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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Удосконалення системи передачі даних бездротовими каналами об'єкту інформаційної 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
_____ Владислав АВРАМЕНКО

Виконав: здобувач вищої освіти групи СЗДМ 61
Владислав АВРАМЕНКО

Керівник: САВЧЕНКО Віталій
д.т.н., професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____ _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2025

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

Кафедра Технічних систем кіберзахисту
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

АВРАМЕНКУ Владиславу Олександровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: «Удосконалення системи передачі даних бездротовими каналами об'єкту інформаційної діяльності»

керівник кваліфікаційної роботи: Савченко В. А., д.т.н, професор

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

2. Вихідні дані до кваліфікаційної роботи:
Стандарти, міжнародні стандарти;
Наукова та технічна література, корпоративна документація;

3. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Проаналізувати основні характеристики засобів безпеки, технічних та програмних, їх взаємодію та ефективність
2. Дослідити особливості програмного забезпечення, уразливих та слабких сторін.
3. Визначити напрями та методи забезпечення інформаційної безпеки підприємства

6. Дата видачі завдання _____20.10.2024 ___ _____

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів Кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	15.10.2024	
2.	Збір та аналіз літератури.	03.11.2024	
3.	Аналіз основних характеристик каналів витоку інформації	15.11.2024	
4.	Дослідження методів та засобів запобігання витоку інформації	20.11.2024	
5.	Виконання практичного завдання	10.12.2024	
6.	Оформлення роботи і презентації	25.12.2024	
7.	Захист в ЕК	21.01.2025	
8.			

Здобувач вищої освіти _____ Владислав АВРАМЕНКО
(підпис) *(ім’я, прізвище)*

Керівник кваліфікаційної роботи _____ Віталій САВЧЕНКО
(підпис) *(ім’я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 85 стор., 14 рис., 0 табл., 23 дж.

Технології захисту інформації в бездротовому середовищі запобігають розповсюдженню та забезпечують безпеку інформації. Поєднання технічних та програмних засобів надає повноцінний захист від загроз проникнення в систему ззовні та небажаного витоку інформації. Використання таких програмних інструментів як VPN, IPsec, SSL, GRE та технічних: пристрої екранування апаратури, ліній зв'язку та приміщень, пристрої ідентифікації і фіксації терміналів суттєво покращують рівень безпеки.

У дослідженні розглянуто проблеми внутрішнього та зовнішнього захисту інформаційної системи, чинника, які впливають на його ефективність.

На основі дослідження наведено кроки для покращення безпеки, рекомендації стосовно підтримки безпеки та недопущення небажаної активності

Об'єкт дослідження - бездротові канали передачі даних.

Предмет дослідження – методи та засоби захисту інфомації в процесі передавання.

Мета роботи – розробити правила захисту мережі в бездротовому середовищі

Метод дослідження – аналітичний із використанням комп'ютерних технологій.

Апробація:

В.О. Авраменко, Удосконалення системи передачі даних бездротовими каналами об'єкту інформаційної діяльності. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.49-50. https://duikt.edu.ua/uploads/p_2661_93669247.pdf

Галузь використання – безпека інформації та її підтримка на підприємстві.

КЛЮЧОВІ СЛОВА: КАНАЛ ВИТОКУ ІНФОРМАЦІЇ, ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ, ПРОГРАМИ, БЕЗДРОТОВІ МЕРЕЖІ.

ABSTRACT

Text part of the qualification work for obtaining a master's degree: 85 pp., 14 fig., 0 tables, 23 sources.

The object of the study is wireless data transmission channels.

The subject of the study is methods and means of protecting information during transmission.

The purpose of the work is to develop rules for protecting the network in a wireless environment

The research method is analytical using computer technologies.

Information protection technologies in a wireless environment prevent the spread and ensure information security. The combination of technical and software tools provides full protection against threats of penetration into the system from the outside and unwanted information leakage. The use of such software tools as VPN, IPsec, SSL and technical ones: devices for shielding equipment, communication lines and premises, devices for identifying and fixing terminals significantly improve the level of security.

The study considers the problems of internal and external protection of the information system, factors that affect its effectiveness.

Based on the study, steps are given to improve security, recommendations for maintaining security and preventing unwanted activity.

Approbation:

V.O. Avramenko, Improvement of the data transmission system via wireless channels of the object of information activity. All-Ukrainian scientific and practical conference: Current problems of security of information and telecommunication systems. Kyiv, November 3, 2024, Kyiv: RVC DUIKT. – 024. P.49-50. https://duikt.edu.ua/uploads/p_2661_93669247.pdf

Field of use – information security and its support at the enterprise.

KEYWORDS: INFORMATION OUTPUT CHANNEL, TECHNICAL INFORMATION OUTPUT CHANNELS, PROGRAMS, WIRELESS NETWORKS.

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 6

ВСТУП 7

1 АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ У БЕЗДРОТОВИХ КАНАЛАХ 8

1.1. Технічні канали витоку інформації 8

1.2. Радіоканал 15

1.3. Поняття інформації та захисту 16

1.4. Рівні безпеки 20

1.5. Концепція і методи технічного захисту інформації 34

2 ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ЗАХИСТУ БЕЗДРОТОВИХ КАНАЛІВ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ 37

2.1. Програмний захист 37

2.2. Апаратний захист 41

3 РОЗРОБКА ТЕХНОЛОГІЇ ЗАХИСТУ БЕЗДРОТОВИХ КАНАЛІВ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ 58

3.1. Розробка схеми корпоративної мережі для дослідження технологій захисту бездротових каналів 58

3.2. Обґрунтування параметрів налаштувань програмних та технічних пристроїв захисту. 59

3.3. Розробка рекомендацій щодо підвищення захищеності системи передачі даних бездротовими каналами на об'єкті інформаційної діяльності 70

ВИСНОВКИ 73

ПЕРЕЛІК ПОСИЛАНЬ ..... Ошибка! Закладка не определена.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SSL – рівень захищених сокетів

ACL – Access control list

SSH – Secure shell

VPN -Virtual Privat Network

WiFi – Wireless Fidelity

IPsec – IP security – безпека ip

ВСТУП

Актуальність дослідження. Швидкий розвиток інформаційних технологій і поширення бездротових мереж роблять питання захисту переданих даних надзвичайно важливим. Обсяги конфіденційної інформації, що циркулюють у таких мережах, постійно зростають, підвищуючи ризики, пов'язані з несанкціонованим доступом, викраденням даних та кібератаками, які можуть призвести до значних фінансових втрат і пошкодження репутації.

Для мінімізації цих ризиків необхідно розробляти та вдосконалювати сучасні методи захисту даних у бездротових мережах. Це особливо актуально з урахуванням міжнародних стандартів безпеки, які передбачають забезпечення конфіденційності, цілісності та доступності інформації.

Такі технології, як VPN, IPsec, SSL, шифрування та ідентифікація користувачів, є важливими інструментами для захисту даних. Однак постійний розвиток кіберзагроз вимагає удосконалення існуючих методів і розробки нових рішень.

Об’єкт дослідження - бездротові канали передачі даних.

Предмет дослідження – методи та засоби захисту інфомації в процесі передавання.

Мета роботи – розробити правила захисту мережі в бездротовому середовищі

Наукові завдання:

дослідження бездротових каналів передачі даних;

аналіз засобів безпеки інформації, яка передається даними каналами;

розробка технологій захисту каналів передачі даних на підприємстві.

Методи дослідження – ознайомлення з літературою, аналіз джерел.

Практичне значення одержаних результатів: наведено кроки для покращення безпеки, рекомендації стосовно підтримки безпеки та недопущення небажаної активності.

РОЗДІЛ 1.
АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ У БЕЗДРОТОВИХ КАНАЛАХ

1.1. Технічні канали витоку інформації

Витік інформації – це неконтрольоване розповсюдження даних, яке стає причиною їх несанкціонованого отримання.

Витік інформації здійснюється через відповідний канал. Оскільки засоби розвідки противника зазвичай мають технічний характер, канали витоку також називають технічними [1].

Також беруть до уваги завади, що впливають на вхід технічного засобу розвідки.

Канал витоку інформації – це фізичний шлях небезпечного сигналу (носія інформації) від джерела конфіденційних даних до зловмисника, через який той може отримати доступ до захищених відомостей. Канал витоку інформації також включає потенційні напрямки несанкціонованого доступу, зумовлені архітектурою, технологічними схемами роботи електронно-обчислювальної техніки, а також недотриманням організаційно-режимних заходів.

Небезпечний сигнал – це сигнал (поле), зокрема паразитний (побічний), або його компоненти (фрагменти) будь-якого фізичного походження, що містять інформацію з обмеженим доступом і можуть бути перехоплені засобами технічної розвідки [2].

Носій інформації – небезпечний сигнал чи хімічна речовина, які містять інформацію з обмеженим доступом.

Носієм інформації можуть бути:

- електричний струм;
- електромагнітне поле;
- світло (електромагнітне поле в світловому діапазоні частот);

– лазерний промінь (електромагнітне поле в оптоелектронному діапазоні частот);

– акустичне поле;

– вібраційне поле;

– хімічні матеріали, речовини тощо;

– інші носії [3].

Середовище поширення небезпечного сигналу включає повітряні, водні та інші фізичні середовища; хімічні речовини; струмопровідні та пружні матеріали, лінії електроживлення, зв'язку, сигналізації, управління, спостереження; кінцеве та з'єднувальне обладнання; інженерні комунікації й споруди, огороджувальні будівельні конструкції, а також світлопроникні елементи будинків і споруд.

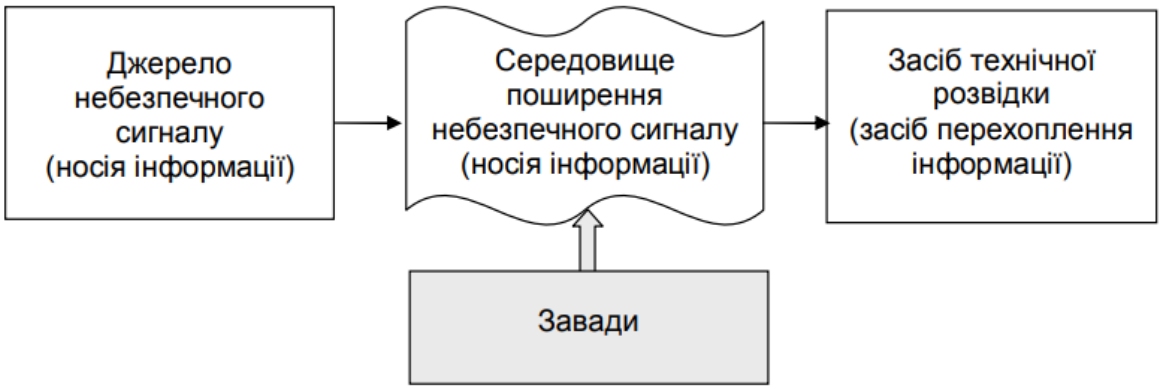


Рис. 1.1 – Технічний канал витоку інформації

Основними джерелами утворення ТКВІ(рис.1.1):

• перетворювачі фізичних величин;

• випромінювачі електромагнітних коливань;

• паразитні зв'язки і наведення на провідники і елементи електронних пристроїв.

Рис. 1.2 - Класифікація джерел утворення каналів втрати інформації

Причини виникнення електричних каналів витоку інформації**:**

1. Гальванічні з'єднання між з'єднувальними лініями ТЗПІ (технічні засоби перетворення інформації), лініями ВТСС (допоміжні технічні системи, засоби) та сторонніми провідниками;

2. Наведення побічних електричних випромінювань ТЗПІ на з'єднувальні ліній ВТСС і сторонні провідники;

3. Наведення побічних електричних випромінювань ТЗПІ на ланцюзі електроживлення і заземлення ТЗПІ;

4. «Просочування» інформаційних сигналів у колі електроживлення і заземлення ТЗПІ [4].

Одним із видів технічних каналів витоку інформації, що виникають під час

експлуатації засобів і систем інформатизації (електронно-обчислювальна, телевізійна та інша техніка), є канали, що формуються через побічні електромагнітні випромінювання та наведення. До найбільш поширених каналів витоку інформації внаслідок наведень належать канали, що утворюються в мережі електроживлення технічних засобів і систем. Розроблений до сьогодні арсенал заходів і засобів блокування каналів витоку інформації через випромінювання відзначається конкретністю та повнотою [5]. Водночас, методи та інструменти захисту інформації від витоку через наведення, зокрема в мережах електроживлення, не характеризуються різноманіттям. Їх впровадження часто пов'язане з надмірним запасом захищеності та призводить до невиправдано високих фінансових витрат.

Схеми електропостачання технічних засобів і систем інформатизації

Дослідження схем електроживлення технічних засобів і систем (ТСС) інформатизації на різних об'єктах підприємств та організацій свідчить, що живлення цих ТСС, як правило, здійснюється від трансформаторних підстанцій ТП 6-10 / 0,4 кВ за радіальною схемою. Нагадаємо, що радіальна схема передбачає живлення кожного окремого споживача або групи споживачів по окремій лінії від відповідного комутаційного вузла [6].

Таким чином, в залежності від кількості проміжних ланок між трансформаторною підстанцією ТП 6-10 / 0,4 кВ та споживачами, радіальна схема електропостачання може бути:

- **одноступеневою**, коли електроенергія подається на РЩ (розподільчий щит) безпосередньо з ТП;
- **двоступеневою**, якщо між ТП та РЩ встановлено один проміжний розподільний пункт (ПРП 1);
- **триступеневою**, при наявності двох послідовно з'єднаних проміжних розподільних пунктів (ПРП 1 та ПРП 2).

Слід зазначити, що сама трансформаторна підстанція (ТП) отримує живлення від центрального розподільного пункту (ЦРП) або головної знижувальної підстанції (ГЗП).

Одноступінчата і двоступенева схеми електропостачання ТСС інформатизації наведені на рис. 1.3.

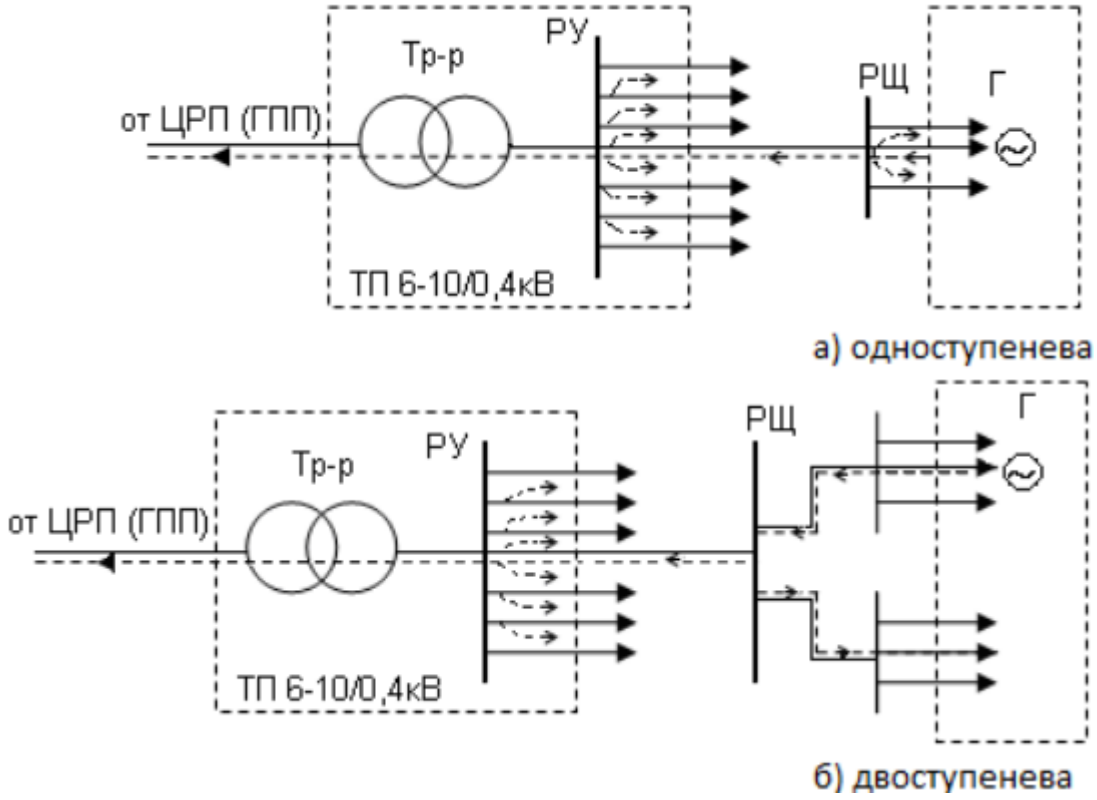


Рис. 1.3 - Одноступінчата і двоступенева схеми електропостачання ТСС

Отже, межі контрольованої зони на об'єктах, де функціонують ТСС інформатизації, можуть суттєво відрізнятись. В одних випадках під контролем знаходиться весь шлях електроенергії від ЦРП (або ГЗП) до самих ТСС, в інших - лише ділянка від трансформаторної підстанції ТП 6-10 / 0,4 кВ.

Можливі ситуації, коли не лише розподільні пристрої, а й самі трансформаторні підстанції ТП 6-10 / 0,4 кВ, що забезпечують електроживлення ТСС інформатизації, виявляються поза межами контрольованої території. При цьому, як вже зазначалось, досить часто від ТП або розподільних пристроїв, окрім ТСС інформатизації, живляться й інші споживачі, розташовані за кордоном контрольованої зони [7].

Рекомендації щодо захисту інформації, що обробляється технічними засобами і системами інформатизації, від витоку за рахунок наведень в

мережу їх електроживлення

Захист інформації від витоку через наведення в мережу електроживлення ТСС інформатизації, як правило, ґрунтується на наступних принципах:

1. **Фізичне виключення** окремих шляхів розповсюдження інформативних сигналів. Це може досягатись, наприклад, шляхом гальванічної розв'язки, екранування, фільтрації.
2. **Маскування** інформативного сигналу за допомогою спеціально створеної шумової завади.
3. **Зниження** рівня інформативного сигналу в тракті його розповсюдження до величин, що унеможливлюють його перехоплення та декодування.

Застосування цих принципів на практиці реалізується через комплекс організаційних та технічних заходів, спрямованих на забезпечення інформаційної безпеки ТСС [8].

Що стосується заходів захисту, які базуються на принципі фізичного усунення шляхів розповсюдження інформативних сигналів, то деякі з них вже були розглянуті раніше. Зокрема, йшлося про необхідність виключення з ланцюгів електропостачання ТСС інформатизації сторонніх споживачів, які живляться від тієї ж трансформаторної підстанції ТП 6-10 / 0,4 кВ.

Рекомендації, що представляють собою заходи захисту, в основу яких покладено третій принцип.

1. При проведенні робіт із захисту інформації від витоку за рахунок наведень в мережі електроживлення ТСС інформатизації необхідно мати на увазі наступне:

- Слід зазначити, що з ростом частоти інформативних сигналів, наведених в мережу електроживлення ТСС інформатизації, їх перехоплення, як правило, ускладнюється внаслідок збільшення загасання в трактах розповсюдження. Проте, існують смуги частот, де частотні характеристики загасання мають провали, що може сприяти перехопленню. З іншого боку, збільшення частоти призводить до зниження рівнів шумів, що покращує співвідношення сигнал/шум і, відповідно, полегшує перехоплення [9].

- Для підвищення ефективності захисту інформації можна збільшити ослаблення інформативних сигналів, наведених в мережу електроживлення ТСС інформатизації. Це досягається за рахунок збільшення власного загасання елементів трактів розповсюдження та їх хвильової неузгодженості в діапазонах частот наведених сигналів (при цьому узгодження на частоті 50 Гц повинно зберігатись).

2. З метою збільшення ослаблення рівнів інформативних сигналів в мережах електроживлення ТСС інформатизації застосовувати розділові трансформатори, завадоподавляющі фільтри, джерела безперебійного живлення. При цьому в обов'язковому порядку враховувати, що практично кожне із зазначених технічних засобів ефективно з точки зору придушення наведених інформативних сигналів лише в певних смугах частот, часто не збігаються з діапазонами частот таких сигналів.

3. При побудові систем електроживлення ТСС інформатизації доцільно використовувати трифазні силові трансформатори мінімально можливої потужності. Це ж стосується і розділових трансформаторів — їх потужність також має бути мінімально необхідною [10].

4. При наявності можливості вибору ланцюгів електроживлення ТСС інформатизації слід віддавати перевагу тим, які містять максимальну кількість елементів (кабелів, трансформаторів тощо) на ділянці від ТСС до межі контрольованої зони. При цьому довжина силових кабелів в межах контрольованої зони має бути максимально можливою.

Такий підхід дозволяє збільшити загальне загасання інформативних сигналів в ланцюгах електроживлення і, як наслідок, знизити ймовірність їх перехоплення.

Типи технічних каналів витоку інформації

Окрім безпосереднього випромінювання інформативних сигналів у простір, технічні засоби та системи здатні виконувати роль приймачів акустичних та електромагнітних випромінювань завдяки наявності мікрофонних ефектів та антенних властивостей. Прийняті сигнали можуть бути перетворені в

електричні та передані по лініях зв'язку, що, зазвичай, не контролюються, за межі об'єкта на значні відстані. Технічні канали витоку інформації класифікують за типом фізичного процесу, що лежить в основі передачі інформації. Розрізняють такі типи каналів:

- **радіоканали**, де носієм інформації є електромагнітні хвилі радіодіапазону;
- **акустичні канали**, що використовують звукові коливання в різних середовищах;
- **електричні канали**, де інформація передається за допомогою електричних сигналів в провідниках;
- **оптичні канали**, в яких задіяно електромагнітне випромінювання оптичного діапазону (інфрачервоне, видиме, ультрафіолетове);
- **матеріально-речові канали**, де носіями інформації є фізичні об'єкти (документи, фотографії, магнітні носії тощо) [11].

В даній роботі розглянемо детальніше радіоканал.

1.2. Радіоканал

У радіоелектронному каналі передачі інформація поширюється за допомогою електричного струму та електромагнітного поля в широкому діапазоні частот — від звукових до десятків ГГц. Серед технічних каналів витоку інформації радіоелектронний канал виділяється своєю високою інформативністю. Це обумовлено низкою факторів:

- стабільність роботи: канал функціонує незалежно від часу доби та пори року, а його параметри мало залежать від погодних умов;
- висока достовірність інформації: особливо при перехопленні даних з функціональних каналів зв'язку (якщо не враховувати можливість дезінформації);
- великий обсяг інформації: канал дозволяє отримувати значні обсяги даних;
- оперативність: інформація може бути отримана в режимі реального часу;
- скритність: перехоплення сигналів та радіо-теплові спостереження можуть

здійснюватись непомітно.

Причини утворення радіоканалів витоку інформації:

- недосконаліть елементної бази технічних засобів;
- помилки при проектуванні схем та виробів;
- зношування та старіння обладнання;
- злочинні дії (навмисне створення умов для витоку інформації, блокування засобів захисту, зміна характеристик обладнання).

Утворенню каналів РМ повинні сприяти визначені просторово почасові й енергетичні умови, а також відповідні засоби сприйняття і фіксації інформації, як з боку зловмисника, так і з позиції можливого РМ.

Джерелами сигналів в таких каналах можуть бути:

- передавачі функціональних каналів зв'язку;
- джерела небезпечних сигналів;
- об'єкти, що відображають радіочастотну енергію;
- об'єкти, які генерують власне (теплове) радіовипромінювання.

Поширення сигналів в радіоелектронному каналі відбувається через атмосферу, безповітряний простір, а також по направляючих системах — електричних дротах різних типів та хвилеводах [12].

Для передачі хвиль різної природи (електромагнітних, звукових тощо) використовуються спеціальні структури — хвилеводи, в яких хвиля обмежена в одному або двох вимірах за рахунок повного внутрішнього відбиття на межі. Інформаційне повідомлення, представлене у вигляді електричного струму, передається по дротах, а електромагнітне поле — в атмосфері, безповітряному просторі або по хвилеводах. Приймач забезпечує селекцію (виділення) потрібного сигналу за частотою, його посилення та демодуляцію — зчитування інформації.

1.3. Поняття інформації та захисту

В сучасному науковому дискурсі прийнято розрізняти два типи інформації.

По-перше, це об'єктивна інформація, яка являє собою властивості матеріальних об'єктів та явищ, що передаються іншим об'єктам і відображаються в їх структурі.

По-друге, суб'єктивна інформація, що формується свідомістю людини на основі об'єктивної інформації. Вона відображає зміст об'єктивної інформації за допомогою слів, образів, відчуттів і фіксується на матеріальних носіях.

У повсякденному житті під інформацією ми розуміємо будь-які відомості про навколишній світ та явища, що відбуваються в ньому. Ці відомості можуть сприйматись як людиною, так і спеціальними пристроями. Однак, для розгляду питань захисту інформації більш придатними є наукові визначення. Наприклад, Клод Шеннон визначав інформацію як знання, що усувають невизначеність. Тобто, отримуючи інформацію, ми зменшуємо рівень невідомого. Інший підхід пропонував В.М. Глушков, який розглядав інформацію як міру неоднорідності розподілу матерії та енергії у просторі та часі. Згідно з цим визначенням, інформація пов'язана з будь-якими змінами в світі. Розглядаючи поняття "інформація", варто звернути увагу на його трактування різними організаціями та нормативними документами. Так, ЮНЕСКО визначає інформацію як універсальну субстанцію, що пронизує всі сфери діяльності людини. Інформація є носієм знань, думок, забезпечує спілкування, взаєморозуміння та співпрацю, формує стереотипи мислення та поведінки. В Законі України "Про інформацію" дається вужче визначення: інформація — це документовані або публічно оголошені відомості про події та явища в суспільстві, державі та природі. Незалежно від конкретного визначення, інформація володіє певними властивостями, які визначають її сутність та роль в житті суспільства.

З практичної точки зору найбільш важливими є цінність, що визначається тим, наскільки інформація сприяє досягненню мети, поставленої перед її отримувачем; достовірність, яка відображає ступінь відповідності інформації реальному стану речей та актуальність, що характеризує відповідність інформації поточному моменту часу з урахуванням її цінності та достовірності.

Крім перерахованих, існують й інші властивості інформації, які можуть

бути важливими в різних контекстах, наприклад, часові характеристики (час створення, час зберігання тощо).

Розглядаючи властивості інформації з точки зору її захисту, необхідно виділити ті, які потребують захисту в першу чергу. До них належать:

- конфіденційність: забезпечує захист інформації від доступу несанкціонованих осіб;
- цілісність: гарантує неможливість несанкціонованої зміни або знищення інформації;
- доступність: захищає інформацію від несанкціонованого блокування, тобто забезпечує доступ до неї уповноваженим користувачам.

Деякі фахівці виділяють також таку властивість, як спостережність. Вона означає, що інформація повинна постійно знаходитись під контролем системи захисту на всіх етапах її обробки та передачі [13].

В умовах стрімкої інформатизації суспільства та зростаючої потреби в мобільному доступі до мережі Internet все більшої популярності набувають бездротові мережі. Сучасні технології забезпечують якість зв'язку в них на рівні мереж з використанням фізичного середовища передачі даних, при цьому кількість користувачів може бути значно більшою.

Однак, широке застосування бездротових мереж актуалізує проблему захисту інформації, що передається. Враховуючи високу ймовірність і потенційну небезпеку загроз інформаційним ресурсам, використання ефективних механізмів захисту і шифрування даних в бездротових мережах стає вкрай важливим завданням.

Отже, з огляду на вищевикладене, дослідження методів підвищення ефективності захисту інформації в бездротових комп'ютерних мережах набуває особливої актуальності. Для проведення таких досліджень необхідно, перш за все, проаналізувати можливі загрози, оцінити наслідки їх впливу та здійснити системний аналіз існуючих методів захисту. Справді, фундаментом для побудови бездротових мереж є стандарт IEEE 802.11, який визначає набір протоколів для передачі даних. Цей стандарт постійно розвивається і

оновлюється, про що свідчать нові версії, опубліковані в 1999, 2007, 2012 роках. Наступне оновлення очікується в 2016 році.

Для захисту інформації в бездротових мережах використовують різні методи, які можна умовно поділити на основні та допоміжні. До основних належать протоколи:

- WEP (Wired Equivalent Privacy) — перший стандарт захисту бездротових мереж, який на сьогоднішній день вважається застарілим і ненадійним.
- WPA (Wi-Fi Protected Access) — протокол, розроблений на заміну WEP, що забезпечує більш високий рівень безпеки.
- WPA2 (Wi-Fi Protected Access II) — вдосконалена версія WPA з покращеними механізмами шифрування.

Важливу роль в захисті бездротових мереж відіграє також стандарт IEEE 802.1X, який регламентує процес інкапсуляції даних протоколу EAP (Extensible Authentication Protocol). EAP використовується для аутентифікації користувачів і забезпечення доступу до мережі лише авторизованим пристроям.

Найпростішим способом захисту від криптографічних атак є використання WPA2 [14]. Протоколи WPA/WPA2 суттєво підвищують рівень захищеності бездротових мереж, однак ціною підвищення складності протоколу. Атаки на WPA можна умовно розділити на дві категорії: спрямовані на процедуру аутентифікації та спрямовані на алгоритми шифрування.

Впровадження протоколу WPA2, безумовно, є найоптимальнішим рішенням для забезпечення безпеки бездротових мереж. Разом з тим, додаткового захисту можна досягти за рахунок таких заходів: захист паролів, фільтрація за MAC-адресами, генерація складних паролів.

Таким чином, поєднання протоколу WPA2 з додатковими заходами безпеки дозволить значно зміцнити захист бездротової мережі та мінімізувати ризики несанкціонованого доступу.

З метою ефективного управління мережевою структурою та типами пакетів, що передаються бездротовими мережами, було проведено аналіз протоколів захисту на основі документації IEEE, а також основних протоколів

WEP, WPA, WPA2 та відповідних алгоритмів шифрування.

Широке розповсюдження бездротових мереж стимулювало розробку механізмів безпеки, які, на жаль, не завжди здатні протистояти атакам зловмисників. Тому виникає потреба в комплексному підході до захисту мережі.

Одним з найбільш ефективних рішень є впровадження технології WPA2 в усіх типах бездротових мереж. При цьому важливо дотримуватись комплексної методології, що включає: створення надійних паролів, розробку плану забезпечення безпеки, використання захищеного програмного забезпечення.

1.4. Рівні безпеки

Рівень 1: Фізична безпека. Фізична безпека справді є фундаментом захисту інформації. Вона забезпечує цілісність і недоторканність пристроїв та даних, перешкоджаючи таким фізичним загрозам, як викрадення обладнання, його пошкодження або крадіжка конфіденційної інформації [10]. Безперечно, дотримання елементарних правил фізичної безпеки дозволяє значно знизити ризики для інформації. Варто завжди пам'ятати про необхідність зберігати пристрої та носії інформації в безпечних місцях з обмеженим доступом. Не менш важливим є використання паролів та інших методів захисту, які унеможливлюють несанкціонований доступ до інформації. Також слід забезпечити належні умови експлуатації обладнання, зокрема встановлювати його в приміщеннях з відповідним охолодженням та вентиляцією, особливо якщо воно працює в режимі підвищених температур. Це допоможе запобігти перегріву та пошкодженню апаратури, а отже, і втраті даних.

Фізичні засоби захисту є важливою складовою системи безпеки. Вони являють собою різноманітні пристрої та конструкції, які створюють перешкоди на шляху зловмисників і запобігають несанкціонованому доступу до інформації. До них можна віднести механічні замки, ґрати, сейфи, а також електронні системи контролю доступу, сигналізації, системи відеонагляду тощо. Використання таких засобів дозволяє значно ускладнити доступ зловмисників до

приміщень, де розміщено обладнання і зберігаються дані, а також до самих носіїв інформації.

Використання фізичних засобів захисту дозволяє вирішити широкий спектр завдань, пов'язаних із забезпеченням безпеки. Так, за їх допомогою можна забезпечити:

Надійну охорона території підприємства і постійне спостереження за нею;

Захист будівель і внутрішніх приміщень від несанкціонованого доступу і контроль за ними;

Охорона матеріальних цінностей — обладнання, продукції, фінансів, а також захист інформації від крадіжки та пошкодження;

Встановлення контрольованого доступу до будівлі та приміщень, що дозволяє обмежити коло осіб, які мають право входу.

Отже, всі фізичні засоби захисту об'єктів можна класифікувати за принципом їх дії на три категорії: засоби попередження, засоби виявлення та системи ліквідації загроз. До засобів виявлення загроз, наприклад, належать охоронна сигналізація та охоронне телебачення. Вони дозволяють вчасно виявити спроби несанкціонованого проникнення на об'єкт або інші злочинні дії. Засоби попередження покликані перешкоджати вчиненню злочинів. Прикладом таких засобів є паркани навколо об'єктів, які ускладнюють несанкціоноване проникнення на територію. Посилені двері, стіни, стелі, ґрати на вікнах та інші подібні заходи слугують захистом як від проникнення, так і від інших злочинних дій. Не слід забувати і про такий важливий захід безпеки, як відключення та від'єднання пристроїв, що не використовуються. Це дозволить запобігти їх пошкодженню або використанню зловмисниками для несанкціонованих цілей. Дотримання правил фізичної безпеки є важливою складовою захисту інформації, тому їх необхідно дотримуватися завжди, незалежно від того, який рівень захисту використовується [10].

Рівень 2: Мережева безпека. Наступним рівнем захисту інформації після фізичного є мережева безпека. Вона забезпечує захист мережевих з'єднань та

систем від несанкціонованого доступу, а також захищає інформацію, що зберігається в мережі або передається по ній, від крадіжки, пошкодження або знищення.

Для забезпечення мережевої безпеки використовують спеціалізоване програмне забезпечення, яке реалізує функції аутентифікації, авторизації та контролю доступу користувачів до мережевих ресурсів. Це дозволяє гарантувати, що доступ до інформації отримають лише уповноважені користувачі, і запобігти несанкціонованим діям з їх боку.

Мережева безпека передбачає захист від різноманітних загроз, таких як віруси, черв'яки, троянські програми, шпигунське програмне забезпечення та інші шкідливі програми, які можуть призвести до витоку конфіденційної інформації або завдати шкоди системам.

Для боротьби з цими загрозами використовують комплексний підхід, який передбачає застосування антивірусних програм, брандмауерів, систем виявлення вторгнень та іншого спеціалізованого програмного забезпечення, що гарантує надійний захист мережі.

Важливим елементом мережевої безпеки є контроль доступу до мережевих ресурсів. Його можна реалізувати за допомогою системи ролей та прав користувачів. Це дає змогу диференціювати доступ до конфіденційної інформації, надаючи його лише уповноваженим користувачам або групам користувачів.

Важливим аспектом мережевої безпеки є також захист від DDoS-атак, метою яких є перевантаження мережевих ресурсів і зрив їх нормального функціонування. Для протидії таким атакам використовують спеціалізовані системи захисту від DDoS, які забезпечують стабільну роботу мережі навіть в умовах надвисокого навантаження [11].

Рівень 3: Програмна безпека. Типи шкідливого програмного забезпечення. Шкідливе програмне забезпечення — це загальна назва для будь-яких програм або файлів, які створюють загрозу для комп'ютера чи його користувача. До найбільш поширених типів шкідливого ПЗ належать

комп'ютерні віруси, програми-вимагачі, черв'яки, троянські коні та шпигунські програми.

Ці шкідливі програми можуть мати різноманітні негативні наслідки для користувача, зокрема: викрадення, шифрування або видалення конфіденційних даних, зміна або блокування важливих функцій комп'ютера, а також отримання зловмисниками контролю над інфікованим пристроєм.

Для поширення шкідливого програмного забезпечення кіберзлочинці використовують різноманітні методи, як фізичні, так і віртуальні. Наприклад, атака програми-вимагача WannaCry швидко поширилася завдяки експлуатації відомої вразливості в операційних системах. Одним із найбільш розповсюджених способів доставки шкідливого ПЗ є фішинг. Зловмисники надсилають електронні листи, замасковані під повідомлення від відомих компаній або організацій, які містять шкідливі посилання або вкладення. При переході за посиланням або відкритті вкладення на комп'ютер користувача потрапляє шкідлива програма [11].

У складних атаках зловмисного програмного забезпечення часто використовується командно-контрольний сервер, який дає змогу кіберзлочинцям встановлювати зв'язок з інфікованою системою, викрадати конфіденційні дані з жорсткого диска або отримувати віддалений доступ до пристрою.

Сьогодні кіберзлочинці розробляють все більш витончені види шкідливого програмного забезпечення, які використовують різноманітні методи ухилення та обфускації. Це робиться для того, щоб ввести в оману користувачів, фахівців з безпеки та антивірусні програми.

Методи ухилення можуть бути досить простими, наприклад, приховування IP-адреси джерела атаки. Інший підхід — використання поліморфного шкідливого ПЗ, яке постійно змінює свій код, щоб уникнути виявлення антивірусами, що базуються на сигнатурах.

Ще один приклад — безфайлове шкідливе ПЗ, яке існує тільки в оперативній пам'яті комп'ютера і не записується на диск. Це значно ускладнює

його виявлення традиційними антивірусними засобами.

Типи шкідливих програм. Вірус — це різновид шкідливого програмного забезпечення, який при запуску починає самостійно копіювати себе і впроваджувати свій код в інші комп'ютерні програми, змінюючи їх. Успішна реплікація вірусу призводить до інфікування уражених ділянок комп'ютера [12].

Для зараження систем і поширення вірусів їх автори вдаються до методів соціальної інженерії та експлуатують вразливості в програмному забезпеченні. Основними цілями для вірусів є операційні системи Microsoft Windows і Mac. Щоб уникнути виявлення антивірусами, віруси часто використовують складні стратегії маскування.

Цілі створення вірусів можуть бути різними: отримання прибутку (наприклад, за допомогою програм-вимагачів), розсилка повідомлень, розваги, демонстрація вразливостей, саботаж і створення відмов в обслуговуванні. Деякі віруси створюються з метою дослідження проблем кібербезпеки, штучного життя та еволюційних алгоритмів.

Комп'ютерні віруси завдають значних економічних збитків, які обчислюються мільярдами доларів. Ці збитки пов'язані з різними факторами: збої в роботі систем, витрати ресурсів на боротьбу з вірусами, пошкодження даних, збільшення витрат на обслуговування інфікованих систем, викрадення особистої інформації (наприклад, номерів кредитних карток) та інші негативні наслідки.

Комп'ютерний хробак — це вид шкідливого програмного забезпечення, яке здатне до самостійного розмноження. Основна мета хробака — заразити якомога більше комп'ютерів, створюючи свої копії і поширюючи їх по мережі. При цьому хробак залишається активним в інфікованих системах, продовжуючи свою шкідливу діяльність**.**

Для свого поширення хробаки зазвичай використовують комп'ютерні мережі, проникаючи на комп'ютери через наявні вразливості або прогалини в системі безпеки. Навіть якщо хробак не завдає прямої шкоди файлам, він все одно негативно впливає на роботу мережі, споживаючи її пропускну здатність.

В цьому полягає основна відмінність хробаків від вірусів, які майже завжди пошкоджують або змінюють файли на комп'ютері жертви.

WannaCry — яскравий приклад криптохробака-вимагача, який поширюється автоматично, без участі користувача, експлуатуючи вразливість EternalBlue.

Слід зазначити, що навіть хробаки, які не мають на меті змінювати системи, а лише поширюються мережею, можуть спричинити серйозні проблеми. Наприклад, хробаки Morpiса та Mydoom, незважаючи на відсутність шкідливого корисного навантаження, викликали значні збої в роботі мереж через перевантаження мережевого трафіку.

Троянський кінь, або просто троян, — це різновид шкідливого програмного забезпечення, який маскується під нешкідливу або корисну програму, щоб ввести в оману користувачів і проникнути на їхні комп'ютери. Назва походить від відомого міфу про троянського коня, за допомогою якого греки захопили Трою.

Поширення троянів найчастіше відбувається за допомогою методів соціальної інженерії, таких як фішинг. Наприклад, користувачеві можуть надіслати електронний лист із вкладенням, яке виглядає як звичайний файл (наприклад, документ Excel). Однак при відкритті цього файлу запускається шкідливий код, і троян встановлюється на комп'ютер.

Хоча трояни можуть виконувати різноманітні дії, найчастіше вони працюють як бекдор, тобто надають зловмиснику прихований доступ до зараженого комп'ютера. Це дозволяє зловмисникам отримувати доступ до особистої інформації користувача, такої як історія переглядів в інтернеті, дані для входу в банківські системи, паролі тощо. Трояни також можуть використовуватись для здійснення атак програм-вимагачів.

Важливою відмінністю троянів від комп'ютерних вірусів і хробаків є те, що вони не намагаються самостійно поширюватись або впроваджувати свій код в інші файли. Їхня основна мета — отримати доступ до системи і виконати певні дії в інтересах зловмисника.

Руткіт — це комплекс шкідливих програм, спрямованих на отримання несанкціонованого доступу до комп'ютера або його програмного забезпечення. При цьому руткіт зазвичай намагається приховати свою присутність в системі, а також може маскувати інші шкідливі програми.

Встановлення руткіта може здійснюватись автоматично або вручну зловмисником, що має права адміністратора.

Зловмисники можуть отримати доступ до системи різними шляхами: використовуючи вразливості, підбираючи паролі або застосовуючи методи фішингу.

Виявлення руткіта — складне завдання, оскільки він може блокувати роботу антивірусних програм. Для виявлення руткітів використовують різні методи, такі як застосування довірених операційних систем, аналіз поведінки системи, пошук сигнатур, сканування на наявність відмінностей та аналіз дампа пам'яті.

Видалення руткіта може бути дуже складним або навіть неможливим, особливо якщо він впроваджений в ядро системи. У деяких випадках для видалення руткіта може знадобитись заміна апаратного забезпечення або використання спеціального обладнання.

Програми-вимагачі — це тип шкідливого програмного забезпечення, який блокує доступ до комп'ютерної системи або даних користувача і вимагає сплати викупу за відновлення доступу. Поширення програм-вимагачів здійснюється через фішингові електронні листи, шкідливу рекламу, заражені веб-сайти або шляхом експлуатації вразливостей в програмному забезпеченні.

Наслідки атак програм-вимагачів можуть бути дуже серйозними: простої в роботі, витік даних, крадіжка інтелектуальної власності та порушення цілісності даних.

Суми викупу, які вимагають зловмисники, варіюються від сотень до сотень тисяч доларів. Як правило, викуп вимагають сплачувати в криптовалюті, наприклад, біткойнах.

Кейлоггери, або реєстратори натискань клавіш, — це вид шкідливого

програмного забезпечення, яке відстежує і записує всі натискання клавіш на комп'ютері або смартфоні. Зібрана інформація передається зловмиснику, який може використати її для отримання конфіденційних даних, таких як логіни, паролі та номери кредитних карт.

Термін "сіре програмне забезпечення" (grayware) з'явився у вересні 2004 року. Він позначає програми або файли, які не можна однозначно віднести до шкідливих, але вони негативно впливають на продуктивність комп'ютера і можуть становити загрозу кібербезпеці.

Як мінімум, сіре ПЗ викликає роздратування у користувачів своєю небажаною поведінкою. В гіршому ж випадку воно може отримати контроль над системою і таємно передавати інформацію зловмисникам.

До сірого ПЗ належать, наприклад, рекламне та шпигунське ПЗ. На щастя, більшість сучасних антивірусів здатні виявляти та видаляти такі програми.

Зазвичай видалення рекламного та шпигунського ПЗ не становить труднощів, оскільки вони не такі небезпечні, як інші види шкідливих програм.

Найбільшу тривогу викликає не стільки наявність сірого програмного забезпечення як такого, скільки механізми, які воно використовує для проникнення на комп'ютер: соціальна інженерія, неоновлене програмне забезпечення та інші вразливості. Адже ті ж самі методи можуть бути використані і більш небезпечними видами шкідливого ПЗ, наприклад, програмами-вимагачами.

Виявлення рекламного ПЗ на комп'ютері має стати сигналом тривоги для користувача. Це означає, що в системі є слабкі місця, які необхідно негайно усунути, щоб запобігти проникненню більш небезпечних загроз.

Безфайлове шкідливе програмне забезпечення — це особливий тип шкідливого ПЗ, який використовує для зараження комп'ютера легітимні програми. На відміну від інших видів шкідливого ПЗ, воно не залишає слідів на жорсткому диску, що значно ускладнює його виявлення та видалення антивірусами. Безфайлове ПЗ існує виключно в оперативній пам'яті комп'ютера.

Хоча безфайлове шкідливе ПЗ стало широко відомим як серйозна

кіберзагроза в 2017 році, воно існує вже досить давно. Першими прикладами безфайлових атак були Frodo, Number of the Beast і The Dark Avenger. З недавніх прикладів можна згадати атаки на Національний комітет Демократичної партії та Equifax.

Оскільки безфайлове шкідливе ПЗ не записує жодних даних на жорсткий диск, воно є стійким до багатьох традиційних методів комп'ютерної криміналістики, таких як білий список файлів, виявлення сигнатур, перевірка апаратного забезпечення, аналіз шаблонів або відміток часу. Це залишає дуже мало слідів для фахівців з кібербезпеки. Проте, оскільки таке ПЗ працює тільки в пам'яті, воно зазвичай зникає після перезавантаження системи.

Рекламне програмне забезпечення — це один з видів сірого ПЗ, яке призначене для показу реклами на екрані користувача, наприклад, в браузері або у вигляді спливаючих вікон.

Зазвичай рекламне ПЗ "чесно" повідомляє про себе або поширюється разом з іншими програмами, "підсовується" користувачеві при їх встановленні на комп'ютер, планшет чи смартфон.

Хоча рекламне ПЗ і може викликати роздратування у користувачів, воно є одним з найменш шкідливих видів ПЗ і одночасно одним з найбільш прибуткових. Його популярність особливо зросла з поширенням мобільних пристроїв. Прибуток від рекламного ПЗ отримується за рахунок автоматичного показу реклами користувачам.

Шкідлива реклама, різновид шкідливої реклами — це використання реклами для розповсюдження зловмисного програмного забезпечення. Зазвичай це включає введення зловмисної реклами або реклами, наповненої зловмисним програмним забезпеченням, у легальні рекламні мережі та веб-сторінки.

Реклама є чудовим способом розповсюдження зловмисного програмного забезпечення, оскільки в рекламу вкладають значні зусилля, щоб залучити користувачів до продажу чи реклами продукту.

Шкідлива реклама також приносить користь від репутації сайтів, на яких вона розміщується, наприклад, гучних і авторитетних веб-сайтів новин.

Шпигунське програмне забезпечення — це вид шкідливого ПЗ, яке потай збирає інформацію про користувача або організацію і передає її зловмисникам без відома і згоди жертви.

Основні цілі шпигунського ПЗ:

- відстеження дій користувача в інтернеті і продаж зібраних даних;
- викрадення даних кредитних карток і банківських рахунків;
- збір персональних даних користувачів.

Деякі види шпигунського ПЗ можуть також встановлювати на пристрій інші програми і змінювати налаштування системи.

На щастя, шпигунське ПЗ зазвичай не становить такої серйозної загрози, як інші види шкідливого ПЗ, і його можна легко видалити.

Бот — це комп'ютер, який був заражений шкідливою програмою і тепер перебуває під контролем зловмисника.

Зловмисник може використовувати бот для різних цілей, наприклад, для здійснення нових кібератак або для включення його до складу ботнету — мережі заражених комп'ютерів.

Ботнети часто використовуються для проведення DDoS-атак (розподілених атак на відмову в обслуговуванні), поширення програм-вимагачів, кейлогерів та інших видів шкідливого ПЗ**.**

Бекдор — це прихований метод, який дозволяє обійти стандартні процедури аутентифікації або шифрування в комп'ютері, програмі, пристрої (наприклад, маршрутизаторі) чи іншому компоненті системи.

Зазвичай бекдори використовуються для отримання віддаленого доступу до комп'ютера або для доступу до зашифрованих файлів.

Отримавши доступ до системи через бекдор, зловмисник може викрадати, пошкоджувати, видаляти або передавати конфіденційні дані.

Бекдор може бути реалізований різними способами: як прихована частина програми (троян), окрема програма або код, вбудований в мікропрограму чи операційну систему.

Деякі бекдори створюються навмисно, інші є результатом помилок в

програмному забезпеченні. В деяких випадках бекдори мають легітимне застосування, наприклад, для скидання паролів користувачів виробником пристрою.

Викрадач браузера — це програма, яка змінює налаштування веб-браузера, перенаправляючи користувача на інші сторінки, змінюючи домашню сторінку, встановлюючи небажані панелі інструментів, показуючи рекламу або перенаправляючи на інші сайти.

Злочинне програмне забезпечення — це клас шкідливих програм, розроблених спеціально для автоматизації кіберзлочинів.

Основні функції злочинного ПЗ:

- крадіжка особистих даних за допомогою методів соціальної інженерії або прихованого доступу до фінансових рахунків жертви;
- викрадення грошей або здійснення несанкціонованих транзакцій;
- викрадення конфіденційної інформації з метою корпоративного шпигунства.

Важливо пам'ятати, що не всі програми, доступні в App Store і Google Play, є безпечними. App Store вважається більш надійним, оскільки програми в ньому проходять ретельнішу перевірку перед публікацією.

Шкідливі програми для мобільних пристроїв можуть виконувати різноманітні шкідливі дії: викрадати дані користувачів, шантажувати їх, отримувати доступ до корпоративних мереж, змушувати переглядати рекламу або встановлювати бекдори.

Скрапер оперативної пам'яті — це вид шкідливого ПЗ, яке збирає дані, що тимчасово зберігаються в оперативній пам'яті комп'ютера. Часто таке ПЗ атакує POS-термінали (касові апарати), оскільки в них можуть зберігатись незашифровані номери кредитних карт протягом короткого часу, поки вони не будуть зашифровані і передані на сервер.

Підроблене програмне забезпечення безпеки — це ще один підступний вид шкідливого ПЗ. Воно імітує програми захисту і повідомляє користувачеві про наявність проблем безпеки (наприклад, вірусів), пропонуючи сплатити за їх

вирішення. Насправді ж саме це ПЗ є шкідливим і потребує видалення.

Криптоджекінг — це вид шкідливої діяльності, при якій зловмисники використовують обчислювальні ресурси жертви для майнінгу криптовалюти без її відома і згоди.

Баги. Помилки в програмному забезпеченні, подібно до соціальної інженерії та фішингу, не є шкідливим ПЗ самі по собі, але вони створюють вразливості, які можуть бути використані зловмисниками. Вразливість EternalBlue в операційних системах Windows, що призвела до масштабної атаки WannaCry, є яскравим прикладом цього.

Програмна безпека — це рівень захисту, який забезпечується програмним забезпеченням системи. Він включає в себе захист від різноманітних загроз: вірусів, хробаків, шкідливих програм, витоку даних тощо.

Для забезпечення програмної безпеки необхідно регулярно оновлювати ПЗ, встановлювати антивіруси та інші захисні програми, контролювати доступ до даних та вживати інших заходів для захисту інформації. Також можуть використовуватись методи криптографічного захисту, які забезпечують конфіденційність даних шляхом шифрування та дешифрування [13].

Рівень 4: Персональна безпека. Протоколи безпеки. SSL / TLS. SSL/TLS — це криптографічний протокол, який забезпечує безпечне з'єднання між клієнтом (наприклад, браузером) та сервером в інтернеті. Протокол SSL (Secure Sockets Layer) був розроблений компанією Netscape Communications у 1994 році, а TLS (Transport Layer Security) є його вдосконаленою версією.

SSL/TLS гарантує конфіденційність, цілісність та аутентифікацію даних при їх передачі мережею. Для цього використовуються криптографічні алгоритми, які шифрують дані, перевіряють їх цілісність і підтверджують автентичність сервера.

Протокол SSL/TLS широко використовується в браузерах для захисту конфіденційної інформації (паролів, даних кредитних карт тощо) при її передачі мережею. Крім того, SSL/TLS застосовується в інших мережевих протоколах, таких як SMTP, IMAP та FTP, для захисту даних від несанкціонованого доступу.

Існує кілька версій протоколу SSL/TLS, які відрізняються між собою використовуваними криптографічними алгоритмами. Найбільш захищені версії використовують сильні алгоритми шифрування та складні процедури аутентифікації.

Проте, незважаючи на високий рівень захисту, SSL/TLS, як і будь-який інший криптографічний протокол, не є абсолютно безпечним. Він може бути вразливим до різних атак, таких як атаки "людина посередині", криптографічні атаки тощо.

VPN. VPN (Virtual Private Network) — це технологія, яка дозволяє створювати віртуальні приватні мережі поверх інтернету. VPN забезпечує безпеку і конфіденційність мережевого з'єднання, дозволяючи використовувати публічний інтернет як приватну мережу.

Основні переваги VPN:

- захист від несанкціонованого доступу до мережі;
- захист від DDoS-атак;
- запобігання перехопленню трафіку;
- захист конфіденційної інформації від витоку.

Існує багато різних типів VPN, таких як PPTP, L2TP, IPsec, OpenVPN та інші. Кожен з них має свої особливості, переваги та недоліки. Вибір конкретного типу VPN залежить від потреб користувача [15].

VPN широко використовується для забезпечення безпеки на робочому місці та вдома. VPN дозволяє підключатись до корпоративної мережі з будь-якого місця, що забезпечує можливість працювати віддалено. Також VPN надає доступ до віддалених серверів та програм, що підвищує продуктивність праці.

Всі дані, що передаються через VPN, шифруються, що гарантує безпеку з'єднання. VPN забезпечує конфіденційність інформації, що передається мережею. VPN може використовуватись для захисту відеозв'язку, месенджерів та інших сервісів, які працюють з конфіденційною інформацією.

Ipsec. IPsec — це протокол, який забезпечує безпеку мережевого трафіку шляхом шифрування та аутентифікації пакетів даних. Це запобігає

несанкціонованому доступу, перехопленню та зміні даних під час їх передачі мережею.

IPsec працює на мережевому рівні, тому може захищати будь-які протоколи вищого рівня, такі як TCP, UDP тощо. IPsec може працювати в двох режимах:

- тунельний режим: захищає весь трафік між двома мережами;
- транспортний режим: захищає трафік між двома кінцевими пристроями.

Для забезпечення безпеки IPsec використовує кілька протоколів:

- ESP (Encapsulating Security Payload): шифрує дані;
- AH (Authentication Header): аутентифікує пакети;
- IKE (Internet Key Exchange**):** забезпечує обмін ключами шифрування.

IPsec є важливим інструментом для захисту великих мереж. Він дозволяє забезпечити конфіденційність, цілісність та доступність даних, що передаються мережею.

SSH. SSH (Secure Shell) — це мережевий протокол, який забезпечує безпечний зв'язок між комп'ютерами. За допомогою шифрування трафіку між клієнтом та сервером SSH робить передачу даних безпечною і захищеною від зловмисників.

Для забезпечення безпеки SSH використовує дві ключові технології: асиметричні шифри та криптографічні хеш-функції. Асиметричні шифри захищають ключ шифрування, який використовується для шифрування даних. Криптографічні хеш-функції створюють цифровий підпис, що підтверджує автентичність сервера та цілісність даних.

SSH застосовується для віддаленого керування комп'ютером або сервером. Користувач може підключитися до віддаленого комп'ютера через SSH, використовуючи свій логін та пароль, і виконувати на ньому команди, ніби він знаходиться безпосередньо перед ним. Крім того, SSH може використовуватись для копіювання файлів між комп'ютерами, захищаючи їх від несанкціонованого доступу.

SSH є стандартом безпечного зв'язку в багатьох галузях, таких як веб-

хостинг, мережеве управління та системне адміністрування. Це надійний протокол, який забезпечує безпеку даних при передачі по мережі [20].

1.5. Концепція і методи технічного захисту інформації

Технічний захист інформації охоплює широкий спектр заходів, спрямованих на запобігання несанкціонованому доступу до інформації з різних каналів витоку. Він також передбачає захист від спеціальних впливів на інформацію, таких як знищення, спотворення або блокування доступу до неї [7].

Сукупність методів і засобів захисту інформації включає:

- апаратні засоби;
- програмні засоби;
- захисні перетворення;
- організаційні заходи

Апаратний, або схемний, захист передбачає вбудовування в пристрої ЕОМ та інші технічні засоби обробки інформації спеціальних схем, призначених для захисту та контролю інформації. Прикладами таких схем є схеми контролю на цілісність, які стежать за правильністю передачі інформації між різними пристроями, та екрануючі пристрої, що локалізують електромагнітні випромінювання.

Програмні методи захисту являють собою комплекс алгоритмів і програм, призначених для розмежування доступу до інформації та запобігання її несанкціонованому використанню.

Одним з ключових програмних методів є захисне перетворення інформації. Суть його полягає в тому, що інформація, яка зберігається в системі або передається каналами зв'язку, представляється в спеціальному коді. Це унеможливлює її використання без відповідного декодування.

Організаційні заходи з захисту інформації включають в себе різноманітні дії, спрямовані на забезпечення безпеки інформаційної системи. Це може бути ретельний підбір та перевірка персоналу, який працює з інформацією, чітке регламентування процесів розробки та експлуатації системи тощо.

Важливо розуміти, що лише комплексне застосування різних методів

захисту може гарантувати надійну безпеку інформації. Кожен окремий метод або захід має як переваги, так і недоліки.

Концепція захисту інформації — це система поглядів на проблему інформаційної безпеки та методи її забезпечення, яка офіційно прийнята і враховує сучасні тенденції розвитку технологій та методів кіберзлочинності.

Концепція захисту інформації є методологічною основою для розробки конкретних заходів захисту. Розробка концепції захисту здійснюється в три етапи:

1. **Визначення об'єктів захисту.** На цьому етапі необхідно чітко визначити, які саме цінності, виробничі процеси, програми та дані потребують захисту. Також важливо провести диференціацію об'єктів за їх значимістю.

2. **Аналіз потенційних загроз.** На цьому етапі проводиться детальний аналіз можливих злочинних дій щодо об'єктів, які підлягають захисту. Необхідно визначити ступінь реальної небезпеки найбільш типових злочинів та проаналізувати ймовірні дії зловмисників.

3. **Розробка заходів захисту.** На цьому етапі аналізуються всі обставини, включаючи місцеві умови, особливості виробничих процесів, наявні технічні засоби захисту тощо. Концепція захисту повинна містити перелік організаційних, технічних та інших заходів, які забезпечать максимальний рівень безпеки при мінімальних витратах на їх реалізацію.

Висновки до розділу 1

У першому розділі досліджено поняття витоку інформації та розглянуто детально технічні канали витоку інформації (ТКВІ). Зокрема, розглянуто радіоканали, які є досить ефективними ТКВІ через їхню незалежність від часу доби та пори року, високу достовірність видобутку інформації, великий обсяг та оперативність отримання інформації, а також скритність перехоплення сигналів.

Також, в розділі 1 проаналізовано такі поняття як інформація та її захист, розглянуто різні рівні безпеки, включаючи фізичну, програмну мережеву та

персональну безпеку. Крім того, розглянуто концепцію та методи технічного захисту інформації, включаючи використання захищеного обладнання, регламентування роботи користувачів, архітектури систем, інженерно-технічне оснащення споруд та комунікацій, а також пошук та блокування закладних пристроїв.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ЗАХИСТУ БЕЗДРОТОВИХ КАНАЛІВ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Для гарантування технічного захисту конфіденційної інформації в комп'ютерних системах та обчислювальній техніці, що використовуються для обробки та зберігання даних, застосовується комплексний підхід. Він включає в себе конструкторські, організаційні, програмні та технічні заходи, що впроваджуються на всіх стадіях життєвого циклу цих систем, від їх розробки до використання.

Сукупність методів і засобів захисту інформації включає програмні й апаратні засоби, захисні перетворення та організаційні заходи(рис 2.1):

Рисунок 2.1 – Методи і засоби захисту інформації

I

2.1. Програмний захист

Для забезпечення та підтримки безпеки на об'єкті інформаційної діяльності можуть застосовуватись наступні інструменти як **NordLayer, ManageEngine Log360, ManageEngine Vulnerability Manager Plus** [15]**.**

NordLayer має наступні функції:

1. VPN для безпечного віддаленого доступу: якщо будь-які співробітники працюють віддалено, VPN NordLayer може шифрувати їх підключення до офісної мережі, забезпечуючи безпеку даних у загальнодоступних Wi-Fi або домашніх мережах. Кожен співробітник використовував клієнт NordLayer на своєму ПК для безпечного підключення до мережі компанії, доступу до сервера та інших спільних ресурсів.

2. Доступ до мережі з нульовою довірою (ZTNA): NordLayer може реалізувати політики нульової довіри, щоб користувачі мали доступ лише до необхідних ресурсів. Наприклад, працівникам можна дозволити підключатися лише до сервера або певного програмного забезпечення, яке їм потрібно використовувати, а не мати відкритого доступу до всіх мережевих пристроїв (наприклад, принтерів або інструментів адміністратора). Це зменшує потенційні ризики, обмежуючи доступ до конфіденційних даних.

3. Багатофакторна автентифікація (MFA): Щоб забезпечити доступ до мережевих ресурсів лише авторизованим користувачам, функція MFA NordLayer може додати додатковий рівень безпеки на додаток до облікових даних користувача. Це особливо корисно для сервера, де можуть зберігатися конфіденційні дані компанії.

4. Брандмауер і захист від загроз: NordLayer містить брандмауер і функцію захисту від загроз, що допомагає захистити сервер і ПК від зловмисного програмного забезпечення та підозрілого трафіку. Запустивши функції безпеки NordLayer на кожному пристрої, компанія могла фільтрувати потенційно зловмисну об’єктність і підтримувати захист мережі.

5. Внутрішня сегментація: за допомогою NordLayer можна сегментувати мережу таким чином, щоб різні ролі в компанії (наприклад, бухгалтерія, менеджмент) мали доступ лише до необхідних програм або серверних областей. Це зменшує ризик несанкціонованого доступу до даних і спрощує відповідність, якщо компанія обробляє конфіденційну інформацію.

6. Контроль доступу до принтера: якщо працівникам дозволено друкувати документи лише за умови підключення через NordLayer, це гарантує, що лише автентифіковані користувачі друкуватимуть конфіденційну інформацію, зберігаючи конфіденційність.

Застосування програмного забезпечення:

Налаштуйте захищений шлюз: розгорніть захищений шлюз NordLayer, щоб створити приватну віртуальну мережу для офісу. Усі офісні пристрої підключаються до цього шлюзу, який шифрує трафік і ізолює внутрішню мережу від зовнішніх загроз. Використовуйте NordLayer для призначення різних привілеїв доступу. Наприклад:

Адміністратори: повний доступ до сервера, налаштувань мережі та принтера.

Звичайні користувачі: доступ лише до певних папок на сервері та функції друку.

Запровадьте Zero Trust Network Access (ZTNA), щоб користувачі мали пройти автентифікацію перед доступом до ресурсів.

Аби забезпечити пристрої від несанкціонованого доступу необхідно оснастити кожен офісний комп’ютер клієнтською програмою NordLayer для маршрутизації всього трафіку через безпечну VPN. Це допоможе запобігти несанкціонованому доступу та зашифрує передачу даних.

Також необхідно захистити мережеві пристрої, такі як принтер, ізолюючи їх у захищеній підмережі(див. Розділ 3).

Персонал, який працює віддалено, може підключитися до офісної мережі через VPN NordLayer. Це забезпечує безпечний зв’язок і доступ до спільних файлів без загрози офісної мережі.

Моніторинг: використовуйте інформаційну панель адміністратора NordLayer, щоб контролювати підключення та налаштовувати сповіщення про підозрілу діяльність. У разі виявлення аномалії IT-персонал може миттєво скасувати доступ.

ManageEngine Log360

Використовується для виявлення інцидентів з безпекою або порушення даних, які створюють проблеми для організації використовуючи наступні інструменти:

Механізм кореляції подій у реальному часі

Використовуйте важливу інформацію з різних подій безпеки для виявлення загроз безпеці [22].

Інтелект загроз

Отримує сповіщення про IP-адреси з чорного списку та URL-адреси, розпізнані з каналів на основі STIX/TAXII, і запобігає потенційним атакам.

Аналітика поведінки користувачів і організацій (UEBA)

Використовуючи зміни в поведінці користувачів і організацій виявляє аномальну об’єктність у мережі.

Аналітика загроз

Має розширену технологію аналізу загроз (ATA), щоб аналізувати дані журналу та виявляти підозрілу об’єктність у мережі.

В арсеналі доступні наступні функції:

Централізоване керування журналами: установіть агенти Log360 на всіх офісних пристроях для збору журналів (наприклад, із засобу перегляду подій Windows, журналів сервера та журналів мережевих пристроїв). Налаштуйте центральний сервер для отримання журналів і аналізу дій користувачів, таких як спроби входу, доступ до файлів і використання програм.

Моніторинг поведінки користувачів:

Використовуйте модуль аналізу поведінки користувачів і суб’єктів (UEBA) Log360 для відстеження та аналізу поведінки користувачів. Виявляйте аномалії, наприклад незвичний час входу, надмірну кількість невдалих входів або неавторизований доступ до конфіденційних даних.

Сповіщення в реальному часі:

Налаштуйте сповіщення про критичні події, як-от спроби несанкціонованого доступу до сервера, великі передачі даних вказують на можливу викрадання даних, використання неавторизованих програм, IT-

адміністратори отримують миттєві сповіщення, щоб розслідувати ці події та вжити заходів.

Аудит і відповідність:

Використовуйте функції звітування про відповідність Log360, щоб створювати звіти за такими стандартами, як GDPR, HIPAA або PCI DSS. Плануйте регулярні перевірки дій користувачів і дозволів доступу, щоб забезпечити дотримання внутрішньої політики [21].

Безпека принтера та пристрою:

Контролюйте доступ до мережевих принтерів та інших пристроїв. Виявляйте підозрілі дії, наприклад неавторизований друк конфіденційних документів.

Приклад використання: IT-менеджер помічає сплеск невдалих спроб входу на сервер. Використовуючи інформаційну панель Log360, вони відстежують діяльність певного облікового запису користувача. Аналізуючи журнали, вони виявляють, що доступ до облікового запису здійснювався з незвичайного місця. Вони блокують обліковий запис і проводять подальше розслідування, запобігаючи потенційному злому.

2.2. Апаратний захист

Основними методами та засобами технічного захисту інформації є:

– використання захищеного обладнання;

– регламентування роботи користувачів, технічного персоналу, програмних засобів, елементів баз даних і носіїв інформації з обмеженим доступом (розмежування доступу);

– регламентування архітектури автоматизованих систем і засобів обчислювальної техніки;

– інженерно-технічне оснащення споруд і комунікацій, призначених для експлуатації автоматизованих систем і засобів обчислювальної техніки;

– пошук, виявлення і блокування закладних пристроїв.

До основних засобів захисту інформації можна віднести такі: фізичні засоби, апаратні засоби, програмні засоби, апаратно-програмні засоби, криптографічні та організаційні методи [16].

З метою запобігання несанкціонованому доступу до інформаційних систем та обчислювальної техніки, використовуються фізичні засоби захисту. Вони являють собою спеціалізовані засоби, що створюють фізичні перепони на шляху потенційних зловмисників, обмежуючи їх проникнення на територію, доступ до обладнання та, відповідно, до конфіденційних даних.

Для забезпечення базового рівня захисту інформації від несанкціонованого доступу (НСД) може бути застосований режим автономного використання персонального комп'ютера (ПК) одним користувачем у спеціально відведеному приміщенні. В даній ситуації роль захисного периметру виконують фізичні бар'єри приміщення: стіни, підлога, стеля, вікна та двері.

Надійність такого захисту безпосередньо залежить від міцності стін, відсутності комунікаційних люків, а також наявності охоронної сигналізації на вікнах та дверях, особливо у неробочий час. Технічні характеристики сигналізації будуть визначальним фактором стійкості захисту інформації.

У робочий час, коли ПК працює, можливий витік інформації каналами побічного електромагнітного випромінювання. Для усунення такої загрози здійснюються спеціальні дослідження щодо апаратних засобів та їх випромінювання, основним змістом яких є атестування та категорування засобів і об'єктів електронно-обчислювальної техніки (ЕОТ) з видачею відповідного дозволу на експлуатацію. Крім того, двері приміщення повинні бути обладнані механічним або електромеханічним замком. У деяких випадках, коли відсутня охоронна сигналізація, на період тривалої відсутності користувача ПК для підвищення безпеки доцільно системний блок і машинні носії інформації зберігати в сейфі. Використання в деяких ЕОМ у системі вводу-виводу BIOS апаратного паролю, що блокує завантаження і роботу ПК, не зовсім надійно забезпечує захист від загроз НСД, оскільки при відсутності на корпусі системного блоку механічного замка та самого власника-користувача апаратна

частка BIOS-носія паролю може бути замінена на іншу таку ж, оскільки вузли BIOS уніфіковані, але вже з відомим значенням паролю. Саме тому механічний замок, що блокує вмикання і завантаження ПК, найбільш ефективний захід у цьому випадку.

Спектр сучасних фізичних засобів захисту дуже широкий. До цієї групи засобів захисту належать також різні засоби екранування робочих приміщень та каналів передачі даних.

Апаратні засоби захисту - це різні електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв'язку тощо.

Основні функції апаратних засобів захисту:

- заборона несанкціонованого (неавторизованого) зовнішнього доступу віддаленого користувача;
- заборона несанкціонованого (неавторизованого) внутрішнього доступу до баз даних в результаті випадкових чи умисних дій персоналу;
- захист цілісності програмного забезпечення. Ці функції реалізуються шляхом:
- ідентифікації суб'єктів (користувачів, обслуговуючого персоналу) і об'єктів (ресурсів) системи;
- аутентифікації суб'єкта за наданим ним ідентифікатором;
- перевірки повноважень, яка полягає в перевірці дозволу на певні види робіт;
- реєстрації (протоколювання) при звертаннях до заборонених ресурсів;
- реєстрації спроб несанкціонованого доступу.

Реалізація цих функцій здійснюється за допомогою застосування різних технічних пристроїв спеціального призначення. До них, зокрема, належать:

− джерела безперебійного живлення апаратури, а також: пристрої стабілізації, що оберігають від стрибкоподібних перепадів напруги і пікових навантажень у мережі електроживлення;

− пристрої екранування апаратури, ліній зв'язку та приміщень, в яких знаходиться комп'ютерна техніка;

− пристрої ідентифікації і фіксації терміналів і користувачів при спробах несанкціонованого доступу до комп'ютерної мережі;

− засоби захисту портів комп'ютерної техніки тощо.

Засоби захисту портів виконують декілька захисних функцій, а саме:

− "звірка коду ". Комп'ютер захисту порту звіряє код санкціонованих користувачів з кодом у запиті;

− "камуфляж". Деякі засоби захисту портів камуфлюють існування портів на лінії телефонного зв'язку шляхом синтезування людського голосу, який відповідає на виклик абонента;

− "дзвінок назустріч". У пам'яті засобу захисту портів зберігаються не тільки коди доступу, але й ідентифікаційні номери телефонів;

− ведення автоматичного "електронного журналу" доступу в комп'ютерну систему з фіксацією основних дій користувача.

Для реалізації логічного та інтелектуального захисту інформації в системах використовуються програмні засоби захисту. Вони інтегровані в програмне забезпечення системи та виконують функції контролю доступу, шифрування, аутентифікації, аналізу поведінки та інші, спрямовані на забезпечення безпеки даних.

З допомогою програмних засобів захисту реалізуються наступні задачі безпеки:

− контроль завантаження та входу в систему за допомогою системи паролів;

− розмежування і контроль прав доступу до системних ресурсів, терміналів, зовнішніх ресурсів, постійних та тимчасових наборів даних тощо;

− захист файлів від вірусів;

− автоматичний контроль за роботою користувачів шляхом протоколювання їх дій.

Апаратно-програмні засоби захисту - це засоби, які основані на синтезі програмних та апаратних засобів [20].

Апаратно-програмні засоби захисту відіграють важливу роль у забезпеченні безпеки, особливо в таких чутливих сферах, як банківські системи. Їх основне призначення полягає в аутентифікації користувачів, тобто підтвердженні їх особистості перед наданням доступу до ресурсів системи.

Процес аутентифікації передбачає ідентифікацію користувача за допомогою його унікального імені (або псевдоніма) та пароля, який є конфіденційним кодом, відомим лише цьому користувачу. Пароль виступає своєрідним ключем, що дозволяє отримати доступ до системи, файлів, обладнання тощо.

Важливим аспектом застосування апаратно-програмних засобів є створення електронно-цифрових підписів (ЕЦП). У банківських системах широкого поширення набули смарт-карти, які слугують для зберігання паролів та ключів користувачів, забезпечуючи додатковий рівень безпеки при проведенні операцій та підтвердженні автентичності транзакцій.

Ідентифікаційні картки, кодовані за принципом Віганда

Картки Віганда представляють собою пластикову картку, в яку при виготовленні запресовані хаотично розташовані відрізки проводів зі спеціального магнітного сплаву. Зчитування карти відбувається за допомогою електромагнітного поля, індукованого зчитувачем. При проведені карти через щілину зчитувача два ряди проводків, запаяних в карту, викликають різнополярні сплески індукційного струму, який перетворюється в двійковий код. Карти Віганда мають хороші експлутаційні характеристики.

Завдяки відсутності рухомих частин і герметичності корпусу карта відрізняється високою надійністю і довговічністю функціонування, високою стійкістю по відношенню до спроб фізичного руйнування і несприятливим кліматичним умовам, зокрема, може працювати в діапазоні температур від -40

до + 70 ° С. До недоліків цієї технології можна віднести досить високу (у порівнянні з магнітними) вартість виготовлення карток при їх короткому життєвому циклі. Крім того, в порівнянні з магнітною доріжкою щільність запису інформації тут менше приблизно на третину

Рис. 2.2 - Безконтактна карта (інтерфейс Віганда)

Безконтактні радіочастотні проксіміті-карти

Зчитувач генерує електромагнітне випромінювання певної частоти і при внесенні карти в зону дії зчитувача це випромінювання через вбудовану в карті антену живить чіп карти. Отримавши необхідну енергію для роботи, карта пересилає на зчитувач свій ідентифікаційний номер за допомогою електромагнітного імпульсу певної форми і частоти. Сама проксіміті-карта складається з приймально-передавальної антени і електронного чіп.

Ідентифікаційні картки з прихованим штрих-кодом (бар-код)

Невидимий штриховий код впечатується в основу картки і зчитувача за допомогою випромінювання інфрачервоного спектру. Код утворюється за рахунок зміни тіней при проходженні ІЧ-випромінювання через картку і має високий ступінь захищеності від підробки. Однак ця технологія доволі дорого коштує, хоча вартість таких карток і нижче, ніж вартість карток Віганда.

Оптичні ідентифікаційні картки

Кодування інформації на таких картках здійснюється приблизно так само, як під час запису даних на оптичних дисках - комп'ютерних носіях. Зчитування проводиться лазером. Сучасна технологія забезпечує дуже високу щільність

запису, тому ємність пам'яті таких карток обчислюється мегабайтами. Це дозволяє зберігати не тільки букви і цифри даних, але і зображення і звукову інформацію. Картки цього типу мають низьку вартість і високу ступінь захищеності від несанкціонованого копіювання. Однак висока щільність зберігання інформації вимагає досить дбайливого ставлення і складних пристроїв, що зчитують терміналів. Виготовляються корпорацією Drexler Technology Corp., США (картка LaserCard) і торонтскою фірмою Optical Recording Corp.

Голографічні ідентифікаційні картки

Використовувані при виготовленні таких ідентифікаційних документів тривимірні голограми формуються на основі інтерференції двох або кількох когерентних хвильових полів. Застосування голограми поряд з підвищеним захистом документів від фальсифікації забезпечує високу щільність запису інформації (до 10 біт інформації, що міститься в зображенні на 1 мм). Підвищена захищеність документів обумовлена тим, що технічна реалізація методів голографії відрізняється достатньою складністю і вимагає застосування спеціальної апаратури [17].

Одним з видів голограм, нанесення яких не пов'язане зі значними витратами, є друковані голограми. За допомогою так званої «райдужної голограми» формується друкована основа, на яку потім може бути нанесено велике число голографічних відмінних ознак справжності ідентифікаційного документа. Істотним достоїнством друкованих голограм є те, що вони можуть наноситися на використовувані в даний час документи. Це дозволяє помітно підвищити рівень захищеності посвідчень від фальсифікацій при порівняно низьких витратах.

Більш високий рівень захисту забезпечують голограми, засновані на ефекті об'ємного відображення Інформація, що міститься в них, може зчитуватися безпосередньо при звичайному освітленні (т. б. без допоміжної апаратури). Дані, що наносяться на документ за допомогою голограми, можуть являти собою як окремі букви і цифри знаки, так і складну комбінацію букв і цифр, графічних і

фотографічних символів.

Біометричні ідентифікатори: Забезпечують високий рівень безпеки завдяки використанню унікальних фізичних характеристик користувача.

- Відбитки пальців: Один із найпоширеніших видів біометричних ідентифікаторів, що забезпечує точне і надійне ідентифікування особи. Зчитування відбувається швидко і безпомилково.
- Розпізнавання обличчя: Інноваційний метод, що дозволяє ідентифікувати людину без потреби у фізичному контакті. Система використовує алгоритми розпізнавання, щоб точно ідентифікувати користувача.
- Розпізнавання сітківки ока: Використовується для зон з підвищеними вимогами до безпеки. Цей метод має високу точність, що робить його ідеальним для стратегічних об'єктів.

Мобільні ідентифікатори: Використовують смартфони та інші мобільні пристрої для доступу до системи контролю.

- Смартфони та інші мобільні пристрої: Сучасний підхід до контролю доступу, який дозволяє використовувати мобільні додатки або інші технології безконтактної передачі даних для ідентифікації користувача.

Електронні ключі та брелоки: Компактні та зручні ідентифікатори, які легко носити з собою.

- RFID-брелоки: Компактні пристрої, що забезпечують зручний доступ до закритих зон. Вони можуть бути прикріплені до ключів або носитися в кишені, що робить їх ідеальними для щоденного використання.

Організаційні заходи захисту засобів комп'ютерної інформації складають сукупність заходів щодо підбору, перевірки та навчання персоналу, який бере участь у всіх стадіях інформаційного процесу.

Досвід зарубіжних країн свідчить про те, що найефективнішим захистом інформаційних систем є введення до штату організації посади фахівця з комп'ютерної безпеки або створення спеціальних служб, як приватних, так і централізованих, виходячи з конкретної ситуації. Наявність такого відділу (служби) в банківській структурі, за оцінками зарубіжних фахівців, удвічі

знижує ймовірність вчинення злочинів у сфері використання комп'ютерних технологій.

Згідно законодавства України, у державних установах та організаціях можуть створюватись підрозділи, служби, які організують роботу, пов'язану із захистом інформації, підтримкою рівня захисту інформації в автоматизованих системах і несуть відповідальність за ефективність захисту інформації. Зазначимо, що ця норма за характером не є обов'язковою, а рекомендованою. З її змісту в поєднанні з іншими нормами Закону "Про захист інформації в автоматизованих системах" витікає, що захист інформації в автоматизованих системах є обов'язковою функцією, проте необов'язково під цю функцію може створюватися окрема функціональна організаційна структура. Ця функція може бути складовою іншої організаційної структури, тобто здійснюватися у поєднанні з іншими функціями.

Однак в фінансових установах створення спеціальних структур для захисту інформації, фінансової безпеки є обов'язковим. В них мають бути створені спеціальні відділи комп'ютерної безпеки в рамках діючих служб економічної безпеки та фізичного захисту, діяльністю яких має керувати один із спеціально призначених для цих цілей заступник начальника служби безпеки, який має у своєму розпорядженні відповідні людські, фінансові і технічні ресурси для вирішення поставлених завдань.

До функціональних обов'язків таких осіб (структурних підрозділів) має входити здійснення, передусім, таких організаційних заходів:

- забезпечення підтримки з боку керівництва конкретної організації вимог захисту засобів комп 'ютерної техніки;
- розробка комплексного плану захисту інформації;
- визначення пріоритетних напрямів захисту інформації з урахуванням специфіки діяльності організації;
- складання загального кошторису витрат фінансування охоронних заходів відповідно до розробленого плану та затвердження його як додатку до плану керівництвом організації;

- визначення відповідальності співробітників організації за безпеку інформації в межах встановленої компетенції шляхом укладення відповідних договорів між співробітником та адміністрацією;
- розробка, впровадження і контроль за виконанням різного роду інструкцій, правил та наказів, які регламентують форми допуску, рівні секретності інформації, конкретних осіб, допущених до роботи з секретними (конфіденційними) даними тощо;
- розробка ефективних заходів боротьби з порушниками захисту засобів комп'ютерної техніки.
- Надійним засобом підвищення ефективності заходів інформаційної безпеки є навчання та інструктаж працюючого персоналу щодо організаційно-технічних заходів захисту, які застосовуються в конкретній організації. Крім цього, обов'язково мають бути реалізовані наступні організаційні заходи:
- для всіх осіб, що мають право доступу до засобів комп'ютерної техніки, потрібно визначити категорії допуску, тобто коло службових інтересів коленої особи, види інформації, до яких вона має право доступу, а також: вид такого дозволу, правомочність особи, яка уповноважується для здійснення тих або інших маніпуляцій з засобами комп'ютерної техніки;
- слід визначити адміністративну відповідальність за збереження і санкціонування доступу до інформаційних ресурсів. При цьому, за кожний вид ресурсів відповідальність повинна нести одна конкретна особа;
- налагодити періодичний системний контроль за якістю захисту інформації шляхом проведення регламентних робіт як особою, відповідальною за безпеку, так і залученням компетентних фахівців (експертів) з інших організацій;
- провести класифікацію інформації відповідно до Ті важливості, диференціювати на основі цього заходи захисту; визначити порядок охорони та знищення інформації;
- організувати фізичний захист засобів комп'ютерної техніки.

Криптографічні методи захисту. З метою захисту інформації при її

передачі зазвичай використовують різні методи шифрування даних перед їх введенням до каналу зв'язку або на фізичний носій з наступною розшифровкою. Методи шифрування дозволяють досить надійно захищати комп'ютерну інформацію від злочинних посягань.

Застосування криптографічного захисту, тобто кодування тексту з допомогою складних математичних алгоритмів, завойовує все більшу популярність. Звичайно, жоден з шифрувальних алгоритмів не дає цілковитої гарантії захисту від зловмисників, але деякі методи шифрування настільки складні, що ознайомитися зі змістом зашифрованих повідомлень практично неможливо. Основні криптографічні методи захисту:

- шифрування з допомогою датчика псевдовипадкових чисел, яке полягає в тому, що генерується гамма шифру за допомогою датчика псевдовипадкових чисел і накладається на відкриті дані з врахуванням зворотності процесу;
- шифрування з допомогою криптографічних стандартів шифрування даних (з симетричною схемою шифрування), в основі якого використовуються перевірені і випробувані алгоритми шифрування даних з великою криптостійкістю;
- шифрування з допомогою пари ключів (з асиметричною системою шифрування), в яких один ключ є відкритим і використовується для шифрування інформації, другий ключ - закритим і використовується для розшифрування інформації.

Лише комплексне використання різних заходів (рис. 2.3) може забезпечити надійний захист інформації, тому що кожний метод або захід має слабкі та сильні сторони.

Рис. 2.3 – Класифікація способів захисту конфіденційної інформації

Система управління контролю доступом (СКУД)

Захист будь-якого об'єкта включає кілька рубежів, число яких залежить від рівня режимності об'єкта. При цьому у всіх випадках важливим рубежем буде система управління контролю доступом (СКУД) на об'єкт [18].

Під СКУД розуміється сукупність програмно-технічних і організаційно-методичних засобів, за допомогою яких вирішується завдання контролю і управління доступом до приміщення підприємства і окремих приміщень, а також оперативний контроль за пересуванням персоналу і часу його знаходження на території підприємства.

Такі системи можуть здійснювати контроль переміщення людей і транспорту по території охоронюваного об’єкта, забезпечувати безпеку персоналу і відвідувачів, а також збереженість матеріальних і інформаційних ресурсів підприємства. Системи контролю й керування доступом використовуються на промислових підприємствах, в офісах, магазинах, на автостоянках і автосервісах, в житлових приміщеннях.

Інтерес до систем контролю і управління доступом зростає ще й тому, що наявність такої системи важливо для ефективної роботи підприємства. Контроль не тільки істотно підвищує рівень безпеки, але й дозволяє оперативно реагувати

на поведінку персоналу і відвідувачів. Також важливим завданням для багатьох підприємств є необхідність контролювати графік і вести облік робочого часу. Особлива увага приділяється системам, що дозволяє вибудовувати необхідні конфігурації з стан дротяних блоків, враховуючи всі особливості підприємства [19].

Існуючі керівні документи у цілому поділяють СКУД за наступними ознаками:

- за способом управління;
- число контрольованих точок доступу;
- функціональні характеристики;
- виду об'єктів контролю;
- рівню захищеності системи від несанкціонованого доступу.

Також відповідно до керівних документів всі СКУД діляться на чотири класи.

СКУД 1-го класу - малофункціональні системи малої ємності, що працюють в автономному режимі і здійснюють допуск всіх осіб, які мають відповідний ідентифікатор. У такій системі використовується ручне або автоматичне керування виконавчими пристроями, а також світлова або/і звукова сигналізація.

СКУД 2-го класу - монофункціональні системи. Вони можуть бути однорівневими і багаторівневими і забезпечують роботу як в автономному, так і в мережевому режимах. Допуск осіб (груп осіб) може здійснюватися за датою, тимчасових інтервалах. Система здатна забезпечити автоматичну реєстрацію подій і автоматичне управління виконавчими пристроями.

СКУД 3-го і 4-го класів, як правило, є мережевими. У них використовуються більш складні ідентифікатори та різні рівні мережевої взаємодії (клієнт-сервер, інтерфейси зчитувачів карт Віганда або магнітних карт, спеціалізовані інтерфейси та ін.)

Основні можливості системи контролю й керування доступом

Основні можливості, які надає установка СКУД на об’єкті, що

охороняється:

- **Контроль і керування доступом** – це основна функція системи. Як уже було помічено раніше, за допомогою даної функції виробляється поділ прав доступу співробітників у певні приміщення, а також відмова в доступі небажаним особам. Крім того, можливо дистанційне керування пристроями, що блокують (замки, турнікети та ін.). СКУД дозволяє заборонити прохід для співробітників у святкові й вихідні дні, а також після закінчення робочого дня.
- **Збір і надання статистики**. СКУД збирає інформацію про осіб, які пройшли через певні крапки контролю доступу. По кожному співробітнику можливе одержання наступної інформації: час входу й виходу, спроби доступу в заборонені для нього приміщення й зони, а також спроби проходу в недозволений час. Також можливо відстежити переміщення співробітника по території із вказівкою місця й часу. Таким чином, всі виявлені порушення трудової дисципліни можуть бути занесені в особисту справу співробітника, а керівництво порушника сповіщене в робочому порядку. Крім того, випливаючи інформації про останню крапку проходу, СКУД дозволяє визначити місцезнаходження співробітника в будь-який момент часу.
- **Доступ співробітника тільки по особистому ідентифікаторі.** При проході за допомогою ідентифікаційної карти на екрані монітора в пункті охорони може відображатися вся інформація зі співробітника і його фотографія, що виключає можливість проходу по чужому ідентифікаторі. Також на рівні правил реакції СКУД можна забезпечити захист від передачі ідентифікатора іншій особі й блокувати повторний вхід на територію об'єкта по тій же самій карті доступу.
- **Облік робочого часу**. За допомогою убудованої в СКУД системи обліку робочого часу, реєструється час виходу на роботу й час відходу з робочого місця. У результаті надається можливість визначити сумарний час перебування співробітника на робочому місці з урахуванням обідів. А на самому початку дня, наприклад, в 9:30 система обліку робочого часу, убудована в СКУД, може формувати груповий звіт про співробітників, що не пройшли через контрольну

крапку входу на територію. Це дозволяє в масовому порядку виявляти спізнілих або не співробітників, що з'явилися на робоче місце. Аналогічний звіт можна одержати й наприкінці робочого дня на пункті виходу з території підприємства або офісу.

- **Автономність роботи системи**. СКУД оснащується системою безперебійного живлення, що дозволяє не переривати роботу у випадку відключення електрики в будинку. Також система контролю доступом завдяки функціоналові контролера має можливість продовжувати роботу, наприклад, при виході керуючого комп'ютера з ладу.
- **Охорона об'єкта в реальному часі**. СКУД дає можливість ставити певні приміщення на охорону й знімати їх з охорони. Крім того, у реальному часі можна одержувати відомості про всілякі позаштатні й тривожні ситуації через спеціальні оповіщення відповідальних осіб. Крім цього в базі дані системи реєструються всі тривожні події й події, що дає можливість доступу до цієї інформації надалі при необхідності. Завдяки наявним у СКУД засобам, співробітник охорони зі свого робочого місця за допомогою комп'ютера має можливість не тільки управляти дверима й турнікетами, але й подавати сигнали тривоги. У комп'ютер СКУД у співробітника охорони можуть бути занесені плани поверхів будинку зі схемою розташування контролерів обмеження доступу.
- **Віддалене керування системою через інтернет або з мобільного телефону.** Якщо при установці підключити СКУД до мережі Інтернет, то в адміністрації з'являється можливість вести віддалене керування й контроль за роботою системи. Аналогічне можна сказати й про можливість керування СКУД зі свого мобільного телефону.
- **Інтеграція СКУД з іншими системами безпеки й охорони.** Системи контролю й керування доступом прекрасно сполучаються й вбудовуються з іншими системами безпеки: системою відеоспостереження, охоронною й пожежною сигналізацією. Так, наприклад, контроль доступом

разом з відеоспостереженням забезпечують абсолютний контроль над охоронюваними приміщеннями.

Склад системи контролю та управління доступом

Ідентифікатор користувача - це пристрій або ознака, за якою визначається користувач. Для ідентифікації застосовуються атрибутні і біометричні ідентифікатори. Як атрибутні ідентифікатори використовують автономні носії ознак допуску: магнітні картки, безконтактні проксіміті-карти, брелоки «тач-мемори», різні радіобрелоки. Біометричні - зображення райдужної оболонки ока, відбиток пальця, відбиток долоні, риси обличчя і багато інших фізичні ознаки. Кожен ідентифікатор характеризується певним унікальним двійковим кодом. У СКУД кожному коду ставиться у відповідність інформація про права і привілеї власника ідентифікатора [19]. У даний час застосовуються:

- безконтактні радіочастотні проксіміті-карти (proxmity) - найбільш перспективний в даний час тип карт. Безконтактні картки спрацьовують на відстані і не вимагають чіткого позиціонування, що забезпечує їх стійку роботу і зручність використання, високу пропускну здатність;

- магнітні картки - найбільш широко поширений варіант.

Існують карти з низькокоерцитивною і висококоерцитивною магнітною смугою і з записом на різні доріжки;

- карти Виганда (Wiegand) - названі по імені вченого, який відкрив магнітний сплав, у якого прямокутної петлею гистерезиса;

- штрих-кодові карти - на карту наноситься штриховий код. Є окремі норми-яття більш складний варіант - штрих-код закривається матеріалом,

- прозорим тільки в інфрачервоному світлі, зчитування відбувається в ІЧ-області;

- ключ-брелок «тач-меморі» (touch-memory) - металева таблетка, всередині якої розташований чіп ПЗУ.

Ідентифікатори користувачів СКУД можуть мати різний статус. Для забезпечення більшості необхідних в реальному житті вимог, як мінімум, треба,

щоб контролери підтримували такі типи карт:

- постійна: для співробітників підприємства;
- тимчасова: з обмеженням терміну дії;
- «разова»: автоматично анулюється після вичерпання числа проходів;
- одноразова - окремий випадок разової карти.

Висновок до розділу 2

У другому розділі кваліфікаційної роботи проведено дослідження технологій захисту інформації на об'єкті інформаційної діяльності. Розглянуто програмні засоби захисту, такі як NordLayer, ManageEngine Log360 та ManageEngine Vulnerability Manager Plus, які забезпечують комплексний захист мережі та даних. NordLayer дозволяє створити захищений шлюз та застосувати політики нульової довіри, обмежуючи доступ до конфіденційних даних. ManageEngine Log360 допомагає виявляти інциденти з безпекою та порушення даних, аналізуючи журнали подій та поведінку користувачів.

Крім того, в розділі 2 розглянуто апаратні засоби захисту, включаючи фізичні засоби, апаратні засоби, програмні засоби, апаратно-програмні засоби, криптографічні та організаційні методи. Зокрема, детально описано систему управління контролю доступом (СКУД), яка дозволяє контролювати та керувати доступом до приміщення підприємства, а також вести облік робочого часу та інтегруватися з іншими системами безпеки.

РОЗДІЛ 3 РОЗРОБКА ТЕХНОЛОГІЇ ЗАХИСТУ БЕЗДРОТОВИХ КАНАЛІВ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

3.1. Розробка схеми корпоративної мережі для дослідження технологій захисту бездротових каналів

IT Technology

Компанія займається наданням IT послуг іншим компаніям, в тому числі у форматі аутсорсингу. У компанії в наявності 10 ПК, з них 5 персональних комп'ютерів і 5 ноутбуків підключені до комутатора Cisco. Також в мережі наявний файловий сервер на якому зберігається корпоративна документація та вебсайт компанії.

В даній схемі використовується обладнання Cisco.

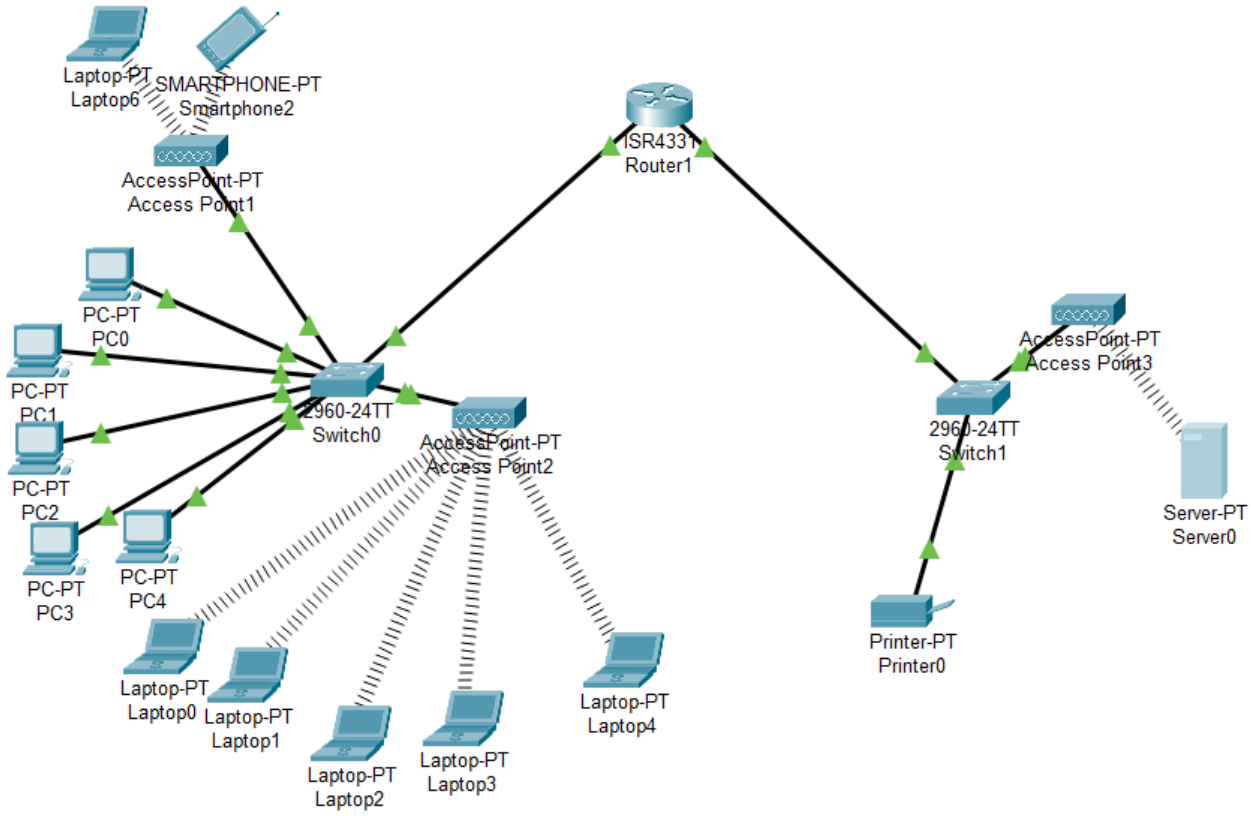


Рис. 3.1 – Схема мережі на підприємстві

3.2. Обґрунтування параметрів налаштувань програмних та технічних пристроїв захисту.

В даній конфігурації використовуються комутатори 2960-24TT та роутер ISR4331.

Конфіг роутера

```
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router1
#прописуємо виключення для ip адрес аби роутер не надавав ці адреси новим або існуючим пристроям
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.11.1
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.2.3
ip dhcp pool VLAN10
#налаштовуємо pool адрес для 10-го влану
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 8.8.8.8
ip dhcp pool VLAN11
#налаштовуємо pool адрес для 11-го влану
network 192.168.11.0 255.255.255.0
default-router 192.168.11.1
dns-server 8.8.8.8
ip dhcp pool LAN1
network 192.168.2.0 255.255.255.0
```

default-router 192.168.2.1

dns-server 8.8.8.8

ip cef

no ipv6 cef

spanning-tree mode pvst

interface GigabitEthernet0/0/0

ip address 192.168.1.1 255.255.255.0

ip access-group 1 out

duplex auto

speed auto

interface GigabitEthernet0/0/0.10

encapsulation dot1Q 10

ip address 192.168.10.1 255.255.255.0

#прописуємо блокування трафіку в VLAN10

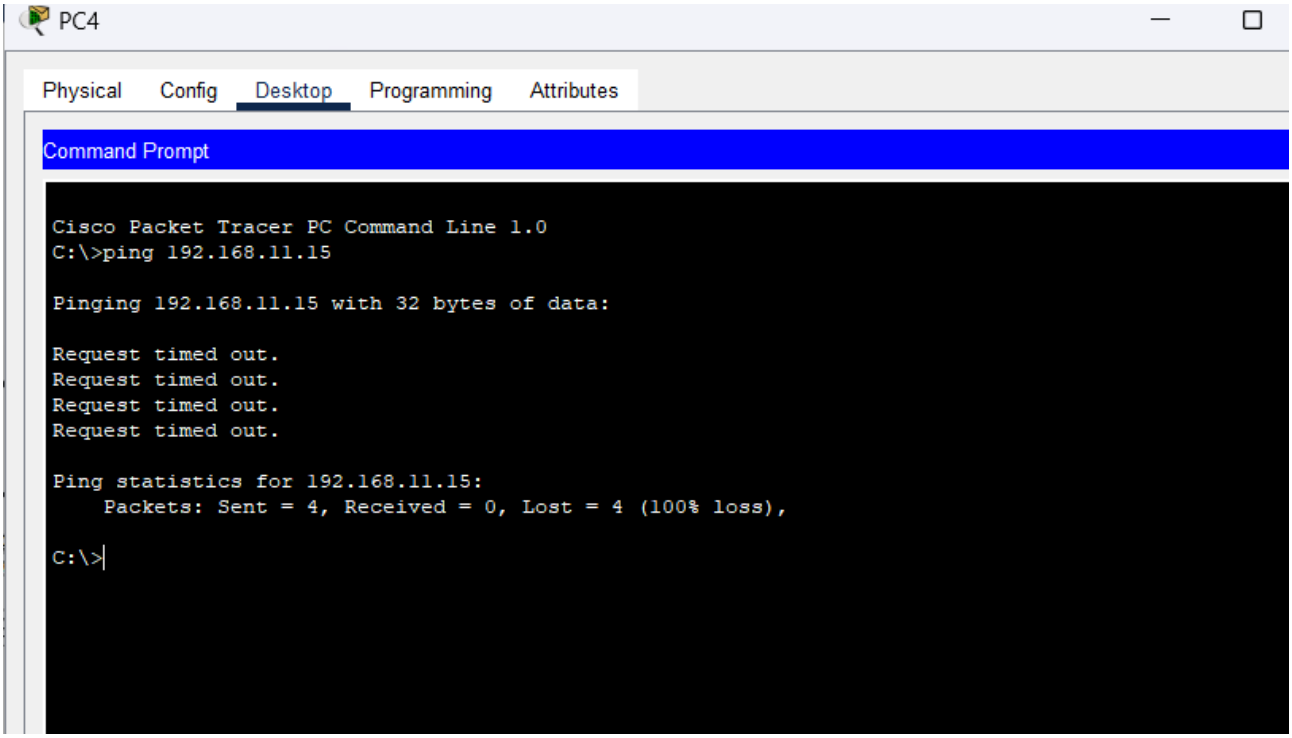


Рис. 3.2 – Блокування трафіку від VLAN10 до VLAN11

ip access-group BLOCK_VLAN_10 in

interface GigabitEthernet0/0/0.11

encapsulation dot1Q 11

ip address 192.168.11.1 255.255.255.0

#прописуємо блокування трафіку у VLAN11

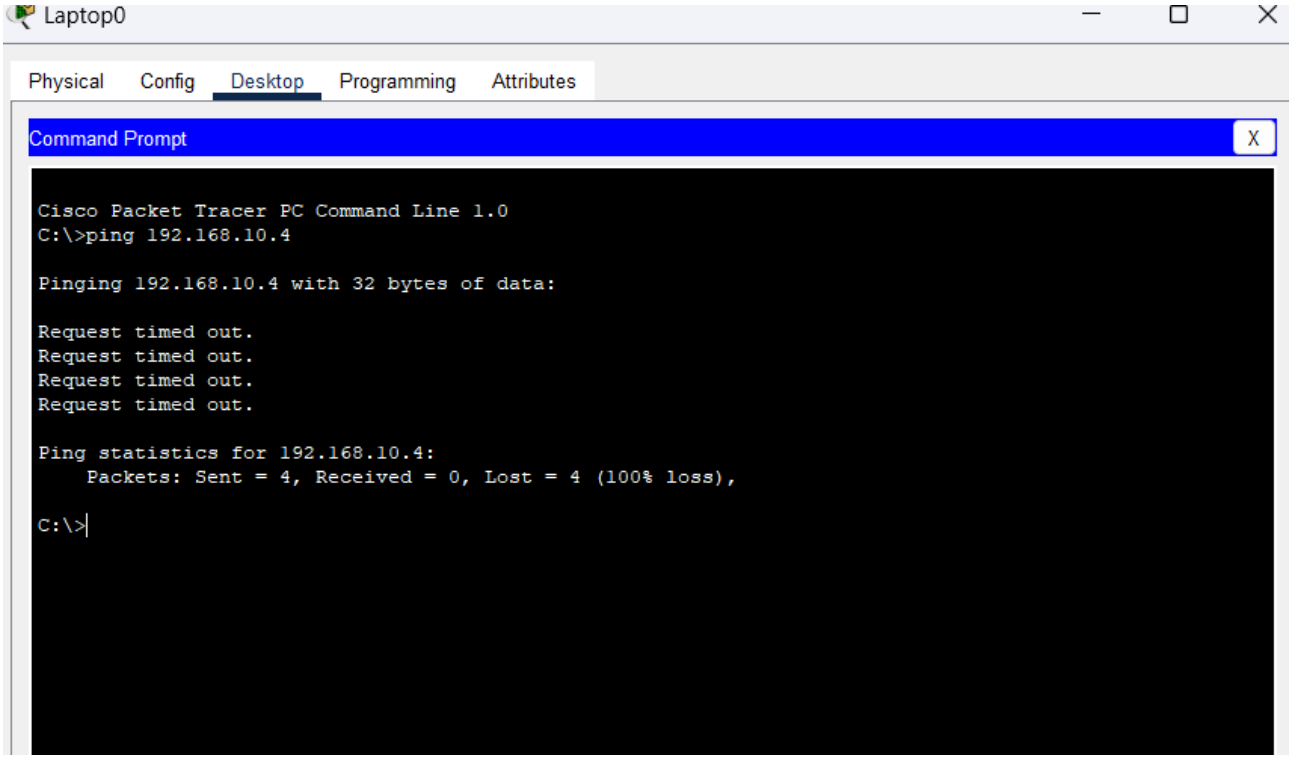


Рис. 3.3 – Блокування трафіку від VLAN11 до VLAN10

ip access-group BLOCK_VLAN_11 in

interface GigabitEthernet0/0/1

ip address 192.168.2.1 255.255.255.0

#прописуємо правило для даного порту

ip access-group 1 in

duplex auto

speed auto

interface GigabitEthernet0/0/2

no ip address

duplex auto

speed auto

shutdown

interface Vlan1

no ip address

shutdown

interface Vlan10

mac-address 000b.becc.1c01

no ip address

interface Vlan11

mac-address 000b.becc.1c02

no ip address

ip classless

ip flow-export version 9

access-list 1 deny host 192.168.2.3

access-list 1 permit any

ip access-list extended BLOCK_VLAN_10

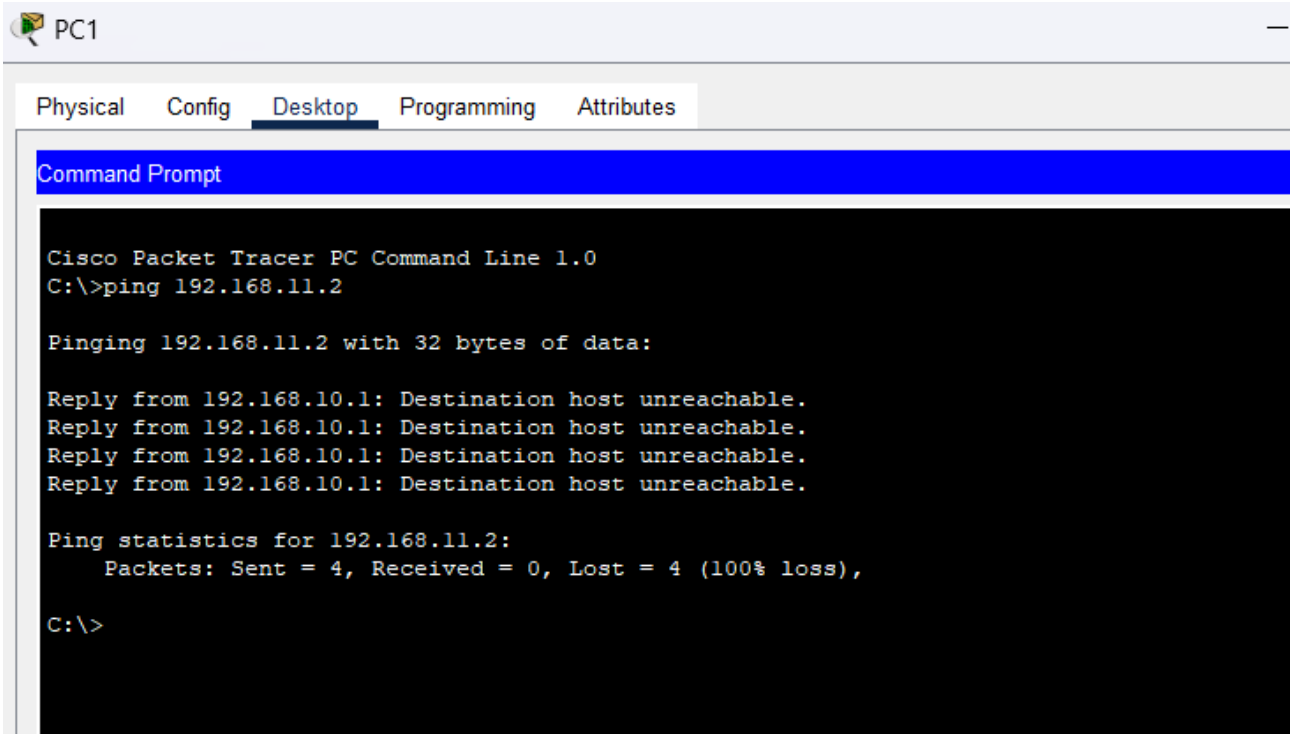


Рис. 3.4 – Недосяжність ПК у VLAN10 до ПК у VLAN11

#відповідне правило для блокування трафіку між вланами

deny ip 192.168.10.0 0.0.0.255 192.168.11.0 0.0.0.255

permit ip any any

ip access-list extended BLOCK_VLAN_11

deny ip 192.168.11.0 0.0.0.255 192.168.10.0 0.0.0.255

permit ip any any

line con 0

line aux 0

line vty 0 4

login

End

Конфіг світча в мережі компів

П’ять ПК(стаціонарні) прив’язані до VLAN10. Решта п’ять ноутбуків прив’язані до VLAN11. Порт GigabitEthernet0/1 налаштований в trunkmode для передачі трафіку між вланами. Нові пристрої приєднуються автоматично до VLAN12

За допомогою access lists обмежений доступ з VLAN10 до VLAN11.

version 15.0

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Switch

spanning-tree mode pvst

spanning-tree extend system-id

interface FastEthernet0/1

switchport access vlan 10

interface FastEthernet0/2

switchport access vlan 10

switchport mode access

interface FastEthernet0/3

switchport access vlan 10
switchport mode access
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
interface FastEthernet0/5
switchport access vlan 10
switchport mode access
interface FastEthernet0/6
switchport access vlan 11
switchport mode acces
interface FastEthernet0/7
switchport access vlan 11
switchport mode access
interface FastEthernet0/8
switchport access vlan 11
switchport mode access
interface FastEthernet0/9
switchport access vlan 11
switchport mode access
interface FastEthernet0/10
switchport access vlan 11
switchport mode access
interface FastEthernet0/11
switchport access vlan 11
switchport mode access
interface FastEthernet0/12
interface FastEthernet0/13

interface FastEthernet0/14

```
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet0/1
switchport mode trunk

interface GigabitEthernet0/2

interface Vlan1
no ip address
shutdown

line con 0
line vty 0 4
login
line vty 5 15
login
End
```

В мережі принтера і сервера:

За допомогою access lists з VLAN10 та VLAN11 обмежений доступ до ip сервера 192.168.2.2. Всі нові пристрої мають змогу з’єднуватись із сервером.

На відміну від принтера сервер має статичну ip адресу аби кожного разу при увімкнені роутера ip адреса сервера не змінювалась.

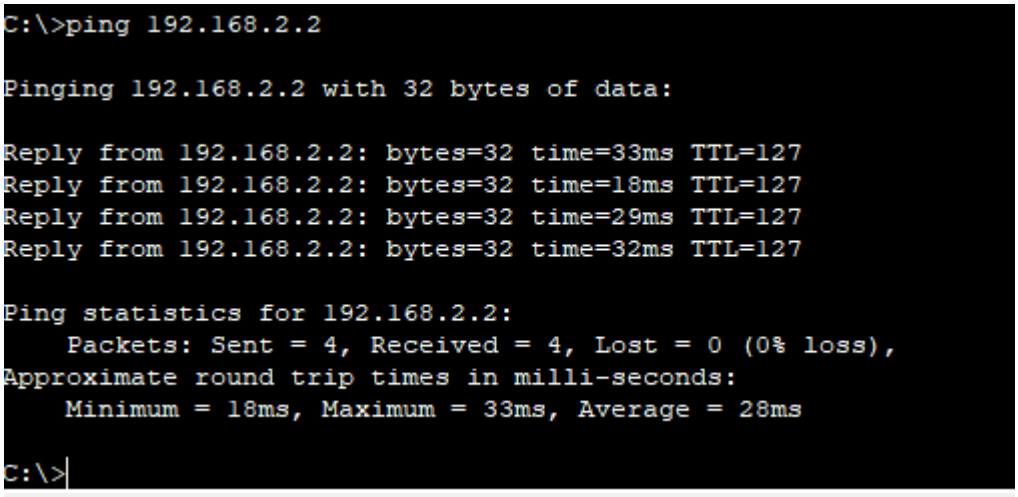


Рис. 3.6 – Пінг сервера

version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname Switch

spanning-tree mode pvst
spanning-tree extend system-id

interface FastEthernet0/1

interface FastEthernet0/2

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5

interface FastEthernet0/6

interface FastEthernet0/7

interface FastEthernet0/8

interface FastEthernet0/9

interface FastEthernet0/10

interface FastEthernet0/11

interface FastEthernet0/12

interface FastEthernet0/13

interface FastEthernet0/14

interface FastEthernet0/15
interface FastEthernet0/16

interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19

```
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24

interface GigabitEthernet0/1
switchport mode trunk

interface GigabitEthernet0/2

interface Vlan1
no ip address
shutdown

line con 0

line vty 0 4
login
line vty 5 15
login
End
```

Надання дозволів на сервері. Аби налаштувати дозволи для читання, записування або видалення файлів на файловому сервері нам необхідно створити користувачів та, відповідно надати їм необхідні права. Я створю для прикладу 2 користувача, один з яких буде керівник, а інший – це будь – який користувач з обмеженими правами.

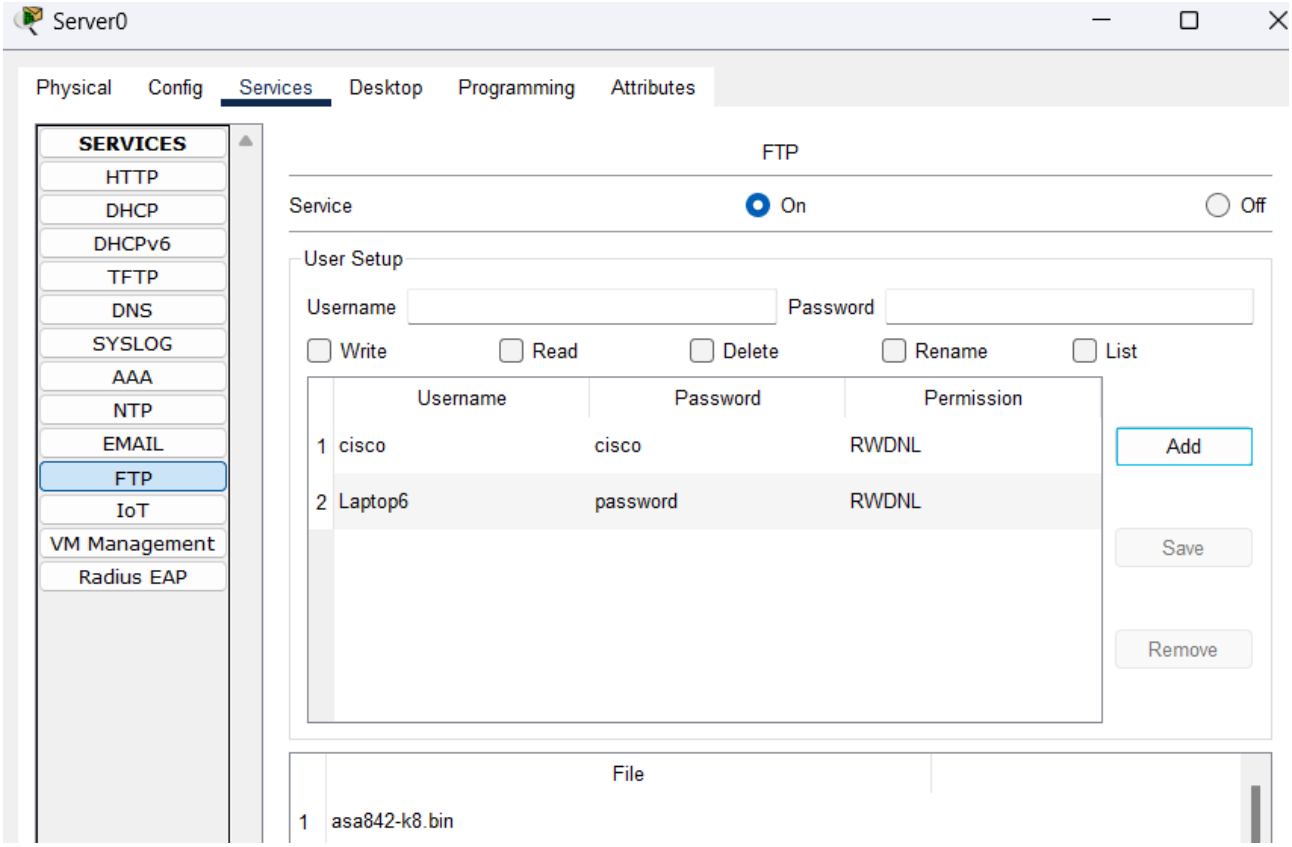


Рис. 3.7 – Створення користувача Laptop6

Користувач з логіном Laptop6 має повні права на даному сервері.

Я створив файл Job.txt та надіслав його на сервер

Рис. 3.8 – Створення текстового файлу Job.txt

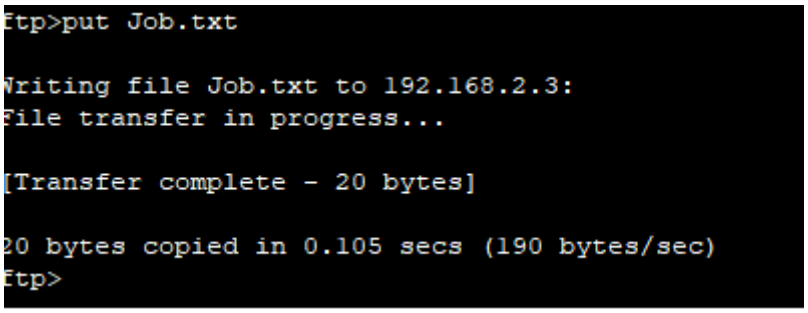


Рис. 3.9 – Надсилання файлу на FTP-сервер

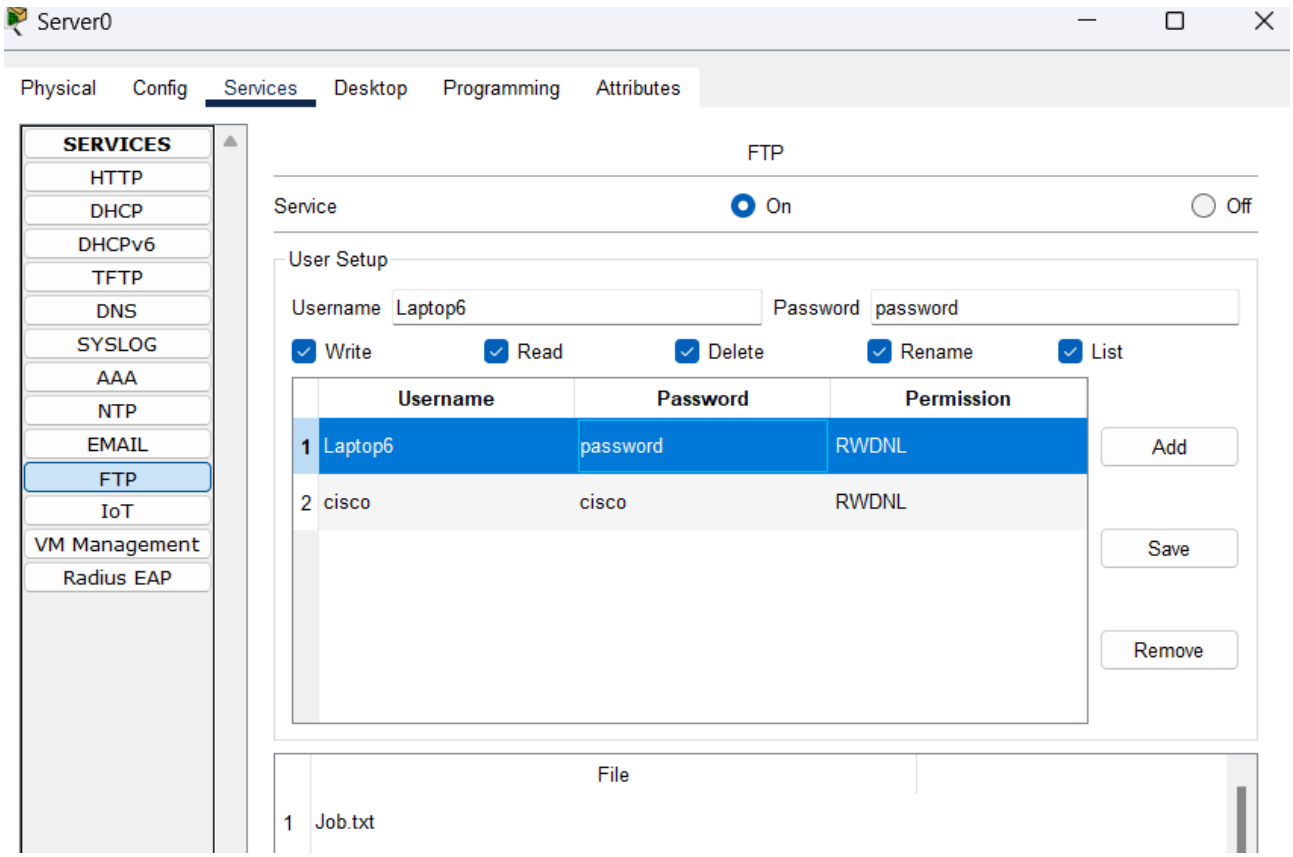


Рис. 3.10 – Переданий файл Job.txt з ПК на сервер

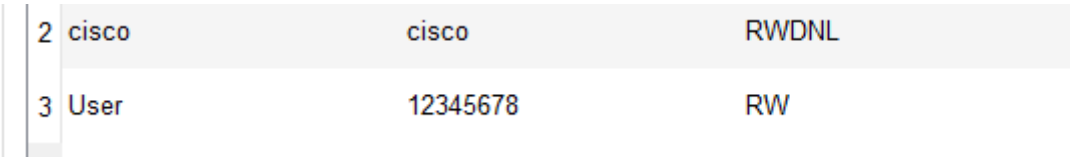


Рис. 3.11 – Створення користувача User з обмеженими правами: лише Read – читання та Write – запис

3.3. Розробка рекомендацій щодо підвищення захищеності системи передачі даних бездротовими каналами на об’єкті інформаційної діяльності

1. Використання WPA2-Enterprise:

- Замість WPA2-Personal використовуйте WPA2-Enterprise з сервером RADIUS для автентифікації користувачів. Це забезпечить централізоване керування доступом та більш надійну автентифікацію.

2. Зміна стандартного пароля:

- Обов'язково змініть стандартний пароль для точки доступу та виберіть надійний пароль, що містить різні типи символів (букви, цифри, спеціальні символи).

3. Приховування SSID:

- Вимкніть трансляцію імені мережі (SSID), щоб зловмисники не могли легко її знайти.

4. Фільтрація MAC-адрес:

- Дозвольте доступ до мережі тільки пристроям з певними MAC-адресами. Це створить додатковий бар'єр для несанкціонованого доступу.

5. Регулярне оновлення прошивки:

- Переконайтеся, що прошивка точки доступу та інших мережевих пристроїв завжди оновлена до останньої версії. Це допоможе усунути відомі вразливості безпеки.

7. Обмеження доступу до мережевих ресурсів:

- Налаштуйте брандмауер та інші засоби безпеки для обмеження доступу до мережевих ресурсів, таких як принтери та сервери, тільки для авторизованих користувачів.

8. Моніторинг мережі:

- Використовуйте системи моніторингу мережі для виявлення підозрілої активності та аномалій. Це допоможе швидко реагувати на потенційні загрози.

Висновки до розділу 3

У третьому розділі кваліфікаційної роботи було проведено розробку технології захисту бездротових каналів на об'єкті інформаційної діяльності. Зокрема, було розроблено схему корпоративної мережі для дослідження технологій захисту бездротових каналів, яка включає в себе використання обладнання Cisco, такого як комутатори 2960-24TT та роутер ISR4331. Було проведено обґрунтування параметрів налаштувань програмних та технічних пристроїв захисту, включаючи налаштування конфігурації роутера та світча в

мережі комп'ютерів, а також налаштування дозволів на сервері.

Крім того, було розроблено рекомендації щодо підвищення захищеності системи передачі даних бездротовими каналами на об'єкті інформаційної діяльності, які включають в себе використання WPA2-Enterprise, зміну стандартного пароля, приховування SSID, фільтрацію MAC-адрес, регулярне оновлення прошивки, обмеження доступу до мережевих ресурсів та моніторинг мережі.

ВИСНОВКИ

В даній кваліфікаційній роботі досліджується проблема захисту корпоративної мережі з бездротовими каналами передачі даних. Проаналізовано уразливості цих каналів, причини можливого витоку інформації та запропоновано шляхи усунення причин.

Для забезпечення високого рівня захисту застосовувались списки доступу ACL, паролі на WiFi та було створено кілька облікових записів з різним рівнем доступу.

Розглянуті технології, що можуть надати підвищений контроль над мережею; такі як VPN, IPsec, SSH і т. д. Особливу увагу приділено технічним засобам захисту інформації: пристрої екранування апаратури, джерела безперебійного живлення апаратури.

Отже, запропоновані кроки для покращення системи безпеки, що включають регулярне оновлення ПЗ, моніторинг мережі, приховування SSID та ін.

ЛІТЕРАТУРА

1. https://elartu.tntu.edu.ua/bitstream/123456789/20131/2/ConfATMT_2016vII_Kovalenko_V_S-Methods_of_protecting_wireless_53.pdf
2. https://ua5.org/protect/1688-rivni-ta-protokoly-informaczijnoyi-bezpeky.html
3. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.)
4. Опорний конспект лекцій з дисципліни «Технічні засоби захисту інформації» для студентів освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні спеціальності 125 «Кібербезпека» / Укл.: Яцків В.В., Кулина С.В. – Тернопіль 2023. – 88 с.
5. https://nordlayer.com/blog/nordlayer-use-case-internet-access-security/
6. https://nordlayer.com/blog/nordlayer-use-case-network-and-resources-access-management/
7. https://nordlayer.com/blog/cyber-security-tips-for-small-business/
8. https://bakotech.ua/ua/vendor/cyberark/
9. https://yubikey.com.ua/shcho-potribno-znaty-biznesu-pro-zakhyst-informatsii-ohliad-tekhnichnykh-zasobiv?srsltid=AfmBOoq88Chk8ugURVN4ZxcvgwuV8mvJJHT50oSjluPILolF5M67LeX0
10. https://e-tk.lntu.edu.ua/mod/resource/view.php?id=3266
11. https://tilsecurity.com/understanding-cybersecurity-assets-protection-significance/#Types_of_Cybersecurity_Assets
12. Dema Matruk Aloun Commercial Cybersecurity
13. https://docs.cyberark.com/pam-self-hosted/11.3/en/content/newui/newui-monitor-sessions.htm
14. Малюк А.А. Інформаційна безпека: Концептуальне і методологічні основи захисту інформації. Навчальний посібник для вузів. –М.: Гаряча лінія – Телеком, 2014. – 280 с.

15. Хорев А.А. Способи і засоби захисту інформації. - М.: МО РФ, 2014. - 316с.

16. Бузов Г. А. Б90 Практичний посібник з виявлення спеціальних технічних засобів несанкціонованого отримання інформації. — М.: Гаряча лінія Телеком, 2015. 240 с; ил.

17. Юдін О. К. Інформаційна безпека держави / О. К. Юдін. — К.: Консум. — 2005. — 576 с.

18. Pankanti Sh., Bolle R.M., Jain A. Biometrics The future of identification. London, 2010. 167 c.

19. https://deps.ua/ua/knowegable-base/reference-information/7824.html

20. https://www.zkteco.com/en/

21. https://books.google.com.ua/books?id=XPC9ucFbddsC&pg=PA1&hl=ru&source=gbs_toc_r&cad=1#v=onepage&q&f=false

22. https://www.imperia.org.ua/catalog/identifikatori

23. Методичні матеріали до дисципліни «Технології виявлення уразливостей та протидії злоякісному програмному забезпеченню».

ДОДАТКИ

Презентаційні матеріали

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

Кваліфікаційна робота здобувача освітнього ступеня «МАГІСТР»

УДОСКОНАЛЕННЯ СИСТЕМИ ПЕРЕДАЧІ ДАНИХ БЕЗДРОТОВИМИ КАНАЛАМИ ОБ’ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Спеціальність: 125 – Кібербезпека та захист інформації
Виконав: Владислав АВРАМЕНКО
Керівник: д.т.н., проф. Віталій САВЧЕНКО

Київ – 2025

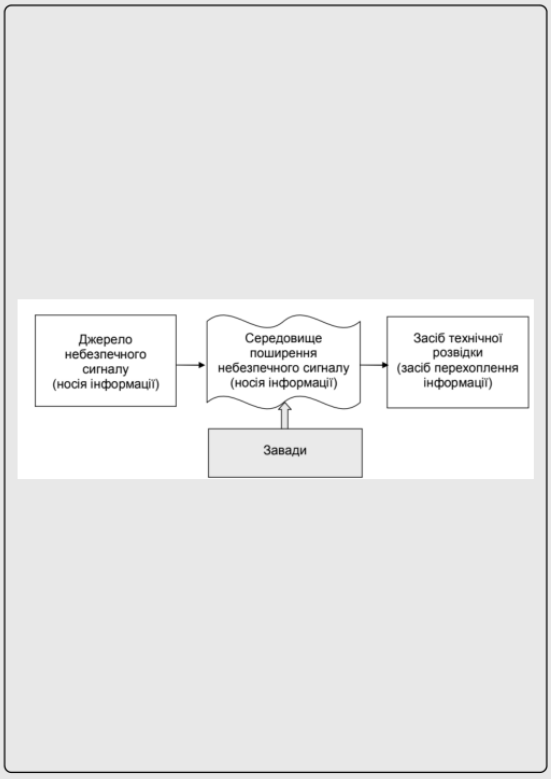
АКТУАЛЬНІСТЬ, МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

- Актуальність зумовлена швидким розвитком інформаційних технологій, поширенням бездротових мереж і зростанням ризиків несанкціонованого доступу.
- Об’єкт дослідження - бездротові канали передачі даних.
- Предмет дослідження - методи та засоби захисту інформації в процесі передавання.
- Мета роботи - розробити правила захисту мережі в бездротовому середовищі.
- Завдання: дослідити бездротові канали, проаналізувати засоби безпеки та розробити технології захисту каналів передачі даних на підприємстві.

ЗДОБУТІ РЕЗУЛЬТАТИ РОБОТИ

1	**РОЗДІЛ 1**	Проаналізовано технічні канали витоку інформації, радіоканал, поняття інформації та базові рівні безпеки.
2	**РОЗДІЛ 2**	Досліджено програмні й апаратні технології захисту бездротових каналів на об’єкті інформаційної діяльності.
3	**РОЗДІЛ 3**	Розроблено схему корпоративної мережі та обґрунтовано параметри налаштувань програмних і технічних засобів захисту.
4	**ВИСНОВКИ**	Запропоновано рекомендації щодо підвищення захищеності системи передачі даних бездротовими каналами.

ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

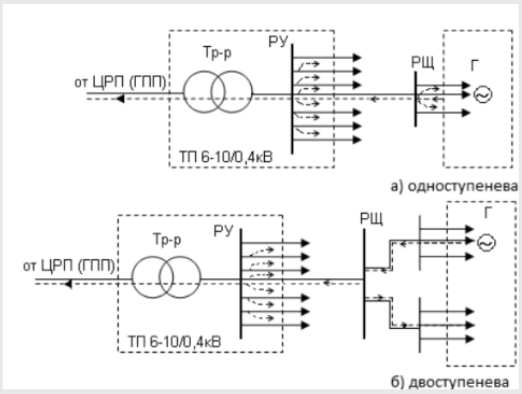


- Канал витоку інформації розглядається як фізичний шлях небезпечного сигналу від джерела конфіденційних даних до засобу технічної розвідки.
- Носіями інформації можуть бути електричний струм, електромагнітне поле, акустичне або вібраційне поле, світло та інші фізичні середовища.
- Захист має враховувати джерело сигналу, середовище поширення, завади та можливості перехоплення.

КЛАСИФІКАЦІЯ ДЖЕРЕЛ УТВОРЕННЯ КАНАЛІВ ВИТОКУ

- Джерелами технічних каналів витоку є акустичні перетворювачі, випромінювачі електромагнітних коливань, паразитні зв’язки та наведення.
- Електричні канали можуть виникати через гальванічні з’єднання, наведення на лінії живлення та заземлення, а також просочування інформаційних сигналів.
- Під час побудови захисту необхідно враховувати як прямі, так і побічні канали витоку.

РАДІОКАНАЛ ЯК ОБ’ЄКТ ЗАХИСТУ



- Радіоканал є високоризиковим технічним каналом, оскільки електромагнітне випромінювання може поширюватися за межі контрольованої зони.
- Для зменшення ризиків застосовують екранування, фільтрацію, зашумлення та правильну організацію електроживлення технічних засобів.
- Важливим є урахування меж контрольованої зони та наявності сторонніх споживачів у ланцюгах живлення.

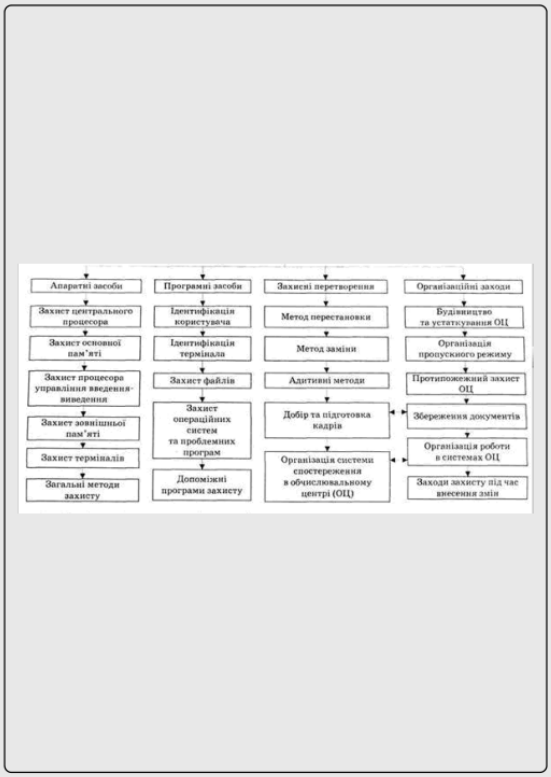
БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ

- Бездротові мережі потребують комплексного захисту, оскільки дані передаються у відкритому радіосередовищі.
- Базові методи захисту включають WEP, WPA та WPA2; найбільш доцільним для практичного використання є WPA2.
- Додатковий захист забезпечують складні паролі, фільтрація MAC-адрес, приховування SSID та контроль доступу до мережевих ресурсів.
- Для аутентифікації користувачів може застосовуватися IEEE 802.1X та EAP.

РІВНІ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ

- Фізична безпека забезпечує захист обладнання, носіїв інформації та приміщень від викрадення, пошкодження або несанкціонованого доступу.
- Мережева безпека спрямована на захист з’єднань, мережевих ресурсів і переданих даних від атак та шкідливої активності.
- Програмна безпека включає антивірусний захист, контроль уразливостей, оновлення програмного забезпечення та запобігання шкідливому ПЗ.
- Організаційні заходи доповнюють технічний захист правилами доступу, регламентами та контролем дій користувачів.

ТЕХНОЛОГІЇ ЗАХИСТУ БЕЗДРОТОВИХ КАНАЛІВ



- Захист бездротових каналів потребує поєднання апаратних засобів, програмних засобів, захисних перетворень та організаційних заходів.
- Програмний захист включає ідентифікацію користувачів і терміналів, захист файлів, операційних систем і проблемних програм.
- Апаратні засоби забезпечують захист пам’яті, процесора, зовнішньої пам’яті, терміналів і центрального процесора.

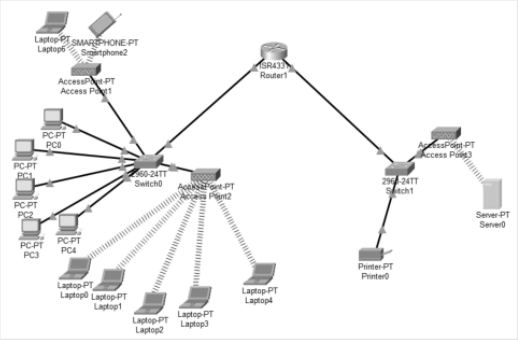
ПРОГРАМНИЙ ЗАХИСТ БЕЗДРОТОВИХ КАНАЛІВ

- У роботі розглянуто застосування VPN, IPsec, SSL, SSH та інших програмних інструментів для захисту переданих даних.
- VPN забезпечує створення захищеного тунелю для доступу до корпоративних ресурсів.
- IPsec дозволяє захищати трафік на мережевому рівні, забезпечуючи конфіденційність, цілісність і автентичність пакетів.
- SSH забезпечує безпечне адміністрування та передавання даних через зашифроване з’єднання.

АПАРАТНИЙ ТА ОРГАНІЗАЦІЙНИЙ ЗАХИСТ

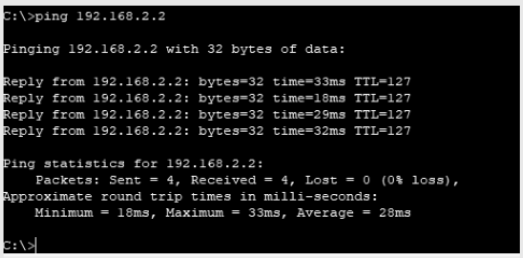
- Класифікація способів захисту охоплює заходи за метою дії, напрямом забезпечення, видом загрози, об’єктами та рівнем охоплення.
- Для об’єкта інформаційної діяльності важливими є екранування апаратури, контроль доступу, захист приміщень та регламентація роботи користувачів.
- Система захисту має поєднувати активні, пасивні, технічні, програмні й організаційні заходи.

СХЕМА КОРПОРАТИВНОЇ МЕРЕЖІ ДЛЯ ДОСЛІДЖЕННЯ



- Розроблено схему корпоративної мережі підприємства з використанням обладнання Cisco.
- У мережі передбачено персональні комп’ютери, ноутбуки, точки доступу, комутатор, маршрутизатор, сервер і принтер.
- Схема дає змогу дослідити налаштування бездротових каналів, сегментацію доступу та обмеження взаємодії між вузлами.

ПРАКТИЧНА ПЕРЕВІРКА НАЛАШТУВАНЬ



- У практичній частині виконано налаштування доступу до серверних ресурсів і перевірку мережевої взаємодії.
- Застосовано ACL та розмежування доступу для різних користувачів і пристроїв у мережі.
- Перевірка зв’язності підтверджує працездатність налаштованої мережевої інфраструктури.

ДЯКУЮ ЗА УВАГУ!

Доповідь підготував здобувач вищої освіти Владислав АВРАМЕНКО

Тема: «Удосконалення системи передачі даних бездротовими каналами»

Київ – 2025