Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі
Назва теми

КРКБ 180127.18.01.03 ПЗ
Шифр

Галузь знань 12 «Інформаційні технології»
Шифр, назва

Спеціальність 125 «Кібербезпека»
Шифр, назва

Освітня програма «Кібербезпека»
Назва

Виконав: студент IV курсу, група КБ–18–1 _____ О.Б.Кажуро
Підпис Ініціали, прізвище

Керівник _____ 14.06.22 В.С. Орленко
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ С.В. Мостовий
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки _____ Ю.П. Кльоц
Підпис Ініціали, прізвище

«21» 06 2022 р.

Хмельницький 2022

Формат	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
А4		1		Завдання на кваліфікаційну роботу	1	
А4		2		Анотація	1	
А4		3	КРКБ.180127.18.01.03 ПЗ	Система захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі Пояснювальна записка	57	
А4		4	КРКБ.180127.18.01.03 Е1	Підключення вимірювальної апаратури каналів витоку інформації Схема структурна	1	
А4		5	КРКБ.180127.18.01.03 Е2	Схема установки для контролю на ЕАП Схема структурна	1	
А4		6	КРКБ.180127.18.01.03 Е3	Зображення перехоплення інформації з каналів витоку Схема структурна	1	
А4		7	КРКБ.180127.18.01.03 Е4	Побудована локальна мережа для захисту каналів витоку Схема структурна	1	

Зм.	Арк.	№ Докум.	Підп.	Дата	КРКБ.180127.18.01.03 ВП		
Розробив		Кажуро О.Б.		14.06	Система захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі Відомість проєкту	Літера	Аркуш 1	Аркушів 2
Перев.		Орленко С.В.		14.06		н		
Н. контр.		Мостовий С.В.		21.06.22		ХНУ, КБ-18-1		
Затв.		Кльоц Ю.П.		21.06.22				

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет *Інформаційних технологій*

Кафедра *кібербезпеки*

Освітній рівень *бакалавр*

Галузь знань *12 «Інформаційні технології»*

Спеціальність *125 «Кібербезпека»*

Освітня програма *освітньо-професійна програма підготовки бакалавра*

ЗАТВЕРДЖУЮ:

Завідувач кафедри Ю.П. Кльоц

"1" 03 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Кажуро Олександру Борисовичу

Прізвище, ім'я, по батькові студента

1. Тема роботи Система захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі

Керівник роботи к.т.н. Орленко В.С.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 1.03.2022 № 18 додаток №10

2. Строк подання студентом роботи на кафедру 6.06.2022 р.

3. Вихідні дані до роботи різновиди інформаційних мереж, каналів витоку інформації, способів несанкціонованого доступу до інформаційних мереж, сучасні методи захисту каналів витоку інформації та несанкціонованого доступу

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Дослідження каналів витоку інформації, методів несанкціонованого доступу в інформаційній мережі. Проєктування системи захисту каналів витоку інформації виявлення несанкціонованого доступу в інформаційній мережі

Втілення апаратної системи захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі та її тестування

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Приклади роботи програмно-апаратної системи

Блок-схеми роботи алгоритмів захисту

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В., ст. викладач		
Антиплагіат	Мостовий С.В., ст. викладач		

7. Дата видачі завдання 1.03.2022

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір та узгодження тематики кваліфікаційної роботи	Січень	-
2	Аналіз предметної області; формування задач і мети аналізу;	Січень	-
3	Робота над розділом 1 – дослідження області темаики та постановка задачі	Лютий	-
4	Робота над розділом 2 – аргументація вибраних засобів для реалізації поставленої задачі		-
5	Робота над розділом 3 – проектування системи захисту	Березень	-
6	Робота над розділом 4 – втілення програмно-апартної системи	Березень-Квітень	-
7	Оформлення пояснювальної записки згідно вимог	Травень	-
8	Попередній захист ВКР		виконано
9	Захист ВКР на засіданні ЕК	Червень 2022 року	виконано

Студент _____ Олександр КАЖУРО
Підпис Ініціали, прізвище

Керівник роботи _____ Вікторія ОРЛЕНКО
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі».

Автор роботи: Кажуро Олександр Борисович.

Керівник роботи: Орленко Вікторія Сергіївна.

Пояснювальна записка: 57 с., 12 рис., 1 дод., 15 джерел.

Графічна частина: 4 плакати.

КАНАЛИ ВИТОКІВ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНА МЕРЕЖА, НЕСАНКЦІОНОВАНИЙ ДОСТУП, СИСТЕМА ЗАХИСТУ.

Метою роботи є проектування системи захисту та її реалізація для виявлення та захисту каналів витоку інформації та несанкціонованого доступу в інформаційній мережах.

Під час реалізації кваліфікаційної роботи було проведено ознайомлення з різновидами інформаційних мереж, їх складових. Досліджено різновиди каналів витоку інформації, методи їх захисту, методи боротьби з несанкціонованим доступом. Також було проведено аналіз існуючих систем захисту каналів витоку інформації та несанкціонованого доступу в інформаційних мережах.

Практична цінність роботи полягає в побудованій системі захисту яка дає змогу виявляти та захищати канали витоку інформації, а також розпізнавати отримання несанкціонованого доступу в інформаційній мережі.

Підпис студента

14.06.2022

Дата

ЗМІСТ

ВСТУП

В сучасному світі захисту інформації потрібно приділяти особливу увагу. Технології стрімко розвиваються, кількість, як персональних данних, так і іншої конфіденційної та важливої інформації, яка потрапляє в мережу надзвичайно зростає. Людство оцифровує більшу частину процесів для спрощення та пришвидшення інших процесів. Проте є люди які навмисно полюють на цю інформацію.

З найдавніших часів будь-яка діяльність людей ґрунтувалася на одержанні і володінні інформацією, тобто на інформаційному забезпеченні. Саме інформація є одним з найважливіших засобів рішення проблем і завдань, як на державному рівні, так і на рівні комерційних організацій і окремих осіб. Але тому що одержання інформації шляхом проведення власних досліджень і створення власних технологій є досить дорогим, те часто вигідніше витратити певну суму на добування вже існуючих відомостей.

Таким чином, інформацію можна розглядати як товар. А бурхливий розвиток техніки, технології і інформатики в останні десятиліття викликало ще більш бурхливий розвиток технічних пристроїв і систем розвідки. У створення пристроїв і систем ведення розвідки завжди вкладалися і вкладаються величезні засоби у всіх розвинених країнах. Сотні фірм активно працюють у цій області.

Серійно виробляються десятки тисяч моделей «шпигунської» техніки. Цьому багато в чому сприяють недоліки правової бази України. Хоча останнім часом органи влади приділяють питанням захисту інформації більше пильна увага. Ця галузь бізнесу давно і стійко зайняла своє місце в загальній системі економіки Заходу і має під собою міцну законодавчу базу у відношенні як юридичних, так і фізичних осіб, тобто строго регламентована і реалізована в чітко налагодженому механізмі виконання.

Не дивлячись на широке впровадження автоматизованих і комп'ютеризованих систем обробки інформації, людська мова залишається одним з найважливіших шляхів інформаційної взаємодії. Більш того, при децентралізації економічної і політичної системи і відповідному збільшенні частки оперативної інформації, що зв'язує в ухваленні рішень людей, важливість мовного обміну зростає. Одночасно посилюється потреба в забезпеченні конфіденційності мовного обміну.

Захист переговорів, що відбуваються в приміщенні або на контрольованій території завжди вимагає фінансових затрат і може створювати певний дискомфорт для персон, що ведуть переговори.

Суб'єкт, який зацікавлений у захищеному обміні інформацією може обрати наступні шляхи:

- підключення до захищеної державної системи зв'язку;
- організація інформаційного обміну мережами зв'язку загального користування із забезпеченням власними силами захисту від перехоплення або спотворення інформації в каналах зв'язку.

В будь-якому випадку однією із задач захисту мовної інформації є забезпечення її захисту від витоку через технічні канали.

У відповідності до сказаного, метою кваліфікаційної роботи є проектування та реалізація системи захисту каналів витоку інформації а також виявлення несанкціонованого доступу в інформаційних мережах.

Тематики розробок на ринку промислового шпигунства охоплюють практично всі сторони життя суспільства, безумовно, орієнтуючись на найбільш фінансово-вигідні.

Згідно сформованої мети, в роботі розглянуто і виконано такі етапи:

- дослідження каналів витоку інформації, їх класифікація;
- аналіз методів захисту каналів витоку інформації в інформаційних мережах, виявлення несанкціонованого доступу;

- визначення технічних засобів та програмного забезпеченя, що буде використуваватися при реалізації системи захисту;
- розгортання системи захисту для виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі;
- реалізація системи логування апаратних пристроїв, підключення та активності в мережі;
- моделювання роботи інформаційної мережі із системою захисту.

1 ДОСЛІДЖЕННЯ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ, ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Поняття інформаційних мереж та їх класифікація

Перед початком створення системи захисту інформаційної мережі потрібно дослідити що таке інформаційна мережа, а також які їх різновиди бувають.

Інформаційна мережа – це сукупність інформаційних систем (ІС) які призначені для обробки, передачі, зберігання інформації.

До складу ІС належать комп’ютери, користувачі, програми пов’язані між собою.

Для комунікації між собою об’єкти використовуються комунікаційні канали.

Особливостями складових інформаційної мережі являється наявність мережевої карти (мережевого адаптера), каналу для передачі даних, а також мережеве програмне забезпечення [1].

Канали зв'язку (data link) утворюються за лініями зв'язку за допомогою фізичних засобів зв’язку та мережевого устаткування. Фізичні засоби зв'язку утворені на основі витих пар, оптичних каналів, коаксіальних кабелів, або ефіру.

За допомогою фізичних каналів комунікаційної мережі і вузлів комутації між взаємодіючими ІС встановлюються логічні канали.

Логічний канал – маршрут між системами, для передачі. Прокладання логічного каналу відбувається по маршруту в одному або декількох

фізичних каналах. Логічний канал можна описати, як маршрут що проходить через фізичні канали і вузли комутації.

Інформація в мережі передається через блоки даних по процедурах обміну між об'єктами. Такі процедури звуться протоколами передачі даних.

Протокол – це певний набір правив, що встановлює формат і процедуру обміну інформацією між двома та більше пристроями.

Завантаження мережі характеризується таким параметром як трафік.

Трафік (traffic) – потік повідомлень в мережі передачі даних. Під ним розуміють кількісну характеристику блоків даних і їх довжини, що проходять в бітах в секунду, у вибраних точках мережі. (потік даних каналом зв'язку, а також об'єм цього потоку в байтах називають трафіком).

На характеристику мережі впливає метод доступу.

Метод доступу – це метод визначення того, який з об'єктів мережі зможе наступним використовувати канал зв'язку і як управляти доступом до каналу зв'язку (кабелю).

Мережа фізично сполучає робочі станції між собою каналами зв'язку за встановленою топологією (по певній структурі).

Топологія – описує фізичні з'єднання в мережі, надаючи інформацію які робочі станції можуть комунікувати між собою. Тип топології визначає такі параметри робочих станцій як працездатність, продуктивність та надійність експлуатації, а також час звернення до файлового сервера. Залежно від топології мережі залежить який метод доступу буде використовуватися.

Архітектура мережі впливає на склад основних елементів.

Архітектура – це концепція, що визначає взаємозв'язок, структуру і функції взаємодії робочих станцій в мережі. Вона передбачає логічну, функціональну і фізичну організацію технічних і програмних засобів

мережі. Архітектура визначає принципи побудови і функціонування апаратного і програмного забезпечення елементів мережі [2].

Завдяки розвитку мереж передачі даних високоефективним способом обробки, передачі, зберігання інформації є – комп'ютерна мережа.

Комп'ютерна мережа – сукупність пристроїв, поєднаних каналами передачі даних, для спільного використання апаратними, програмними та інформаційними ресурсами під управлінням спеціального програмного забезпечення.

Комп'ютерні мережі призначені для:

- швидкого обміну даними між комп'ютерами даних;

- віддаленого керування комп'ютерами;

- спільного доступу до периферійних пристроїв.

Комп'ютери можуть мати різні функції у комп'ютерній мережі. Комп'ютер, який керує розділенням ресурсів мережі, називають сервером (від англ. server – той, хто подає); комп'ютери, що використовують ресурси мережі, називають клієнтами, або робочими станціями.

Класифікація комп'ютерних мереж наведена на рисунку 1.1.

Згідно з пропонованою класифікацією комп'ютерні мережі можна розділити на 4 групи:

- за топологією;

- за територією;

- за способом передачі інформації;

- за розподілом функцій.

За територіальним розміщенням комп'ютерні мережі поділяють ще на кілька груп:

– персональні;

– локальні;

– регіональні та міські;

– глобальні.

Рисунок 1.1 – Класифікація комп’ютерних мереж

Персональні (PAN, Personal Area Network – перекладається як мережа особистого простору, персональна мережа) – належать одній людині, поєднують особисті електроні пристрої: смартфони, планшети, персональні комп’ютери, ноутбуки, комунікатори.

Локальні (LAN, Local Area Network – перекладається як мережа локального простору) – це об’єднання пристроїв, що розташовані на відносно невеликій відстані один від одного, зазвичай у межах одної, кількох сусідніх будівель.

До прикладу, це є мережа підприємства, навчального закладу.

Регіональні та міські (MAN, Metropolitan Area Network – перекладається як мережа міського простору) – це обласні й національні мережі.

До прикладу, www.ukr.net – це є українська національна мережа.

Глобальні (WAN, від англ. Wide Area Network – мережа широкого простору) – поєднують комп'ютерні мережі. Найбільш відомою глобальною мережею є Інтернет [3].

1.2 Дослідження каналів витоку інформації, їх різновиди

Витік інформації – це отримання конфіденційної інформації за межі підприємства, кола осіб кому належала ця інформація. Витік інформації під собою завжди має незаконне отримання доступу до конфіденційної інформації незалежно яким шляхом вона була отримана (явно, таємно, усвідомлено чи випадково). Втрата інформації може відбуватися при наявності каналів витоку чи розголошення.

Канал витоку інформації – відплив цінних данних від закінченого джерела до конкурента або зловмисника чи, в несанкціонованому режимі, до третьої особи [4].

Причиною відпливу інформації до третіх осіб можуть слугувати:

- ігнорування чи незнання правил захисту інформації співробітниками підприємства;

- втрата конфіденційних документів або записів;

- у разі неналежного розподілу доступу до конфіденційної інформації, коли будь–який співробітник може отримати доступ до чутливої інформації;

- при стихійних лихах, можливе часткове виведення систем з ладу, та мимовільний витік інформації.

Треті особи, на відміну від зловмисників, можуть отримати доступ до конфіденційної інформації випадково і вони не зацікавленні в отримані цієї інформації. В результаті отримання конфіденційної інформації третіми особами утворюється випадковий канал витоку інформації.

Зловмисники в свою чергу ставлять собі за мету отримання конфіденційної інформації. Вони навмисно розшукують або утворюють канали витоку інформації.

Такі канали втрати або ж витоку інформації розподіляються на організаційні та технічні.

Основні представлення організаційних каналів витоку інформації:

- працевлаштування на технічну або якусь другорядну посаду в підприємстві яке визначене ціллю для доступу до інформації;

- вливання зловмисником в колектив підприємства, отримання довіри від працівників які мають доступ до конфіденційної інформації;

- кримінальний або грубий метод доступу до інформації, а саме крадіжка будь яких об’єктів що містять конфіденційну інформацію або ж самі крадіжка інформації напряму, шантаж або підкуп працівників;

- отримання інформації випадковим чином, від будь–якого каналу витоку, джерела інформації.

Технічні канали витоку інформації (ТКВІ) – утворюються при застосуванні різних передавачів, приймачів інформації та інших технічних, радіоелектронних, програмних засобів. Такі канали витоку інформації містять в собі найбільший потенціал інформації яку можливо отримати [5]. Структуру ТКВІ можна представити системою передачі інформації (рис. 1.2).

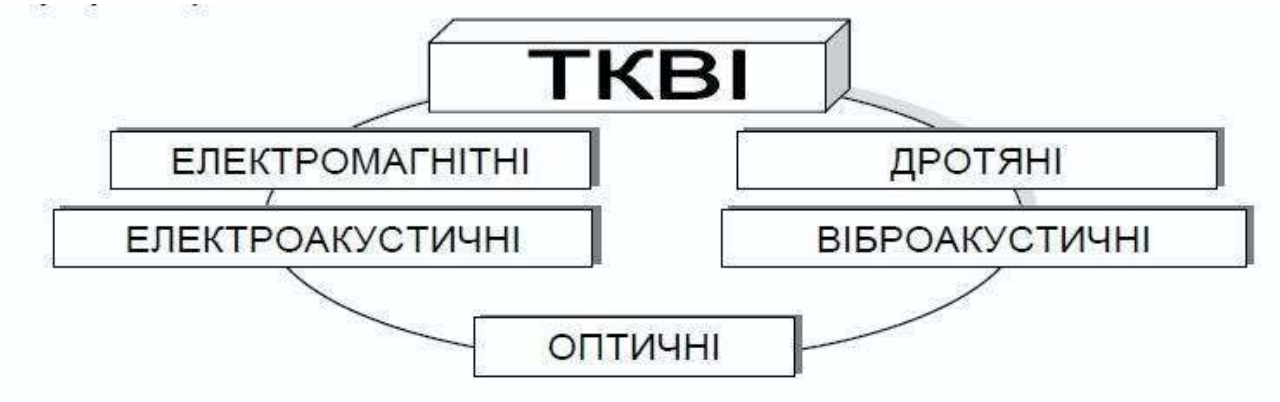

Рисунок 1.2 – Структура ТКВІ

Акустичні канали витоку інформації утворюються за допомогою ряду способів (рис 1.3):

- розповсюдження акустичних коливань в навколишньому середовищі;
- взаємодії звукових коливань з конструкціями будівель та її елементами;
- дії звукових коливань на технічні засоби оброблення інформації.

Середовищем поширення акустичних КВІ являється повітря. Витік акустичної інформації може відбуватися 3 шляхами:

- за рахунок мембранного ефекту;
- пряме розповсюдження через акустичні отвори (тріщини, щілини, отвори);
- шляхом перетворень акустичних коливань, акустичні – віброакустичні – акустичні. При такому перетворенні частина енергії акустичних віброакустичних коливань відбивається в твердих частинках.

Рисунок 1.3 – Утворення акустичних каналів витоку інформації

Схематичне відображення принципу витоку акустичної інформації зображено на рис 1.4.

Прийняти акустичну інформацію можливо, як без засобів технічної розвідки, при випадковому прослуховуванні (тобто без умисних дій, спрямованих на отримання цієї інформації), так і з використанням засобів технічної розвідки.

Це також має враховуватись при створенні системи захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі.

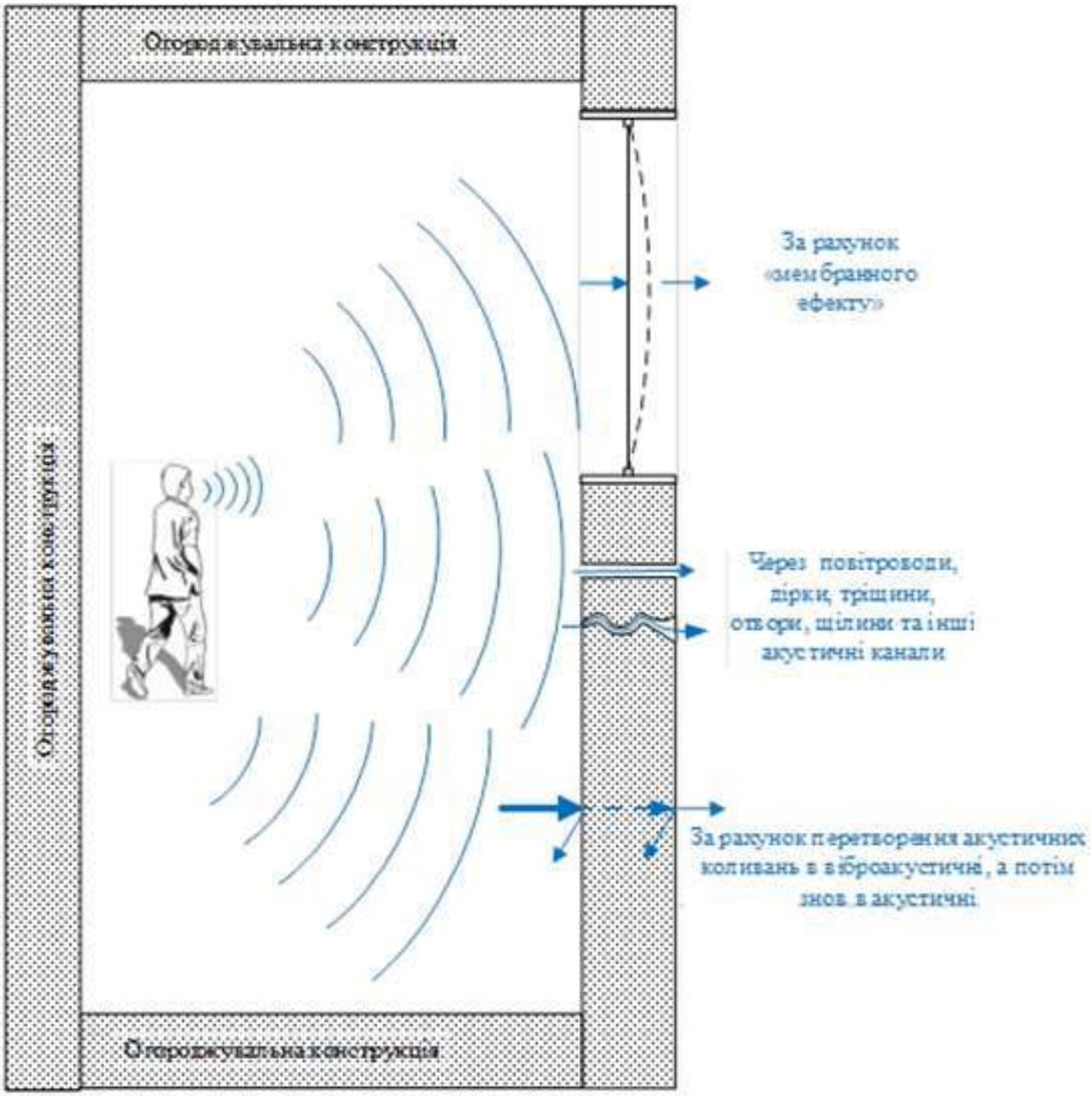

Рисунок 1.4 – Схематичне відображення шляхів витоку акустичної інформації за межі огороджувальної конструкції

Щоб перехопити акустичну інформацію можна використовувати високочутливі мікрофони або спрямовані мікрофони, такі, які мають вузьку діаграму спрямованості (рис 1.5). Перехоплену інформацію можна передавати радіоканалами, оптичними каналами, з'єднувальними лініями,

мережами електроживлення, сторонніми провідниками, інженерними комунікаціями, а також записувати на різноманітні компактні записуючі пристрої (диктофони) тощо [6].

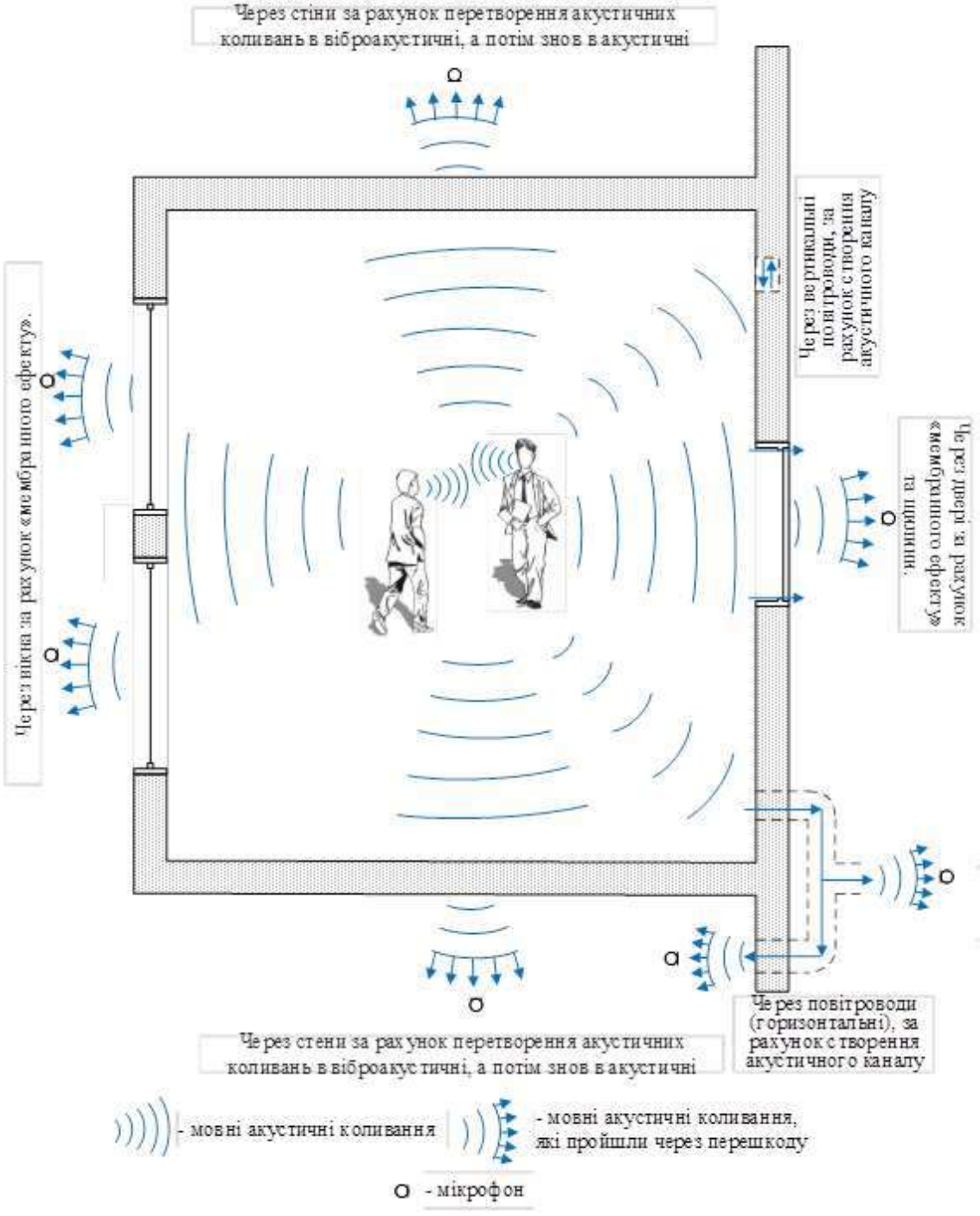

Рисунок 1.5 – Приклад перехоплення мовної інформації акустичних каналів витоку інформації

Віброакустичні канали витоку інформації – середовищем поширення мовної інформації цього типу являються конструкції будівельних приміщень (стіни, вікна, двері, перекриття) і інженерні комунікації. Для отримання такої інформації використовують акселерометри або ще як їх називають контактні мікрофони (рис. 1.6).

Електромагнітні КВІ характеризуються побічним випромінюванням 3 типів:

- електромагнітне (ЕМ) випромінювання елементів технічних засобів обробки інформації (ТЗОІ) (носіями інформації являються напруга, сила струму, електричний струм, частота або фаза якого змінюються за законом інформаційного сигналу);

- ЕМ випромінювання на частотах роботи високочастотних генераторів ТЗОІ (через зовнішній впливів на інформаційний сигнал на елементах генераторів наводяться електричні сигнали, які можуть спричинити незловмисну модуляцію власних коливань на високій частоті та їх випромінення в навколишнє середовище);

- ЕМ випромінювання на частотах самозбудження підсилювачів низької частоти ТЗОІ (самозбудження утворюється в результаті утворення випадкових перетворень негативних зворотніх в паразитні додатні зв’язки, що спричиняє переведення підсилювача з підсилення у режим автогенерування сигналу модульованого інформаційним сигналом).

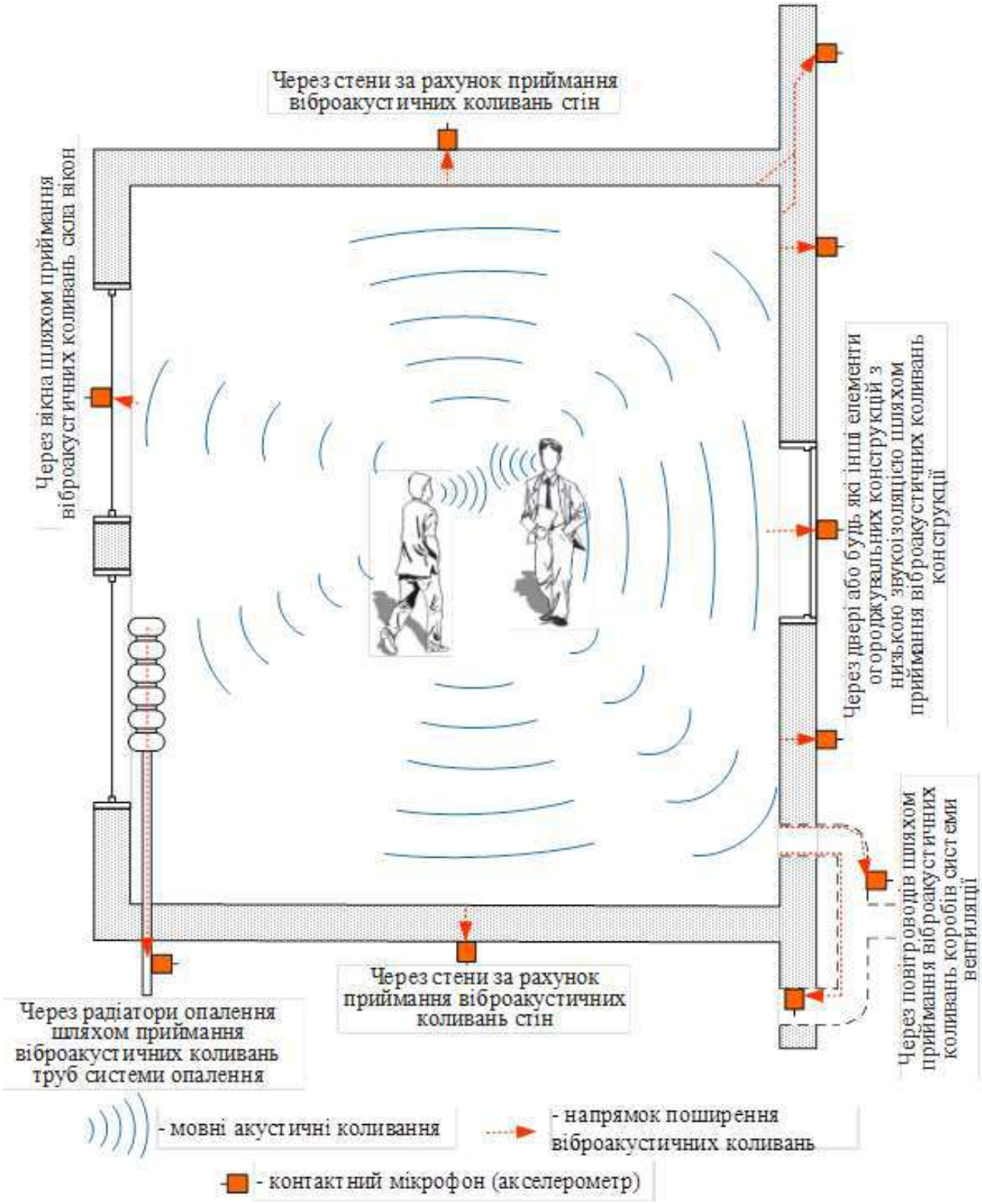

Рисунок 1.6. – Приклад перехоплення мовної інформації віброакустичних каналів витоку інформації.

1.3 Ознайомлення з методами захисту каналів витоку інформації

Для створення системи захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі важливо розглянути методи захисту каналів витоку інформації.

Захист інформації від витоку технічними каналами забезпечують проектно–архітектурними рішеннями, проведенням організаційних та технічних заходів, а також виявленням портативних закладних пристроїв.

Організаційні заходи – це спрямовані на захист інформації заходи, проведення яких не потребує спеціально розроблених технічних засобів.

До основних організаційних заходів відносять:

– залучення до робіт для захисту інформації організацій, що мають ліцензії відповідних органів на діяльність в області технічного захисту інформації (ТЗІ);

– категорування й атестацію об'єктів ТЗПІ та приміщень, виділених для проведення секретних заходів (виділених приміщень) щодо відповідності вимогам забезпечення захисту інформації під час проведення робіт з відомостями відповідного ступеня секретності;

– використання на об'єкті сертифікованих ТЗПІ та ДТЗС;

– встановлення КЗ навколо об'єкта;

– залучення до робіт із монтування апаратури, будування чи реконструкції об'єктів ТЗПІ організацій з відповідними ліцензіями;

– організацію контролю та обмеження доступу на об'єкти ТЗПІ та у виділені приміщення;

– введення територіальних, частотних, енергетичних, просторових і часових обмежень у режимах використання технічних засобів, що підлягають захисту;

– відключення технічних засобів, що мають елементи властивостей електроакустичних перетворювачів, від ліній зв'язку на період проведення секретних заходів.

Технічні заходи – це спрямовані на захист інформації заходи, проведення яких передбачає використання спеціальних технічних засобів, а також реалізацію технічних рішень.

Технічні заходи слугують для закриття каналів витоку інформації за рахунок ослаблення рівня інформаційних сигналів або зменшення відношення сигнал або завада у місцях можливого розміщення ТЗР або їх датчиків до рівнів, що унеможливлюють виділення інформаційних сигналів засобами розвідки. Під час проведення таких заходів використовують активні та пасивні методи.

До технічних заходів із використанням пасивних методів відносять такі:

1. контроль і обмеження доступу на об'єкти ТЗПІ та у виділені приміщення (установлення на об'єктах ТЗПІ та у виділених приміщеннях технічних засобів та систем обмеження і контролю доступу);

2. локалізація випромінювання:

- екранування ТЗПІ та з'єднувальних ліній;
- заземлення ТЗПІ та екранів їх з'єднувальних ліній;
- звукоізолювання виділених приміщень;

3. розв'язування інформаційних сигналів:

- установлення спеціальних захисних засобів типу Граніт, Рікас у ДТЗС із мікрофонним ефектом і таких, що мають вихід за межі КЗ;
- установлення спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалення, водозабезпечення і каналізації, що виходять за межі КЗ;

- установлення автономних або стабілізованих пристроїв електроживлення ТЗПІ (наприклад, мотор–генераторів);

- установлення в мережах електроживлення ТЗПІ, а в лініях освітлювальної та розеткової мережі виділених приміщень – завадоподавляючих фільтрів типу ФП, ФСП, ФС–2.

До технічних заходів із використанням активних методів належать такі:

1. просторове зашумлення (рис 1.7):

- просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних завад відповідними засобами (за умови виявлення та з'ясування частоти випромінювання закладного пристрою або ПЕМВ ТЗПІ);

- створення акустичних і вібраційних завад із використанням генераторів акустичного шуму – шумотронів;

- подавлення працюючих у режимі запису диктофонів за допомогою подавляючих пристроїв.

Рисунок 1.7 – Приклад просторового зашумлення

2. лінійне зашумлення:

- мереж електроживлення та кіл заземлення (рис. 1.8);
- сторонніх дротів та з'єднувальних ліній ДТЗС, що виходять за межі КЗ;

Рисунок 1.8 – Приклад лінійного зашумлення.

3. знешкодження підключених до лінії закладних пристроїв за допомогою спеціальних генераторів імпульсів (випалювачів «жучків»).

Виявити закладні пристрої можна завдяки спеціальним обстеженням (візуальний огляд без залучення технічних засобів) і спеціальним перевіркам (із використанням технічних засобів) об'єктів ТЗПІ та виділених приміщень.

Для виявлення закладних пристроїв використовують:

1. Пасивні методи:

- установлення засобів і систем виявлення лазерного випромінювання (підсвітлення скла на вікнах);
- установлення стаціонарних детекторів диктофонів;
- розшук закладних пристроїв за допомогою індикаторів поля, інтерсепторів, частотомірів, сканувальних приймачів та програмно–апаратних комплексів контролю;

- організація радіоконтролю (постійно або на час проведення конфіденційних заходів) побічних електромагнітних випромінювань ТЗПІ;

2. Активні методи:

- спеціальна перевірка виділених приміщень із використанням нелінійних локаторів;

- спеціальна перевірка виділених приміщень, ТЗПІ та ДТЗІ з використанням рентгенівських комплексів.

1.4 Висновок

В цьому розділі було проведено дослідження інформації за тематикою кваліфікаційної роботи та надано визначення всіх основних понять які допомогли перейти на інший етап кваліфікаційної роботи. Було досліджено канали витоку інформації в інформаційних мережах, на які види та підгрупи вони поділяються. Розглянуто основні чинники утворення каналів витоку інформації та способів витоку інформації через

Також було проаналізовано інформацію щодо інформаційних мереж та суміжних понять, які бувають види інформаційних мереж та їх складовими.

Завдяки проведеному аналізу інформації сформована теоретична база яка буде слугувати підгрунтям для створення системи захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі.

2 ОБГРУНТУВАННЯ ВИБРАНИХ МЕТОДІВ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ

2.1 Опис технологій створення системи захисту від несанкціонованого доступу до інформації

Несанкціонований доступ – доступ до інформації з порушенням службових повноважень працівника, доступ до закритої для громадськості інформації осіб, не уповноважених на доступ до цієї інформації. Так само несанкціонованим доступом іноді називають доступ до інформації особи, яка має право на доступ до цієї інформації понад те, що необхідно для виконання публічних завдань.

Несанкціонований доступ до інформації (НСД) – Доступ до інформації, що порушує правила обмеження доступу за допомогою стандартних засобів, наданих комп'ютерною технікою або автоматизованими системами.

Причини несанкціонованого доступу до інформації (рис. 2.1):

- помилка конфігурації;
- слабкий захист засобів авторизації (крадіжка паролів, смарткарт, фізичний доступ до погано охоронюваного обладнання, доступ до незаблокованих робочих місць для співробітників за відсутності співробітників);
- програмна помилка;
- зловживання службовим становищем (крадіжка резервних копій, копіювання інформації на зовнішніх носіях з правом доступу до інформації);
- слухання каналів зв'язку під час використання незахищених з'єднань всередині локальної мережі;

- використання клавіатури–шпигуна, вірусів і троянів на персональних комп’ютерах для персоналізації.

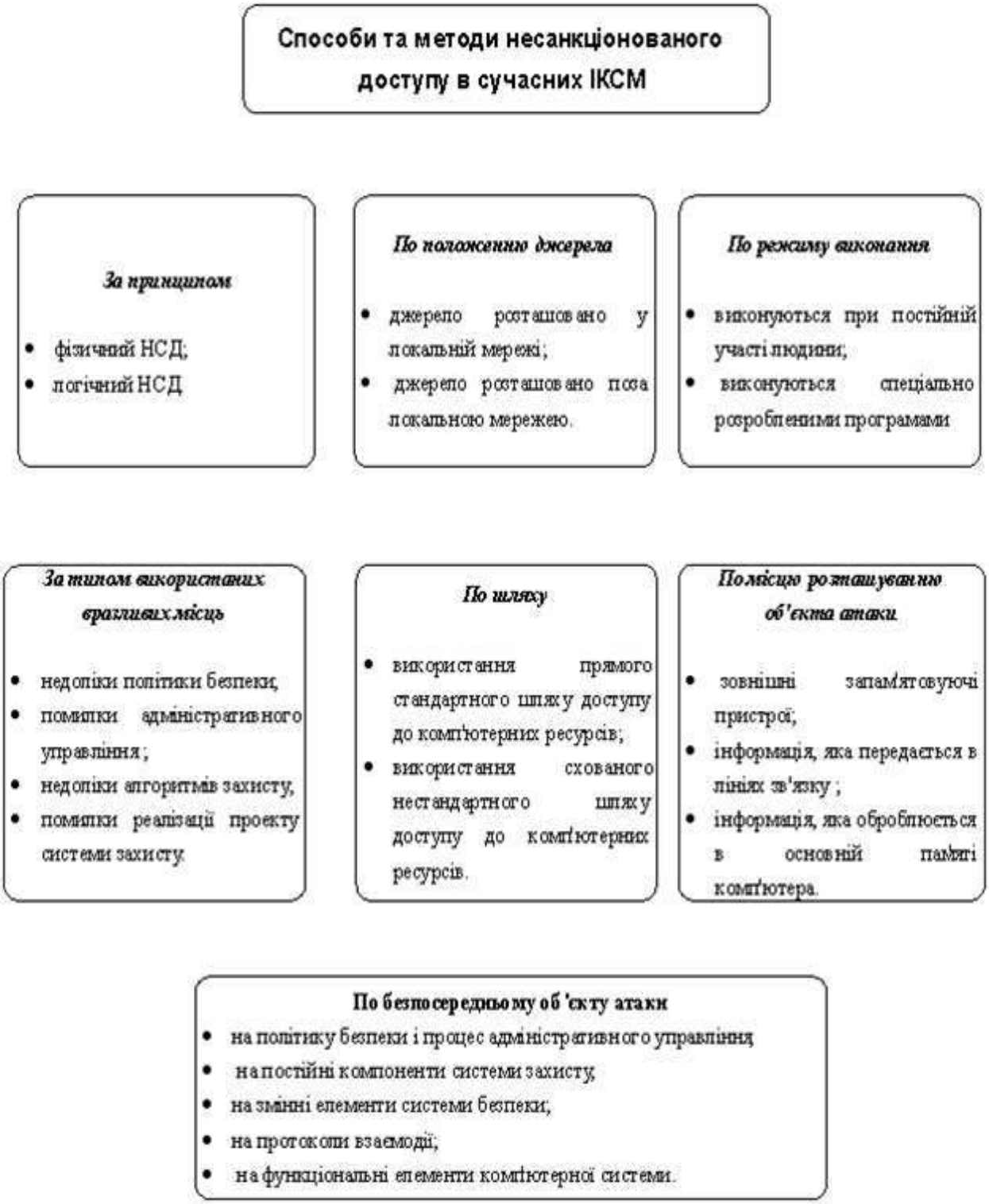

Рисунок 2.1 – Способи та методи НСД в сучасних ІКСМ

Для створення системи захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі розглянемо методи несанкціонованого доступу, які ще мають враховуватись.

З розвитком технологій обробки інформації набули поширення методи несанкціонованого доступу до інформації.

Найпоширенішими є такі методи:

– робота між лініями – підключення до ліній зв'язку та впровадження в комп'ютерну систему шляхом використання пробілів у діях законного користувача;

– відмова в обслуговуванні – несанкціоноване використання комп'ютерної системи в особистих цілях (наприклад, для безкоштовного вирішення своїх завдань) або блокування системи для відмови інших користувачів у наданні послуг. Для реалізації такого зловживання використовуються так звані «жадібні програми» – програми, які можуть монополізувати певний ресурс у системі;

– повторне використання об'єктів – це відновлення та повторне використання зовнішніх системних об'єктів. Прикладом реалізації такого зловживання є видалення файлів з операційної системи. Коли операційна система надсилає повідомлення про те, що файл видалено, це не означає, що інформація в цьому файлі буквально пошкоджена. Інформація, яка була в цьому блоці, не зникає, доки в це місце не буде записана інша інформація. Одним із видів повторного використання об’єктів є робота з комп’ютерним «сміттям».

Під правопорушником взагалі можна вважати особу або групу осіб, які в результаті умисних або ненавмисних дій забезпечує реалізацію загроз інформаційній безпеці.

Щодо права постійного або одноразового доступу на контрольовану територію, порушників можна розділити на два види:

– порушники, які не мають права доступу на контрольовану територію (приміщення) – зовнішні порушники;

– порушники, які мають право доступу до контрольованої території (приміщення) – внутрішні порушники.

Керівний документ РД Державної технічної комісії (ДТЕК) «Концепція захисту комп'ютерної техніки та автоматизованих систем від несанкціонованого доступу до інформації встановлює нижченаведену класифікацію.

Порушники у зазначеній РД класифікуються за рівнем можливостей, наданих їм звичайними фондами АС та СВТ, поділяються на чотири рівні.

– перший рівень визначає найнижчий рівень можливостей діалогу в ас – запуск завдань (програм) із фіксованого набору, що реалізує наперед визначені функції для обробки інформації;

– другий рівень визначається можливістю створювати та запускати власні програми з новими можливостями обробки інформації;

– третій рівень визначається можливістю керувати роботою ас, тобто впливом на базове програмне забезпечення системи та склад і конфігурацію обладнання;

– четвертий рівень визначається повним набором можливостей людей, які займаються проектуванням, впровадженням та ремонтом технічних фондів, аж до включення до складу власних технічних фондів свт з новими функціями обробки інформації.

Таким чином, правопорушник на рівні є експертом з найвищою кваліфікацією, знає все про АС і особливо про систему та засоби її захисту.

Так само модель злочинця може мати таку картину:

– розробник;

– обслуговуючий персонал (системний адміністратор, персонал підтримки ІС);

– користувачі;

– несанкціонований користувач.

Модель порушника інформаційної безпеки може бути доповнена деякими показниками через особливості природи людини. Потенційними порушниками можуть бути працівники об'єкта, що охороняється, які беруть участь у процесах передачі інформації.

Проблема створення системи інформаційної безпеки включає два взаємодоповнюючих завдання:

– розробка системи захисту інформації (синтез);

– оцінка розробленої системи захисту інформації.

Друге завдання вирішується шляхом аналізу її технічних властивостей, щоб визначити, чи відповідає система захисту інформаційному набору вимогам до цих систем. На сьогодні це завдання вирішується практично виключно експертами шляхом сертифікації засобів захисту інформації та сертифікації систем інформаційної безпеки в процесі впровадження.

Методи та засоби захисту інформації наведені на рисунку 2.2.

Дослідимо основний зміст представлених методів захисту інформації, які становлять основу механізмів захисту.

Перешкоди – методи фізичного блокування шляху зловмисника до захищеної інформації (до обладнання, носіїв тощо).

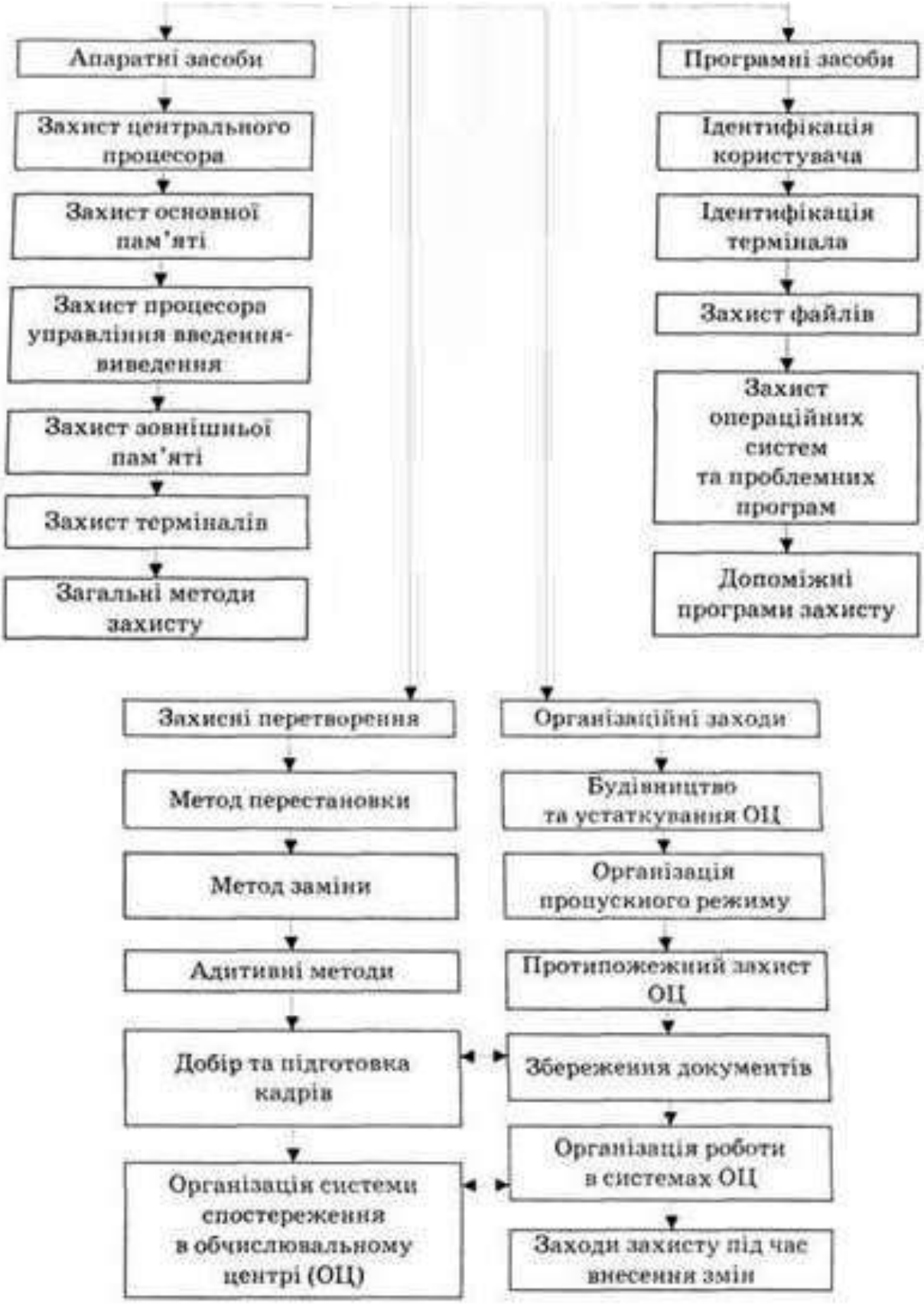

Рисунок 2.2 – методи та засоби захисту інформації

Контроль доступу – метод захисту інформації шляхом регулювання використання всіх ресурсів інформаційної системи даних (елементів баз даних, програмного та апаратного забезпечення). Контроль доступу включає такі функції безпеки:

– ідентифікація користувачів, персоналу та ресурсів системи (присвоєння персонального ідентифікатора кожному об'єкту);

– ідентифікація (встановлення автентичності) об'єкта або суб'єкта пред'явленого їм ідентифікатора;

– перевірка повноважень (перевірка відповідності дня тижня, часу доби, запитуваних ресурсів і процедур встановленим нормам);

– дозвіл та встановлення умов праці в межах встановленого регламенту;

– реєстрація (реєстрація) звернень до захищених ресурсів;

– реєстрація (сигналізація, відключення, затримка роботи, відхилення запиту) у разі спроби несанкціонованих дій.

Маскування – метод захисту інформації шляхом криптографічного закриття.

Цей метод широко використовується за кордоном як для обробки, так і для зберігання інформації, в тому числі на дискетах. Цей метод є єдиним надійним при передачі інформації по довгих каналах зв'язку.

Регулювання – спосіб захисту інформації, що створює такі умови для автоматизованої обробки, зберігання та передачі захищеної інформації, де можливість несанкціонованого доступу до неї буде зведена до мінімуму.

Примус – це спосіб захисту, при якому користувачі та працівники системи змушені дотримуватися правил обробки, передачі та використання інформації, яка захищається під загрозою матеріальної, адміністративної чи кримінальної відповідальності.

Мотивація – це спосіб захисту, який спонукає користувача та працівників системи не порушувати встановлений порядок, дотримуючись усталених морально–етичних норм (як регламентованих, так і неписаних).

Оцінені методи забезпечення безпеки реалізуються на практиці шляхом використання різноманітних засобів захисту, таких як технічні, програмні, організаційні, законодавчі та морально–етичні. Основні засоби захисту, які використовуються для створення механізму безпеки, включають наступне.

2.2 Постановка задачі проектування кваліфікаційної роботи

Базуючись на інформації з поточного та попереднього розділів необхідно скласти постановку задачі кваліфікаційної роботи на тему система захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі.

Отже, в розділі було вияснено що канали витоку інформації становлять досить високу загрозу підприємствам чи окремим людям, якщо не приділяти достатньо уваги кібербезпеці, правилам кібергігієни та решти організаційних питань.

Щоб побудована система захисту працювала максимально ефективно, потрібно використати комплекс рішень, систем та на, для охоплення максимальної кількості каналів витоку. Проте це і дороге задоволення.

Згідно мети роботи, результатом роботи має бути створення системи захисту виявлення каналів витоку інформації в інформаційних мережах. Проєктована система має виконувати такі функції :

- захист каналів витоку інформації;

- виявлення каналів витоку інформації;
- захист інформації від несанкціонованого доступу в інформаційній мережі.

3 ПРОЕКТУВАННЯ СИСТЕМИ ЗАХИСТУ

3.1 Загальний опис інструментів запобігання витоку інформації

На основі інформації знайденої та дослідженої в попередніх розділах, відповідно до теми даної кваліфікаційної роботи та суміжної предметної області, можемо ще раз виділити такі канали витоку інформації:

- технічні КВІ;
- організаційні КВІ;

Для запобігання витоку інформації технічними каналами використовуються різноманітні програмні, апаратні та комплексні програмно–апаратні засоби, зокрема:

- Базальт–2ГС.(рис. 3.1) Прилад захищає об’єкти від витоку мовної інформації через лінію електропередач. Принцип роботи полягає в подавлені сигналів прослуховуючих та передавальних пристроїв, що можуть бути під’єднані до електромережі шляхом генерування псевдовипадкової завади сигналів акустичних перетворень [8].
- Базальт–3 (рис 3.2) один з популярних приладів, який призначений щоб захищати телефонний зв’язок методом фільтрування та нелінійної комутації сигналів можливих акустичних перетворень.
- Базальт–4ГА (рис. 3.3) Прилад що надає змогу захищати як акустоелектричні канали витоку інформації так і віброакустичні. Являється двоканальним генератором електрочного шуму.

Рисунок 3.1 – Приклад приладу захисту лінії електропередач

Рисунок 3.2 – Прилад захисту телефоного зв’язку

Рисунок 3.3 – Приклад прилладу для захисту акустоелектричних та віброакустичних каналів витоку

Для запобігання витоку інформації організаційними каналами використовуються різноманітні організаційні заходи, програмні, апаратні та комплексні програмно–апаратні засоби, зокрема:

- Складання політики безпеки для підприємства, подальше ознайомлення працівників з набором правил кібергігієни. Проведення регулярних зібрань на рахунок вдосконалення
- Захист інтелектуальної власності належним чином
- Аналіз конкурентів на предмет недобросовісної конкуренції
- Заходи щодо протидії будь–яких видів шпигнуства

3.2 Планування захисних заходів щодо уникнення несанкціонованого доступу в інформаційних мережах

Для захисту від несанкціонованого доступу, що призводить до дестабілізуючих наслідків, необхідно використовувати технічні засоби

захисту інформації та дотримуватися правил безпеки.

На етапі організаційних заходів необхідно:

- інший перелік інформації з обмеженим доступом, що підлягає технічному захисту (визначається власником інформації відповідно до чинного законодавства України);

- підтримувати розробку та впровадження захисних заходів для врахування матеріальних чи інших збитків, які могли бути завдані внаслідок можливої несправності або витоку технічних каналів; встановити перелік окремих приміщень, де не допускається здійснення загроз та витоку інформації з обмеженим доступом;

- вибір переліку технічних засобів, які будуть використовуватися як ОТЗ (основні технічні засоби);

- додаткові технічні засоби, застосування яких не виправдано потребою в обслуговуванні та виробництві та які підлягають розбиранню;

- наявність задіяного та невикористаного повітря, ґрунту, стіни та прокладених у прихованій каналізації кабелів, ланцюгів та проводів, що виходять за межі окремих приміщень;

- послуги демонтованої системи, які потребують переобладнання кабельних мереж, ланцюгів живлення, заземлення або встановлення в них пристроїв захисту.

Основними заходами є підготовчі технічні заходи для блокування електроакустичних перетворювачів і лінійних з'єднань, що виходять за межі окремих просторів. Блокування ліній зв'язку можна використовувати такими способами:

– від'єднання ліній зв'язку для ЦПІ та СДС або встановлення найпростіших схем захисту;

демонтаж окремих технічних засобів, кабелів, ланцюгів, проводів, що працюють за межами окремих приміщень;

– видалення окремих елементів технічними засобами за межі окремих приміщень, які можуть бути джерелом каналу витоку інформації.

Блокування можливих каналів витоку ISOD у стаціонарних і нульових телефонних системах може бути використано:

– відключення (звичайних) телефонних ліній; встановлення в ланцюг телефону невідключеної розетки для тимчасового відключення;

– установка найпростіших захисних пристроїв.

Запобігання витоку через існуючі системи передачі гучномовців та директорського зв'язку за допомогою таких захисних заходів:

– встановлення вимикачів у витяжних штангах; установка на вході динаміків перемикачів (реле), які дозволяють розірвати ланцюг по двох проводах;

– забезпечує можливість відключення живлення мікрофонних підсилювачів;

– установка найпростіших захисних пристроїв.

Захист від витоку через мережу мовлення, що виходить за межі радіо, приміщення, можна забезпечити шляхом:

– відключення колонок по двох проводах; в тому числі найпростіші пристрої захисту. Для послуги сповіщення необхідно призначити наступні абонентські одиниці поза кімнатою;

– ланцюги для цих пристроїв необхідно прокладати моніторним кабелем. Запобігання витоку через системи пожежної та охоронної сигналізації. Відключення датчиків пожежної та охоронної сигналізації на період важливих заходів, які включають або використовують датчики, які не потребують спеціального захисту.

Блокування витоків через систему електронної оргтехніки та кондиціонування повітря може бути забезпечено такими заходами: розміщенням цих систем всередині контрольованої зони без виносу окремих компонентів за її межі; електропостачання систем від підстанції, що знаходиться в межах підконтрольної території. Якщо перераховані вище умови не дотримані, систему необхідно підключити до електромережі через два дроти.

Захист від витоків через електропостачання та живлення побутових ланцюгів забезпечується шляхом підключення цих ланцюгів до окремого фідера на трансформаторі до трансформаторної станції, до підключення якого сторонні користувачі не мають права. У разі невиконання цієї вимоги електроприлади на період закритої діяльності повинні бути включені в ланцюги електроживлення.

Технічні заходи є основним етапом роботи з технічним захистом і полягають у монтажі УТС, що дає ЦПІ та ВТСС агрегатів ТЗІ. При виборі, монтажі, заміні технічного обладнання слід керуватися паспортами, що додаються, технічними описами, інструкціями з експлуатації, рекомендаціями з монтажу, монтажу та експлуатації. УТС слід, якщо це можливо, розташувати ближче до центру будинку або до більшої частини контрольованої зони. Складні елементи УТС слід розміщувати в одній кімнаті або в суміжних. Якщо виконання цих вимог неможливе, необхідно вжити додаткових заходів захисту:

– встановити високочастотну АТС в екранованому приміщенні (камеру);

– встановлювати спеціальні фільтри та пристрої в незахищених каналах зв'язку, лініях, проводах і кабелях;

– прокладання проводів і кабелів в екрануючих конструкціях; зменшити довжину паралельних прокладок кабелів і проводів до різних систем з проводами і кабелями, що несуть ІСО;

– виконувати технічні заходи щодо захисту ІСОД від витоку через заземлення та ланцюги живлення.

До засобів технічного захисту належать:

– фільтри–обмежувачі та спеціальні пристрої захисту абонентів для блокування витоку мовлення ISOD по двопровідним телефонним лініям, системам директора та диспетчерської;

– пристрій захисту абонентських однопрограмних динаміків для блокування витоку мовлення ISOD по лініях радіомовлення;

– мережеві фільтри для блокування витоку мовлення ISOD на ланцюгах змінного (прямого) живлення;

– фільтри захисту лінійні (високочастотні) для встановлення в лініях з пристроями телеграфного (телеккодового) зв'язку;

– лінійні генератори шуму; генератори просторових шумів;

– екрановані камери спеціальної розробки.

Рекомендується використовувати побутові пристрої, сумісні із захисними пристроями передачі ISOD. Іноземні телефони можна використовувати за умови спеціального дослідження та позитивного висновку компетентних організацій в системі ТСІ про їх сумісність із охоронними пристроями.

Вибір способів і способів захисту елементів ЦПІ та ВТСС, що мають мікрофонний ефект, залежить від величини їх вхідного опору на частоті 1 кГц. Рекомендується від'єднувати елементи з вхідним опором менше 600 Ом (головки динаміків, двигуни вентиляторів, трансформатори тощо) на два дроти або встановлювати в розімкнений ланцюг пристрою захисту з високим

вихідним опором для зниження до мінімальної інформаційної потужності. компонент.

Елементи з високим вхідним опором (електричні дзвінки, телефонні капсули, електромагнітні реле) рекомендується не тільки відключати від ланцюгів, але і замикати на низький опір або замикати накоротко, щоб зменшити електричне поле від цих елементів за рахунок акустичної напруги.

Слід пам'ятати, що обраний спосіб захисту не повинен заважати працездатності технічного засобу та погіршувати його технічні параметри. Високочастотні автогенератори, підсилювачі (мікрофон, прийом, передача, гучномовець) та інші пристрої, що містять активні компоненти, рекомендується відключати від шнурів живлення в «режимі очікування» або «очікування дзвінка».

Рекомендується захистити ISOD від витоку з кабелів і проводів шляхом:

– використання екрануючих конструкцій;
– роздільне прокладання кабелів УТС, ЦПІ та ВТСС.

При неможливості виконання вимог щодо розділення силових кабелів, ОТС, ЦПІ та ВТСС живлення останніх має здійснюватися або екранованими кабелями, або від систем розділення, або через лінійні фільтри. Утворення петель і контурів кабельних ліній не допускається. Кабельні траси різного призначення рекомендується перетинати під прямим кутом один до одного.

Напруга та струм живлення до UTS повинні бути стабілізовані для нормальних умов експлуатації для UTS та безпечних стандартів безпеки. У ланцюгах випрямлячів живлення необхідно встановлювати фільтри нижніх частот. Фільтри необхідно фільтрувати через симетричні та асиметричні шляхи поширення.

Необхідно забезпечити відключення електромережі від джерела живлення УТС у разі втрати напруги в мережі, у разі відхилення параметрів електропостачання від норм, зазначених у технічних умовах, та при появі несправностей у ланцюгах електроживлення.

Усі металеві конструкції УТС (шафи, панелі, з'єднувальні корпуси та металеві оболонки кабелів) повинні бути заземлені. Заземлення УТС повинно виконуватися від загального контуру заземлення, розташованого в межах контрольованої території, з опором заземлення на постійному струмі відповідно до вимог стандартів. Система заземлення повинна бути однаковою для всіх елементів УТС і бути побудована на радіальній формі. Дисплеї кабельних ліній UTS за межами контрольованої зони повинні бути заземлені в місцях перетину загального контуру заземлення в одній точці, щоб виключити можливість появи шлейфів на моніторі та корпусах.

Ось досить умовна класифікація пошукових підрозділів для засобів технічної розвідки:

1. Блоки для пошуку активного тину, тобто для дослідження реакції на будь–який вплив:

– нелінійні локатори – для дослідження реакції на вплив електромагнітних полів;

– рентгенометри – опромінення за допомогою рентгенівського обладнання;

– магнітно–резонансні локатори, що використовують явище орієнтації молекул у магнітному полі; акустичні коректори.

2. Пошукові пристрої пасивного типу:

– металошукачі;

– теплові камери;

прилади та системи пошуку електромагнітного випромінювання;

блок пошуку для зміни параметрів телефонної лінії (напруга, індуктивність, ємність, добротність);

– пошукові пристрої але зміни магнітного поля (детектори реєструючого обладнання).

З різних причин не всі перераховані технічні засоби знайшли практичне застосування. Наприклад, рентгенівське обладнання є дуже дорогим і громіздким і використовується виключно спеціальними державними організаціями. Те ж саме, але в меншій мірі, стосується магнітно–резонансних локаторів.

Теплові камери, пристрої, які можуть виявляти різницю температур, що вимірюється в сотнях градусів, можуть виявляти теплову потужність близько 1 мкВт. Ці відносно недорогі пристрої, до складу яких входить комп'ютер, можуть бути дуже ефективними та універсальними у пошуку технічних засобів комерційної розвідки, оскільки всі технічні засоби при роботі виділяють тепло в навколишній простір.

Швидше за все, поява ринку подібних пристроїв – справа найближчого майбутнього. Зупинимося на пристроях, які порівняно широко представлені на вітчизняному ринку.

Перш за все, це пасивні пошукові блоки, засновані на дослідженні приймачів електромагнітного випромінювання, сканерів, шумомірів, детекторів інфрачервоного випромінювання, аналізаторів спектру, частотомірів.

Далі перейдемо до створення системи захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі за умовами завдання.

3.3 Проектування системи захисту виявлення каналів витоку інформації

На підставі дослідженої та коротко описаної у попередньому підрозділі інформації, перейдемо до безпосереднього проектування системи захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі.

Проектування відбуватиметься у відповідності до сформованої мети та згідно до поставлених задач кваліфікаційної роботи.

Для виконання поставленого завдання та безпосереднього створення системи захисту виявлення каналів витоку інформації, з її подальшою програмно–апаратною реалізацією, ми притримуватимемось наступного алгоритму дій:

- проаналізуємо можливі канали витоку інформації;
- проаналізуємо ефективні засоби їх усунення на прикладі конкретного середовища;
- теоретично змоделюємо комплексну систему захисту, на основі окремих рішень;
- підготуємо спроектовану систему до практичної реалізації.

У попередніх підрозділах нами було виділено основні канали витоку інформації, а саме ТКВІ та Організаційні КВІ.

Це стане основою нашої системи захисту виявлення каналів витоку інформації, оскільки ефективний захист кожного з цих каналів окремо та подальше їх комплексне поєднання гарантуватиме достатньо високий рівень захищеності.

Для більш ефективного та всебічного захисту, спроектовані системи запобігання витоку інформації ми об’єднаємо в єдину комплексну систему.

Для якісного функціонування даної системи ми самостійно розробимо програмну утиліту в ході практичної реалізації. Дана утиліта збиратиме, оброблятиме, частково аналізуватиме та логуватиме дані з різноманітних пристроїв, групуючи необхідну інформацію в одному місці.

Це дозволить більш швидко та якісно реагувати на загрози що виникають у мережі, висвітлюватиме оперативну обстановку та даватиме можливість в реальному часі контролювати стан речей.

Таким чином ми теоретично спроектували комплексну систему захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі.

3.4 Висновок

У цьому розділі нами було спроектовано комплексну систему захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі.

Дана система в повній мірі задовольняє усі поставлені перед нею вимоги, а програмна утиліта, що буде створена в подальшій реалізації зробить окремі спроектовані системи захисту цілісною структурою, що комплексно виконуватиме поставленні завдання, висвітлюватиме оперативну обстановку та даватиме можливість в реальному часі контролювати стан речей.

Керуючись напрацюваннями, описаними у даному розділі, перейдемо до безпосередньої програмно–апаратної реалізації спроектованої системи захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі.

4 РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ВИЯВЛЕННЯ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ ТА НЕСАНКЦІОНОВАНОГО ДОСТУПУ В ІНФОРМАЦІЙНІЙ МЕРЕЖІ

4.1 Визначення інструментів та технологій, що будуть використані в процесі реалізації системи захисту

На основі інформації із попередніх розділів, а також з використанням напрацювань у розробці системи захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі, перейдемо до її безпосередньої реалізації.

Перед початком опису технічних та програмних рішень визначимось з технологіями використаними під час розробки системи проектування, а саме:

Cisco Packet Tracer, як можна зрозуміти з назви, є інструментом, створеним Cisco. Цей інструмент забезпечує моделювання мережі для відпрацювання мереж різної складності, як простих так і складних мереж.

Оскільки протоколи, на данний момент, реалізовані тільки лиш програмним методом, цей інструмент не такий ефективний, як апаратні маршрутизатори або комутатори. Проте цікаво, що цей інструмент містить в собі не тільки продукти від компанії Cisco, але й велику кількість інших мережевих пристроїв інших підприємств та компаній.

Використання Packet Tracer як інструменту широко заохочується, оскільки він являється частиною навчальної програми, як–от CCNA, CCENT, де факультети користуються Packet Trace для демонстрації технічних концепцій та мережевих систем. Студенти отримують та

виконують завдання за допомогою цього інструменту, працюючи як самостійно так і в команді.

Інженери вважають хорошою практикою тестувати будь–які протоколи на Cisco Packet Tracer перед тим як їх впровадити в реальну мережу. Крім того, інженери, які хотіли б розгорнути будь–які зміни у виробничій мережі, вважають за краще використовувати Cisco Packet Tracer, щоб спершу впевнитися в коректної роботи оновлення, перевірити необхідні зміни і тільки після цього приступити до розгортання, якщо і тільки якщо все працює, як очікувалося.

Це спрощує роботу інженерів, надаючи їм можливість додавати або видаляти імітовані мережеві пристрої за допомогою інтерфейсу комбінованих інтерфейсів, а саме командного рядка (рис. 4.1) та інтерфейсу користувача з перетягуванням (рис. 4.2).

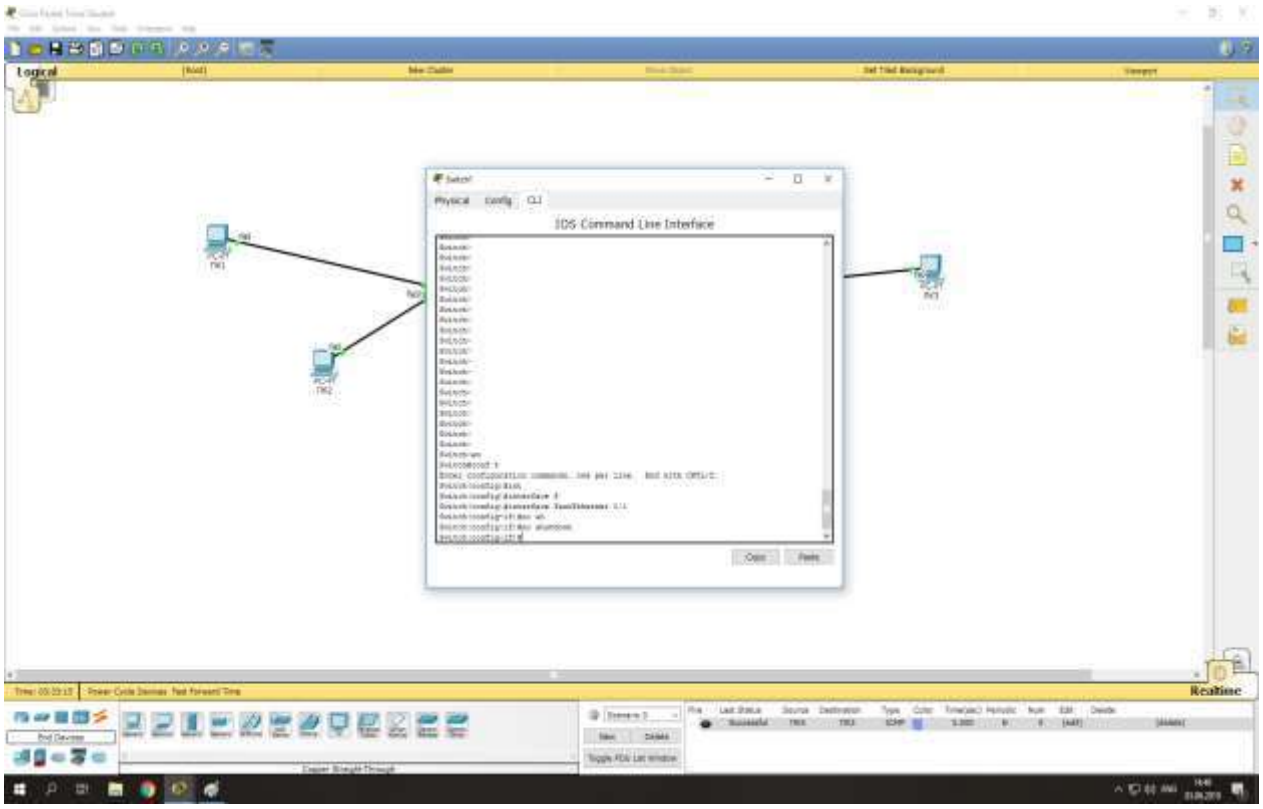

Рисунок 4.1 – Приклад інтерфейсу командного рядка у Packet Tracer.

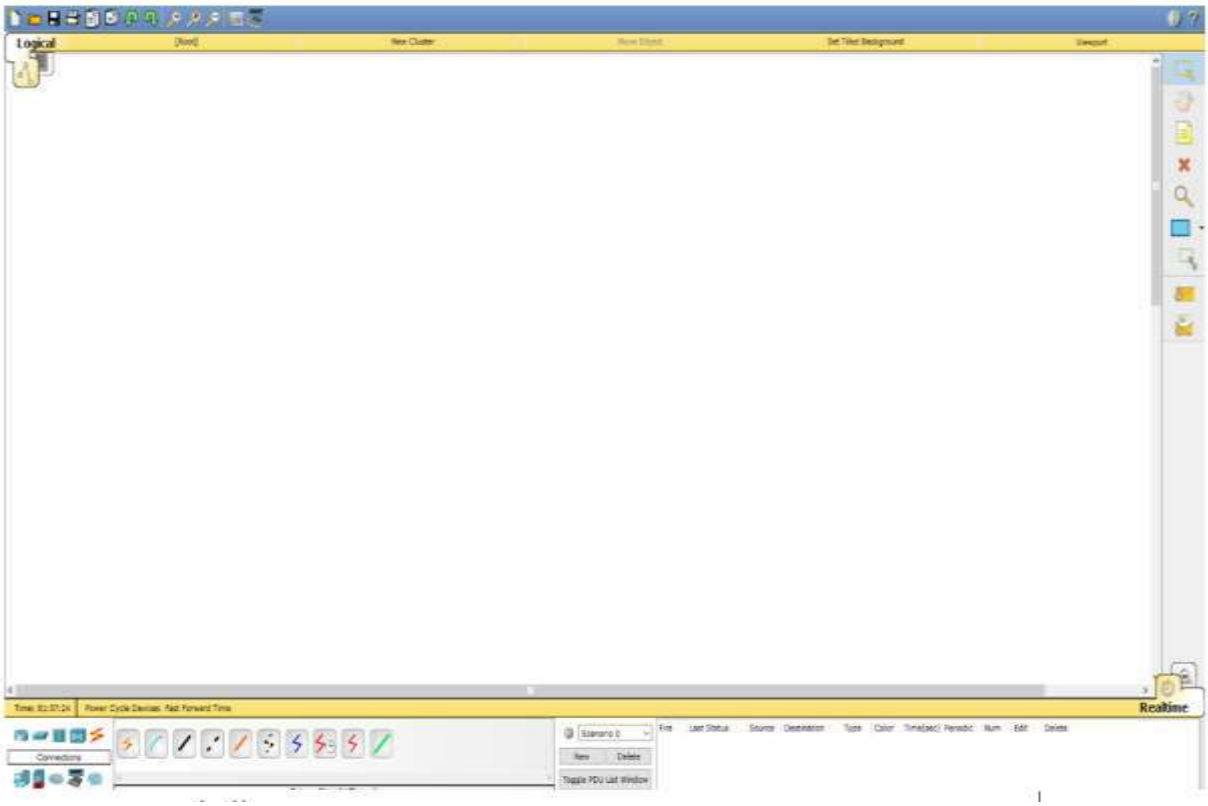

Рисунок 4.2 – Приклад інтерфейсу користувача з перетягуванням у Packet Tracer

Cisco Packet Tracer також надають свої послуги такими мовами, як німецька, іспанська та французька. Packet Tracer дозволяє студентам створювати складні та величезні мережі, що часто неможливо за допомогою фізичного обладнання зважаючи на вартість. Packet Tracer підтримується на багатьох платформах та оперційних системах, таких як Linux, Windows, MacOS, Android та iOS [8].

Серед технологій які будуть використовуватися під час розробки ситеми можна відзначити Python.

Python – це багатопарадигмальна, універсальна, інтерпретована мова програмування високого рівня. Python дає змогу програмістам використовувати різні стилі програмування для створення програм різної складності, що простих так і складних, отримання швидших результатів і

написання коду майже так, ніби розмовляючи людською мовою. Деякі з популярних систем і програм, які використовували Python під час розробки, включають Google Search, YouTube, BitTorrent, Google App Engine, Eve Online, Maya та iRobot.

Є дві основні переваги, які роблять час розробки програмного забезпечення в Python швидшим, ніж в інших мовах програмування:

Python є інтерпретованою мовою, що виключає необхідність компіляції коду перед виконанням програми, оскільки Python виконує компіляцію у фоновому режимі. Оскільки Python є мовою програмування високого рівня, він абстрагує багато складних деталей із коду програмування. Python настільки зосереджений на цій абстракції, що її код може бути зрозумілий більшості початківців програмістів [9].

Код Python, як правило, коротший, ніж аналогічні коди. Хоча Python пропонує швидкий час розробки, він трохи відстає з точки зору часу виконання коду. У порівнянні з мовами, що повністю компілюються, такими як C і C++, програми Python виконуються повільніше. Звичайно, зі швидкістю обробки комп'ютерів у наші дні, різниця в швидкості зазвичай спостерігається лише в тестах порівняльного аналізу, а не в реальних операціях. У більшості випадків Python вже включено в дистрибутиви Linux і машини Mac OS X.

4.2 Розгортання мережі із системою захисту каналів витоку інформації

На данному етапі кваліфікаційної роботи приступимо до розгортання локальної мережі з подальшим покращенням рівня захисту, базуючись на інформації та висновків які ми отримали під час дослідження.

Для побудови мережі було використано вже згадане програмне забезпечення Packet Tracer.

Щоб отримати функціонуючу мережу було використано таке обладнання:

- 5 персональних комп’ютерів;
- сервер;
- мережевий комутатор 2 рівня;
- мережевий комутатор 3 рівня;
- Wi–Fi роутер;
- Ip камера.

Сервер – в нашому випадку це комп’ютер який відіграє роль централізованого джерела доступу до обладнання IoT пристроїв, камер відеоспостереження, а також буде містити в собі інформацію щодо підключень до локальної мережі, логування подій виконаних в тій ж мережі. Також сервер можна використати для налаштування доступу до ресурсів локальної мережі.

Мережевий комутатор – є ще однією фундаментальною частиною багатьох мереж, оскільки вони прискорюють роботу. Комутатори дозволяють різним вузлам (точці мережевого підключення, як правило, комп'ютеру) мережі взаємодіяти безпосередньо один з одним плавним і ефективним способом [10].

Існує багато різних типів комутаторів і мереж. Перемикачі, які забезпечують окреме підключення для кожного вузла у внутрішній мережі компанії, називаються комутаторами локальної мережі. По суті, комутатор локальної мережі створює серію миттєвих мереж, які містять лише два пристрої, які спілкуються один з одним у певний момент.

Після того як ми визначилися з ключовими складовими локальної мережі можемо приступити до розміщення апартного обладнання, та подальшим під'єднанням один до одного утворюючи спільну мережу (рис 4.3.).

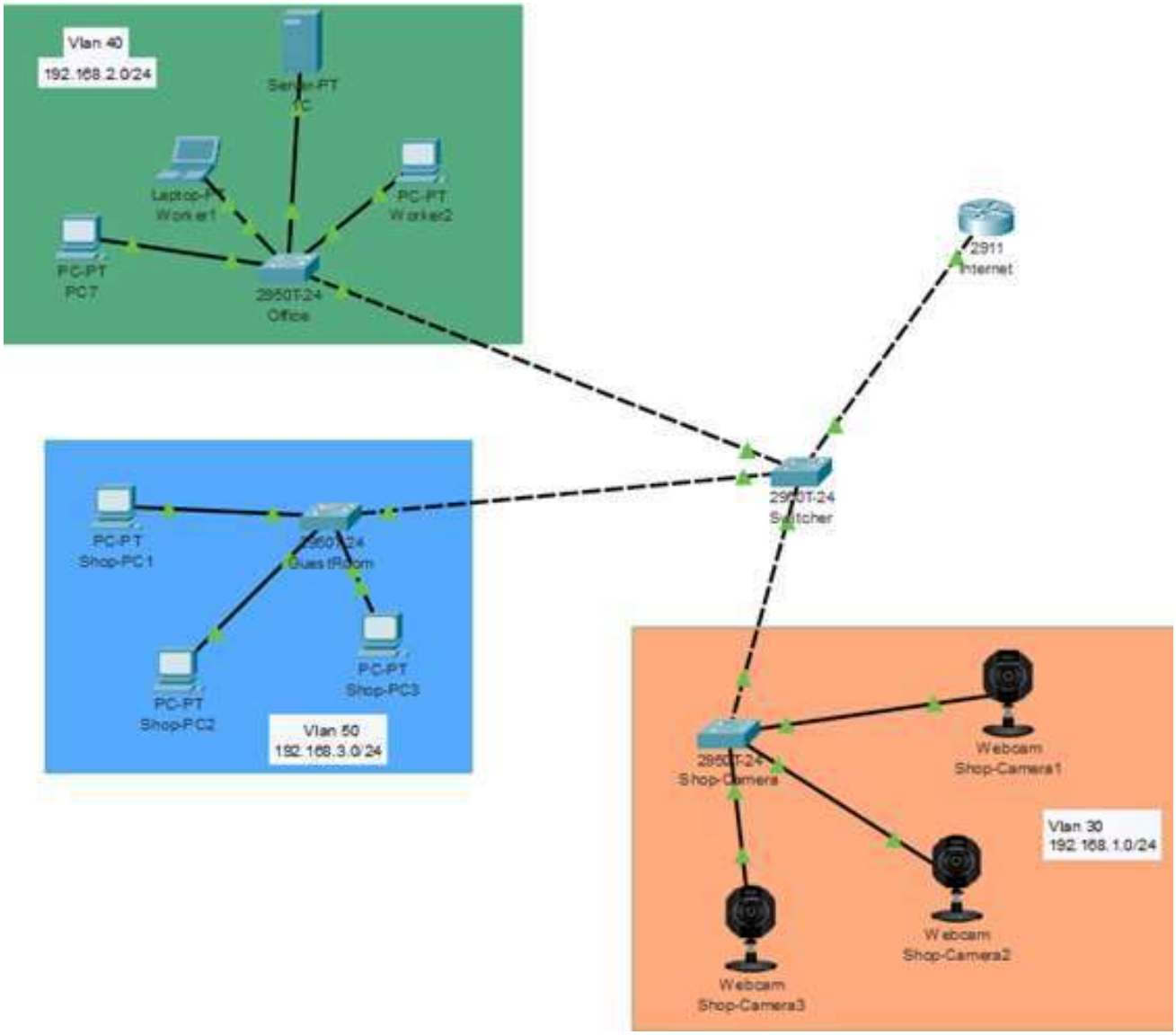

Рисунок 4.3 – Вигляд мережі після розміщення та з'єднання складових.

Після того як локальна мережа була успішно побудована приступимо до налаштування самої мережі, а саме налаштування Wi–Fi роутера.

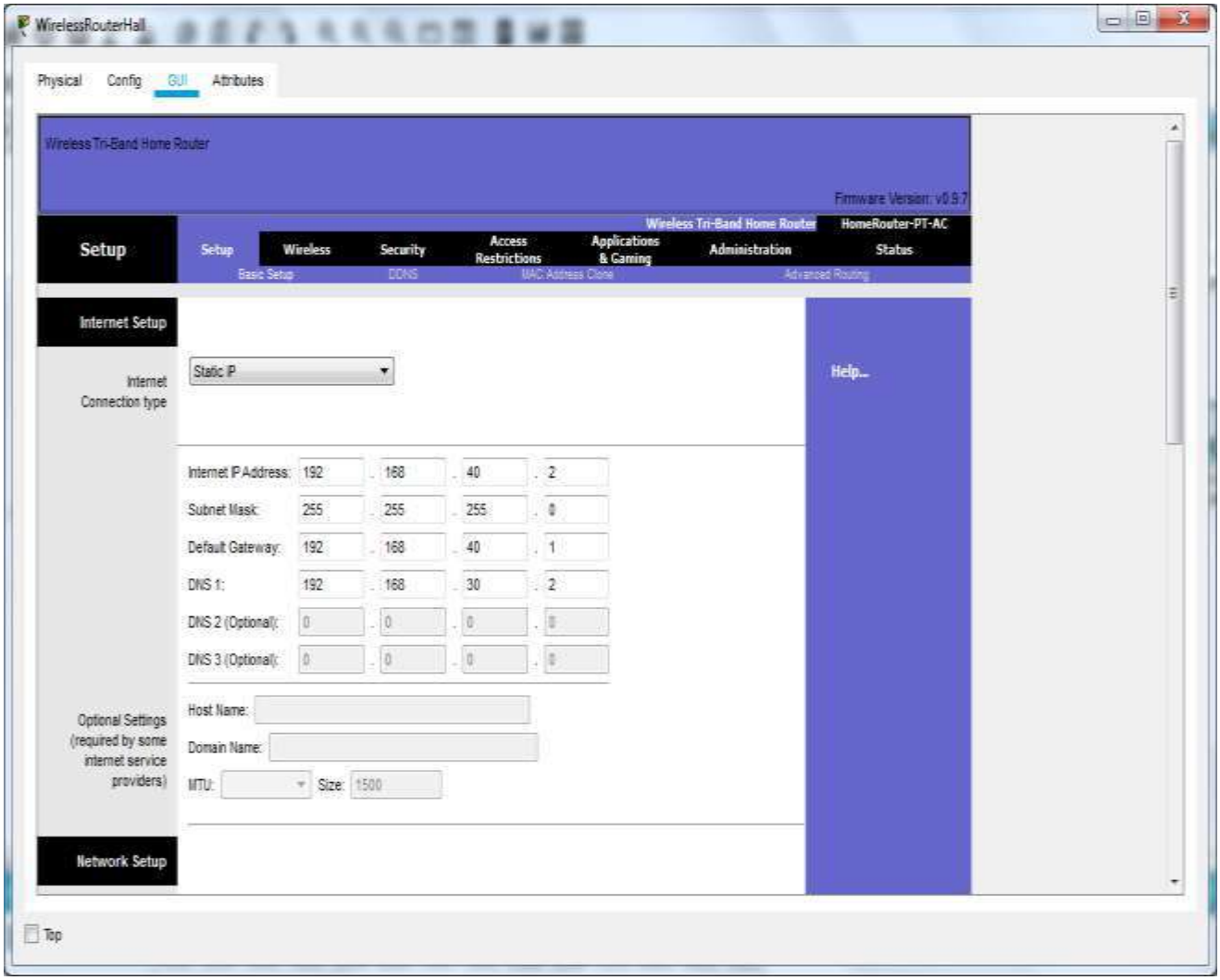

Рисунок 4.4 – Налаштування роутера локальної мережі

Відразу після налаштування роутера та IP комп’ютерів необхідно перевірити чи все було виконано правильно, чи налаштування працює. Для перевірки доступності пристроїв локальної мережі, потрібно відкрити командний інтерфейс Packet Tracer та пропінгувати усі пристрої (рис 4.5.).

За результатами перевірки ми можемо спостерігати що пристрої підключені та налаштовані коректно і, як наслідок, ми маємо функціонуючу мережу з системою захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі.

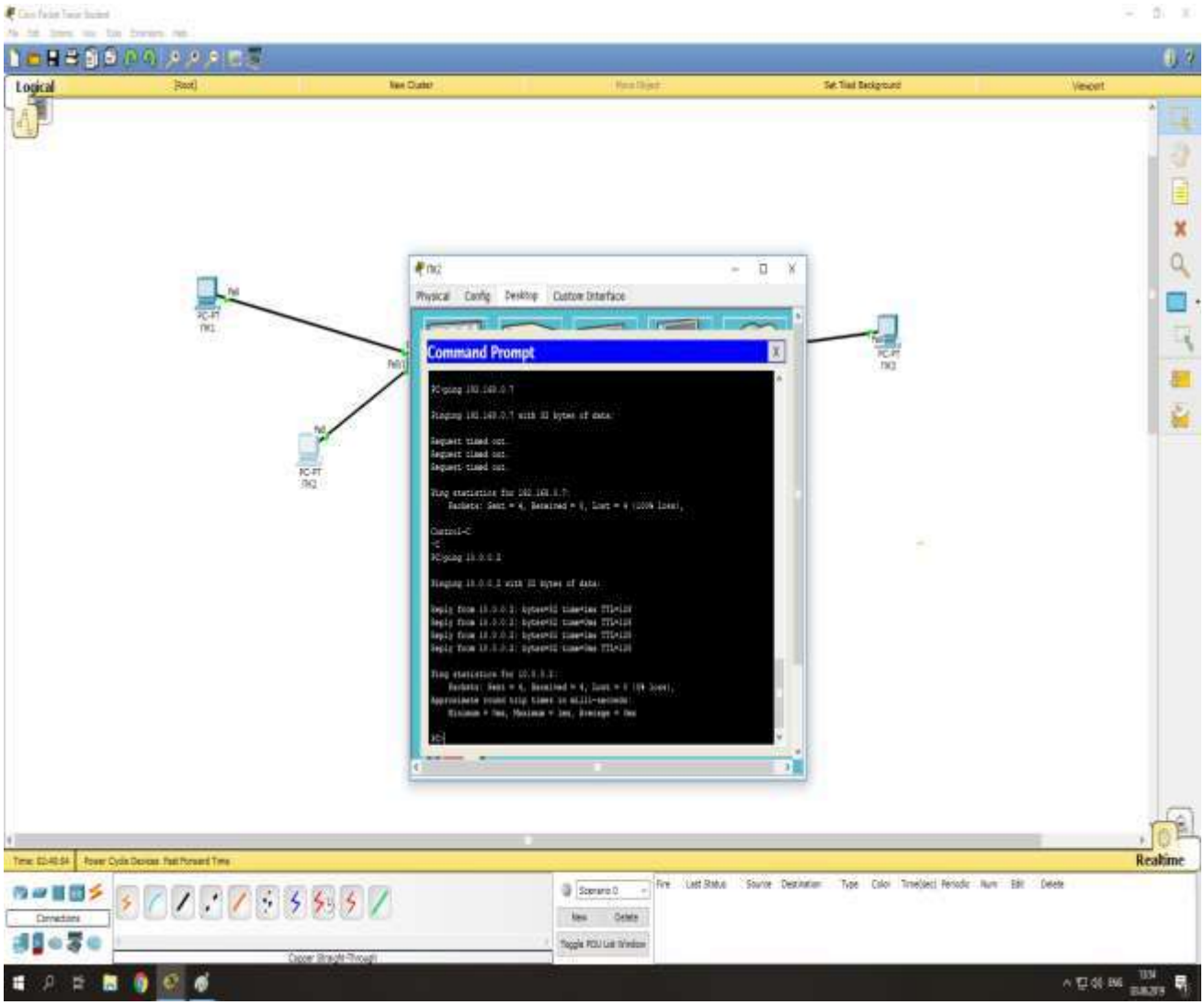

Рисунок 4.5 – Приклад перевірки коректного з’єднання пристроїв локальної мережі

4.3 Висновок

В даному розділі було розгорнуто та реалізовано систему захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі, зокрема зроблене визначення інструментів та технологій, що будуть використані в процесі реалізації системи захисту, а

також здійснено Розгортання мережі із системою захисту каналів витоку інформації.

Одержані результати відповідають вимогам завдання кваліфікаційної роботи з проектування та реалізація системи захисту каналів витоку інформації а також виявлення несанкціонованого доступу в інформаційних мережах.

ВИСНОВКИ

У цій кваліфікаційній роботі було зроблено:

- аналіз інформаційних мережі, їх різновидів та складових частин;
- дослідження предметної області, класифікація каналів витоку інформації в інформаційних мережах;
- було проаналізовано методи захисту каналів витоку інформації, способи боротьби з несанкціонованим доступом в інформаційних мережах;
- спроектовано систему захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі;
- розгорнуто локальну мережу із системою захисту каналів витоку інформації.

У першому розділі ми дослідили предметну область за темою роботи, освоїли теоретичну базу по напрямкам канали витоку інформації, інформаційні мережі, дізналися що входить в складові інформаційних систем.

У другому розділі ми ознайомилися з методами захисту каналів витоку інформації від несанкціонованого доступу в інформаційній мережі, проаналізували існуючі програмно-апаратні, апаратні, технічні та організаційні рішення по бородьбі з несанкціонованим доступом в інформаційних мережах, захисту каналів витоку інформації.

В третьому розділі, опираючись на інформацію із попередніх розділів, нами було переглянуто більш конкретні методи регулювання несанкціонованого доступу, спроектували систему захисту каналів витоку інформації та несанкціонованого доступу, яка в подальшому була реалізована

У четвертому розділі ми займалися розробкою системи захисту каналів витоку а також від несанкціонованого доступу в інформаційній мережі, обрали технічні засоби для реалізації системи, описали використані технології.

Таким чином, мета та завдання кваліфікаційної роботи повністю виконані.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Класифікація комп’ютерних мереж за розташуванням. Pidruchniki. URL:https://pidru4niki.com/16580925/informatika/informatsiyni_tehnologiyi_kompyuternih_merezh (дата звернення 21.03.2022)

2. Основні поняття інформаційних мереж. Computing.ucoz.net URL: https://computing.ucoz.net/index/osnovni_ponjattja_informacijnikh_merezh/0–43 (дата звернення 21.03.2022)

3. Класифікація комп’ютерних мереж. Kppk URL: https://kppk.com.ua/ELLIB/ebook/Gorbenko/IKT/13/13.htm(дата звернення 21.03.2022)

4. Класифікація каналів витоку інформації. Google URL: https://sites.google.com/site/kanalivitokuinformaciie/klasifikacia–kanaliv–vitoku–informaciie/kanali–vtrati–konfidencijnoie–informaciie

5. Акустичні канали витоку інформації. URL: https://tzi.com.ua/akustichn–kanali–vitoku–nformacz.html

6. Об’єкти захисту інформації. URL: https://ela.kpi.ua/bitstream/123456789/10950/1/13_p88.pdf

7. Засоби захисту технічних каналів витоку інформації. Kiev. URL: https://usts.kiev.ua/

8. What is Cisco Packet Tracer? Tutorialspoint. URL: https://www.tutorialspoint.com/what–is–cisco–packet–tracer

9. What is Python? Python.URL: https://www.python.org/doc/essays/blurb/

10. What is lan Switch? Howstufforks. URL: https://computer.howstuffworks.com/lan–

switch.htm#:~:text=Switches%20that%20provide%20a%20separate,other%20at%20that%20particular%20moment.

11. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level / Editors : Robert M. Clark, Simon Hakim. – Cham, Switzerland : Springer, 2016. – 360 p.

12. Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software Level / Editors : Michael Schwartz, Maciej Machulak. – Apress, 2018. – 377 p.

13. Антивірусний захист. URL: https://www.esetnod32.ru/ (дата звернення: 15.05.2022)

14. Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice / Elias G. Carayannis, David F. J. Campbell, Marios Panagiotis Efthymiopoulos. – New York : Springer, 2014. – 360 p.

15. Fundamentals of InformationSystems Security / Editors : David Kim, Michael G. Solomon. – Burlington, Massachusetts : Jones & Bartlett Learning, 2018. – 548 p.

ДОДАТОК А

ДРКІ.015082.15.03.07

					КРКБ.180127.18.01.03 Е8		
Зм	Арк.	Ndокум.	Підпис	Дата	Підключення вимірювальної апаратури до сторонніх проводів через вхідні пристрої	Літера	Маса / Масштаб
Розроб.		Кажуро О.Б.				Н	
Перевір.		Орленко В.С				Аркуш 1	Аркушів
Т.контр.							
Н.контр.		Мостовий С.В.				ХНУ, КБ-18-1	
Затв.		Кльоц Ю.П.					

ДРКІ.015082.15.03.07

КРКБ.180127.18.01.03 Е8

Зм.	Арк.	Ndokум.	Підпис	Дата
Розроб.		Кажуро О.Б.		
Перевір.		Орленко В.С.		
Т.контр.				
Н.контр.		Мостовий С.В.		
Затв.		Кльоц Ю.П.		

Схема установки для проведення контролю на ЕАП

Літера	Маса	Масштаб
Н		
Аркуш 2	Аркушів	

ХНУ, КБ-18-1

ДРКІ.015082.15.03.07

Зм.	Арк.	Докум.	Підпис	Дата	КРКБ.180127.18.01.03 Е8			
Розроб.		Кажуро О.Б.			Схематичне зображення перехоплення інформації з каналів витоку інформації	Літера	Маса	Масштаб
Перевір.		Орленко В.С				Н		
Т.контр.						Аркуш 3	Аркушів	
Н.контр.		Мостовий С.В.				ХНУ, КБ-18-1		
Затв.		Кльоц Ю.П.						

ДРКІ.015082.15.03.07

Зм.	Арк.	Ndокум.	Підпис	Дата
Розроб.		Кажуро О.Б.		
Перевір.		Орленко В.С.		
Т.контр.				
Н.контр.		Мостовий С.В.		
Затв.		Кльоц Ю.П.		

КРКБ.180127.18.01.03 Е8

Реалізована локальна мережа для захисту каналів витоку інформації та несанкціонованого доступу

Літера	Маса	Масштаб
Н		
Аркуш 1	Аркушів	

ХНУ, КБ-18-1

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Кажуро Олександра Борисовича
ПІБ здобувача вищої освіти
студента ФІТ, 4 курсу, групи КБ-18-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

18.06.2022
дата

підпис

Tue Jun 21 12:17:53 EEST 2022, Мостовий Сергій Володимирович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 9%**

ID: 106386 Название: Система захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі Добавлено в БД: 2022-06-21 Авторы: Кажуро Олександр Борисович Руководители: Джулій В.М. Консультанты: Опоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	49832	785	1167 (2%)	19 (2%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1011627990

Дата перевірки:
21.06.2022 13:13:42 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
21.06.2022 13:15:55 EEST

ID користувача:
100008300

Назва документа: **Кажуро КвРоб**

Кількість сторінок: **57** Кількість слів: **7619** Кількість символів: **60713** Розмір файлу: **1.13 MB** ID файлу: **1011495503**

17.6%
Схожість

Найбільша схожість: **6.73%** з Інтернет-джерелом (https://infopedia.su/1x9790.html)

15.1% Джерела з Інтернету | 59 ..... Сторінка 59

3.29% Джерела з Бібліотеки | 11 ..... Сторінка 60

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Система захисту виявлення каналів витоку інформації та несанкціонованого доступу в інформаційній мережі

Автор: Кажуро Олександру Борисович
Спеціальність: 125 – Кібербезпека
Освітня програма: освітньо-професійна
Науковий керівник: Чешун Віктор Миколайович, к.т.н, доцент
Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 82,4%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності в Хмельницькому національному університеті (https://www.khnu.km.ua/root/files/01/10/03/0101.pdf), така авторська робота визнається роботою з достатньою унікальністю тексту.

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1. В якості запозичень системою Unichek розпізнано типові елементи стандартних рамок пояснювальної записки.
2. Запозиченнями системою Unichek визнано збіги в назвах використаних друкованих видань, розміщених в переліку джерел посилань, які оформлені за вимогами стандартів і не можуть не співпадати з описами аналогічних джерел в інших роботах.
3. Запозиченнями системою Unichek визнано зміст декількох абзаців в розділах з оглядом існуючих рішень, де виконавець посилається на джерело запозичення інформації і на авторство яких здобувач не претендує.
4. Інші збіги є загальновживаними фразами.

Керівник роботи — Вікторія Орленко

Гарант ОП — Віктор Чешун

Завідувач кафедри КБ — Юрій Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Кажуро Олександр Борисович

Тема Система захисту виявлення каналів витоку інформації та несанкіонованого доступу в інформаційній мережі

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 4 ; кількість сторінок записки 57 .

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі створено систему захисту від несанкціонованого доступу в інформаційній мережі .

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у достатній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, чітко визначено об'єкт, предмет та методи дослідження, сформульована актуальність. Визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. У першому розділі проведено огляд використовуваних в комп'ютерних системах методів захисту конфіденційної інформації, виконане обгрунтування актуальності теми дослідження і виконана постановка задачі. В другому розділі наведені засоби та технології використані для побудови системи захисту. В третьому розділі визначено основні положення системи та розроблено алгоритми її роботи. Четвертий розділ було присвячено апробації системи захисту та алгоритмів її реалізації.

4. Позитивні сторони роботи Кваліфікаційна робота має комплексну практичну цінність. Практична цінність полягає у розробці модуля лексичного аналізу з допомогою якого визначається ступінь конфіденційності даних. На основі даного аналізу в подальшому здійснюється керуючий вплив на витік конфіденційних даних. Практична цінність результатів кваліфікаційної роботи полягає у створені системи захисту від витоків даних та несанкціонованого доступу, що може бути підлаштована для будь якої категорії даних, і у описі оптимальних моделей функціонування систем захисту подібного характеру.

5. Негативні сторони роботи Розроблена система захисту від витоків даних досить чутлива до навантаження.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження Окремі описи в пояснювальній записці подано занадто деталізовано, що ускладнює сприйняття матеріалу фахівцями в обраній предметній галузі.

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Лисенко Сергій Миколайович, д.т.н., професор кафедри комп'ютерної інженерії та інформаційних систем

« 18 » 06 2022. (підпис)