектральних кореляційних зв'язків - не менше ніж 2.0;
- Генератор включено до Переліку засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України, формується Адміністрацією

Держспецзв'язку України.[31]

Вибір системи охоронної сигналізації

Охоронна сигналізація призначена виявлення проникнення (спроби проникнення) на об'єкт, що охороняється, забезпечення обробки, збору, подання та передачі інформації про проникнення (спроби проникнення).(рис.3.6) [22, 23,36]

Рис.3.6 Системи охоронної сигналізації

Виходячи з розглянутих вище характеристик доцільним для нашої системи є використання системи охоронної сигналізації **Tecsar Alert Ward** через її перевеги:

- низька ціна;
- наявність вбудованої сирени та відправлення повідомлень на пульт керування у випадку спроби проникнення;
- зручність у використанні та встановленні;
- можливість управління за допомогою мобільного додатку.[41]

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

Окрім вже оглянутого обладнання постає необхідність застосування захисної металізованої тонуючої плівки на вікні приміщення, що підлягає захисту. Завдяки наявності декількох шарів з вкрапленнями металів та своїй структурі захисна плівка виключає можливість витоку інформації по віброакустичному та електромагнітному каналам. У нашій системі захисту ми будемо використовувати захисну плівку Ultra Vision R Silver (Рис.3.7).[37]

Характеристики плівки **Ultra Vision R Silver** показано в таблиці 3.8.

Ще одним необхідним засобом захисту в приміщенні з обмеженим доступом є діелектричні втулки, що встановлюються на батареї (радіатори) опалювання. Втулки діелектричні представляють собою вкладиші, що не проводять струм та встановлюються в місці розбірного сполучення елементів трубопроводу. Головним завданням діелектричних втулок є захист від

блукаючого електричного струму.

Таблиця 3.8

Характеристики плівки Ultra Vision R Silver

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

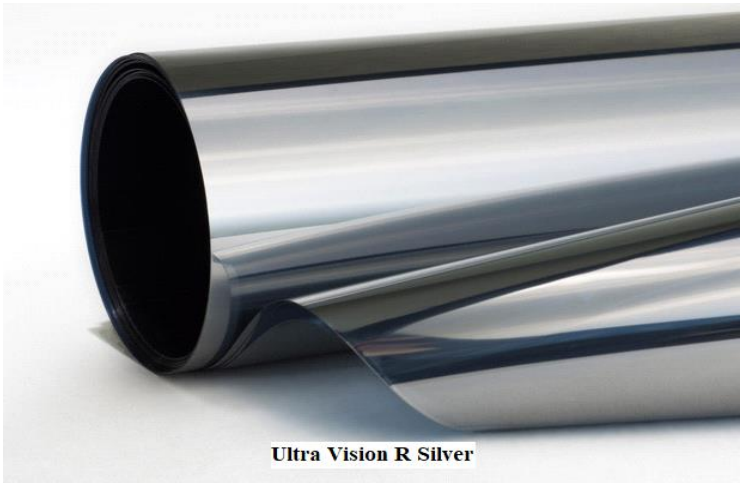


Рис.3.7 Захисна металізована плівка

Для забезпечення найбільш високого рівня захисту приміщення буде звукоізольовано. Для звукоізоляції будуть використовуватись акустичні панелі **ECOSOUND PYRAMID GAIN BLACK** типу піраміда, що мають більш широкий спектром звукопоглинання в порівнянні зі своїми аналогами за рахунок спеціального рельєфу, який дозволяє краще поглинати звукові хвилі в пористу структуру акустичного поролону. Гранично прості в монтажі і транспортуванні, не схильні до механічних пошкоджень за рахунок еластичності використовуваного матеріалу [17,38].

Розрахуємо кількість акустичних панелей, що нам потрібні для звукоізоляції [17,38]:

Висота стелі = 2.7 м.

Довжина приміщення = 5 м;

Площа приміщення = 13.5 кв.м;

Ширина приміщення = 2.7 м;

Отже, площа бокових стін : 2× (5м×2.7м) +2× (2.7м×2.7м) = 41.58 кв.м;

Площа підлоги та площа стелі: 2×(5м×2.7м) = 27 кв.м;

Загальна площа приміщення 41.58кв.м + 27 кв.м ≈ 69 кв.м

3.5 Висновки по розділу

1. Розроблено рекомендації щодо організації фізичного захисту об’єкту інформаційної діяльності. Обґрунтовано застосування механічних, електричних, електронних пристроїв та систем, котрі функціонують автономно, перешкоджаючи діяльності зовнішніх впливів, направлених на доступ до конфіденційної інформації

2. Розроблено рекомендації щодо порядку застосування засобів технічного захисту об’єкту інформаційної діяльності. Вказані рекомендації включають технічний захист, апаратне забезпечення захисту інформації, мережений захист, програмний захист. З метою підтримання функціонування та ефективного використання запропоновано ряд заходів щодо технічної підтримки засобів технічного захисту.

3. Розроблено рекомендації по розробці та втіленню системи контролю та управління доступом. Обґрунтовано склад системи контролю та управління доступом та її інтеграція з іншими системами технічного захисту та мережева взаємодія.

4. Розроблено систему фізичного захисту інформації на об'єкті інформаційної діяльності. Визначено склад обладнання та обґрунтовано його вибір.

ВИСНОВКИ

У процесі підготовки кваліфікаційної роботи були виконані наступні задачі:

- проведено огляд процесів обробки та захисту конфіденційних даних на об’єктах інформаційної діяльності;

- проаналізовано систему запобігання несанкціонованого доступу до конфіденційних даних на об’єкті інформаційної діяльності;

- розроблено рекомендацій щодо удосконалення система захисту об’єкту інформаційної діяльності від витоку конфіденційних даних технічними каналами.

1. У першому розділі кваліфікаційної роботи подано порядок обробки та розподілу інформації на об’єкті інформаційної діяльності. Визначено класифікацію інформації за змістом та порядком доступу. Подано способи та режими доступу до інформації. Визначено інформацію, яка підлягає захисту та подано критерії інформаційної безпеки.

Проведено аналіз загроз та визначено канали витоку технічної інформації. Показана структура технічного каналу витоку інформації.

Здійснено аналіз технічних каналів витоку інформації та подана їх класифікація. А саме: розподіл за видом інформаційної діяльності, принципом формування небезпечного сигналу, за середовищем поширення небезпечного сигналу, за способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника.

2. У другому розділі кваліфікаційної роботи розкрито сутність змісту та основні поняття у сфері технічних систем охорони та захисту інформації. Розглянуто основи застосування фізичних, апаратних, програмних та криптографічних засобів захисту інформації. Подано опис та можливості застосування активних інфрачервоних засобів руху. Подано склад та опис окремих елементів технічна системи спостереження на об’єкті інформаційної діяльності. Розглянуто порядок застосування систем відео спостереження,

пасивних інфрачервоних засобів виявлення, ультразвукових сенсорів, магніто контактних сповіщувачів, фотоелектричних сенсорів, вібросенсорів, сповіщувачів розбиття скла та їх комбінованих систем, призначення, принцип дії та галузь застосування приймально-контрольних і контрольних панелей, призначених для охорони, спостереження та пожежної сигналізації.

3. У третьому розділі кваліфікаційної роботи розроблено рекомендації щодо організації фізичного захисту об’єкту інформаційної діяльності. Обґрунтовано застосування механічних, електричних, електронних пристроїв та систем, котрі функціонують автономно, перешкоджаючи діяльності зовнішніх впливів, направлених на доступ до конфіденційної інформації

Розроблено рекомендації щодо порядку застосування засобів технічного захисту об’єкту інформаційної діяльності. Вказані рекомендації включають технічний захист, апаратне забезпечення захисту інформації, мережений захист, програмний захист. З метою підтримання функціонування та ефективного використання запропоновано ряд заходів щодо технічної підтримки засобів технічного захисту.

Розроблено рекомендації по розробці та втіленню системи контролю та управління доступом. Обґрунтовано склад системи контролю та управління доступом та її інтеграція з іншими системами технічного захисту та мережева взаємодія.

Розроблено систему фізичного захисту інформації на об'єкті інформаційної діяльності. Визначено склад обладнання та обґрунтовано його вибір.

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.

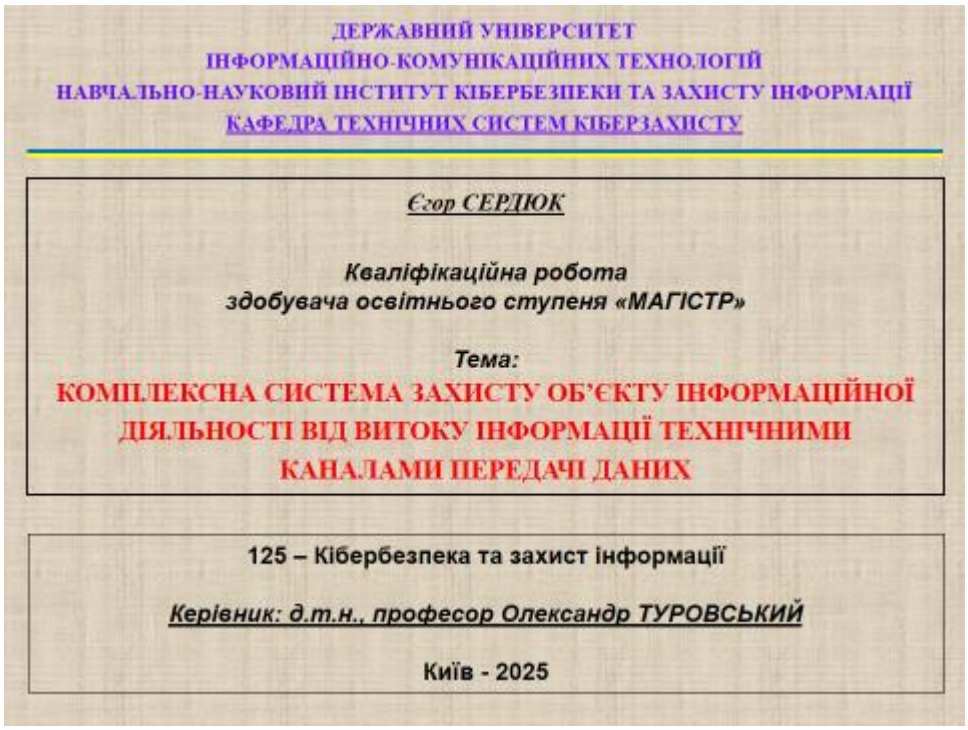
36. https://tzi.com.ua/zagalnij-oglyad-sistem-vbroakustichnogo-zashumlennya.html.

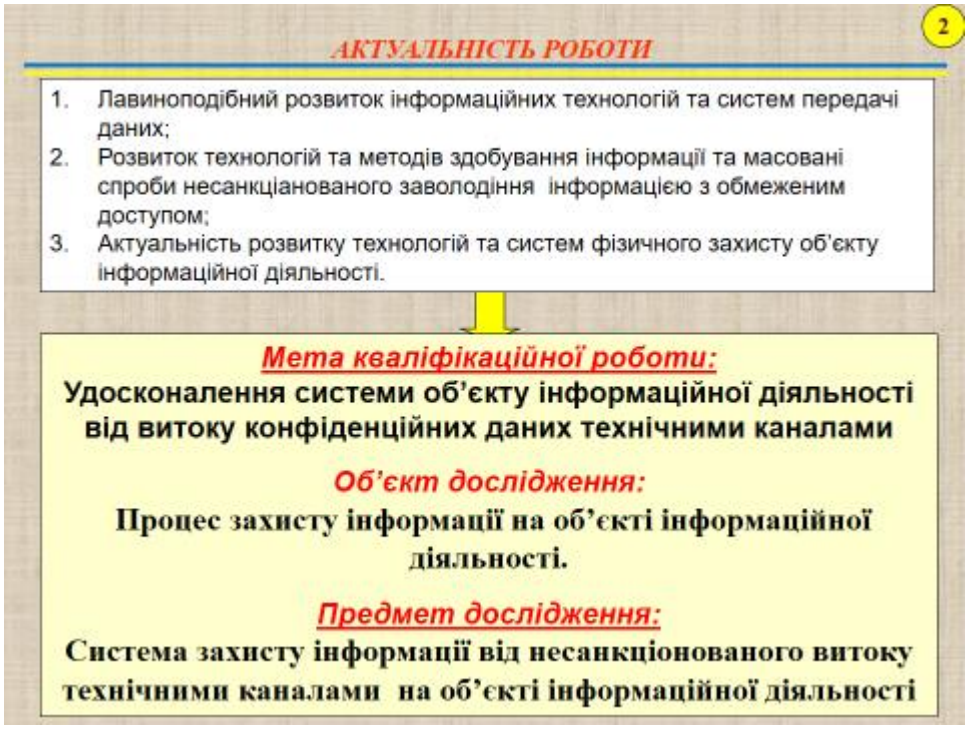
37. https://plenka.market/ua/ultra_vision_r_silver_20_1524_m/

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

Додаток А

Оформлення слайдів та роздаткового матеріалу





ЗДОБУТІ РЕЗУЛЬТАТИ РОБОТИ

3

1. **РОЗДІЛ 1**: ОБРОБКА ТА ЗАХИСТ КОНФІДЕНЦІЙНИХ ДАНИХ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

2. **РОЗДІЛ 2**: СИСТЕМА ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОМУ ДОСТУПУ ДО КОНФІДЕНЦІЙНИХ ДАНИХ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

3. **РОЗДІЛ 3**: ДОСЛІДЖЕННЯ НАПРЯМКІВ УДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ВІД ВИТОКУ КОНФІДЕНЦІЙНИХ ДАНИХ ТЕХНІЧНИМИ КАНАЛАМИ

4. **ВИСНОВКИ**: Узагальнено одержані результати

4

ПЕРШИЙ РЕЗУЛЬТАТ
ОБРОБКА ТА ЗАХИСТ КОНФІДЕНЦІЙНИХ ДАНИХ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Режим доступу до інформації

5

ПЕРШИЙ РЕЗУЛЬТАТ

Критерії інформаційної безпеки :

1. **Цілісність** - властивість інформації бути захищеною від несанкціонованого знищення, модифікації;
2. **Конфіденційність** - властивість інформації бути захищеною від несанкціонованого ознайомлення;
3. **Доступність - властивість інформації бути захищеною від несанкціонованого доступу.**

Технічні канали витоку інформації:

Структура технічного каналу витоку інформації

6

ПЕРШИЙ РЕЗУЛЬТАТ

Класифікація технічних каналів витоку інформації :

1. **За видом** інформаційної діяльності на ОІД
2. **За принципом** (фізичним ефектом, процесом) формування небезпечного сигналу (носія інформації)
3. **За середовищем** поширення небезпечного сигналу
4. **За способом** перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника

→

1. Радіоканал;
2. Електричний;
3. Акустичний;
4. Оптичний;
5. Матеріально-речовий.

7

ДРУГИЙ РЕЗУЛЬТАТ

СИСТЕМА ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОМУ ДОСТУПУ ДО КОНФІДЕНЦІЙНИХ ДАНИХ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Основні поняття у сфері технічних систем охорони та захисту інформації :

Технічний засіб охорони – апаратура, яка використовується у складі комплексів (систем) технічних засобів призначених для охорони об'єктів (територій, будівель, приміщень) від несанкціонованого проникнення

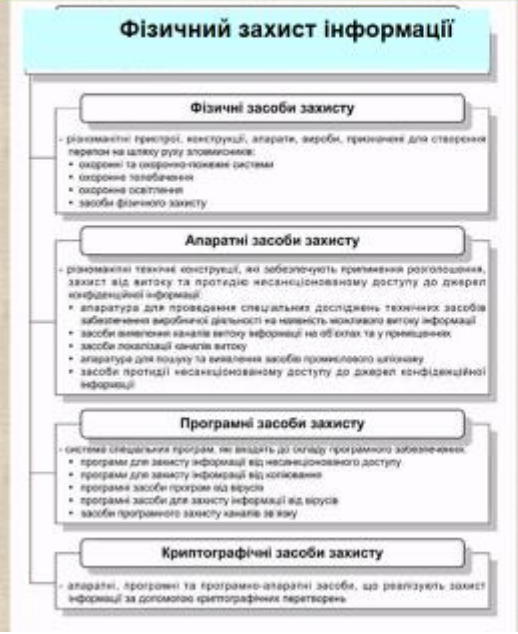
Засіб виявлення - це пристрій, призначений для автоматичного формування сигналу із заданими параметрами унаслідок вторгнення або подолання об'єктом виявлення чутливої зони даного пристроюю

Чутливий елемент - це первинний перетворювач, що реагує на дію на нього (пряме або непряме) об'єкта виявлення і сприймає зміну стану навколишнього середовища

Комплексом ТЗОС - сукупність функціонально зв'язаних засобів виявлення, системи збору і обробки інформації і допоміжних засобів і систем (системи тривожного сповіщення, системи охорони периметра і ін..), об'єднаних завданням по виявленню порушника

8

ДРУГИЙ РЕЗУЛЬТАТ



Завдання інженерно-технічного захисту інформації :

- **Охорона території підприємства на спостереження за нею;**
- **Охорона будівель, внутрішніх приміщень та контроль за ними;**
- **Охорона обладнання, продукції, фінансів та інформації;**
- **Здійснення контрольованого доступу до будівель та приміщень.**

9

ТРЕТІЙ РЕЗУЛЬТАТ

НАПРЯМКІВ УДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ВІД ВИТОКУ КОНФІДЕНЦІЙНИХ ДАНИХ ТЕХНІЧНИМИ КАНАЛАМИ

Рекомендації щодо організації фізичного захисту ОІД

1. Території та приміщення, які відповідають цінностям інформації, які підлягають захисту;
2. Периметр безпеки має точно визначений;
3. Додаткове обладнання має розміщуватися таким чином, щоб мінімізувати ризик НСД до ІзОД;
4. Фізичні бар'єри мають за потреби діставати стелі, для запобігання несанкціонованого доступу (НСД) до режимних приміщень;
5. Стороннім особам не можна надавати інформацію про дії на режимних територіях;
6. Заборона виконувати роботу наодинці без належного контролю;
7. ІС необхідно розміщувати у спеціально визначених місцях, окремо від обладнання, контрольованого будь-якими сторонніми підрозділами;
8. У неробочий час територія об'єкту має бути фізично недоступні та перевірятися охороною;
9. У межах режимних територій, не має застосовуватися фото та відео фіксація;
10. Необхідно забезпечити належний контроль доступу.

10

ТРЕТІЙ РЕЗУЛЬТАТ

Рекомендації щодо порядку застосування засобів технічного захисту об'єкту інформаційної діяльності

Типова ситуація	Канал витоку інформації	Методи і засоби	
		отримання інформації	захисту інформації
Розмови в приміщенні та на вулиці	Акустичний	Підслуховування (диктофон, мікрофон тощо)	Шумові генератори, пошук закладних пристроїв, захисні фільтри, обмеження доступу
	Віброакустичний	Стетоскоп, вібродатчики	
	Акустоелектромагнітний	Спеціальні радіоприймачі	
Розмови по телефону:	Акустичний	Підслуховування (диктофон, мікрофон тощо)	Шумові генератори, пошук закладних пристроїв, захисні фільтри, обмеження доступу
- провідному	Сигнал у лінії	Паралельний телефон, прилад підімкнення, електромагнітний датчик, диктофон, телефонна закладка	Маскування, скремблювання, шифрування, спецтехніка
	Наведення	Спеціальні радіотехнічні пристрої	Спецтехніка
- радіотелефону	ВЧ-сигнал	Радіоприймачі	Маскування, скремблювання, шифрування, спецтехніка

11

ТРЕТІЙ РЕЗУЛЬТАТ

Дії з документом на паперовому носії: – виготовлення	Безпосередньо сам документ	Крадіжка, прочитування, копіювання, фотографування	Обмеження доступу, спецтехніка
	Продавлення отворів або папору	Крадіжка, прочитування	Оргтехзаходи
	Акустичний шум принтера	Апаратура акустичного контролю	Пристрої шумонагодження
	Паразитні сигнали, наведення	Спеціальні радіотехнічні засоби	Екранування
– поштове відправлення	Безпосередньо сам документ	Крадіжка, прочитування	Спеціальні методи
Документ на машинному носії: – виготовлення	Носій	Крадіжка, копіювання, прочитування	Контроль доступу, фізичний захист, криптозахист
	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	Імітація підключення, імітація зареєстрованого користувача	Криптозахист
Виробничий процес	Відходи, використані тощо	Спецапаратура різного призначення	Оргтехзаходи, фізичний захист

12

ТРЕТІЙ РЕЗУЛЬТАТ

Рекомендації по розробці та втіленню системи контролю та управління доступом

Основні завдання СКУД:

1.Управління доступом на задану територію, включаючи також обмеження доступу на задану територію;

2. Ідентифікація особи, яка має доступ на задану територію;

4. Ведення бази персоналу/відвідувачів;

3. Розрахунок заробітної плати (при інтеграції з системами бухгалтерського обліку);

5. Інтеграція зі всіма системами безпеки:
- з системою відеоспостереження;
- з системою охоронної сигналізації;
- з системою пожежної сигналізації .

13

ТРЕТІЙ РЕЗУЛЬТАТ

Класифікація СКУД

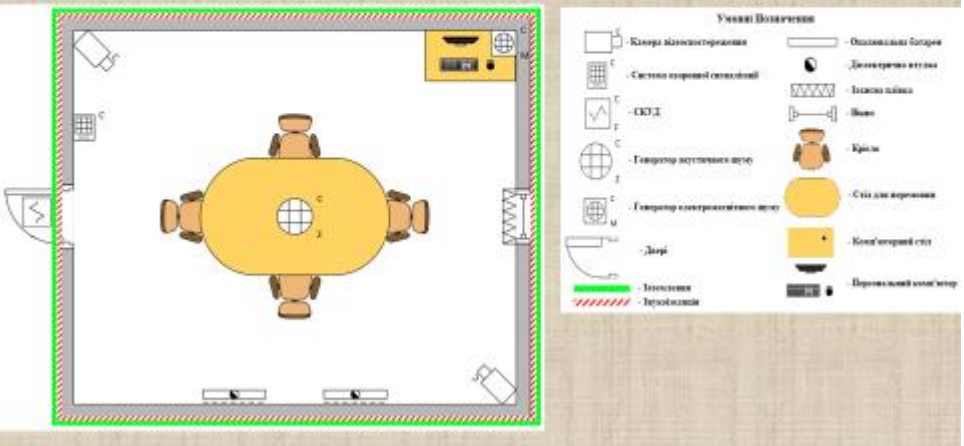
За технічними характеристиками і функціональними можливостями	- рівень ідентифікації; - кількість контрольованих місць; - пропускна здатність; - кількість користувачів; - умови експлуатації
За рівнем ідентифікації доступу	- одноріневі (ідентифікація здійснюється за однією ознакою, наприклад, з зчитування коду картки); - багаторіневі (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]

14

ТРЕТІЙ РЕЗУЛЬТАТ

Системи фізичного захисту інформації на об'єкті інформаційної діяльності

Об'єкт інформаційної діяльності



15

ТРЕТІЙ РЕЗУЛЬТАТ

Вибір каме

Вибір системи контролю та

Вибір генератора акустичного

Вибір генератора акустичного

Вибір системи охоронної

Захисна металізована плівка

16

ВИСНОВКИ:

У процесі підготовки кваліфікаційної роботи були виконані наступні задачі:

1. 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.

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

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

АПРОБАЦІЯ:

Є.Р. Сердюк, Р. С. Марчук, О. В. Рожков. **Напрямки удосконалення єдиної моделі комплексної системи захисту від витоку інформації технічними каналами.** *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем.* м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.92-93.

ДЯКУЮ ЗА УВАГУ !