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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Системи санкціонованого доступу до технічних каналів передачі інформації об'єкту банківської діяльності»

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
_____ Юрій ЖЕРЕБОК

Виконав: здобувач вищої освіти групи СЗДМ 61
Юрій ЖЕРЕБОК

Керівник: ПОНОЧОВНИЙ Петро
Доктор філософії (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2026

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

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____ Олександр Туровський

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Жеребку Юрію Володимировичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Системи санкціонованого доступу до технічних каналів передачі інформації об'єкту банківської діяльності»
керівник кваліфікаційної роботи Поночовний Петро, доктор філософії
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: об'єкті інформаційної діяльності, канали витоку інформації з обмеженим доступом на об'єкті інформаційної діяльності, методи, способи та механізми ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Захист інформації на об'єктах інформаційної діяльності.
4.2. Огляд методів і засобів ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.
4.3. Розробка та вдосконалення механізмів багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом

5. Перелік графічного матеріалу: ___Презентаційний матеріал на слайдах._____

6. Дата видачі завдання 15.10.2025

КАЛЕНДАРНИЙ ПЛАН

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

Здобувач вищої освіти _____ Юрій ЖЕРЕБОК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Петро ПОНОЧОВНИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 77 сторінок, має 9 рисунків, 5 таблиць. Список використаних джерел містить 26 найменувань і займає 3 сторінки.

Метою кваліфікаційної роботи є підвищення ефективності функціонування системи захисту інформації об’єкту критичної інфраструктури.

В кваліфікаційній роботі вирішено наступні завдання. Проведено аналіз основних загроз несанкціонованого доступу до конфіденційної інформації через технічні канали передачі даних об’єкту критичної інфраструктури. Дослідження напрямків удосконалення системи управління доступом на об’єкті критичної інфраструктури. Розробка системи управління доступом на об’єкті критичної інфраструктури.

Апробація:

Ю.В. Жеребок, І.В. Довбня, О.І. Лихогод, Особливості функціонування та завдання системи захисту технічних каналів передачі інформації об’єктів банківської діяльності. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-комунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.32-33. https://duikt.edu.ua/uploads/p_2779_72486260.pdf.

Ключові слова: ОБ’ЄКТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ, КОМПЛЕКСНА СИСТЕМИ ЗАХИСТУ ІНОФРМАЦІЇ, СИСТЕМИ УПРАВЛІННЯ ДОСТУПОМ.

ABSTRACT

The qualification work consists of an introduction, four sections, general conclusions, a list of sources used, the total volume of the work is 77 pages, has 9 figures, 5 tables. The list of sources used contains 26 items and takes up 3 pages.

The purpose of the qualification work is to increase the efficiency of the functioning of the critical infrastructure object protection system.

The following tasks are solved in the qualification work. An analysis of the main threats of unauthorized access to confidential information through technical data transmission channels of the critical infrastructure object was conducted. Research on areas for improving the access control system at the critical infrastructure object. Development of an access control system at the critical infrastructure object. A review of the issues of lithosphere pollution within the framework of environmental protection problems was conducted.

Approbation:

Yu.V. Zherebok, I.V. Dovbnya, O.I. Lykhogod, Features of the functioning and tasks of the system for protecting technical information transmission channels of banking facilities. All-Ukrainian Scientific and Practical Conference: Current Problems of Security of Information and Communication Systems. Kyiv, November 5, 2025, Kyiv: DUIKT Research and Development Center. – 2025. P.32-33. https://duikt.edu.ua/uploads/p_2779_72486260.pdf.

Keywords: CRITICAL INFRASTRUCTURE OBJECT, COMPREHENSIVE INFORMATION PROTECTION SYSTEM, ACCESS MANAGEMENT SYSTEM.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІзОД	–	Інформація з обмеженим доступом
ОІД	–	Об’єкт інформаційної діяльності
СТЗІ	–	Система технічного захисту інформації
ТКВІ	–	Технічний канал витоку інформації
ОТЗС	–	Основні технічні засоби і системи
ТЗПІ	–	Технічний засіб перетворення інформації
ДТЗС	–	Допоміжні технічні засоби системи
ПЕМВ	–	Побічні електромагнітні випромінювання
ТЗОС	–	Технічні засоби охоронної сигналізації
АС	–	Автоматизована система
КЗЗ	–	Комплекс засобів захисту
КСЗІ	–	Комплексна система захисту інформації
НСД		Несанкціонований доступ
ОС		Обчислювальна система
ДТЗС		Допоміжні технічні засоби та системи
ІТС		Інформаційно-телекомунікаційна система
КС		Комп’ютерна система
НД		Нормативний документ
НД ТЗІ		Нормативний документ системи технічного захисту інформації

ВСТУП

Важливим та актуальним питанням сьогодення є забезпечення безпеки національних установ, підприємств, загальнонаціональних систем та мереж (тобто критичної інфраструктури). Враховуючи швидкі темпи технологічного розвитку, зростаючу складність економічного життя та соціальних відносин, а також постійно розвиваються технології, що підтримують ці установи, можна зробити висновок, що інформація є одним із ключових факторів забезпечення якості їхньої роботи. Тому ефективне забезпечення безпеки технічних систем критичної інфраструктури та запобігання витоку інформації через технологічні канали є нагальним завданням та предметом цієї роботи.

Метою кваліфікаційної роботи Метою кваліфікаційної роботи є підвищення ефективності функціонування системи захисту інформації об’єкту критичної інфраструктури.

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

– проведено аналіз основних загроз несанкціонованого доступу до конфіденційної інформації через технічні канали передачі даних об’єкту критичної інфраструктури.

– дослідження напрямків удосконалення системи управління доступом на об’єкті критичної інфраструктури.

– розроблено систему управління доступом на об’єкті критичної інфраструктури.

Об’єкт дослідження. Система захисту каналів передачі інформації на об’єкті критичної інфраструктури.

Предмет дослідження. Системи контролю та управління доступом на об’єкт критичної інфраструктури.

РОЗДІЛ 1
АНАЛІЗ ОСНОВНИХ ЗАГРОЗ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ЧЕРЕЗ ТЕХНІЧНІ КАНАЛИ ПЕРЕДАЧІ ДАНИХ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Класифікація та структуризація масивів корисних даних на об'єкті критичної інфраструктури

Інформація — це будь-яка інформація та/або дані, які можуть зберігатися на фізичному носії або відображатися в електронному вигляді[1].

За змістом інформацію можна класифікувати на такі типи[1,2,3,4]:

– Персональна інформація;

– Довідкова та енциклопедична інформація;

– Інформація про стан навколишнього середовища (екологічна інформація);

– Інформація про продукцію (роботи, послуги);

– Науково-технічна інформація;

– Податкова інформація;

– Правова інформація;

– Статистична інформація;

– Соціальна інформація;

– Інші види інформації[1].

Однак у практичному застосуванні важливішою є класифікація на основі прав доступу. Відповідно, інформацію можна розділити на: публічну інформацію та інформацію з обмеженим доступом (Рисунок 1.1)[2].

Публічна інформація — вся інформація є публічною, за винятком інформації, обмеженої законом. Основною характеристикою відкритої інформації є те, що будь-хто зацікавлений може отримати до неї доступ, а

обмеження доступу до відкритої інформації заборонені[1,2]. Забезпечення доступу до відкритої інформації [1,2,3,4]:

– Систематично публікувати інформацію в офіційних друкованих виданнях (оголошення, збірники статей);

– Поширювати інформацію через засоби масової інформації;

– Надавати інформацію безпосередньо зацікавленим громадянам, державним органам та юридичним особам [1,2].

Рис.1.1 Режим доступу до інформації

Інформація (ІзОД) стосується інформації, що становить державну таємницю або іншу законодавчо визначену таємницю, а також секретної інформації, яка належить державі або підлягає захисту за законом [1,5].

Секретна інформація стосується інформації у сферах оборони, економіки, науки і техніки, дипломатії, національної безпеки та правоохоронної діяльності. Її розголошення може загрожувати національній безпеці України, тому класифікується як державна таємниця відповідно до законодавчо встановлених

процедур та охороняється державою. Інформація, що становить державну таємницю, додатково класифікується відповідно до Закону України «Про державну таємницю» [1,5].

Секретна інформація стосується інформації, яка перебуває у власності, використовується або розпоряджається фізичними або юридичними особами та розкривається відповідно до їхніх запитів та встановлених умов. Для інформації, що належить державі та використовується державними органами або органами місцевого самоврядування, підприємствами, установами та організаціями різних форм власності, можуть бути встановлені обмеження доступу на законодавчому рівні, а також може бути надано статус секретної інформації з метою захисту цієї інформації [1,5].

Згідно із Законом про захист інформації в інформаційно-телекомунікаційних системах, у системі захищається така інформація [1,5]:

- Інформація, що є публічною власністю, визначена Законом України про інформацію як статистична, правова, соціальна, довідкова та енциклопедична інформація, що використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, та інформація щодо діяльності таких органів, опублікована в Інтернеті, інших глобальних інформаційних мережах та системах або передана через телекомунікаційні мережі (далі – «інформація, що є публічною власністю»);

- Конфіденційна інформація, що є власністю держави або вимагається законом для захисту, включаючи конфіденційну інформацію щодо фізичних осіб (далі – «конфіденційна інформація»);

- Інформація, що становить таємницю, визначену державним або іншим законодавством (конфіденційна інформація).

Інформація, що є публічною власністю, повинна зберігатися недоторканою під час обробки системою, що забезпечується шляхом запобігання несанкціонованим операціям, які можуть призвести до випадкової або навмисної зміни чи знищення інформації. Усі користувачі повинні мати право доступу до інформації, що є публічною власністю. Змінювати або

знищувати інформацію, що є публічною власністю, можуть лише автентифіковані та авторизовані користувачі.

Конфіденційна та секретна інформація повинна бути захищена від несанкціонованого та неконтрольованого доступу, зміни, знищення, копіювання та розповсюдження [1,5].

Усі операції, пов'язані з обробкою інформації з обмеженим доступом, здійснюються в межах Засобу інформаційної діяльності. За визначенням, об'єкти інформаційної діяльності – це будівлі, майданчики, транспортні засоби або інші інженерні споруди, функціональним призначенням яких є сприяння потоку інформації з обмеженим доступом [1,5]. Інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб та держави [1,5].

Обробка інформації об'єктами інформаційної діяльності забезпечує інформаційну безпеку, що відображається у підтримці таких стандартів інформаційної безпеки [1,2,3,4]:

- Цілісність: атрибут інформації, тобто інформація захищена від несанкціонованого знищення або зміни;

- Конфіденційність: атрибут інформації, тобто інформація захищена від несанкціонованого доступу;

- Доступність: атрибут інформації, тобто інформація захищена від несанкціонованого блокування.

Для задоволення інформаційних потреб державні органи, місцеві та регіональні органи самоврядування створюють інформаційні служби, системи, мережі, бази даних та банки даних. Порядок їх створення, структури, права та обов'язки визначаються Кабінетом Міністрів України або іншими державними органами та місцевими та регіональними органами самоврядування [1,5].

Основні види інформаційної діяльності включають отримання, використання, поширення та зберігання інформації [1,5].

Отримання інформації – це отримання та накопичення громадянами, юридичними особами або державою зареєстрованої або загальнодоступної інформації відповідно до чинного законодавства України [1,5].

Використання інформації – це задоволення інформаційних потреб громадян, юридичних осіб та держави. Поширення інформації – це розповсюдження, публікація та впровадження зареєстрованої або загальнодоступної інформації відповідно до законодавчо встановлених процедур [1,6].

Зберігання інформації – це забезпечення належного стану інформації та її фізичних носіїв [5,6].

Отримання, використання, поширення та зберігання зареєстрованої або загальнодоступної інформації здійснюється відповідно до процедур, передбачених цим законом та іншими законами та нормативними актами в галузі інформації. Крім того, можна виділити діяльність, пов'язану з інформаційним забезпеченням, таку як отримання, оцінка, зберігання та обробка даних, створених для прийняття управлінських рішень. Це стосується різних видів діяльності, таких як виробництво та збут, послуги, включаючи покращення технологічності, якість продукції, зниження собівартості, реклама, інформація про асортимент продукції, інформація про ціни, організація послуг тощо [5,6].

Жоден вид інформаційної діяльності (включаючи інформаційний бізнес) не може здійснюватися ізольовано. Її учасники (торгові контрагенти), тобто продавці чи покупці, роботодавці чи працівники, діють у певному середовищі, яке визначає їхнє становище, відомому як підприємницьке (підприємницьке) середовище [5,6].

Жоден бізнес не може функціонувати без бюджету. Системи управління, що базуються на встановлених бюджетах, координують різні види діяльності, керують операціями відділів, а також проводять контроль та оцінку ефективності. На початку звітного періоду бюджет відображає очікування керівництва щодо продажів, витрат та інших фінансових операцій у наступному

періоді; він відображає прогнози керівництва. Наприкінці звітного періоду бюджет виступає інструментом вимірювання, що дозволяє керівництву реагувати на відхилення: порівнювати фактичні результати із запланованими значеннями та відповідно коригувати наступні дії. Якщо бюджети та прогнози базуються на одному наборі вихідних даних та припущень щодо доходів, витрат, рівня запасів та рівня ділової активності, вони відповідатимуть один одному, утворюючи взаємозалежну систему. Раціональне використання коштів допоможе ефективніше використовувати технології, тим самим покращуючи діяльність компанії, стратегії розвитку та інформаційну безпеку компанії в цілому та її матеріальних активів [5,6].

1.2. Технічні канали несанкціонованого витоку інформації на об’єкті критичної інфраструктури

Для визначення вимог до захисту від витоку інформації та організації заходів захисту від витоку інформації, спрямованих на технічні канали, технічні канали були класифіковані за певними характеристиками.

Зокрема, витоки інформації технічного зв'язку (ВТЗІ) розрізняються на основі таких характеристик [6,7]:

- На основі типу інформаційної активності на ІЗІ,
- На основі принципу формування (фізичного ефекту, процесу) сигналу небезпеки (носія інформації),
- На основі середовища поширення сигналу небезпеки,
- На основі методу, за допомогою якого технічна розвідка противника перехоплює (ліквідує) сигнал небезпеки.

На основі типу інформаційної активності на ІЗІ, ВТЗІ можна класифікувати на такі типи:

- Технічні канали витоку голосової інформації,
- Технічні канали витоку інформації, що обробляється в ОТЗС,
- Технічні канали витоку візуальної інформації,

- Матеріальні канали витоку інформації.

Рекомендується класифікувати ТКВІ за вищезазначеними типами ТКВІ на основі принципу формування (фізичного ефекту, процесу), середовища поширення та методу, за допомогою якого технічна розвідка противника перехоплює (ліквідує) сигнал небезпеки.

На основі цих характеристик технічні канали витоку голосової інформації можна класифікувати наступним чином [7,8]:

- Акустичні канали.

- Вібраційні (вібраційні акустичні) канали.

- Акустооптичні (лазерні акустичні) канали.

- Електроакустичні канали.

- Аудіовізуальні канали.

- Канали радіочастотних перешкод (використовуються для ліквідації голосової інформації).

- Канали витоку голосової інформації на основі вбудованих пристроїв.

Технічні канали витоку інформації, що обробляються ОТЗС, можна класифікувати наступним чином [7,8]:

- Канали бічного електромагнітного випромінювання.

- Канали бічних електромагнітних перешкод.

- Канали паразитної модуляції радіочастотних сигналів генератора.

- Канали паразитної генерації радіочастот підсилювачів.

- Канали перехоплення (видалення) інформації з волоконно-оптичних ліній передачі даних.

- Канали перехоплення (видалення) інформації з каналів зв'язку.

- Канали радіочастотних перешкод (використовуються для видалення інформації, що обробляється ОТЗС).

- Канали витоку інформації обробки ОТЗС на основі вбудованих пристроїв.

Технічні канали витоку візуальної інформації можна класифікувати наступним чином [7,8]:

- Візуальні канали.

- Оптичні візуальні канали.

- Канали витоку візуальної інформації на основі вбудованих пристроїв.

Матеріальні канали витоку інформації [7,8,9,10]:

- Вилучення інформації з магнітних властивостей або інших носіїв інформації несправних пристроїв ЕОТ.

- Вилучення інформації з чернеток документів, виробництва, публікацій, офісних відходів тощо.

- Хімічні канали.

- Виходячи з носія інформації та принципу формування сигналу небезпеки, можна виділити такі ТКВІ [7,8]:

1. Канали витоку електромагнітної інформації, включаючи канали бічного електромагнітного випромінювання, канали генерації високої частоти "паразитного" підсилювача, канали модуляції високочастотного генератора "паразитного" типу та канали перехоплення інформації ліній радіозв'язку (радіорелейного, стільникового, мобільного) тощо;

2. Канали витоку інформації електричних сигналів, включаючи канали електромагнітних перешкод на стороні зв'язку та канали вилучення інформації з дротових ліній зв'язку;

3. Канали витоку інформації за параметрами, включаючи канали радіочастотних перешкод та канали "паразитної" модуляції.

Залежно від місця розташування інформації, перехопленої методами технічної розвідки противника, можна виділити такі типи каналів витоку технічної інформації [7,8,9,10]:

- Канали перехоплення (видалення) інформації поза зоною контакту;

- Канали перехоплення (видалення) інформації поза зоною контакту, але які позитивно впливають на параметри каналу витоку технічної інформації (наприклад, канали радіочастотних перешкод);

- Канали для вилучення інформації за допомогою методів технічної розвідки, встановлених на цілях витоку інформації (OID) (наприклад, канали витоку технічної інформації, що виконуються вбудованими пристроями).

Наведена вище класифікація каналів витоку технічної інформації допомагає нам систематично зрозуміти ці канали, розробити відповідні системи контролю витоку технічної інформації для захисту інформації від витоку та визначити відповідні вимоги та заходи.

1.3. Загрози несанкціонованого витоку інформації на об'єкті інформаційної діяльності

Захист інформації є найважливішим компонентом комплексних заходів Технічного захисту інформації (TIP). Зловмисники можуть перехоплювати інформацію, отримувати до неї доступ без дозволу та використовувати її для інших цілей [1.5,6].

Для незаконного викрадення інформації використовуються різні технічні засоби. Інформація передається від цілі до зловмисника через різні фізичні канали [6,7].

Виходячи з фізичних характеристик джерела інформаційного сигналу, середовища поширення та методів перехоплення інформації, канали витоку технічної інформації можна класифікувати на такі категорії [7,8]:

- Радіоканали;
- Електричні сигнали;
- Акустичні сигнали;
- Оптичні сигнали;
- Матеріальні сигнали [7].

Аналіз фізичних характеристик численних джерел сигналів показує [6,7]:

- Джерела небезпечних сигналів включають компоненти, вузли та провідники виробничого та охоронного обладнання, а також радіо- та електронне обладнання;

- За певних умов кожне джерело небезпечного сигналу може утворювати канал витоку технічної інформації;

Кожна електронна система, що містить компоненти, вузли та провідники, має велику кількість каналів витоку технічної інформації. Причини витоку радіоінформації по каналах включають:

- Ефект мікрофона;
- Магнітне поле;
- Паразитний шум;
- Коло живлення;
- Коло заземлення;
- Взаємний вплив;
- Електромагнітне випромінювання;
- Радіочастотні перешкоди;
- Від волоконно-оптичних систем зв'язку.

Загалом, структура каналу витоку технічної інформації включає (Рисунок 1.2): джерело або передавач сигналу, середовище поширення струму або електромагнітних хвиль та приймач сигналу [7].

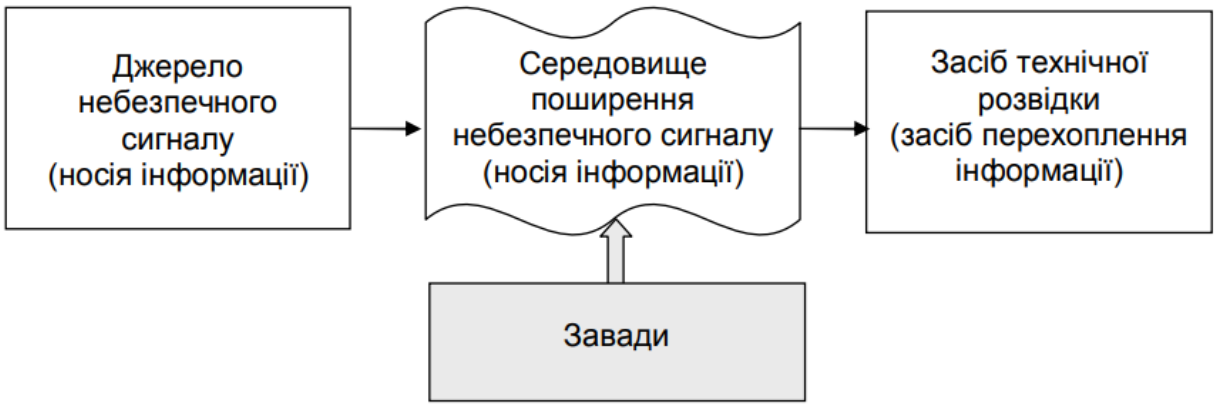


Рис. 1.2 Структура технічного каналу витоку інформації

1.4 Висновки по розділу

1. Описано процес розповсюдження інформації для цілей інформаційної діяльності. Визначено методи класифікації інформації за змістом та процедури доступу. Пояснено методи та закономірності доступу до інформації. Визначено захищену інформацію та представлено стандарти інформаційної безпеки.

2. Проаналізовано загрози та визначено канали витоку технічної інформації. Продемонстровано структуру цих каналів.

3. Проаналізовано та класифіковано канали витоку технічної інформації. Критерії класифікації включають: вид інформаційної діяльності, принципи формування сигналів небезпеки, засоби поширення сигналів небезпеки та методи перехоплення (ліквідації) сигналів небезпеки за допомогою технічної розвідки противника.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ НАПРЯМКІВ УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ДОСТУПОМ НА ОБ'ЄКТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Сучасні технологій організації безпечного доступу на об'єкт інформаційної діяльності

Системи контролю доступу (СКД) безпосередньо застосовуються до критичної інфраструктури через контрольно-пропускні пункти (КПП). Працівники часто нехтують безпекою під час переміщення між офісами, залишаючи двері між офісами та приміщеннями відкритими; тому використання СКД є невід'ємною частиною загальної системи безпеки об'єкта.[24]

Крім того, СКД застосовується до зон об'єкта для обмеження доступу до зон, де зберігаються конфіденційні дані та важлива інформація. Тому дозволи персоналу повинні призначатися відповідно до ролей, щоб забезпечити доступ до об'єкта.[25]

СКД також може застосовуватися до таких зон, як парковки та входи/виходи. СКД реалізується автоматично через бар'єри та зони зберігання.[25]

СКД дозволяє персоналу виконувати рутинні завдання та служить інструментом для забезпечення інформаційної безпеки, підзвітності та управлінського контролю, а також може відігравати певну роль у складних ситуаціях, що вимагають нестандартних рішень. Контроль переміщення людей, транспортних засобів та транспорту — саме це і є функцією системи. Він використовує існуючі засоби та функції для вирішення загроз національній безпеці, спрямування персоналу в охоронювані зони, ведення реєстраційної інформації про людей та транспортні засоби, зберігання інформації про в'їзд та

виїзд з зон, а також генерування звітів для подальшої обробки та аналізу.[28] Цей метод автоматизації може генерувати інформацію про переміщення та реєстрацію людей та транспортних засобів цілодобово та щодня без додаткових ресурсів. Інші системи (наприклад, системи пожежної або охоронної сигналізації, системи відеоспостереження) можуть бути залучені для підвищення безпеки, а це означає, що системи контролю доступу досягають складної безпеки завдяки автоматизованому управлінню [28].

Системи контролю доступу можуть бути автономними або мережевими. Різниця між мережевими та автономними системами полягає в тому, що мережеві системи контролю доступу вимагають додаткового обладнання та програмного забезпечення, що збільшує витрати. Автономні системи контролю доступу збирають такі дані, як номер картки, інформація про власника та дозволений час доступу, які зберігаються в пам'яті контролера [28].

2.2 Огляд існуючих систем контролю і управління доступу на об’єкті критичної інфраструктури

Комп'ютери та сервери з встановленим програмним забезпеченням утворюють верхній рівень традиційної системи контролю доступу до мережі, керуючи підключеними до них контролерами.[29]

Контролер — це спеціалізований, надійний комп'ютер, що містить інформацію про конфігурацію, режими роботи системи, списки уповноваженого персоналу та індивідуальні дозволи на доступ.

Для великих систем може використовуватися кілька контролерів; для простіших систем контролери можуть бути інтегровані в зчитувачі карт.[29]

Зчитувач карт — це другий рівень системи контролю доступу, підключений до контролера. Зчитувач карт — це пристрій, який зчитує інформацію, записану на картці або брелоку. Ця інформація передається на панель керування, яка дозволяє персоналу входити до приміщення. Панель

керування можна налаштувати на запит дозволу у відповідальної особи або автоматичний запит дозволу у системи.[32]

Кожному користувачеві присвоюється унікальний персональний номер, який надає права доступу, дозволяючи йому проходити через двері/турнікети протягом певних періодів часу. Коли картка використовується як ідентифікатор, на картці також відображається фотографія.[33]

Виконавчі пристрої – це компоненти «нижчого рівня» системи контролю доступу, такі як електромеханічні або електромагнітні замки, турнікети, ворота, блокпости, автоматичні двері тощо. Основною функцією таких пристроїв є виконання команд контролера для блокування або розблокування точок доступу[33].

Використання електронних систем контролю доступу не повністю виключає людський фактор. Ефективна система повинна використовувати електронні пристрої лише як засоби безпеки, відповідальні за виконання простих операцій, тоді як відповідальна особа відповідає за виконання загальних функцій контролю та контроль складних, нестандартних ситуацій. Однак сучасні системи контролю доступу можуть ефективно контролювати та контролювати вхід та вихід людей, транспортних засобів та будь-яких інших предметів у межах охоронюваної зони[35].

Залежно від складності, вони можуть виконувати такі функції[35]:

- Запобігання та боротьба з несанкціонованим проникненням, таким як потрапляння людей у заборонені зони;

- Виявлення носіння зброї, контрабанди та речовин;

Фіксація проходження кожної особи, включаючи час та іншу інформацію, для подальшого аналізу та обробки.

Дистанційне керування людьми та транспортними засобами, що в'їжджають та виїжджають з певних зон, може бути здійснене за допомогою спеціалізованих пристроїв керування. Автоматизована робота може працювати цілодобово без помилок, навіть під час виконання повторюваних завдань.

Таким чином, загальна ефективність підвищується, оскільки різні підсистеми безпеки інтегровані в єдину централізовано керовану систему [36]:

- Система контролю доступу (СКУД),
- Система пожежної сигналізації (СПС),
- Відеоспостереження,
- Система автоматизації управління будівлями.

Комп'ютерні системи керування, що використовують потужні можливості електронних пристроїв, вважаються складними та ефективними системами контролю доступу. Системи керування доповнюються безмежним потенціалом програмного та апаратного забезпечення.

За методом керування, системи контролю доступу (СКУД) можна класифікувати наступним чином [36]:

- Автономні системи контролю доступу призначені для керування одним або кількома виконавчими механізмами без обміну інформацією з центральною консоллю керування та без необхідності керування оператором. Ці системи підходять, коли керування потрібне через кілька точок керування, а онлайн-моніторинг подій доступу не потрібен. Такі системи структурно інтегровані зі зчитувачем карток в одному корпусі. Контролер запрограмовано на додавання нових карток до своєї пам'яті та видалення старих карток за допомогою клавіатури або майстра налаштування [36].

Переваги автономних систем контролю доступу включають [37]:

– Низька вартість,
– Просте програмування системи,
– Ефективне встановлення,
– Підходять для невеликих приміщень без спеціального охоронного обладнання та прості у використанні.

Недоліки автономних систем контролю доступу включають: громіздкий процес програмування, коли кількість точок доступу та користувачів велика; неможливість виконувати операції з процесами доступу в режимі реального

часу; та відсутність можливості обробляти протоколи подій та генерувати вибіркові звіти на основі попередньо встановлених критеріїв. Централізовані системи контролю доступу (ЦСКД) – це велика категорія систем контролю доступу, що характеризується можливістю налаштування пристроїв та керування процесами доступу через комп'ютерні термінали. Системи ЦСКД відрізняються архітектурою, масштабом, функціональністю, використовуваними зчитувачами карток та стійкістю до злому. Багато централізованих (також відомих як мережеві) системи ЦСКД зберігають переваги автономних систем, переважно працюючи без потреби в керуючому комп'ютері. Тобто система може працювати самостійно, коли керований комп'ютер вимкнений. Ці системи мають власні буфери пам'яті для зберігання номерів карток користувачів та подій, що відбуваються в системі. Наявність комп'ютера в системі дозволяє співробітникам служби безпеки оперативно втручатися в процес доступу та керувати системою в режимі реального часу. Найважливішим компонентом централізованої системи контролю доступу (ЦСКД) є її програмне забезпечення, яке забезпечує різноманітну функціональність та охоплює широкий спектр завдань.

Переваги мережевих ЦСКД включають [38]:

– Простота програмування.

– Безпосереднє керування об'єктами.

– Візуалізація подій у режимі реального часу.

– Можливість побудови великомасштабних систем.

– Високий потенціал для інтеграції з іншими системами безпеки.

Недоліками мережевих СКУД є необхідність навчання персоналу та вищі витрати на придбання та встановлення порівняно з автономними СКУД [38].

СКУД загального призначення є типом централізованих СКУД — вони можуть переходити в автономний режим роботи у разі збою комп’ютера, відмови мережевого обладнання або переривання зв’язку. СКУД пропонують вищу надійність; однак у деяких системах деякі функції втрачаються при

переході в автономний режим. Важливі функції, які потребують особливої уваги. Рівень реалізації архітектури та функцій взаємопов'язаний на апаратному рівні.

2.3 Аналіз функціонування та вимоги до виконавчих пристроїв систем і управління доступу об’єкту критичної інфраструктури

Працівникам надається унікальний ключ, який вони зберігають за собою протягом усього періоду роботи. Ключ має форму картки або брелока з унікальним кодом (відвідувачам також надається картка або брелок для перебування, якщо це необхідно; картку або брелок необхідно повернути керівнику після виїзду)[7]. Картки призначаються співробітникам, а дані вносяться в базу даних на робочому місці. Зчитувачі карток встановлюються в точках контролю доступу для ідентифікації кодів карток та передачі їх контролеру. Контролер порівнює дані в базі даних зі зчитаними кодами та визначає, чи дозволено доступ. Якщо доступ дозволено, турнікет або шлагбаум випромінюватиме дозволений колір або сигнал; якщо доступ заборонено, активується система пожежної сигналізації (ПСС), контроль доступу, функція блокування турнікета або шлагбауму або інші функції, що забезпечуються системою контролю доступу (СКД). Такі дані, як особа, яка проходить, та час її проходження, записуються в базу даних. На основі цього система генерує звіти для відстеження робочого часу, виявлення порушників трудової дисципліни або відстеження потенційних зловмисників[27]. Перевага централізованих систем контролю доступу (СКУД) полягає в їхній високій масштабованості

(наприклад, їх можна розширювати, коли потрібно збільшити ресурси, персонал тощо). Тобто такі СКУД можуть використовуватися як у приватних будинках та невеликих організаціях, так і у великих установах та для конкретних цілей інформаційної діяльності [8].

Для побудови СКУД необхідно чітко визначити та поставити завдання, які вона повинна вирішувати: вона повинна надійно запобігати несанкціонованому проникненню, забезпечуючи при цьому безперешкодний доступ для уповноваженого персоналу та зручність використання [8]. Сучасні системи контролю доступу (СКУД) – це інтегровані апаратно-програмні системи, які можуть керувати входами, дверима, турнікетами та обертовими воротами в режимі реального часу за допомогою одного ключа (наприклад, електронного ключа з чіпом, бездротового пульта дистанційного керування, безконтактної карти або біометричної інформації (відбиток пальця, відбиток долоні, структура сітківки тощо)). Ці ключі керуються спеціалізованим програмним забезпеченням, яке збирає, обробляє та зберігає дані про персонал, що проходить через безпечні зони, та забезпечує інші функції (наприклад, адаптивне налаштування шаблонів доступу, створення персоналізованих графіків доступу для кожної особи, збір та аналіз інформації про час перебування персоналу, запис спроб небезпечного доступу тощо) [8]. Наприклад, у критичній інфраструктурі з одним входом поруч із дверима встановлюється зчитувач карток для реєстрації входу та виходу. Працівники вставляють свої картки у зовнішній зчитувач карток, щоб відчинити двері, і

система фіксує час входу та особисті дані особи як час проходу та час початку робочого дня. Якщо хтось залишає зону, вставлення картки у зчитувач зафіксує його вихід, що позначить кінець робочого дня. Кількість проходів протягом робочого дня можна налаштувати відповідно до потреб управління організацією, наприклад, чи впливає це на робочий час. Пам'ять контролера може зберігати понад 4000 карток доступу та таку ж кількість журналів подій. Система може працювати автономно, навіть якщо комп'ютер втрачає живлення. Після відновлення зв'язку з комп'ютером усі дані доступу будуть автоматично записані в базу даних [13].

Для місць з кількома входами та виходами слід передбачити настільний зчитувач карток, підключений до комп'ютера через USB, щоб забезпечити керування доступом до мережі та виставлення рахунків на основі часу [13].

Для точок доступу в невеликих місцях критичної інфраструктури, якщо використовується керування доступом до мережі та виставлення рахунків на основі часу, комп'ютер, встановлений у точці доступу, повинен мати можливість зв'язку з контролером, воротами доступу та виконувати фото- або відеоверифікацію. Комп'ютер відділу персоналу відповідає за реєстрацію карток персоналу та управління системою контролю доступу [15]. Вимоги до обладнання для виконання системи контролю доступу

Вимоги до обладнання для ідентифікації накладають певні обмеження на зчитувачі карток. Ці зчитувачі повинні мати можливість надійно зчитувати

ідентифікаційний код та перетворювати його на електричний сигнал, який потім передається до контролера[15].

Зчитувач карт повинен мати можливість запобігати таким атакам, як атаки методом грубої сили, підбір пароля та радіочастотне сканування[18].

Якщо введено неправильний пароль, система заблокується на певний час. Конкретна інформація щодо часу блокування повинна бути чітко вказана в інструкції з експлуатації обладнання та специфікаціях обладнання. Різні моделі обладнання можуть вимагати різних даних, і залежно від типу системи контролю доступу, адміністратор також може самостійно налаштувати час блокування. Налаштування часу блокування повинно забезпечувати виконання заданих вимог до пропускної здатності, обмежуючи при цьому кількість спроб підбору пароля. Наприклад, якщо кількість неправильних спроб пароля досягає 3, має відображатися сповіщення. Якщо система працює в автономному режимі, сповіщення буде надіслано на аудіовізуальний детектор; якщо система працює в мережевому режимі, сповіщення буде надіслано на центральну консоль керування та може бути перевірено аудіовізуальним детектором. Варто зазначити, що сповіщення також буде видано у разі людського саботажу[12].

Дизайн та зовнішній вигляд, ідентифікатори та зчитувачі не повинні призводити до розголошення конфіденційності коду. Пристрої ідентифікації повинні бути захищені від шкідливих зовнішніх факторів та людського саботажу.[13]

Виробники повинні забезпечити унікальність ідентифікаційного коду та його неповторюваність (тобто, згенерованого випадковими значеннями).[18]

Для автономних систем користувачі можуть змінювати або перевстановлювати код за потреби, але не менше 100 разів. Зміна коду залежить від того, чи попередній код залишається дійсним.[28]

Під час вибору ідентифікатора слід враховувати такі моменти:[26]

– Клавіатури пропонують нижчий рівень безпеки;

– Магнітні картки пропонують середній рівень безпеки;

– Датчик наближення, ключі Wiegand та електронні ключі; функція сенсорної пам'яті – високий рівень безпеки;

– Біометрія – надзвичайно високий рівень безпеки.

Вимоги до виконавчих механізмів [26]:

– Пристрій забезпечує відкриття/закриття замикаючого механізму або пристрою, надаючи сигнали від контролера та з пропускною здатністю, необхідною для даного об'єкта;

– Параметри керуючих сигналів повинні бути вказані відповідно до стандартів та/або технічних специфікацій для конкретного типу пристрою;

– Рекомендована напруга становить 12 В або 24 В. Однак для певних типів приводів виконавчих механізмів допускається живлення від мережі 220 В/380 В;

– Зловмисне пошкодження зовнішніх електричних з'єднань не повинно призводити до відкриття бар'єрного пристрою;

– Якщо пристрій втрачає живлення, він повинен забезпечувати резервне живлення та можливості аварійного механічного відкриття;

– Система аварійного відкриття повинна забезпечувати захист від безконтактних заходів безпеки (NSD);

– Пристрій повинен мати можливість захищати себе від шкідливих зовнішніх факторів та людського саботажу. Вимоги до пристроїв СКУД [26]:

1) Незалежно працюючі контролери повинні забезпечувати можливість отримання інформації від зчитувача карт, обробки цієї інформації та генерації керуючих сигналів для виконавчих механізмів.

2) Контролери, здатні працювати в мережевому режимі, повинні забезпечувати:

– Обмін інформацією між контролером та керуючим комп'ютером через лінії зв'язку;

– Збереження пам'яті, пристроїв та ідентифікаторів у разі переривання зв'язку з керуючим комп'ютером, відключення живлення або перемикання на резервне живлення;

– Керування лініями зв'язку між контролерами та між контролером та керуючим комп'ютером.

Для забезпечення належної роботи СКУД відстань між компонентами не повинна перевищувати значень, зазначених у паспорті та технічних характеристиках [28].

Протоколи обміну інформацією та інтерфейси повинні бути стандартизовані. Тип та параметри інтерфейсів повинні бути зазначені в паспорті та технічних характеристиках відповідно до чинних нормативних актів [28].

Рекомендовані типи інтерфейсів:

– Інтерфейс між контролерами RS 485;

– Інтерфейс між контролерами RS 485 та керуючим комп'ютером.

Тип та рівень захисту пристрою або системи повинні бути чітко вказані в паспорті. Відповідна інформація надається в технічній документації, але конфіденційність заходів захисту не повинна розголошуватися.[28]

Програмне забезпечення повинно бути належним чином захищене від непублічного розголошення даних (НРД) та копіювання, якщо це необхідно.

Програмне забезпечення захищене від НРД за допомогою захисту паролем. Рівні доступу за паролем повинні бути не менше двох.[28]

Рекомендується встановлювати рівні доступу відповідно до типу користувача.[16]

– Рівень 1 («Адміністратор») – Доступ до всіх функцій керування та доступу;

– Рівень 2 («Оператор») – Доступ лише до поточних функцій керування;

– Рівень 3 («Системний адміністратор») – Доступ до функцій конфігурації програмного забезпечення, але без доступу до функцій керування пристроєм.

Під час введення пароля на екрані дисплея пароль не повинен відображатися; він має бути прихованим. Пароль повинен містити щонайменше вісім латинських літер (з урахуванням регістру), цифри та спеціальні символи. [16]

Вимоги до живлення

Пристрій СКУД повинен живитися від доступної групи розподільчого щита аварійного освітлення або спеціально встановленого розподільчого щита. Цей розподільний щит повинен бути розташований поза приміщенням, що захищається, у металевій шафі та захищений від відкриття. [16]

Основне джерело живлення СКУД повинно здійснюватися від мережі змінного струму з частотою 50 Гц та номінальною напругою 220 В. СКУД повинен мати можливість нормально працювати з коливаннями напруги від -15% до +10% та коливаннями частоти від ±1 Гц. [16]

Деякі СКУД можуть живитися від інших джерел живлення з різними параметрами вихідної напруги, як зазначено в нормативних актах для конкретного типу системи. [16]

Щоб впоратися з відключенням основного живлення, пристрій СКУД повинен бути підключений до резервного джерела живлення. Автоматичне перемикання на резервне джерело живлення або навпаки має бути забезпечено без впливу на режим роботи та функціональний стан СКУД. Номінальна

напруга резервного джерела живлення повинна становити 12 В або 24 В. Під час використання резервного джерела живлення СКУД повинен мати можливість безперервно працювати не менше 8 годин[16].

2.4 Висновки по розділу

У другій частині підготовки до кваліфікаційного огляду було представлено вступ та аналіз проблем інформаційних систем, з якими щодня стикаються підприємства та організації, вивчено сучасні технології безпечного доступу до організаційних об'єктів та надано огляд існуючих систем контролю доступу на об'єктах критичної інфраструктури. Результати показали, що найпоширенішою системою є мережева система контролю доступу, а саме метод контролю ACS. Більш детально розглянуто принципи роботи мережевої системи контролю доступу, а також визначено вимоги до виконавчих механізмів ACS та джерел живлення [16].

Аналіз виявив деякі недоліки [36]:

1. Існують проблеми із забороною дублювання доступу. Багато систем ACS мають цю функцію, яка контролює не лише вхід, але й вихід. Ця функція призначена для збільшення ймовірності передачі ідентифікаційних ключів іншим особам.

2. Проблеми виникають, коли ідентифікаційні ключі втрачені або забуті вдома. Якщо ви просто залишите свій ключ або картку доступу поза критичною інфраструктурою, охорона надасть новий ключ або картку доступу для вирішення проблеми. Однак, якщо ви втратите ключ або картку доступу на робочому місці та пропустите час автоматичного блокування виходу, проблема ускладниться.

3. Якщо ключ буде викрадено або скопійовано, це поставить під загрозу безпеку всього об'єкта. Крім того, ці системи не можуть гарантувати належний захист для об'єктів з підвищеними вимогами безпеки.

РОЗДІЛ 3
РОЗРОБКА СИСТЕМИ УПРАВЛІННЯ ДОСТУПОМ НА ОБ'ЄКТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1 Передпроектне обстеження офісу об'єкту критичної інфраструктури

Для підготовки до процесу дослідження ми взяли за основу типовий офіс у критично важливому середовищі інфраструктури. План поверху офісу показано на рисунку 2.1.

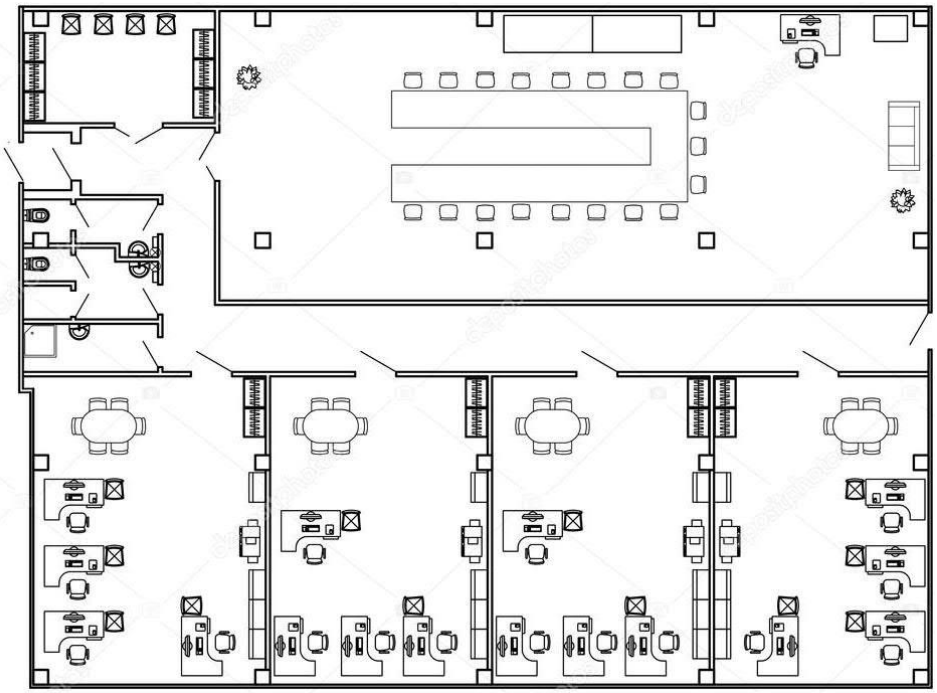


Рисунок 2.1 – План офісу

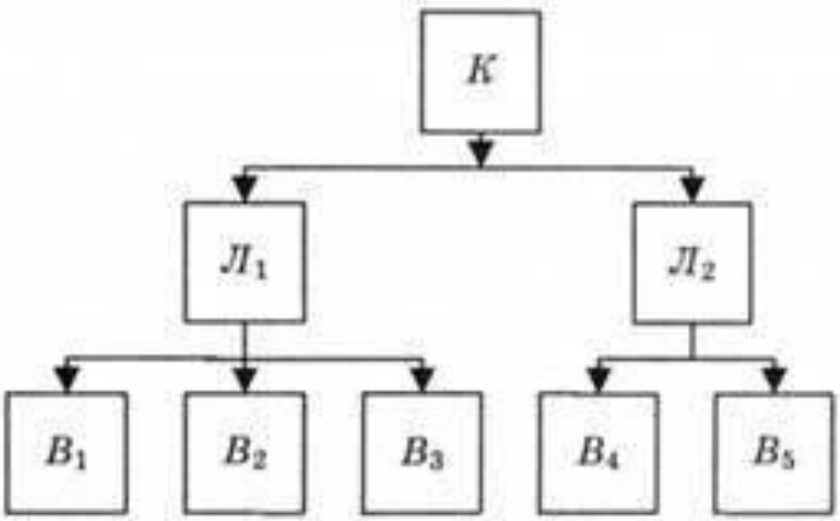


Рисунок 3.2 – Лінійна структура управління: К – генеральний керівник; Л – лінійний керівник; В – виконавець

Цей офіс критичної інфраструктури має чотири робочі місця, кожне з чотирма робочими станціями, та окремий кабінет керівника з однією робочою станцією. У кожному офісі працює чотири співробітники, кожен з яких виконує різні завдання. Загалом у закладі працює 17 співробітників.[16]

Усі робочі станції в закладі підключені до локальної мережі та Інтернету. Високошвидкісна мережа забезпечує голосовий та відеозв'язок між співробітниками в офісі та тими, хто знаходиться у віддалених офісах, усуваючи потребу в телефонних лініях. Високошвидкісна та надійна мережа також дає змогу створювати хмарну інфраструктуру, що дозволяє паралельно обробляти документи без їх зберігання на локальних робочих станціях.[16]

Швидка та надійна мережа підтримує роботу з веб-додатками або віддаленими робочими столами, які працюють на стороні сервера, дозволяючи співробітникам відмовитися від своїх робочих комп'ютерів та працювати з тонкими клієнтами. Такі ініціативи можуть позитивно вплинути на роботу співробітників, оскільки вони можуть отримувати доступ до веб-додатків зі своїх домашніх ПК незалежно від того, де вони працюють, що революціонізує роботу ІТ-відділів.[16]

Швидкість та надійність мережі є рушійними силами всієї критичної інфраструктури. Крім того, неправильна організація офісної мережі може призвести до помилок у будівництві, що призводять до фінансових втрат для організації.[16] Дротові мережі наразі працюють з використанням сучасних стандартів, а саме: витої пари та портів RJ-45. Дротові мережі працюють відповідно до стандарту IEEE 802.3, який включає [33]:

- IEEE 802.3u, з максимальною пропускною здатністю 100 Мбіт/с, для недорогих ноутбуків, старих комп'ютерів, мережевих пристроїв та пристроїв, що не потребують високошвидкісного з'єднання;

- IEEE 802.3ab, з максимальною пропускною здатністю 1000 Мбіт/с, для гігабітних мережевих карт, інтегрованих у материнські плати та мережеві пристрої;

- IEEE 802.3an, з максимальною пропускною здатністю 10 Гбіт/с, для робочих станцій та серверів.

Переваги дротових мереж полягають у їхній високій швидкості та стабільній роботі. Поширена швидкість конфігурації мережі становить 1 Гбіт/с. Ця швидкість є незалежною для кожного клієнта в мережі, з однаковою двонаправленою швидкістю передачі та загальною пропускною здатністю до 2000 Мбіт/с. Вона підтримує великі пакети даних, що може збільшити швидкість передачі великих обсягів даних за рахунок зменшення передачі службової інформації, тим самим зменшуючи навантаження на процесор. Агрегацію каналів можна використовувати для доступу до пропускної здатності, що перевищує 1 Гбіт/с. Вита пара може ефективно використовуватися, якщо довжина кабелю не перевищує 100 метрів, без шкоди для стабільності та швидкості з'єднання [33].

Апаратне забезпечення – Гігабітний дротовий мережевий контролер інтегрований у материнську плату та надається користувачам безкоштовно. Мережеві кабелі відносно недорогі та можуть бути обрізані до будь-якої

необхідної довжини. Користувачі можуть вибрати відповідне мережеве обладнання на основі параметрів та ціни.[33]

Безпека – Застосовуються заходи фізичної безпеки, що вимагають від зловмисників отримання фізичного доступу до будівлі та інших об'єктів для підключення до мережі.[33]

Недоліком дротових мереж є необхідність прокладання кабелів та подальшого налаштування для кожної робочої станції, що часто відбувається під час технічного обслуговування або будівництва будівлі. Тому, якщо інфраструктура змінюється, може знадобитися нова кабельна система. Таким чином, організація місць для співробітників, додавання нових робочих станцій або мережевого обладнання не є простим завданням, оскільки необхідна нова кабельна система.[51]

Важливо зазначити, що кожна робоча станція вимагає окремого кабелю, а такі пристрої, як смартфони та планшети, не можуть підключатися до дротових мереж.[51]

Для бездротового підключення Wi-Fi використовуються такі стандарти.[48]

- IEEE 802.11n, з максимальною пропускною здатністю від 150 до 600 Мбіт/с при використанні чотирьох антен. Стандарт підтримує бездротові мережі 2,4 ГГц та 5 ГГц.

- IEEE 802.11ac, з максимальною пропускною здатністю 6,77 Гбіт/с при використанні восьми антен. Цей стандарт застосовується лише до мереж 5 ГГц.

- IEEE 802.11g, з максимальною пропускною здатністю 54 Мбіт/с, наразі доступний лише у старіших пристроях, але деякі пристрої все ще підтримують цей стандарт.

Наразі існує багато різних пристроїв, що підтримують сучасні стандарти. Бездротові мережі реалізуються різними способами, але варто зазначити, що їхня продуктивність залежить від низки параметрів: підтримуваних стандартів зв'язку, кількості антен та фізичного розташування [48].

Очікується, що показники швидкості бездротового мережевого з'єднання наздоженуть дротові мережі та конкуруватимуть з ними. Однак через певні обмеження реальність не така проста [48].

Перевага бездротових мереж полягає у свободі. Тобто, співробітники можуть використовувати ресурси компанії скрізь, де вони можуть отримати сигнал точки доступу, з ефективним радіусом дії 30-50 метрів за хороших умов зв'язку. У цьому випадку співробітники більше не обмежені робочим місцем і можуть використовувати будь-який пристрій для роботи. Бездротове підключення покращує проведення великих зустрічей у різних кімнатах, особливо коли співробітники працюють у робочих групах і часто змінюють місце розташування [47].

Хоча підключення додаткових робочих станцій не є дорогим, якщо в офісі розгорнута бездротова інфраструктура, пропускна здатність точки доступу використовується всіма клієнтами, а пропускна здатність на кожного клієнта може значно знизитися під час інтенсивного обміну даними [31]. Окрім мобільних телефонів і планшетів, для підключення також можна використовувати принтери з підтримкою Wi-Fi. Отже, робота через Wi-Fi може знизити загальні витрати. Розгортання бездротової інфраструктури також є дорогим і вимагає прокладання кабелів, оскільки кабелі потрібно підключати до точки доступу [31].

Недоліками бездротових мереж є швидкість і стабільність. Тому що в цьому випадку фактична швидкість з'єднання завжди набагато нижча за номінальну швидкість [31].

Обмеження бездротових мереж Wi-Fi включають [2]:

- Швидкість з'єднання розподіляється між усіма клієнтами, тому чим більше клієнтів, тим нижча фактична швидкість;

- Високошвидкісне з'єднання може бути досягнуте лише за допомогою кількох антен. Тобто, якщо маршрутизатор має 8 антен, а телефон має лише 2 антени, швидкість, природно, буде нижчою;

- Швидкість бездротового з'єднання залежить від багатьох факторів: перешкод, відстані до точки доступу, кількості стін та інших перешкод між точкою доступу та клієнтом;

- Бездротові мережі можуть конфліктувати одна з одною під час роботи, тобто швидкість обміну даними буде змінена, коли кілька мереж одночасно використовують одні й ті ж або сусідні канали передачі. Згідно зі стандартом IEEE 802.11, пристрій працює в напівдуплексному режимі, а передача даних є односпрямованою протягом певного періоду часу. Коли вхід і вихід обмінюються даними одночасно, швидкість передачі зменшується вдвічі. Безпека є ще одним недоліком. Оскільки пристрій транслює дані всім, він створює ризик для безпеки; весь трафік можна контролювати, навіть якщо слухач знаходиться поза межами об'єкта маршрутизатора. Хоча встановлення пароля та вибір шифрування можуть зменшити ризик, якщо пароль підключення відсутній, застарілі алгоритми легко зламати. Крім того, точки доступу або клієнтські пристрої також вразливі до злому, і останнім часом з'являється все більше повідомлень про такі інциденти [2].

Аналіз потоку офісних даних

Ця критична інфраструктура має велику кількість апаратного забезпечення через велику кількість співробітників, кожен з яких має свій власний комп'ютер та інші периферійні пристрої. Запис робочих станцій, що використовуються співробітниками, має вирішальне значення [12].

Бізнес-комп'ютери Artline характеризуються низьким енергоспоживанням та високою продуктивністю. Artline Business - це гарне офісне комп'ютерне рішення, яке відповідає потребам офісних комп'ютерів щодо довговічності, ефективності, економічності, простоти використання та простоти

обслуговування. У таблиці 2.1 наведено характеристики ARTLINE Business T17 [12].

Mac mini – це комп’ютер, розроблений компанією Apple Inc. Він має невеликі розміри, а основний блок продається окремо без інших компонентів; докладнішу інформацію наведено в таблиці 3.2 [12].

Таблиця 3.1

Характеристики ARTLINE Business T17

Процесор	Шестиядерный Intel Core i5-8400 (2.8 - 4.0 ГГц)
Кеш третього рівня	3 МБ (у версії з процесором Intel Core i5), 6 МБ (в версії з процесором Intel Core i7), вбудовані в процесор
Пам’ять	32 DDR4, що працює на частоті 2666 МГц
Жорсткий диск	2 ТБ також 256 ГБ SSD
Оптичний привід	відсутній
Графіка	Графічний процесор Intel HD Graphics 4000
Порти	один порт FireWire 800 (800 Мб / с), 4 порти USB 3.0 (5 Гб / с), вихід HDMI, порт Thunderbolt (10 Гб / с), слот для карт SDXC
Аудіо	вбудований динамік, суміщений оптичний цифровий аудіовхід і аудіовихід
Мережевий інтерфейс	вбудований мережевий адаптер 10/100 / 1000BASE-T Gigabit Ethernet
Бездротові інтерфейси	вбудований адаптер AirPort Extreme Wi-Fi (на підставі проекту специфікації 802.11n); сумісність зі стандартом IEEE 802.11a/b/g, вбудований адаптер Bluetooth 4.0.

Таким чином, ці комп'ютери є досить сучасними, відповідають сучасним стандартам, є швидкими та надійними [12].

Усі ці комп'ютери підключені до локальної мережі (LAN) за зірковою топологією, як показано на рисунку 2.3 [12].

У зірковій мережевій топології група комп'ютерів підключена до центрального комп'ютера (який може виступати в ролі комутатора, маршрутизатора або концентратора), а інші периферійні комп'ютери підключені до цього центрального комп'ютера, кожен з яких використовує власну незалежну лінію зв'язку. Недоліками зіркової мережевої топології є висока вартість мережевого обладнання. У разі збою або переривання вся мережа буде непрацездатною. Збільшення кількості вузлів у мережі обмежується кількістю портів концентратора [14].

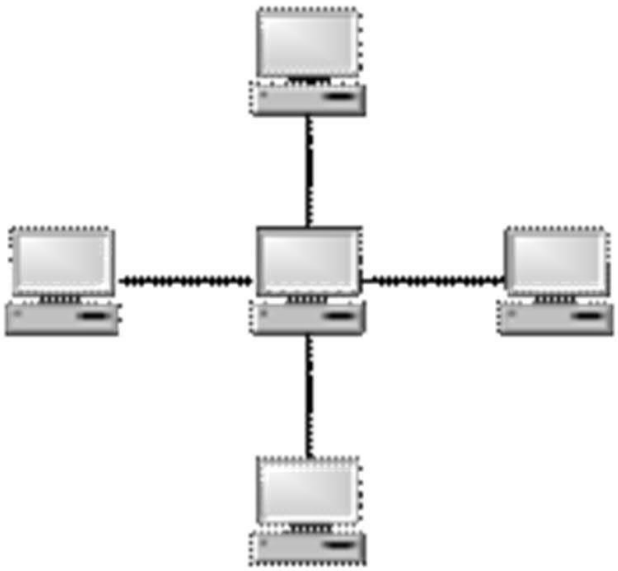


Рисунок 2.3 – Мережева топологія «зірка»

Таблиця 3.2

Характеристики Mac mini 2012

Процесор	2.5 ГГц Intel Core i5 (з можливістю розширення до чотирьох-ядерного Intel Core i7 з частотою 2.3 ГГц)
Кеш третього рівня	3 МБ (у версії з процесором Intel Core i5), 6 МБ (в версії з процесором Intel Core i7), вбудовані в процесор

Системна шина	1600 МГц
Пам'ять	4 ГБ або 8 ГБ пам'яті DDR3 SDRAM, що працює на частоті 1600 МГц, з можливістю розширення до 16 ГБ
Жорсткий диск	500 ГБ з можливістю розширення до 1 ТБ (або 256 ГБ SSD)
Оптичний привід	відсутній
Графіка	Графічний процесор Intel HD Graphics 4000
Порти	один порт FireWire 800 (800 Мб / с), 4 порти USB 3.0 (5 Гб / с), вихід HDMI, порт Thunderbolt (10 Гб / с), слот для карт SDXC
Аудіо	вбудований динамік, суміщений оптичний цифровий аудіовхід і аудіовихід
Мережевий інтерфейс	вбудований мережевий адаптер 10/100 / 1000BASE-T Gigabit Ethernet
Бездротові інтерфейси	вбудований адаптер AirPort Extreme Wi-Fi (на підставі проекту специфікації 802.11n); сумісність зі стандартом IEEE 802.11a/b/g, вбудований адаптер Bluetooth 4.0.

Apple Remote Desktop та Remote Office Manager використовуються для керування мережею [14]:

- Apple Remote Desktop – це система керування робочим столом OS X для розповсюдження програмного забезпечення, керування активами та віддаленої допомоги. Apple Remote Desktop пропонує низку високопродуктивних функцій, включаючи міжсистемний пошук Spotlight та понад 40 дій Automator для легкої автоматизації повторюваних завдань [14].

- Remote Office Manager (ROM) використовується для віддаленого керування комп'ютерами під керуванням Windows. Програма складається з двох частин: сервера (встановленого на віддаленому комп'ютері, якому

потрібен доступ) та клієнта (встановленого на комп’ютері системного адміністратора).

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

Методи фізичного захисту спираються на автономно працююче механічне, електричне та електронне обладнання та системи, призначені для запобігання зовнішньому втручанню з метою отримання конфіденційної інформації [12,13,28].

Такі системи можуть включати захист периметра, контроль доступу на основі смарт-карт та технологію сенсорної пам'яті. Ці системи забезпечують фізичну безпеку місць розташування інформаційних систем, допоміжного обладнання, носіїв інформації та каналів передачі інформації. Основні заходи фізичного захисту спрямовані на запобігання пожежі, воді, пилу, агресивним газам, електромагнітному випромінюванню, вандалізму та несанкціонованому доступу. Вимоги до захисних бар'єрів та їх розташування залежать від цінності інформації, ризику вразливостей безпеки та необхідності дотримання існуючих захисних заходів [13,15,16].

Прийнятний діапазон заходів фізичного захисту для запобігання катастрофам або порушенням. Кожен рівень фізичного захисту має певні обмежені зони, зони або місця для забезпечення відповідного рівня захисту. Для реалізації захисту периметра необхідно встановити системи охоронної та пожежної сигналізації, системи відеоспостереження, системи контролю доступу (СКД) тощо [13,15,16]. Наступні рекомендації [13,15,28,29] слід правильно дотримуватися:

• Зони та місця розташування повинні відповідати цінності інформації, що підлягає захисту;

• Периметри безпеки повинні бути чітко визначені;

• Розміщення додаткового обладнання повинно мінімізувати ризик порушення інформаційної безпеки даних (NSD);

• За необхідності фізичні бар'єри повинні сягати стелі, щоб запобігти потраплянню неавторизованого персоналу до обмежених зон (NSD);

• Інформація щодо діяльності в обмежених зонах не повинна надаватися неавторизованому персоналу;

• Несанкціонована експлуатація без належного нагляду заборонена;

• Інформаційні системи (ІС) повинні бути розміщені у відведених місцях, окремо від обладнання, що контролюється будь-якою третьою стороною;

• У неробочий час зони об'єктів повинні бути фізично ізольовані та оглянуті співробітниками служби безпеки;

• Використання фото- та відеозаписного обладнання заборонено в обмежених зонах;

• Необхідно забезпечити ефективний контроль доступу.

Для впровадження контрольних заходів необхідно виконати наступне [20,29,30]:

• Зафіксувати дату та час входу та виходу відвідувачів;

• Скасувати права доступу колишніх співробітників до обмежених зон;

• Дотримуватися системи контролю доступу організації та внутрішніх правил і положень.

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

Ефективними інструментами захисту від зовнішніх атак є технічні засоби захисту, які базуються на різних методах, призначених для запобігання несанкціонованому доступу до інформації та зловмисному використанню зовнішніх пристроїв для доступу до інформації [20,21,29,30].

Ці технічні методи реалізуються шляхом інтеграції різних пристроїв в апаратне забезпечення систем обробки інформації або шляхом комбінування заходів захисту ресурсів для захисту від атак соціальної інженерії. Ці пристрої можуть запобігати фізичному вторгненню або вторгненню в доступ до інформації (Таблиця 3.1), включаючи маскування інформації [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
– провідному	Сигнал у лінії	Паралельний телефон, приймання підмикання, електромагнітний датчик, диктофон, телефонна закладка	Маскування, скремблювання, шифрування, спецтехніка
	Наведення	Спеціальні радіотехнічні пристрої	Спецтехніка
– радіотелефону	ВЧ-сигнал	Радіоприймачі	Маскування, скремблювання, шифрування, спецтехніка
Дії з документом на паперовому носії:	Безпосередньо сам документ	Крадіжка, прочитування, копіювання, фотографування	Обмеження доступу, спецтехніка
	Продавлення стрічки або паперу	Крадіжка, прочитування	Оргтехзаходи
– виготовлення	Акустичний шум принтера	Апаратура акустичного контролю	Пристрої шумозаглушування
	Паразитні сигнали, наведення	Спеціальні радіотехнічні засоби	Екранування
– поштове відправлення	Безпосередньо сам документ	Крадіжка, прочитування	Спеціальні методи
Документ на машинному носії:	Носій	Крадіжка, копіювання, прочитування	Контроль доступу, фізичний захист, криптозахист
– виготовлення	Відображення на дисплеї	Візуальний, копіювання, фотографування	Контроль доступу, фізичний захист, криптозахист
	Паразитні сигнали, наведення	Спеціальні радіотехнічні пристрої	Контроль доступу, криптозахист, пошук закладок, екранування
	Електричні та оптичні сигнали	Апаратні закладки	
	Програмний продукт	Програмні закладки	
– передавання документа по каналах зв"язку	Електричні та оптичні сигнали	Несанкціоноване підмикання, імітація зареєстрованого користувача	Криптозахист
Виробничий процес	Відходи, випромінювання тощо	Спецапаратура різного призначення	Оргтехзаходи, фізичний захист

Ми також обговорюємо такі пристрої, як замки, віконні решітки, сигналізації, генератори шуму, мережеві фільтри та скануючі радіоприймачі, які можуть запобігти витоку інформації через потенційні технічні канали або виявити такі витоки. Для захисту інформації на апаратному рівні можна використовувати апаратні ключі, системи сигналізації, механізми блокування пристроїв та інтерфейси введення/виведення інформації [20,21,24].

Системи зв'язку використовують засоби захисту мережевої інформації [18,19,20]:

• Брандмауери — використовуються для блокування атак із зовнішнього середовища та контролю передачі мережевого трафіку відповідно до правил безпеки. Брандмауери зазвичай встановлюються в точці входу в мережу, щоб розрізняти внутрішні та зовнішні мережі (наприклад, брандмауери Cisco PIX, Symantec Enterprise Firewall™, Contivity Secure Gateway та Nortel Networks' Alteon Switched Firewall).

• Системи виявлення вторгнень (IDS) — використовуються для захисту від систем захисту мережі (NDS) та атак типу «відмова в обслуговуванні» (DoS). Вони використовують кілька механізмів для блокування шкідливої активності, зменшуючи час простою та витрати на обслуговування мережі після атаки (наприклад, Cisco Secure IDS, Symantec's Intruder Alert та NetProwler).

• Інструменти створення віртуальних приватних мереж (VPN) – використовуються для встановлення безпечних каналів передачі даних у небезпечних середовищах, забезпечуючи прозоре підключення локальної мережі та підтримуючи конфіденційність та цілісність інформації (наприклад, Symantec Enterprise VPN, Cisco IOS VPN та Cisco VPN Concentrator).

• Інструменти аналізу безпеки корпоративної мережі – використовуються для виявлення потенційних каналів реалізації інформаційних загроз, допомагаючи підприємствам запобігати потенційним атакам на мережу, оптимізувати витрати на захист інформації та контролювати поточний стан

безпеки мережі (наприклад, Symantec Enterprise Security Manager та Symantec NetRecon).

Технологічні канали – зовнішнє електромагнітне випромінювання та наведення через акустичні та оптичні канали.

Заходи щодо запобігання витоку інформації через технічні канали зв'язку включають [18,19,21]:

• Використання екранованих кабелів та прокладання електричних кабелів в екранованих конструкціях;

• Встановлення високочастотних фільтрів;

• Створення екранованих середовищ;

• Використання екранованого обладнання;

• Встановлення активних систем шумоподавлення.

1) Витік, спричинений структурним шумом зі стін та стель;

2) Видалення інформації зі стрічок принтера, неповністю стертих дискет тощо;

3) Видалення інформації за допомогою відеозакладок;

4) Програмні та апаратні закладки на персональних комп'ютерах;

5) Радіозакладки в стінах та меблях;

6) Видалення інформації з вентиляційних систем;

7) Видалення акустичної інформації з вікон за допомогою лазерів;

8) Виробничі та технічні відходи;

9) Комп'ютерні віруси, логічні бомби тощо;

10) Отримання інформації шляхом бутстрепінгу та "накладання";

11) Дистанційне відеозахоплення;

12) Отримання акустичної інформації за допомогою записуючого обладнання;

Інформація, що обробляється в типовій одноповерховій будівлі, може бути схильна до таких каналів витоку та несанкціонованого доступу [18,19,21]:

1) Крадіжка носіїв інформації;

2) Високочастотні канали витоку в побутовій техніці;

3) Крадіжка інформації через спрямовані мікрофони;

4) Внутрішні канали витоку інформації;

5) Несанкціоноване копіювання;

6) Витік, спричинений бічним випромінюванням від терміналів;

7) Крадіжка інформації за допомогою "телефонних вух";

8) Крадіжка інформації з клавіатур та принтерів через акустичні канали;

9) Крадіжка інформації з дисплеїв через електромагнітні канали;

10) Крадіжка інформації з дисплеїв та принтерів;

11) Націлювання на лінії зв'язку та зовнішні провідники;

12) Витік через лінії зв'язку;

13) Витік через заземлюючі мережі;

14) Витік через мережі синхронізації;

15) Витік через мережі мовлення та гучномовці;

16) Витік в системах охоронної та пожежної сигналізації;

17) Витік з мережі живлення;

18) Витік у мережах опалення, газопостачання та водопостачання.

Засоби забезпечення технічного захисту інформації (включаючи захист від соціальних технічних атак), постачальники цих засобів, а також послуги з встановлення, монтажу, налаштування та обслуговування визначаються власником та обробляються організацією інформаційної безпеки самостійно або на основі рекомендацій експертів у галузі технічного захисту інформації (ТЗІ) відповідно до чинного законодавства та нормативних актів. Вибір залежить від фрагментації або складності захисту інформації. Фрагментований захист спрямований на конкретні загрози, тоді як комплексний захист спрямований на конкретні загрози [18,19,29,30].

Засоби ТЗІ можуть працювати незалежно або разом із ТЗІ як окремі пристрої або вбудовані компоненти. Для оцінки стану засобів ТЗІ, що обробляються та поширюються в інформаційних системах, комп'ютерних

мережах та системах зв'язку, необхідний огляд поточного стану сфери ТЗІ, щоб зробити висновки для координації рішень. Процедури розрахунку та визначення зон інформаційної безпеки (тобто ЗІБ) розроблені для оцінки ефективності таких заходів захисту та визначення процедур сертифікації відповідних технічних засобів, як це викладено в нормативних документах, пов'язаних з ЗІБ [25]. Перевагами методу ЗІБ є висока надійність, а недоліками – недостатня гнучкість, великий обсяг даних, потреба у великій кількості пристроїв та висока вартість [21,26,29].

3.4. Рекомендації по підбору та обґрунтування вибору обладнання

У ситуаціях з обмеженим доступом вибір відповідного обладнання та технологій для забезпечення інформаційної безпеки в контрольованій зоні стає вирішальним. У цій статті буде розглянуто потенційні варіанти обладнання для побудови такої системи.

Вибір камери

На рисунку 3.2 показано IP-камери, що використовуються для порівняння. [22,23].

Рис.3.2 IP-камери

Далі ми надамо порівняльну таблицю основних характеристик IP-камер та оберемо найбільш підходящий варіант (Таблиця 3.3) [22,23].

Виходячи з вищезазначених характеристик, можна зробити висновок, що для систем безпеки приміщень з обмеженим доступом камера Dahua DH-IPC-T1B20P є найкращим вибором для забезпечення запису подій, що відбуваються всередині об'єкта.

Причини вибору цієї камери такі:

• 16-кратний цифровий зум;

• Низька ціна;

• Відповідність стандарту вандалозахисту IK08;

• Відповідність стандарту пило- та вологостійкості IP67;

• Низьке енергоспоживання;

Таблиця 3.3

Порівняння характеристик IP-камер

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

Крім того, обрана камера також має наступне:

• Інфрачервоне підсвічування завдяки використанню ICR-фільтра.

• Висока якість зображення;

• Дальність виявлення - 43 метри;

• Датчик руху;

• Оснащений системою 3D-DNR шумозаглушення;

Виберіть систему контролю доступу (СКД).

У нашій системі безпеки використання СКД для контролю доступу персоналу є важливим. Використання біометричної СКД є найкращим варіантом для забезпечення безпечного доступу до об'єкта. СКД, що використовується для порівняння, показано на рисунку 3.3 [23,35].

Рис.3.3 Елементи СКУД

На основі аналізу характеристик, Hikvision DS-K1T501SF є найкращим вибором для СКУД.

Переваги цієї СКУД включають:

• Простота експлуатації;

• Вбудована камера;

• Міцний корпус;

• Доступна ціна;

• Захист від пилу та вологи;

Крім того, ця СКУД також має такі характеристики:

• Максимальна кількість відбитків пальців: 5000;

• Підтримка двосторонніх голосових дзвінків;

• Вбудована камера (опційно 2-мегапіксельна);

• Кілька методів автентифікації: QR-код, відбиток пальця, проведення картки, відбиток пальця + пароль, проведення картки + пароль, проведення картки + відбиток пальця + пароль тощо;

• Максимальна кількість карт пам'яті: 50 000, максимальна кількість записів контролю доступу: 200 000;

• Функції виявлення незаконного доступу, розблокування за тайм-аутом, перевірка на наявність недійсних карток на основі часу будильника, аварійна сигналізація тощо [37]

Таблиця 3.4

Порівняння характеристик СКУД

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

Вибір генератора акустичного шуму

Генератори акустичного шуму призначені для запобігання витоку конфіденційної інформації через вібраційну акустику та акустичні канали шляхом генерації маскуючих шумових сигналів. Генератори акустичного шуму, що використовуються для порівняння, показані на рисунку 3.4. [23,36]

Враховуючи характеристики генераторів акустичного шуму, ми зрештою обрали генератор RIAS-2GS.

Цей генератор пропонує такі переваги:

• Конкурентна ціна;

• Широкий робочий діапазон;

• Живлення від батареї;

• 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	20540
Діапазон робочих частот	50…8000 Гц	170 - 5700 Гц	180 Гц до 5,6 кГц	250—6500 Гц
Електроживлення	7...9 В	220 ± 22 В	220 ± 22 В	220В
Вихідна потужність підсилювача	не менше 2.5 Вт	не менше 6 Вт	не менше 10 Вт	не менше 8 Вт
Мінімальний опір навантаження	2 Ом	4 Ом	4 Ом	3 Ом
Можливість роботи від акумулятора	+	—	+	—

Крім того, PIAC-2ГС пропонує низку переваг:

• Глибина регулювання рівня шумового сигналу не менше 20 дБ у робочому діапазоні частот;

• Генератор працює нормально в діапазоні температур від +10 до +40 °С;

• Час технічної підготовки не більше 1 секунди;

• На відстані 1 метра від передавача, з похибкою установки не більше 6 дБ, середній максимальний рівень вихідного акустичного сигналу (відносно

нуля при 2×10^5 Па, тобто рівня звукового тиску) у робочому діапазоні частот становить не менше 70 дБ.

• Цей генератор включено до переліку загальних засобів забезпечення захисту інформаційних технологій, встановленого Державною службою спеціального зв'язку України, а вимоги до його захисту визначаються законодавством України. [21,31]

Вибір генераторів електромагнітного шуму

Генератори електромагнітного шуму призначені для маскування інформаційно-пов'язаних портативних електронних пристроїв, робочих станцій, персональних комп'ютерів та обчислювальних пристроїв шляхом випромінювання та формування широкосмугових шумових сигналів у навколишньому просторі, схемах та інженерних комунікаціях. Генератор електромагнітного шуму для порівняння показано на рисунку 3.5. [23,36]

Салют 2000 Б

Гном-3

Старкад-32

РІАС-1ГМ

Рис.3.5 Генератори електромагнітного шуму

Виходячи з вищезазначених характеристик, найбільш підходящим вибором є генератор електромагнітного шуму RIAS-1GM.

Переваги цього генератора включають:

• Генератор має вбудовану систему автоматичного керування функціями. Індикаторні світлові та звукові сигнали для керування функціями розташовані як на пульті дистанційного керування, так і на генераторі. Генератор можна розмістити на робочому місці користувача або в центрі управління. Панель керування також підтримує дистанційне керування вмиканням/вимиканням генератора;

Таблиця 3.6

Генератори·електромагнітного·шуму¶

Характеристики¤	Салют·2000·Б¤	Гном-3¤	Старкад-32¤	PIAC-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 5 Вт;

• Коефіцієнт спектральної кореляції не менше 2,0;

• Цей генератор включено до переліку загального обладнання для забезпечення захисту інформаційних технологій, розробленого Державною

службою спеціального зв'язку України, а вимоги до його захисту визначаються законодавством України. [31]

Вибір системи охоронної сигналізації

Система охоронної сигналізації призначена для виявлення вторгнення (або спроби вторгнення) на об'єкт, що охороняється, та забезпечення обробки, збору, відображення та передачі інформації про вторгнення (або спробу вторгнення). (Рисунок 3.6) [22, 23, 36]

Рис.3.6 Системи охоронної сигналізації

Виходячи з вищезазначених характеристик та враховуючи переваги системи охоронної сигналізації Tecsar Alert Ward, ми рекомендуємо використовувати її в нашій системі:

• Низька вартість;

• Вбудована сигналізація, яка надсилає повідомлення на контрольну панель у разі спроби крадіжки зі зломом;

• Простота використання та встановлення;

• Керування через мобільний додаток. [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 перевіреного обладнання, на вікна приміщень, що підлягають захисту, необхідно нанести металізовані захисні плівки. Завдяки наявності металевих включень у своїй багатошаровій структурі, ця захисна плівка виключає можливість витоку інформації через вібраційно-акустичні та електромагнітні канали. У нашій системі захисту ми використовуватимемо захисну плівку Ultra Vision R Silver (рисунок 3.7) [37].

Властивості плівки Ultra Vision R Silver наведено в таблиці 3.8.

У приміщеннях з обмеженим доступом ще одним необхідним захисним заходом є встановлення ізоляційних гільз на нагрівальні елементи (радіатори). Ізоляційні гільзи – це непровідні вставки, що встановлюються на роз'ємних з'єднаннях компонентів труб. Основною функцією ізоляційних гільз є запобігання блукаючим струмам.

Таблиця 3.8

Характеристики плівки Ultra Vision R Silver

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

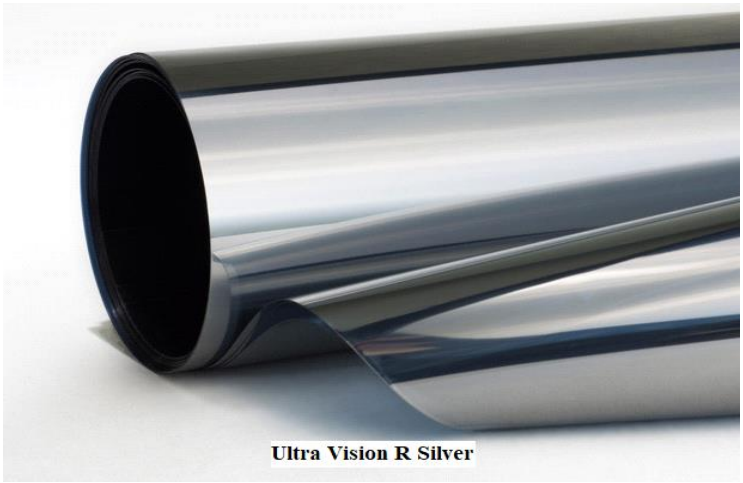


Рис.3.7 Захисна металізована плівка

Для забезпечення найвищого рівня звукоізоляції приміщення буде звукоізольоване. Звукоізоляційним матеріалом будуть пірамідальні звукопоглинальні панелі ECOSOUND PYRAMID GAIN BLACK, унікальна текстура поверхні яких забезпечує їм ширший діапазон звукопоглинання, ніж у аналогічних продуктів, що дозволяє їм краще поглинати звукові хвилі в пористу структуру звукопоглинальної піни. Ці панелі надзвичайно легко

встановлювати та транспортувати, а завдяки еластичності матеріалу вони нелегко пошкоджуються механічними засобами [17,38].

Розрахуємо кількість звукопоглинальних панелей, необхідних для звукоізоляції [17,38]:

Висота стелі = 2,7 метра

Довжина кімнати = 5 метрів

Площа кімнати = 13,5 квадратних метрів

Ширина кімнати = 2,7 метра

Отже, площа бічної стіни: 2 × (5 метрів × 2,7 метра) + 2 × (2,7 метра × 2,7 метра) = 41,58 квадратних метрів; площа підлоги та площа стелі: 2 × (5 метрів × 2,7 метра) = 27 квадратних метрів;

Загальна площа кімнати: 41,58 квадратних метрів + 27 квадратних метрів ≈ 69 квадратних метрів

3.5 Висновки по розділу

1. Розроблено рекомендації щодо організації фізичного захисту об'єктів інформаційної діяльності. Було продемонстровано, що використання автономного механічного, електричного та електронного обладнання та систем запобігає діяльності зовнішнього впливу, спрямованій на отримання конфіденційної інформації.

2. Розроблено рекомендації щодо процедур впровадження заходів технічного захисту об'єктів інформаційної діяльності. Ці рекомендації включають технічний захист, апаратний захист інформації, захист мережі та захист програмного забезпечення. Запропоновано кілька заходів технічної підтримки для забезпечення належної роботи та ефективного використання заходів технічного захисту.

3. Розроблено рекомендації щодо розробки та впровадження систем контролю та управління доступом. Продемонстровано склад систем контролю та управління доступом та їх інтеграцію з іншими системами та мережами технічного захисту.

4. Розроблено систему кіберфізичного захисту об'єктів інформаційної діяльності. Визначено склад обладнання та продемонстровано його вибір.

ВИСНОВКИ

Під час підготовки до кваліфікаційної роботи було виконано такі завдання:

– Проаналізовано основні загрози несанкціонованого доступу до конфіденційної інформації через технічні канали передачі даних критичної інфраструктури.

– Досліджено напрямки вдосконалення систем управління доступом до критичної інфраструктури.

– Розроблено систему управління доступом до критичної інфраструктури.

1. У першій частині кваліфікаційної роботи проаналізовано основні загрози несанкціонованого доступу до конфіденційної інформації через технічні канали передачі даних критичної інфраструктури. Представлено класифікацію та структурування корисних наборів даних у критичній інфраструктурі. Визначено технічні канали та загрози витоку інформації у критичній інфраструктурі.

2. У другій частині кваліфікаційної роботи представлено результати дослідження напрямків вдосконалення систем управління доступом до критичної інфраструктури: У цій роботі представлено результати аналізу функціональності та вимог до виконавчих механізмів системи управління контролем доступу до об'єктів критичної інфраструктури.

3. У третій частині кваліфікаційної роботи представлено систему контролю доступу до об'єктів критичної інфраструктури.

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. Про електронні документи та електронний документообіг: закон України від 22 травня 2003 р. № 851-IV // Урядовий кур'єр — 2003. — №119 – 2 липня. – С. 1– 6.

12. Сарбуков А. Аутентификация В Компьютерных Системах / А. Сарбуков А. Грушо // Системы безопасности. – 2003. - №5 (53). – С. 25-29.

13. Чепиков О. Особенности применения Двухфактор-Ной аутентификации / О. Чепиков // Информационная безопасность. – 2005. – №3. – С.35-41.

14. Конахович Г.Ф., Корченко О.Г., Юдін О.К., Захист інформації в мережах передачі даних: Підручник. – К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714с., іл.

15. Шрамко В. Н. Защита компьютеров: электронные Системы идентификации и аутентификации / В. Н. Шрамко // PCWeek/RE. – 2004. - №12.

16. ГОСТ Р ИСО/МЭК 19794-6-2006. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. – Ч. 6: Данные изображения радужной оболочки глаза. – М.: ИПК Изд-во стандартов, 2006. – 27 с.

17. Горбенко И. Д. Методы биометрической аутентификации для использования в паспортной системе / И. Д. Горбенко, И. В. Олешко // Прикладная радиоэлектроника: научно-техн. журнал. – 2011. – Том 10, № 2. – С. 255 – 258.

18. Олешко І. В. Порівняльний аналіз методів біометричної автентифікації на основі критерію відносної ентропії / І. В. Олешко // Вісник національного університету “Львівська політехніка”. – 2012. – С. 170 – 175.

19. Горбенко Ю. И. Модели и методы оценки защищенности механизмов многофакторной аутентификации / Ю. И. Горбенко, И. В. Олешко // Восточно-европейский журнал передовых технологий: научный журнал. – 2012. – № 6/2(66). – С. 4 – 10.

20. Олешко И. В. Сравнительный анализ протоколов строгой аутентификации [Текст] / И. В. Олешко, И. Д. Горбенко // Радиотехника. – 2012. – №3 – С. 198 – 210.

21. Фесьоха В.В, Фесьоха Н.О., Доброштан О.С. Аналіз існуючих рішень автентифікації користувачів інформаційних систем та мереж спеціального призначення. Збірник наукових праць ВІТІ № 3 – 2020. С. 129-136.

22. Субач І.Ю., Фесьоха В.В., Фесьоха Н.О. Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі, відкритих на основі загальнодоступних ліцензій. Information Technology and Security. 2017. № 1. С. 29 – 41.

23. Горбенко Ю. И. Модели и методы оценки защищенности механизмов многофакторной аутентификации / Ю. И. Горбенко, И. В. Олешко // Восточно-европейский журнал передовых технологий: научный журнал. – 2012. – № 6/2(66). – С. 4 – 10.

24. Горбенко, І. Д. Прикладна криптологія. [Текст]: монографія / І. Д. Горбенко, Ю. І. Горбенко; ХНУРЕ. – Х.: Форт, 2012. - 868 с.

25. Горбенко, Ю. І. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика [Текст] / Ю. І. Горбенко, І. Д. Горбенко. – Х.: Форт, 2010. – 593 с.

26. Чепиков О. Особенности применения двухфакторной аутентификации / О. Чепиков // Информационная безопасность. – 2005. – №3. – С.35-41.

27. Кушлик-Дивульська О. І. Теорія ймовірностей та математична статистика: навч. посіб./ О. І. Кушлик-Дивульська, Н. В. Поліщук, Б. П. Орел, П. І. Штабалюк. – К: НТУУ «КПІ», 2014. – 212 с. − Бібліогр.: с.205. − 300пр.

28. Горбенко И. Д. Метод оценки относительной энтропии и сравнительный анализ источников биометрической информации [Текст] / И. Д. Горбенко, И. В. Олешко // Прикладная радиоэлектроника: Научно-техн. журнал. - 2012. - Том 11, № 2. - С. 255-261

29. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння [Текст]. – введ. 2002 - 28 - 12. - К.: Госпотребстандарт, 2002. – 38 с.

30. ДСТУ ISO/IEC 9798-3-2002 Інформаційні технології. Методи захисту. Автентифікація суб’єктів. Частина 3. Механізми з використанням методу цифрового підпису [Текст]. – введ. 2005 – 09 - 2005. - К.: Госпотребстандарт, 2005. – 17 с.

31. П. Браіловський М.М., Головень СМ. та інші. - Технічний захист інформації на об'єктах

ДОДАТОК А

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

Кваліфікаційна робота здобувача освітнього ступеня «МАГІСТР»

СИСТЕМИ САНКЦІОНОВАНОГО ДОСТУПУ ДО ТЕХНІЧНИХ КАНАЛІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ ОБ’ЄКТУ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

Спеціальність: 125 - Кібербезпека та захист інформації

Виконав: Юрій ЖЕРЕБОК

Керівник: Петро ПОНОЧОВНИЙ, доктор філософії

Київ - 2026

АКТУАЛЬНІСТЬ, МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

- Актуальність роботи визначається необхідністю захисту технічних каналів передачі інформації на об’єктах банківської діяльності та критичної інфраструктури.
- Мета роботи - підвищення ефективності функціонування системи захисту інформації та системи управління доступом на об’єкті критичної інфраструктури.
- Об’єкт дослідження - система захисту каналів передачі інформації на об’єкті критичної інфраструктури.
- Предмет дослідження - системи контролю та управління доступом до об’єкта критичної інфраструктури.
- Завдання: проаналізувати загрози НСД, дослідити напрями удосконалення СКУД, розробити рекомендації щодо фізичного і технічного захисту об’єкта.

СТРУКТУРА ТА ОСНОВНІ РЕЗУЛЬТАТИ РОБОТИ

- Розділ 1 - виконано аналіз інформації з обмеженим доступом, технічних каналів витоку та загроз несанкціонованого доступу.
- Розділ 2 - досліджено технології організації безпечного доступу та системи контролю і управління доступом.
- Розділ 3 - проведено передпроектне обстеження офісу, сформовано рекомендації щодо фізичного захисту та технічних засобів.
- Практичний результат - підібрано обладнання для СКУД, відеоспостереження, охоронної сигналізації, акустичного та електромагнітного захисту.
- Очікуваний ефект - зниження ризиків НСД, підвищення керованості доступу та посилення захисту інформації банківського об’єкта.

РЕЖИМ ДОСТУПУ ДО ІНФОРМАЦІЇ ТА ОБ’ЄКТ ЗАХИСТУ

- Інформація на об’єкті поділяється на відкриту інформацію та інформацію з обмеженим доступом.
- ІзОД включає конфіденційну та таємну інформацію, яка потребує встановленого режиму доступу.
- Для банківського об’єкта важливими є конфіденційність, цілісність і доступність інформаційних ресурсів.
- Система захисту повинна враховувати як інформаційні потоки, так і фізичний доступ до технічних каналів.

СТРУКТУРА ТЕХНІЧНОГО КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ

- Технічний канал витоку включає джерело небезпечного сигналу, середовище його поширення та засіб технічної розвідки.
- До загроз належать радіоканали, електричні, акустичні, оптичні та матеріально-речові сигнали.
- Кожне джерело небезпечного сигналу за певних умов може сформувати канал витоку інформації.
- Протидія таким каналам потребує комплексного поєднання організаційних, технічних і режимних заходів.

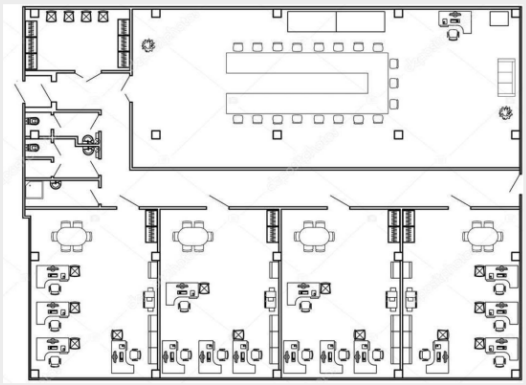
КЛАСИФІКАЦІЯ ЗАГРОЗ ТА КАНАЛІВ НЕСАНКЦІОНОВАНОГО ВИТОКУ

- Технічні канали витоку класифікуються за видом інформаційної діяльності, фізичним принципом формування небезпечного сигналу, середовищем поширення та способом перехоплення.
- До каналів мовної інформації належать акустичні, віброакустичні, акустооптичні, акустоелектричні та канали високочастотного нав’язування.
- Для ОТЗС характерні побічні електромагнітні випромінювання, наведення, паразитна модуляція та канали зняття інформації з ліній зв’язку.
- Загрози НСД мають розглядатися з урахуванням фізичного проникнення, порушення режиму доступу та використання технічних засобів розвідки.

СИСТЕМИ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ

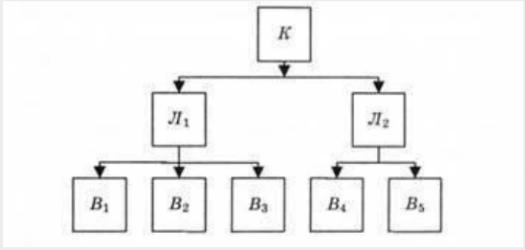
- СКУД застосовується для контролю входів, виходів, зон зберігання ІзОД, паркувальних зон та службових приміщень.
- Основні функції: ідентифікація користувача, перевірка прав доступу, керування виконавчим пристроєм, реєстрація подій і формування звітності.
- Автономні системи мають нижчу вартість і простіше встановлення, але обмежені у масштабуванні та моніторингу подій.
- Мережеві та централізовані системи забезпечують управління в реальному часі, інтеграцію з відеоспостереженням, охоронною і пожежною сигналізацією.

ПЕРЕДПРОЕКТНЕ ОБСТЕЖЕННЯ ОБ’ЄКТА БАНКІВСЬКОЇ ДІЯЛЬНОСТІ



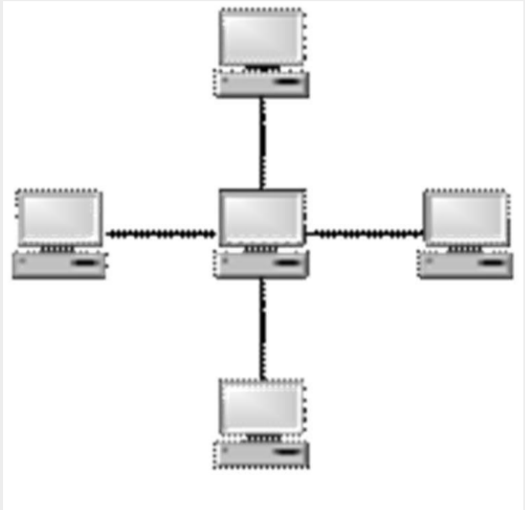
- Передпроектне обстеження визначає планування приміщень, контрольовані зони, робочі місця та маршрути переміщення персоналу.
- Окремо виділяються приміщення з обмеженим доступом, серверні, робочі кабінети та точки входу/виходу.
- Планування є основою для вибору місць встановлення камер, зчитувачів, турнікетів, датчиків і засобів технічного захисту.
- Проект СКУД має забезпечити баланс між безпекою, зручністю доступу та вимогами до режиму роботи об’єкта.

СТРУКТУРА УПРАВЛІННЯ ТА ОРГАНІЗАЦІЯ ДОСТУПУ



- Лінійна структура управління дозволяє чітко визначити відповідальних осіб, виконавців та порядок прийняття рішень щодо доступу.
- Права доступу до зон об’єкта доцільно призначати відповідно до посадових ролей та службових повноважень.
- Усі події входу, виходу, відмови у доступі та аварійного відкривання повинні фіксуватися у журналі подій.
- Організаційна модель доповнює технічні рішення і зменшує вплив людського фактора.

МЕРЕЖЕВА ТОПОЛОГІЯ ТА ІНФРАСТРУКТУРА ЗАХИСТУ



- Для підключення технічних засобів захисту може застосовуватися зіркова мережева топологія.
- Центральний вузол забезпечує керування трафіком, підключення робочих станцій, камер, контролерів та серверних ресурсів.
- Така архітектура спрощує адміністрування, локалізацію відмов і контроль доступу до інформаційних ресурсів.
- Для підвищення надійності доцільно передбачити резервування живлення, резервні канали зв’язку та моніторинг стану обладнання.

АНАЛІЗ РИЗИКІВ І НАПРЯМИ 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, приймання підмикання, електромагнітний датчик, диктофон, телефонна закладка	Маскування, скремблювання, шифрування, спецтехніка
	Наведення	Спеціальні радіотехнічні пристрої	Спецтехніка
– радіотелефону	ВЧ-сигнал	Радіоприймачі	Маскування, скремблювання, шифрування, спецтехніка
Дії з документом на паперовому носії:	Безпосередньо сам документ	Крадіжка, прочитування, копіювання, фотографування	Обмеження доступу, спецтехніка
	Продавлення стрічки або папіру	Крадіжка, прочитування	Оргтехзаходи
– виготовлення	Акустичний шум принтера	Апаратура акустичного контролю	Пристрої шумозаглушування
	Паразитні сигнали, наведення	Спеціальні радіотехнічні засоби	Екранування
– поштове відправлення	Безпосередньо сам документ	Крадіжка, прочитування	Спеціальні методи
Документ на машинному носії:	Носій	Крадіжка, копіювання, прочитування	Контроль доступу, фізичний захист, криптозахист
– виготовлення	Відображення на дисплеї	Візуальний, копіювання, фотографування	Контроль доступу, фізичний захист, криптозахист
	Паразитні сигнали, наведення	Спеціальні радіотехнічні пристрої	Контроль доступу, криптозахист, пошук закладок, екранування
	Електричні та оптичні сигнали	Апаратні закладки	
	Програмний продукт	Програмні закладки	
– передавання документа по каналах зв'язку	Електричні та оптичні сигнали	Несанкціоноване підмикання, імітація зареєстрованого користувача	Криптозахист
Виробничий процес	Відходи, випромінювання тощо	Спецапаратура різного призначення	Оргтехзаходи, фізичний захист

- Оцінка ризиків дозволяє визначити найбільш критичні сценарії НСД та витоку інформації.
- До пріоритетних заходів належать контроль доступу до приміщень, відеоспостереження, охоронна сигналізація, акустичне та електромагнітне зашумлення.
- Ризики слід оцінювати з урахуванням ймовірності реалізації загрози та можливого впливу на конфіденційність, цілісність і доступність.
- Результати аналізу використовуються для обґрунтування вибору конкретних технічних засобів.

СИСТЕМА ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ОБ’ЄКТА

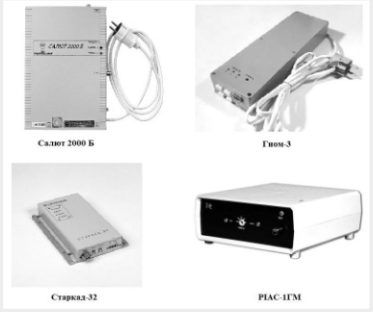
- Для контролю периметра, входів, коридорів і зон зберігання ІзОД запропоновано застосування IP-камер.
- Під час вибору камер враховуються роздільна здатність, кут огляду, дальність виявлення, підтримка інфрачервоного підсвічування та стійкість до умов експлуатації.
- Відеоспостереження підвищує доказовість подій, підтримує розслідування інцидентів та інтегрується з СКУД.
- Камери мають розміщуватися так, щоб мінімізувати сліпі зони та забезпечити контроль критичних точок доступу.

ЕЛЕМЕНТИ СКУД ТА ОБҐРУНТУВАННЯ ВИБОРУ ОБЛАДНАННЯ

- До складу СКУД входять ідентифікатори, зчитувачі, контролери, виконавчі пристрої, програмне забезпечення та база даних користувачів.
- У роботі розглянуто термінали доступу та пристрої, що підтримують картки, біометричну ідентифікацію та реєстрацію подій.
- Виконавчі пристрої повинні забезпечувати надійне блокування точки доступу і коректне розблокування при підтвердженні прав.
- Важливо враховувати кількість користувачів, журнал подій, інтерфейси підключення та можливість інтеграції з іншими системами безпеки.

ЗАСОБИ АКУСТИЧНОГО ТА ЕЛЕКТРОМАГНІТНОГО ЗАХИСТУ

- Генератори акустичного шуму застосовуються для маскування мовної інформації та зниження ризику її перехоплення акустичними каналами.
- Генератори електромагнітного шуму використовуються для протидії побічним електромагнітним випромінюванням і наведенням.
- Вибір засобів зашумлення має враховувати діапазон частот, рівень шуму, кількість каналів, зону покриття та сертифікаційні вимоги.
- Такі засоби доцільно розміщувати у приміщеннях, де обробляється інформація з обмеженим доступом.



- Охоронна сигналізація забезпечує виявлення несанкціонованого проникнення, контроль датчиків та оперативне оповіщення відповідальних осіб.
- Захисна плівка для вікон підвищує стійкість конструкцій до фізичного впливу та ускладнює проникнення у приміщення.
- Ізоляційні вставки, захисні плівки, сигналізація та СКУД формують багаторівневу систему фізичного захисту.
- Комплексне застосування цих рішень зменшує ймовірність витоку інформації через організаційні, технічні та фізичні вразливості.

ДЯКУЮ ЗА УВАГУ!

Доповідь підготував здобувач вищої освіти Юрій ЖЕРЕБОК

Тема: «Системи санкціонованого доступу до технічних каналів передачі інформації»

Київ - 2026