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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Підвищення ефективності захисту конфіденційних даних від витоку технічними каналами передачі інформації 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
_____ Іван ВОЛКОВЕЦЬКИЙ

Виконав: здобувач вищої освіти групи СЗДМ 61
Іван ВОЛКОВЕЦЬКИЙ

Керівник: НІМЧЕНКО Тетяна
к.т.н., доцент (ПРІЗВИЩЕ, Ім’я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім’я)

Київ 2026

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

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСК
_____ Олександр Туровський

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

___Волковецькому Івану Сергійовичу _____
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Система багатофакторної автентифікації користувача при захищеному доступі до конфіденційної інформації»
керівник кваліфікаційної роботи ____Тетяна НІМЧЕНКО, к.т.н., доцент_____
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій
від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: опорний об'єкт інформаційної діяльності, технічні канали витоку інформації, вимоги до захисту інформації з обмеженим доступом, сучасні засоби захисту інформації від витоку технічними каналами, технічні засоби захисту та технічної системи охорони.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Аналіз сутності, властивостей та шляхів утворення технічних каналів витоку інформації, що утворюються основними технічними засобами та системами на об'єкті інформаційної діяльності ;
4.2. Дослідження напрямків розробки та удосконалення єдиної моделі комплексної системи захисту з посиленими заходами від витоку інформації технічними каналами ;
4.3. Розробка комплексної систему захисту об'єкту інформаційної діяльності з підвищеними вимогами до захисту від витоку інформації технічними каналами .

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

6. Дата видачі завдання_____15.10.2025_____

КАЛЕНДАРНИЙ ПЛАН

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

Здобувач вищої освіти _____ Іван ВОЛКОВЕЦЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Тетяна НІМЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 67 сторінок, має 9 рисунків, 4 таблиць. Список використаних джерел містить 26 найменувань і займає 3 сторінки.

Метою кваліфікаційної роботи є підвищення ефективності захисту конфіденційних даних від витоку технічними каналами передачі інформації об’єкту інформаційної діяльності.

У процесі кваліфікаційної перевірки було виконано такі завдання: розглянуто природу, характеристики та методи формування технічних каналів витоку інформації, утворених основними технічними засобами та системами об'єктів інформаційної діяльності; досліджено напрямок розробки та вдосконалення єдиної моделі комплексної системи захисту для посилення заходів проти витоку інформації через технічні канали; розроблено комплексну систему захисту для об'єктів інформаційної діяльності з підвищеними вимогами до захисту від витоку інформації через технічні канали.

Апробація:

Н.А. Андрієнко, І.С. Волковецький, Є. О. Васін. Принципи та методи застосування системи багатофакторної автентифікації для запобігання витоку конфіденційних даних на об’єкті інформаційної діяльності. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-комунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.29-30. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, КОМПЛЕКСНА СИСТЕМИ ЗАХИСТУ ІНОФРМАЦІЇ, ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ.

ABSTRACT

The qualification work consists of an introduction, four sections, general conclusions, a list of sources used, the total volume of the work is 67 pages, has 9 figures, 4 tables. The list of sources used contains 26 items and takes up 3 pages.

The purpose of the qualification work is to increase the effectiveness of protecting confidential data from leakage through technical channels of information transmission to the object of information activity.

During the qualification check, the following tasks were performed: the nature, characteristics and methods of forming technical channels of information leakage formed by the main technical means and systems of objects of information activity were considered; the direction of developing and improving a single model of a comprehensive protection system to strengthen measures against information leakage through technical channels was investigated; a comprehensive protection system was developed for objects of information activity with increased requirements for protection against information leakage through technical channels.

Approbation:

N.A. Andrienko, I.S. Volkovetsky. Principles and methods of applying a multi-factor authentication system to prevent the leakage of confidential data at the object of information activity. All-Ukrainian scientific and practical conference: Current problems of information and telecommunication systems security. Kyiv, November 05, 2025, Kyiv: DUIKT Research and Development Center. – 2025. P.83-84. https://duikt.edu.ua/uploads/p_2661_93669247.pdf

Keywords: OBJECT OF INFORMATION ACTIVITY, COMPREHENSIVE INFORMATION PROTECTION SYSTEM, TECHNICAL CHANNELS OF INFORMATION LEAKAGE

.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

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

ВСТУП

Характерною та важливою проблемою сьогодення стало питання забезпечення безпеки функціонування державних установ, підприємств, загальнонаціональних систем та мереж забезпечення життєдіяльності населення які кваліфікуються як об’єкти інформаційної діяльності. Тобто об’єкти, неналежне функціонування чи вихід зі строю яких можуть значною мірою вплинути на якість управління життєдіяльності населення цілих регіонів. Забезпечення ефективного функціонування системи захисту інформації від витоку технічними каналами на об’єкті інформаційної діяльності є актуальним заданням, вирішенню якого присвячена дана робота.

Метою кваліфікаційної роботи підвищення ефективності захисту конфіденційних даних від витоку технічними каналами передачі інформації об’єкту інформаційної діяльності.

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

– здійснено аналіз сутності, властивостей та шляхів утворення технічних каналів витоку інформації, що утворюються основними технічними засобами та системами на об’єкті інформаційної діяльності;

– проведено дослідження напрямків розробки та удосконалення єдиної моделі комплексної системи захисту з посиленими заходами від витоку інформації технічними каналами;

– розроблена та подана комплексна системи захисту об’єкту інформаційної діяльності з підвищеними вимогами до захисту від витоку інформації технічними каналами.

Об’єкт дослідження. Система технічного захисту об’єкта інформаційної діяльності.

Предмет дослідження. Система захисту інформації від витоку технічними каналами передачі даних

.

РОЗДІЛ 1.
АНАЛІЗ ОСНОВНИХ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

1.1 Класифікація каналів технологій витоку інформації для цілей інформаційної діяльності

Для визначення вимог до каналів технологій витоку інформації та організації роботи з захисту інформації ці канали класифікуються за певними характеристиками. Зокрема, типи каналів технологій розрізняються за такими характеристиками [1,2]:

- За типом інформаційної діяльності цілі інформаційної діяльності;

- За принципом формування (фізичним ефектом, процесом) сигналу небезпеки (носієм інформації);

- За середовищем поширення сигналу небезпеки;

- За способом перехоплення (ліквідації) сигналу небезпеки технічною розвідкою противника.

За типом інформаційної діяльності цілі інформаційної діяльності канали технологій можна розділити на такі категорії [1,2]:

a) Канали технологій витоку голосової інформації;

b) Канали технологій витоку інформації, що обробляються в ОТЗС (Центр інформаційних технологій);

c) Канали технологій витоку візуальної інформації;

d) Канали витоку матеріальної інформації.

Рекомендується класифікувати ТКВІ за вищезазначеними типами ТКВІ на основі принципу формування (фізичного ефекту, процесу), середовища поширення та способу перехоплення (ліквідації) сигналу небезпеки технічною розвідкою противника. [17]

На основі цих характеристик технічні канали витоку голосової інформації можна класифікувати наступним чином [1,2]:

a) Акустичні канали.

b) Вібраційні (вібраційно-акустичні) канали.

c) Акустооптичні (лазерно-акустичні) канали.

d) Електроакустичні канали.

e) Відеоакустичні канали.

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

g) Канали витоку голосової інформації на основі вбудованих пристроїв.

Технічні канали витоку інформації, що обробляються ОТЗС, можна класифікувати наступним чином [1,2]:

1. Канали бічних електромагнітних випромінювань.

2. Канали бічних електромагнітних перешкод.

3. Паразитні канали модуляції радіочастотних сигналів генератора.

4. Паразитні канали генерації радіочастот підсилювачів.

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

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

7. Канал радіочастотних перешкод (використовується для видалення інформації, що обробляється ОТЗС).

8. Канал витоку інформації обробки ОТЗС на основі вбудованих пристроїв.

Технічні канали витоку візуальної інформації класифікуються наступним чином:

1. Візуальний канал.

2. Оптичний канал.

3. Канал витоку візуальної інформації на основі вбудованих пристроїв.

Матеріальні канали витоку інформації:

1. Вилучення інформації з магнетизму або інших носіїв інформації несправних пристроїв ЕОТ.

2. Вилучення інформації з чернеток документів, відходів, що утворюються у виробництві, публікації, офісі тощо.

3. Хімічний канал. [17]

Виходячи з носія інформації та принципу формування сигналу небезпеки, можна виділити такі канали витоку інформації [2,3]:

Електромагнітні канали витоку інформації, включаючи канали бічного електромагнітного випромінювання, канали "паразитної" генерації високої частоти підсилювача, канали "паразитної" модуляції генератора високої

частоти та канали перехоплення інформації радіоліній (радіорелейної, стільникової мережі тощо). Мобільний зв'язок тощо;

Електричні канали витоку інформації, включаючи канали бічних електромагнітних перешкод, що впливають на зв'язок, канали вилучення інформації з дротових ліній зв'язку тощо;

Параметричні канали витоку інформації, включаючи канали радіочастотних перешкод, канали "паразитної" модуляції тощо.

Виходячи з місця перехоплення технічної розвідки противника, витік технічної інформації можна класифікувати на такі типи [2,3,4]:

1) Канали, де інформація перехоплюється (вилучається) за межами контрольованої зони;

2) Канали, де інформація перехоплюється (вилучається) за межами контрольованої зони та позитивно впливає на параметри каналу витоку технічної інформації (наприклад, канали радіочастотних перешкод);

3) Канали, де інформація вилучається через технічну розвідку, встановлену на цільових інформаційних пристроях (OID) (наприклад, канали витоку технічної інформації вбудованих пристроїв).

Наведена вище класифікація каналів витоку технічної інформації допомагає нам систематично зрозуміти їх та сформулювати вимоги та заходи до відповідних систем контролю витоку технічної інформації для захисту інформації від витоку.

1.2. Аналіз каналів витоку інформації, що обробляється основними технічними засобами та системами на об’єкті інформаційної діяльності

Дослідимо природу та методи технологічних каналів витоку інформації (фізичні основи, принципи та процедури), що обробляються основними технічними засобами та системами. Для інформації, що обробляється ОТЗС,

найнебезпечнішим шляхом витоку є канал латерального електромагнітного випромінювання та перешкод (канал PEMVN) [4,5].

Латеральний канал електромагнітного випромінювання ОТЗС

Латеральний канал електромагнітного випромінювання ОТЗС (канал PEMV ОТЗС) утворений латеральними електромагнітними полями, що перехоплюються приймачем засобів технічної розвідки. Ці латеральні електромагнітні поля формуються, коли інформаційні сигнали проходять через електронні компоненти та провідники (петлі) ОТЗС та поширюються за межі контрольованої зони.

У цьому випадку інформаційний сигнал є струмом, що несе інформацію.

Обробка та передача інформації в ОТЗС здійснюються за допомогою струму провідності, який є спрямованим потоком заряджених частинок — електронів. Загальновідомо, що навколо нерухомого електрона або електронної групи завжди існує статичне електростатичне поле. Якщо цей заряд рухається, у полі з'являється магнітна складова, яка перетворюється на електромагнітне поле. Електромагнітне поле поширюється в просторі [4,5].

Навколо ОТЗС, як системи, що складається з електронних компонентів та провідників (схем), згідно з основним принципом роботи ОТЗС, всередині неї циркулює струм, що переносить інформацію, таким чином завжди присутнє поле випромінювання. Оскільки це випромінювання є шкідливим та має паразитні (латеральні) характеристики, його називають латеральним електромагнітним випромінюванням (ЛЕВ). Латеральне електромагнітне випромінювання поширюється у вільному просторі та може бути перехоплене приймачем технічних розвідувальних засобів противника поза межами ЦК, утворюючи таким чином канал PES ОКТС (Рисунок 1.1) [4,5,6]:

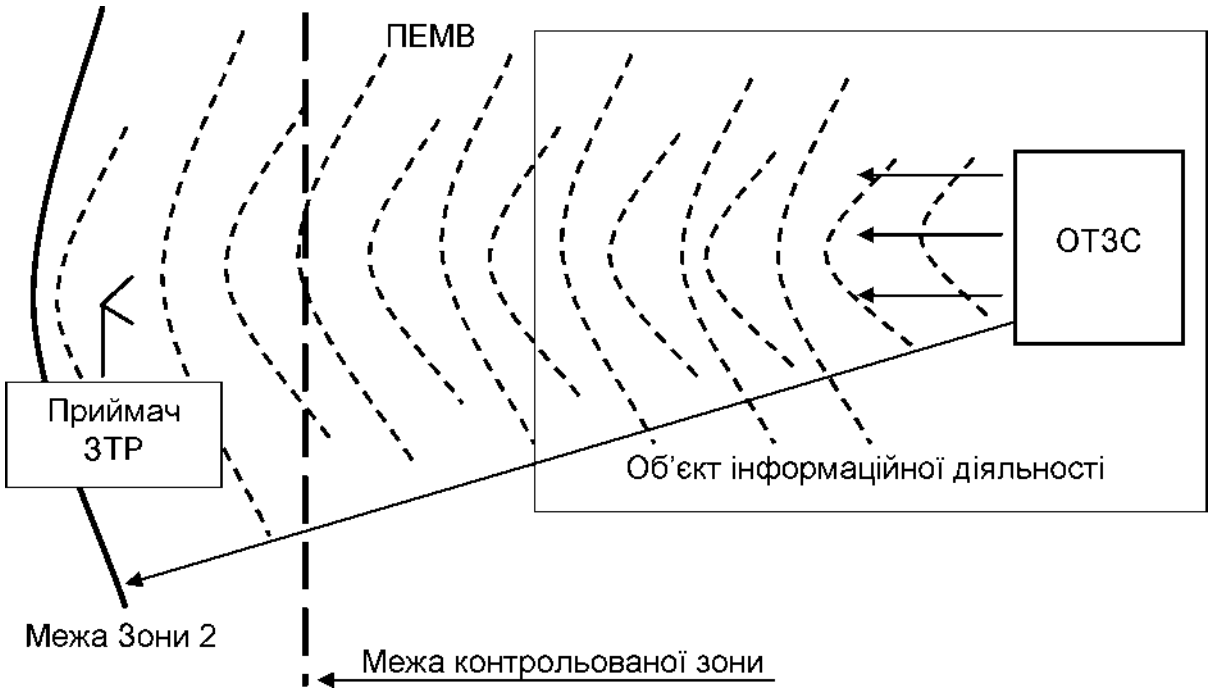


Рис. 1.1. Канал побічних електромагнітних випромінювань ОТЗС.

Згідно з принципами фізики, електромагнітні поля послаблюються під час поширення. Тому на певній відстані від джерела випромінювання (тобто ОТЗС) поле випромінювання послаблюється до такої міри, що стає неприйнятним (неможливим виявити та виміряти його параметри). У цьому випадку небезпечний сигнал, що переноситься полем, ефективно маскується звичайними перешкодами та шумом. Як згадувалося раніше, зона, де співвідношення сигнал/шум не перевищує допустимого стандарту, є Зоною 2 ОТЗС. Якщо приймач ЗТР противника знаходиться поза Зоною 2, він не зможе перехопити інформацію [4,5,6].

Латеральний канал електромагнітного випромінювання ОТЗС.

Латеральний канал електромагнітного випромінювання ОТЗС є каналом ПЕМВ, утвореним шляхом перехоплення небезпечних сигналів у вигляді бічних електромагнітних полів від ОТЗС приймачем технічного розвідувального обладнання. Ці бічні електромагнітні поля

перевипромінюються допоміжним технічним обладнанням та системами, а також зовнішніми провідниками.

Допоміжні технічні засоби та системи, а також зовнішні провідники, якщо вони розташовані в Зоні 1 ОТЗС або проходять на одній лінії з лінією, якою поширюються небезпечні сигнали (включаючи сигнали бічних електромагнітних перешкод) ОТЗС, є випадковими антенами та можуть спричиняти витік інформації через небезпечні сигнали, індуковані на них бічним електромагнітним випромінюванням основних технічних засобів та систем [4,5,6].

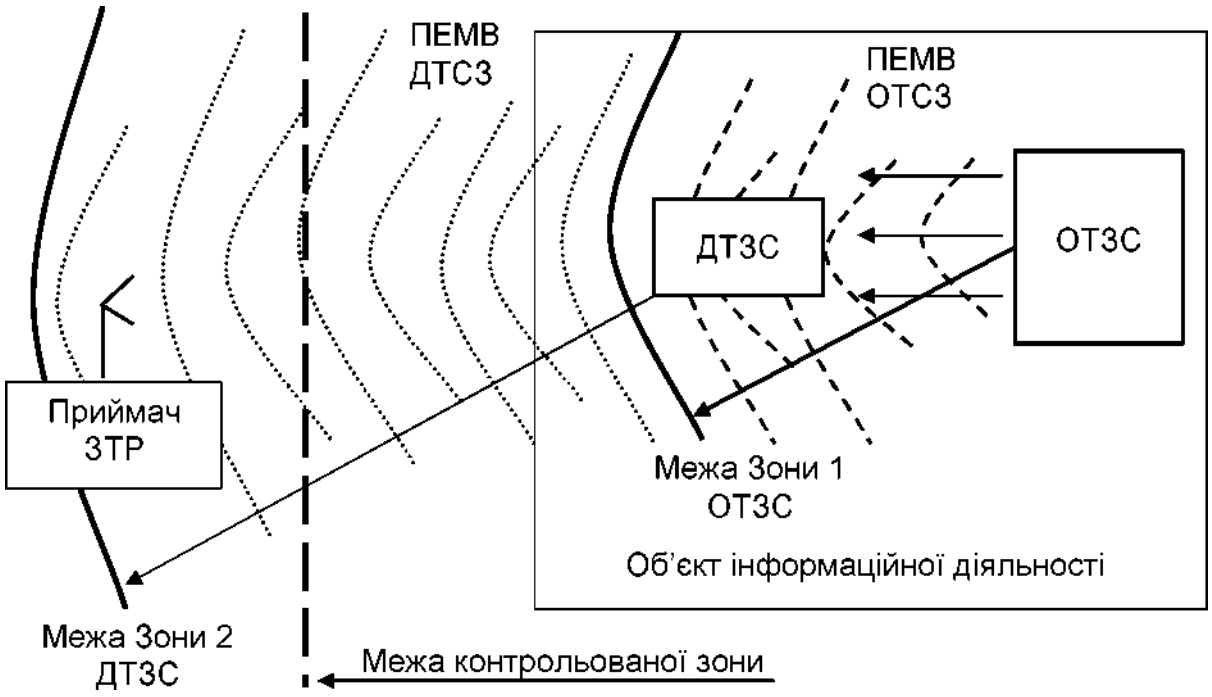


Рис. 1.2. Канал побічних електромагнітних випромінювань ДТЗС.

Канал модуляції сигналу радіочастотного генератора "Паразит"

Канал модуляції сигналу радіочастотного генератора "Паразит", як тип каналу PEMV, формується шляхом модуляції високочастотного сигналу радіочастотного генератора OTZS небезпечним сигналом, передачі модульованого радіочастотного коливання у вільний простір та перехоплення

цих коливань радіоприймальною апаратурою засобів технічної розвідки за межами KZ (рисунок 1.3) [4,5,6].

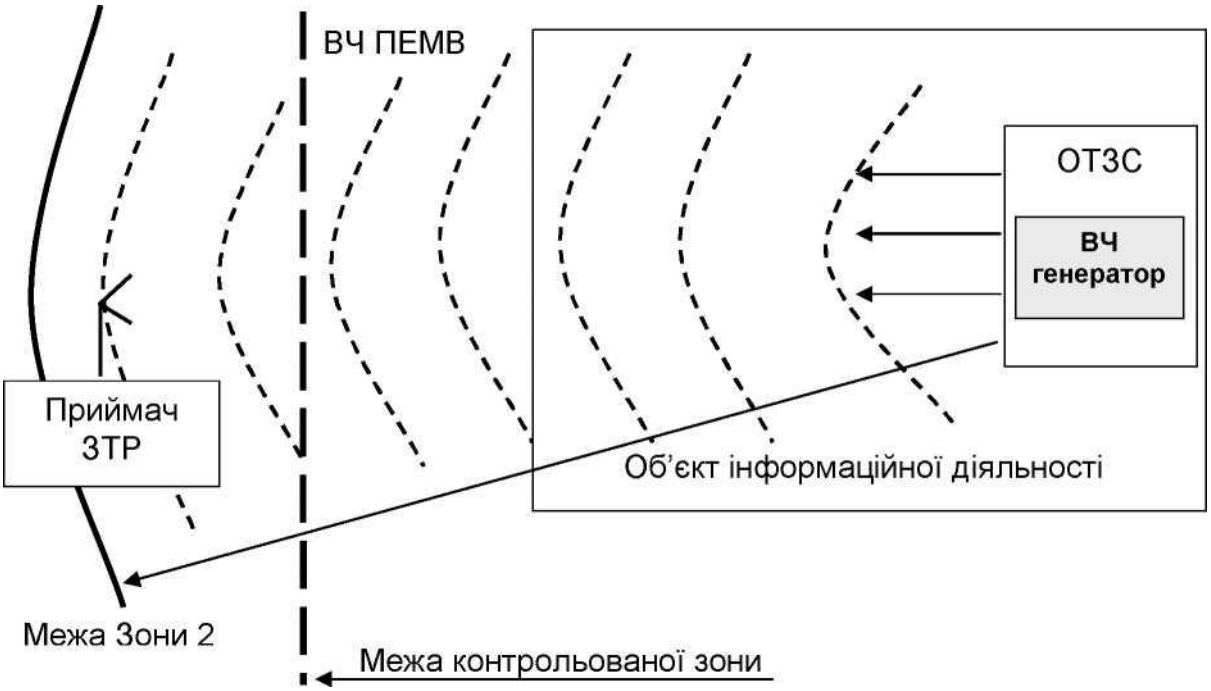


Рис. 1.3. Канал "паразитної" модуляції сигналів ВЧ генераторів.

До основних технічних засобів та систем належить високочастотний генератор (ВЧ-генератор). Майже всі пристрої ЕОТ містять тактовий генератор, гетеродинний генератор та інші високочастотні генератори. Високочастотний сигнал від ВЧ-генератора модулюється низькочастотним сигналом небезпеки, що циркулює в ЕОТ, та випромінюється у вільний простір як електромагнітне поле. Оскільки затухання високочастотного електромагнітного поля менше, ніж низькочастотного, електромагнітне поле поширюється далі. Це, у свою чергу, дає змогу перехоплювати інформацію за межами Зони 2 за допомогою технічної розвідки, яка розраховується на основі немодульованого сигналу. Слід зазначити, що модуляція розширює спектр сигналу, збільшуючи його потужність та завадостійкість. Тому модуляційне випромінювання на частоті ВЧ-генератора ЕОТ слід враховувати при розрахунку Зони 2 [6,7,8].

Підсилювач каналу генерації радіочастотних сигналів "Паразит"

Підсилювач каналу генерації радіочастотних сигналів "Паразит", як тип каналу ПЕМВ, генерується самозбудженням низькочастотного (НЧ) підсилювача ОТЗС на гармоніках сигналу небезпеки. Ці гармоніки поширюються як поле електромагнітного випромінювання та перехоплюються радіоприймачем апаратури технічної розвідки (Рис. 1.4) [6,7,8].

Сучасне обладнання для обробки інформації зазвичай включає низькочастотні (НЧ) підсилювачі. Як правило, будь-який підсилювач складається безпосередньо з підсилювальних (напівпровідникових) елементів та негативного зворотного зв'язку.

Нелінійні характеристики напівпровідникових елементів під час посилення сигналу можуть призвести до появи кількох гармонік у вихідному підсиленому сигналі (тобто гармонік, трійок тощо). Якщо підсилювач та його негативний зворотний зв'язок правильно розраховані, а процес посилення відбувається в межах лінійного сегмента характеристик посилення, сам сигнал буде мінімально посиленим та без спотворень, з дуже низькою кількістю кратних гармонік [6,7,8].

Через старіння або інші причини параметри електронних компонентів та характеристики негативного зворотного зв'язку можуть змінюватися, змінюючи загальний режим роботи підсилювача. Негативний зворотний зв'язок може перетворитися на позитивний, збільшуючи коефіцієнт посилення, але також збільшуючи нелінійність посилення, що призводить до насичення підсилювальних елементів. На певних частотах зворотний зв'язок стає позитивним, і підсилювач стає генератором електромагнітних хвиль. Одночасно, при насиченні, кількість гармонік сигналу значно зростає, а інтенсивність його електромагнітного випромінювання досягає значно високого рівня. Це, у свою чергу, може призвести до перехоплення інформації за межами другої області за допомогою методів, які не враховують генерацію

"паразитних" гармонік [6,7,8].

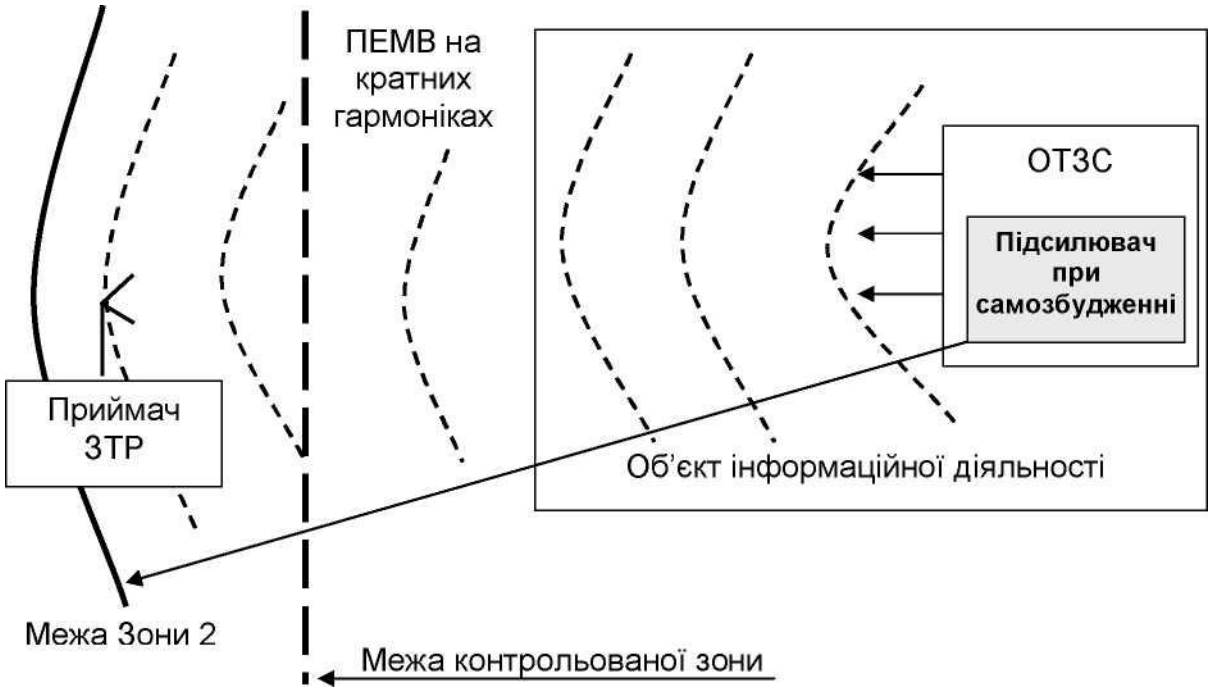


Рис. 1.4. Канал "паразитної" ВЧ генерації підсилювачів.

Характерною рисою ефектів «паразитної» генерації є їх нерегулярність; тому одним із методів запобігання витоку інформації через такі канали є своєчасне виявлення (індикація) сигналів «паразитної» генерації та зупинка роботи ОТЗС.

Методи запобігання витоку інформації через канали «паразитної» високочастотної генерації підсилювача (тобто запобігання створенню таких TCVI) включають [6,7,8]:

- Створення короткого замикання щонайменше зони 2, розрахованого на врахування небезпечних сигналів на кількох гармоніках підсилювача, та організація схем доступу короткого замикання на OID;

- Екранування ОТЗС для запобігання генерації підсилювачем ОТЗС «паразитних» високих частот (часткове екранування підсилювача, оцінка випромінювання та зупинка роботи ОТЗС при виявленні «паразитної»

високочастотної генерації, оцінка, індикація та сигналізація відхилень параметрів підсилювача та зупинка роботи ОТЗС при виявленні позитивного зворотного зв'язку тощо). - Просторовий електромагнітний шум об'єктів ЕОТ [8,9]

Латеральний канал електромагнітних перешкод на лінії електропередачі OTZS (землі)

Латеральний канал електромагнітних перешкод на лінії електропередачі OTZS (землі), як тип латерального каналу електромагнітних перешкод (канал PEMN), формується шляхом зовнішнього технічного виявлення короткого замикання лінії електропередачі OTZS (землі) для безпосереднього усунення небезпечних електричних сигналів, індукованих латеральним електромагнітним полем OTZS та/або витоком (протіканням) у ці лінії (або небезпечних електричних сигналів, що генеруються в лінії електропередачі через нерівномірне споживання потужності під час роботи OTZS) (рис. 1.5) [6,7,8].

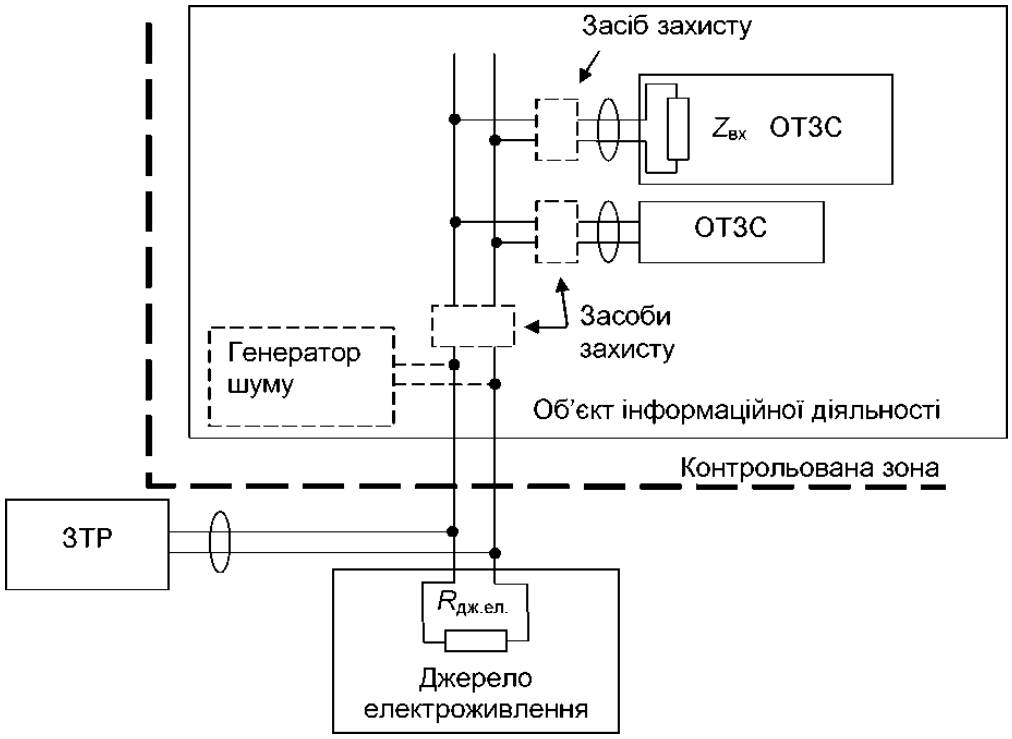


Рис. 1.5. Канал побічних електромагнітних наведень на лінії електроживлення ОТЗС.

Майже всі технології та системи, що використовуються для обробки та передачі інформації, живляться електрично. Лінія живлення (заземлення) ОТЗС даних розташована в Зоні 1 ОТЗС; тому, згідно з принципом електромагнітної індукції, в цих лініях індукується струм. Зміна цього струму нагадує небезпечний електромагнітний сигнал і поширюється вздовж лінії живлення (заземлення).

Крім того, під час обробки інформації вхідний опір ОТЗС змінюється відповідно до характеристик оброблюваного сигналу. Наприклад, підсилювач (критична схема) працює, використовуючи вхідний (керуючий) сигнал для керування опором напівпровідників у колі, тим самим генеруючи посилений сигнал від джерела живлення.

Через коливання вхідного опору кола живлення ОТЗС, небезпечний сигнал генерує змінну складову струму, яка, у свою чергу, генерує змінну складову напруги на опорі самого джерела живлення. Ця остання складова доступна всім користувачам мережі живлення. Якщо джерело живлення знаходиться поза точкою короткого замикання (лінія електропередач проходить за межі точки короткого замикання), ворог може викрасти інформацію, безпосередньо підключивши обладнання технічної розвідки до лінії електропередач [6,7,8].

Окрім електромагнітних перешкод для заземлювальної лінії ОТЗС, існує також ймовірність витоку небезпечних сигналів у контур заземлення.

Під час роботи обладнання для обробки інформації на корпусі цих пристроїв можуть накопичуватися потенціали, що загрожують життю, через ємнісні з'єднання або інші зв'язки. Цей потенціал змінюється відповідно до схеми сигналу небезпеки, і сигнал небезпеки просочується в контур заземлення.

Для забезпечення безпеки персоналу все технічне обладнання заземлюється [8,9].

Заземлення, по суті, передбачає електричне з'єднання корпусу технічного обладнання із «землею», що дозволяє потенціалу, накопиченому на корпусі,

втікати в землю через контур заземлення та повертатися до нуля. Якщо система заземлення надійна та має достатньо низький опір, струм протікає швидше, а корпус обладнання для обробки інформації майже завжди нейтральний [8,9].

Однак, на практиці опір системи заземлення може не завжди відповідати вимогам, чим може скористатися зловмисник. На рисунку 1.6 показано технічний шлях витоку інформації через контур заземлення OTZS [6,7,8].

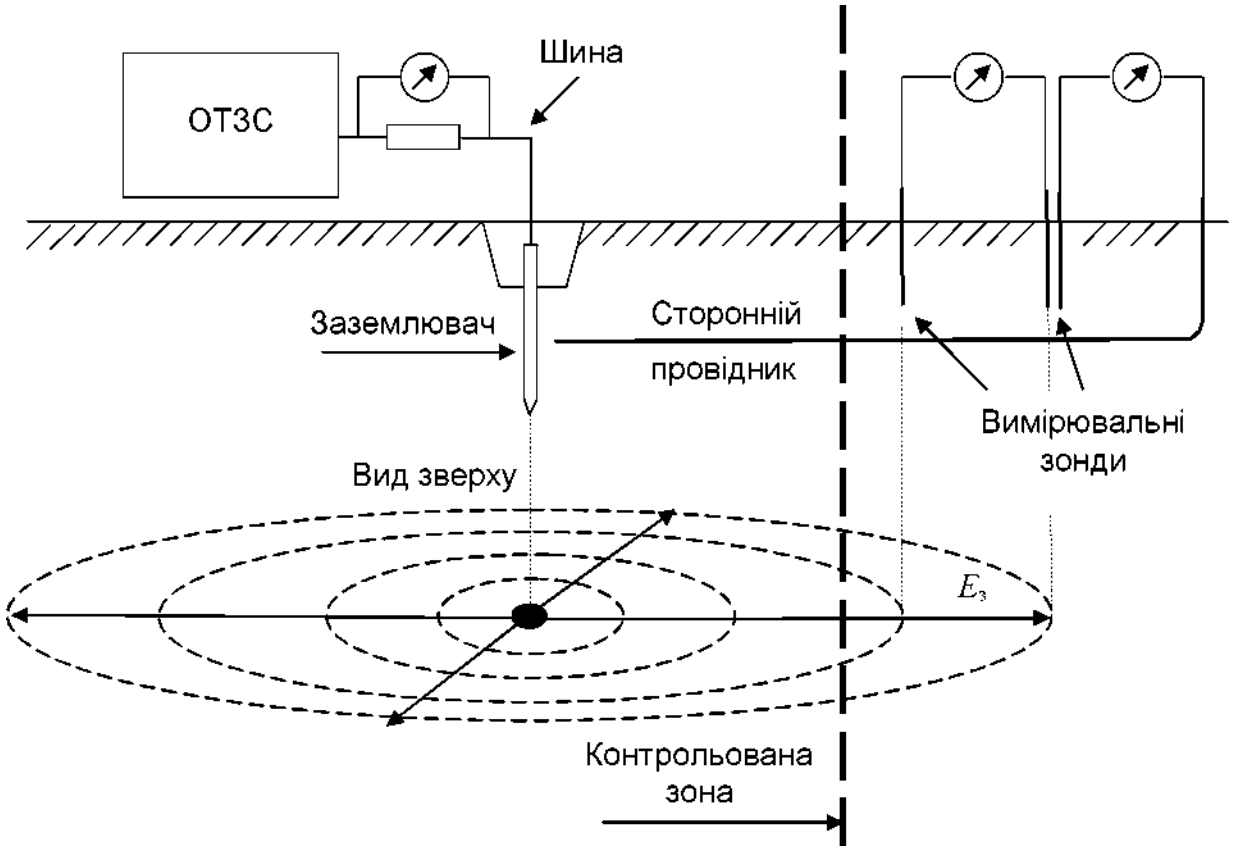


Рис. 1.6. Технічний канал витоку інформації ланцюгами заземлення ОТЗС.

Основні методи перехоплення сигналів небезпеки в заземлювальних контурах [8,9]:

1. Перехоплення сигналів небезпеки з низькоомної частини заземлювального контуру. Наприклад, недостатня міцність зварного шва, окислення контактів або мала площа поперечного перерізу заземлювальної шини.

2. Усунення різниці потенціалів ґрунту далеко від заземлювального провідника (джерела сигналу небезпеки), що можливо при високому опорі заземлення.

3. Усунення потенціалу зовнішніх провідників поблизу заземлювального провідника та ємнісно з'єднаних з ним.

4. Запобігання витоку інформації через бічні канали електромагнітних перешкод на лінії електропередач ОТЗС (запобігання генерації таких ТКВІ).

5. Перехоплення сигналів небезпеки з низькоомної частини заземлювального контуру. Наприклад, недостатня міцність зварного шва, окислення контактів або мала площа поперечного перерізу заземлювальної шини.

6. Усунення різниці потенціалів ґрунту далеко від заземлювального провідника — це джерело сигналу небезпеки, особливо при високому опорі заземлення.

7. Усунути потенціал зовнішніх провідників поблизу заземлювального провідника та ємнісно з'єднаних із ним [8,9,10]:

- Створити коротке замикання та встановити режим короткого замикання на інтелектуальному електронному пристрої (IED);

- Живити OTZS за допомогою незалежного джерела живлення (наприклад, електростанції, акумулятора тощо), розташованого в зоні короткого замикання та без зовнішнього електрообладнання;

- Використовувати пристрої технічного захисту в лінії живлення OTZS, такі як затримки сигналів низького рівня, мережеві фільтри та системи двигун-генератор;

- Виконувати лінійне придушення перешкод на лінії живлення OTZS. [17]

Для запобігання витоку інформації через бічні канали електромагнітних перешкод на заземлювальному проводі OTZS, включаючи витік сигналів небезпеки в контур заземлення (тобто запобігання генерації таких TCVI), можна вжити наступних заходів [8,9,10]:

- Встановити коротке замикання щонайменше зони 2 на OID та встановити метод доступу до короткого замикання;

- Заземлити OTZS та DTZS незалежно;

- Переконатися, що опір встановлення та заземлення OTZS відповідає вимогам;

- Розмістити заземлювальний вимикач та його заземлювальну шину в контрольованій зоні, якомога далі від меж короткого замикання та зовнішніх провідників;

- Виконати лінійне придушення перешкод на заземлювальному дроті OTZS. Бічний канал електромагнітних перешкод у зв'язку DTZS

Бічний канал електромагнітних перешкод у зв'язку DTZS, як тип каналу PEMN, формується шляхом безпосереднього видалення небезпечних електричних сигналів, індукованих у бічному електромагнітному полі OTZS та полі зв'язку OTZS під час роботи зі зв'язком DTZS, від зв'язку DTZS (лінії живлення, заземлення та передачі даних DTZS, лінії зв'язку, лінії безпеки, системи пожежної або загальної безпеки, системи енергопостачання та інші системи) (Рисунок 1.7) [8,9,10].

Якщо DTZS та її лінії живлення, заземлення та передачі даних розташовані в Зоні 1 OTZS, ці лінії індукуватимуть струми, подібні до сигналу небезпеки, засновані на принципі електромагнітної індукції, який поширюватиметься через лінії живлення, заземлення та передачі даних DTZS. Крім того, якщо ці лінії збігаються з лініями, з яких поширюється сигнал небезпеки, сигнал небезпеки може бути перенаправлений на лінії DTZS. Крім того, сигнал небезпеки може просочуватися в лінії живлення DTZS через схему

живлення DTZS. Якщо лінії живлення, заземлення або передачі даних DTZS виходять за межі Зони контролю безпеки (ЗБ), зловмисник може викрасти інформацію, безпосередньо підключивши обладнання технічної розвідки до цих ліній [8,9,10].

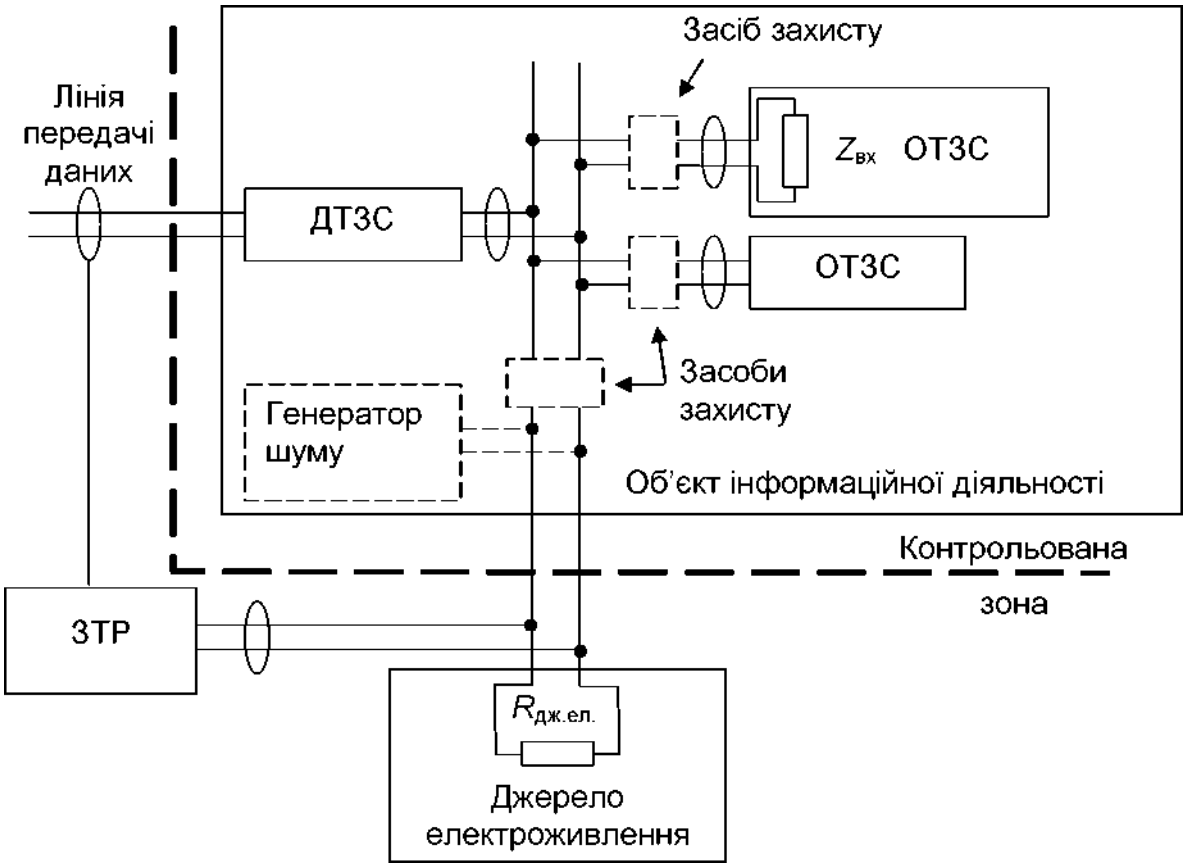


Рис. 1.7. Канали побічних електромагнітних наведень на комунікації ДТЗС.

Для запобігання витоку інформації зі зв'язку DTZS через бічні канали електромагнітних перешкод (тобто для запобігання генерації таких TCVI) можна вжити наступних заходів [8,9,10]:

- Встановити коротке замикання на OID та встановити режим доступу до короткого замикання;

- Розмістити DTZS та її лінії зв'язку поза Зоною 1 OTZS;

- Живити DTZS від незалежного джерела живлення (наприклад, електростанції, акумуляторної батареї тощо), розташованого в зоні короткого замикання;

- Використовувати заходи технічного захисту в лініях живлення DTZS, такі як затримка сигналів низького рівня, мережеві фільтри та генераторні установки;

- Виконувати лінійне придушення перешкод на лініях живлення DTZS;

- Забезпечити відповідність монтажного та заземлюючого опору DTZS вимогам;

- Встановити заземлювальні вимикачі із заземлювальними шинами якомога далі від меж короткого замикання та зовнішніх провідників у контрольованій зоні;

- Виконувати лінійне придушення перешкод на лініях заземлення ДТЗС.

Канал радіочастотних перешкод (для зняття інформації, що обробляється в ОТЗС)

Канал радіочастотних перешкод (для зняття інформації, що обробляється технічними засобами) – це параметричний канал, сформований наступним чином: Спеціально розроблений високочастотний сигнал (радіочастотний сигнал) вводиться в основні та/або допоміжні технічні засоби та системи через зв'язок поза зоною управління, і цей радіочастотний сигнал модулюється сигналом небезпеки, що діє на нелінійні елементи ОТЗС та/або ДТЗС [9,11]:

- Або радіочастотний сигнал відбивається від неузгодженого навантаження в ОТЗС та/або ДТЗС, поширюється за межі КС через зв'язок ОТЗС та/або ДТЗС, та видаляється за допомогою технічної розвідки при безпосередньому підключенні до зв'язку ОТЗС та/або ДТЗС поза КС;

- Або модульований радіочастотний сигнал випромінюється у вільний простір та перехоплюється короткозамкненим зовнішнім радіоприймним пристроєм технічної розвідки (рисунок 1.8) [9,11].

Майже всі методи обробки інформації використовують напівпровідникові електронні компоненти, провідність (опір) яких залежить від різниці потенціалів між їхніми двома полюсами. Якщо технологія обробки інформації піддається впливу високочастотних електромагнітних полів (мегагерцового діапазону), то при протіканні сигналу небезпеки через її ланцюг генеруватиметься індукований радіочастотний струм, який впливатиме на опір напівпровідника та інші параметри ланцюга TSC [9,11].

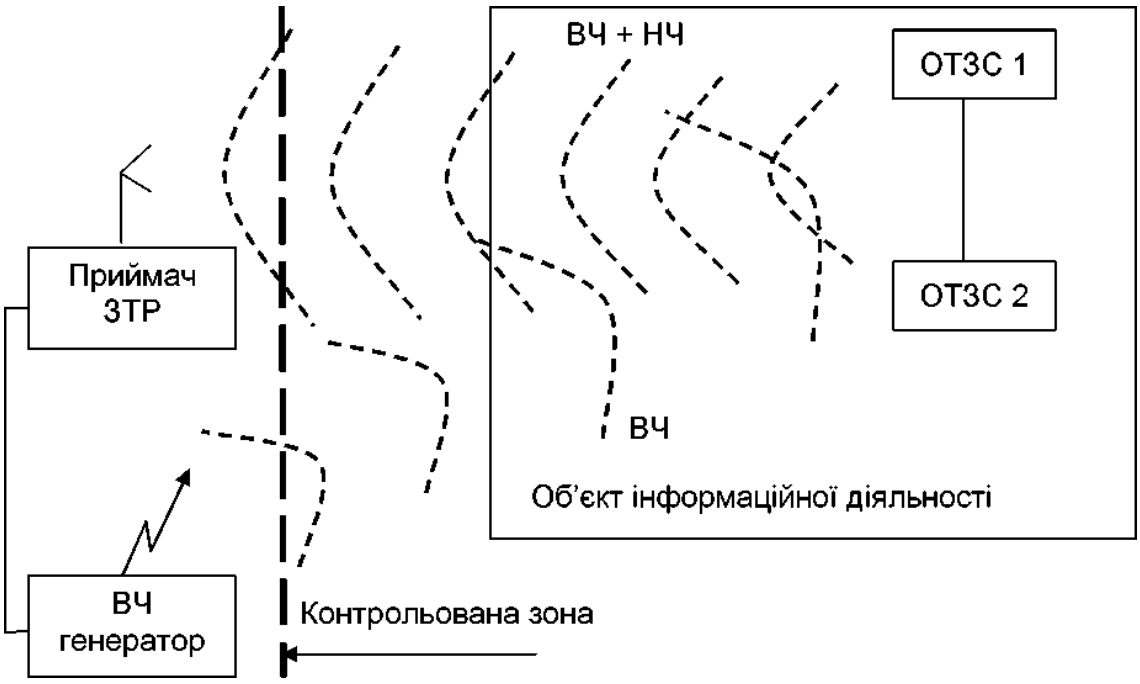


Рис. 3.7. Канал ВЧ нав'язування (для зняття інформації, що обробляється в ОТЗС).

Отже, схема паразитично модулюватиме небезпечний сигнал, зміщуючи його спектр у радіочастотну (РЧ) область. Це перевипромінювання модульованого РЧ-сигналу призводить до витоку інформації [8,9,10].

Слід зазначити, що в цьому випадку когерентні методи прийому можуть легко перехоплювати цей модульований РЧ-сигнал, забезпечуючи максимальну завадостійкість.

Заходи щодо запобігання витоку інформації через канали РЧ-перешкод (тобто там, де такі TCVI неможливо створити) включають:

- Створення коротких замикань щонайменше зони 2, розрахованих на врахування потенційних РЧ-перешкод, та організацію схем доступу коротких замикань на OID;

- Екранування OTZ;

- Екранування просторового електромагнітного шуму на об'єкті ЕОТ;

- Індикацію та випромінювання сигналів поля РЧ-випромінювання та запобігання роботі OTZ.

Тому в цьому розділі розглядаються основні типи каналів витоку технічної інформації, що утворюються під час обробки об'єктів інформаційної діяльності, та основні заходи щодо запобігання витоку інформації через ці канали (запобігання утворенню таких каналів витоку технічної інформації).

1.3 Висновок по першому розділу

У цьому розділі аналізуються основні канали витоку технічної інформації об'єктів інформаційної діяльності.

У цьому розділі класифікуються канали, через які відбувається витік технічної інформації всередині об'єктів інформаційної діяльності.

У цьому розділі розкривається природа, характеристики та методи формування каналів витоку інформації, що виникають з основних технічних засобів та систем обробки, що беруть участь в інформаційній діяльності.

РОЗДІЛ 2.
РОЗРОБКА ЄДИНОЇ МОДЕЛІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ВІД ВИТОКУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ КАНАЛАМИ

2.1. Розробка вимог захисту від витоку технічної інформації

Нижче наведено потенційні канали витоку технічної інформації для інформаційної діяльності:

1. Канал бічного електромагнітного випромінювання (SEM) ОТЗС;

2. Канал бічного електромагнітного випромінювання ДТЗС;

3. Канал бічного електромагнітного випромінювання лінії електропередач ОТЗС (заземлення);

4. Канал бічного електромагнітного випромінювання зв'язку ДТЗС;

5. Канал високочастотних перешкод;

6. Канал витоку оптичної інформації;

7. Встановлення вбудованих пристроїв.

Вищезазначені канали витоку технічної інформації повинні бути запобігнуті наступними вимогами [11,12]:

- Захист бічного каналу електромагнітного випромінювання ОТЗС шляхом екранування ОТЗС або часткового екранування електронних компонентів.

- Захист бічного каналу електромагнітного випромінювання ДТЗС шляхом визначення зони випромінювання R1 та пропозиції розміщення ноутбука поза цією зоною.

- Проблему бічних каналів електромагнітних перешкод (EMI) на лінії електропередачі OTZS (заземленій) можна вирішити шляхом впровадження лінійного придушення шуму на лінії електропередачі OTZS.

- Проблему бічних каналів EMI на зв'язку DTZS можна вирішити шляхом: використання незалежного джерела живлення для DTZS, такого як електростанція або акумулятор; використання пристроїв технічного захисту, що затримують сигнали низького рівня; та встановлення мережевих фільтрів у лінії електропередачі DTZS.

Друге рішення полягає у встановленні лінійних пристроїв придушення шуму в блоці живлення [9,11]:

- Усунення каналів радіочастотних перешкод шляхом екранування OTZS.

- Канали витоку оптичної інформації повинні бути усунені персоналом, який самостійно оцінює навколишнє середовище.

- Встановлення вбудованих пристроїв слід вирішити шляхом впровадження організаційних заходів для запобігання проникненню неавторизованого персоналу до приміщення або шляхом використання пошукового обладнання для огляду приміщення, коли це необхідно.

Загалом, враховуючи вищезазначені впливи, методи запобігання витоку інформації під час обробки EOT та уникнення TCVI включають [9,11]:

- Створення коротких замикань щонайменше Зони 2 (ця Зона 2 повинна враховувати всі технологічні канали витоку інформації, властиві об'єкту EOT);

- Оптимізація методів доступу для коротких замикань та IED;

- Екранування EOT;

- Введення просторового електромагнітного шуму на об'єкт EOT;

- Індикація відхилень параметрів підсилювача та запобігання роботі EOT;

- Розміщення DTZ подалі від Зони 1 EOT та розміщення EOT поблизу його Зони 1, де можуть бути присутні зовнішні провідники;

- Використовування пристроїв технічного захисту в лінії DTZS для затримки сигналів низького рівня;

- Використовування лінійного шуму в лінії DTZS та зовнішніх провідниках;

- Живлення OTZS за допомогою незалежного джерела живлення (наприклад, електростанції, акумулятора);

- Використовування пристроїв технічного захисту в ланцюзі живлення OTZS для затримки сигналів низького рівня та мережевих фільтрів;

- Використання лінійного шуму в ланцюзі живлення ОТЗС;

- Незалежне заземлення ОТЗС;

- Забезпечити виконання вимог до встановлення заземлювального кронштейна OTZS;

- Розмістити заземлювальний вимикач та його заземлювальну шину в контрольованій зоні та якомога далі від меж короткого замикання та зовнішніх провідників;

- Придушити шум від заземлювальних ліній OTZS та DTZS.

2.2. Захисні заходи для запобігання витоку інформації через технічні канали

Створення KSIZ (інформаційного щита безпеки знань) в об'єктах інформаційної діяльності для запобігання витоку інформації через технічні канали повинно базуватися на наступних трьох заходах захисту інформації [9,11,12]:

1. Захист технічної інформації

2. Процедурний захист інформації

3. Організаційний та технічний захист інформації

Фаза 1 створення KSIZ для запобігання витоку інформації через технічні канали

Фаза 1: Забезпечити технічний захист АС (комунікації програм) та запобігти витоку інформації через технічні канали [12,13]. На першому етапі

слід впровадити основні заходи технічного захисту та провести дослідження для визначення PEVMN (Процедурної, Програмної та Технічної Інформаційної Мережі). Зокрема, слід впровадити екранування технічних каналів, встановити пристрої лінійного придушення шуму в блоках живлення електронних пристроїв, а також виявити потенційне випромінювання та перешкоди для подальшого уточнення експлуатаційної документації [12,13].

Впроваджена система технічного захисту для запобігання витоку інформації через технічні канали повинна бути сертифікована. Ця система базується на пасивних заходах захисту та лінійному придушенні шуму, і за результатами сертифікації має бути виданий «Сертифікат сертифікації системи автоматизації» [12,13,14].

Другий етап: Перевірка системи інформаційних технологій (ITC) та підготовка початкових даних до вимог KSZI

На цьому етапі зазвичай виконуються такі завдання [12,13,14]:

- Аналіз відповідних нормативних актів для визначення підстав для обмеження або заборони доступу до певних типів інформації та визначення необхідності забезпечення захисту інформації відповідно до інших стандартів;

- Визначити перелік інформації, яку необхідно обробляти автоматично, та класифікувати її відповідно до відповідних норм на основі рівнів обмеження доступу, вимог до забезпечення цілісності та вимог до забезпечення доступності [8,12,14].

Дослідження повинно враховувати такі аспекти:

- Технічні системи;

- Програмні компоненти;

- Оброблена інформація;

- Користувачі;

- Дозволи на доступ до місцезнаходження.

Фаза третя: Розробка стратегії безпеки

На цьому етапі буде виконано наступну роботу [12,13,14]:

- Аналіз ризиків (вивчення моделей загроз та зловмисників, а також можливих наслідків реалізації потенційної загрози);

- Визначення вимог до заходів, методів та засобів захисту інформації;

- Вибір основних рішень для усунення всіх основних загроз, розробка вимог, правил, обмежень та рекомендацій щодо використання захищених технологій обробки інформації в інтелектуальних транспортних системах (ITC), а також конкретних заходів та засобів захисту інформації та регулювання діяльності різних груп користувачів;

- Документування стратегії інформаційної безпеки [12,13,14].

Політика інформаційних систем повинна враховувати всі характеристики середовища обробки інформації та бути повністю модифікованою відповідальним за захист інформації клієнтської організації. Політика не повинна містити наступні вимоги, перелічені розробниками AS.

Політика повинна бути розроблена як окрема система, що включає [12,13,14]:

- Посібник користувача;

- Посібник системного адміністратора;

- Посібник адміністратора безпеки.

Посібник користувача повинен чітко визначати методи та правила обробки інформації, ігнорування яких може призвести до реалізації загроз та розкриття інформації [12,13,14].

Фаза 4: Розробка технічної специфікації (TOR) на створення KSIZ

Технічна специфікація на створення KSIZ в ITS є початковим організаційно-технічним документом. Вона визначає вимоги до захисту інформації, що обробляються в ITS, процедуру створення KSIZ, процедуру проведення всіх видів тестування KSIZ та процедуру її розгортання як частини ITS.

Технічні умови на створення Інформаційної зони безпеки (ІЗБ) повністю враховують комплексний підхід до побудови ІЗБ, який інтегрує всі необхідні заходи та засоби в єдину систему для вирішення різних загроз інформаційній безпеці на кожному етапі життєвого циклу Інтелектуальної транспортної системи (ІТС) [14,15].

Обсяг повноважень (ТОЗ) для ІЗБ може використовуватися як для новостворених ІТС, так і для модернізації існуючих ІТС.

Обсяг повноважень (ТОЗ) для ІЗБ може бути розроблений такими способами [16,17]:

- Як окремий розділ загальних технічних умов на створення ІТС;

- Як окрема (часткова) сфера повноважень (ТОЗ);

- Як доповнення до загальної області повноважень (ТОЗ) на створення ІТС.

Для інтегрованих ІТС (що складаються з кількох незалежних інформаційних або комунікаційних систем, які можуть працювати незалежно та взаємодіяти одна з одною) рекомендується створювати окрему ІЗБ для кожного компонента ІТС та формалізувати вимоги як окрему область повноважень (ТОЗ). Технічний довідник (ТД) може бути розроблений для кількох ідентичних компонентів Інтелектуальної транспортної системи (ІТС) з описом їхніх відмінностей або характеристик [10,12,16].

Фаза 5: Розробка та впровадження проекту KSIZ в рамках ІТС.

Проект KSIZ розробляється на основі та відповідно до Технічного довідника (ТД), створеного ІТС, та реалізується на таких етапах, створених ІТС: попередній проект, технічний проект та робоча документація.

Під час розробки проекту KSIZ необхідно обґрунтувати та сформулювати проектні рішення, щоб забезпечити сумісність та взаємодію різних компонентів KSIZ, а також різних заходів та засобів захисту інформації [15,16].

Необхідно прийняти необхідні спільні рішення для реалізації вимог Технічного довідника (ТД) KSIZ, включаючи організаційну структуру KSIZ, структуру технологічних та програмних засобів, алгоритми роботи та умови використання засобів захисту, а також впровадження послуг інформаційної безпеки, визначених відповідно до функціонального профілю безпеки.

Фаза 6: Впровадження CSI для запобігання витоку через канали передачі технічних даних. На цьому етапі розробка CSI має бути завершена, система адаптована до операційного середовища, а документація, що міститься в плані захисту, має бути затверджена [15,16].

Усі категорії користувачів ITC (технічний обслуговуючий персонал, звичайні користувачі) повинні пройти навчання з основних умов та процедур документа плану захисту, щоб забезпечити дотримання ними правил політики інформаційної безпеки та правильне використання засобів захисту інформації. [13,15,16]

Встановіть та перевірте програмні продукти, необхідні для обробки інформації та засобів захисту інформації, відповідно до методів обробки та передачі інформації.

Під час встановлення мають бути ввімкнені всі механізми, що обмежують доступ користувачів до інформації та апаратних ресурсів ITC, механізми контролю роботи користувачів, а також механізми моніторингу цілісності програмного забезпечення та захисту бази даних. [16,17]

Введіть інформацію про користувачів AS до засобу захисту та встановіть їхні права доступу до захищених ресурсів та середовища обробки/передачі інформації.

Фаза 7: Попереднє тестування AS

Під час попереднього тестування працездатність системи визначається шляхом обробки інформації користувачем. Розробники системи намагатимуться вплинути на систему, здійснюючи атаки на комп'ютерну

систему. Оцінка системи стосується центральної системи захисту даних [17]. Усі виявлені дефекти та проблеми були усунені. Фаза 8. Державна сертифікація інформаційних систем (АС)

Комплексна система захисту інформації, що перебуває у державній власності, інформації з обмеженим доступом або іншої інформації, що охороняється державою, повинна мати сертифікат відповідності вимогам захисту інформації. Цей сертифікат видається Державною службою захисту інформації та комунікаційних технологій України за результатами державної сертифікації. [17,18,19]

Державна сертифікація інформаційної системи (КСЗІ) має на меті визначити, чи відповідає вона вимогам технічних завдань, відповідним законам та нормативним актам щодо захисту інформації, а також чи може бути введена в експлуатацію як частина інформаційно-технологічної системи (ІТС).

Державна сертифікація КСЗІ є етапом приймальних випробувань ІТС та проводиться відповідно до «Положення про державну сертифікацію у сфері технічного захисту інформації». [17,18,19]

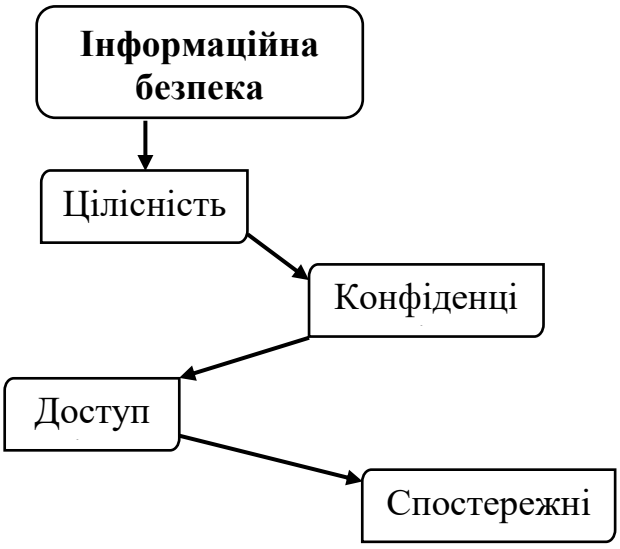
Фаза 9: Підтримка КСЗІ

На цій фазі будуть проводитися роботи із забезпечення організації та функціонування КСЗІ, а також з управління його запланованою модернізацією та заходами захисту інформації відповідно до «Плану захисту» та експлуатаційної документації компонентів КСЗІ. [17,18,19]

Усі дії, пов’язані з модернізацією та обслуговуванням АС, повинні відповідати специфікаціям, викладеним в експлуатаційній документації, та повинні дотримуватися політики захисту інформації.

2.3. Огляд єдиної інтегрованої системи запобігання витокам технологічного каналу

КСЗІ буде побудовано на портативному електронному комп’ютері, що дозволить гнучко та мобільно використовувати як апаратні, так і програмні компоненти. Ця система характеризується значно швидшим розгортанням порівняно з типовими процедурами побудови КСЗІ на персональному комп’ютері.Захист інформації на основі CSI повинен враховувати та забезпечувати цілісність, конфіденційність та доступність інформації, а також дозволяти моніторинг операцій користувачів та роботи системи [18,19,20].



Цілісність інформації – це атрибут інформації, який запобігає її зміні неавторизованими користувачами та/або процесами [19,20].

Конфіденційність інформації – це атрибут інформації, який запобігає доступу до неї неавторизованими користувачами та/або процесами [19,20].

Доступність – це атрибут системних ресурсів (КС, сервісів, об'єктів КС, інформації), що означає, що користувачі та/або процеси з відповідними дозволами можуть використовувати ресурс відповідно до правил, викладених у політиці безпеки, не чекаючи понад заданий (короткий) період часу; тобто ресурс доступний у формі, запитуваній користувачем, у місці, запитуваному користувачем, та в час, запитуваний користувачем [19,20].

Підзвітність – це атрибут КС, який дозволяє реєструвати діяльність користувачів та процесів, використовувати пасивні об'єкти та чітко ідентифікувати ідентифікатори користувачів та процесів, задіяних у певних подіях, для запобігання порушенням політик безпеки та/або забезпечення підзвітності за певні дії [17,20].

Побудова KSIZ повинна відповідати чіткому шаблону схеми без будь-яких відхилень. Для оптимізації термінів розгортання KSIZ всю документацію слід розділити на дві частини [18,19,20]:

- Експлуатаційна документація, яка використовується для запобігання витоку інформації через технічні канали під час розробки KSIZ, є основою для організаційної документації;

- Організаційна документація, що містить початкові вимоги для визначення потреб у підмоделях захищених ноутбуків, і, після того, як ноутбуки будуть використані, включає політики інформаційної безпеки та інструкції з експлуатації користувачів.

Базова політика захисту інформації повинна надаватися разом із ноутбуками та базуватися на їх категорії, функціональності та визначеннях безпеки інформаційних технологій. Внутрішні політики повинні бути розроблені на основі цієї базової політики при розгляді AS.

Окрім забезпечення системи CCDS, запобігання витоку інформації через технічні канали також має вирішальне значення при використанні ноутбуків. Ключові технічні канали витоку інформації описані в розділі 1.1.

2.4. Висновок по другому розділу

У цьому розділі представлені результати дослідження щодо того, як покращити єдину модель для запобігання витоку інформації через технічні канали.

У цьому розділі окреслено вимоги до захисту технічних каналів для запобігання несанкціонованому витоку інформації.

У цьому розділі визначено заходи безпеки для запобігання витоку інформації через технічні канали.

У цьому розділі наведено загальний опис єдиної моделі запобігання витоку інформації через технічні канали.

РОЗДІЛ 3.
КОМПЛЕКСНА СИСТЕМИ ЗАХИСТУ ОБ'ЄКТУ ІНФОРМАЦЙНОЇ ДІЯЛЬНОСТІ ВІД ВИТОКУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ КАНАЛАМИ

3.1 Вимоги законодавства щодо розробки комплексної системи захисту інформації на об'єкті інформаційної діяльності

Побудова ключових зон інформаційної безпеки (КЗІБ) здійснюється відповідно до Національного нормативного акту ТЗІ 3.7-003-05 «Порядок створення інтегрованих систем захисту інформації в інформаційно-комунікаційних системах». Незалежно від того, чи створюється КЗІБ у проектованій ІТС, чи в існуючій ІТС, процедура створення КЗІБ однакова, якщо потрібно забезпечити інформаційну безпеку або модернізувати існуючу КЗІБ [13,14].

Процес створення інтегрованої системи захисту інформації передбачає реалізацію низки взаємоузгоджених заходів, спрямованих на розробку та впровадження інформаційних технологій, що забезпечують відповідність обробки інформації в ІТС відповідним нормативним актам та національним нормам у сфері захисту інформації. Ця Національна директива розглядає процедуру створення складних систем захисту інформації в інтелектуальних транспортних системах (ІТС) як низку хронологічно впорядкованих, взаємопов'язаних та об'єднаних незалежних робочих фаз, реалізація яких є необхідною та достатньою для створення системи захисту критичної інформації (КСЗІ) [18,19,20]. Послідовність реалізації та типовий зміст робіт кожного етапу створення КСЗІ повинні відповідати відповідним етапам та робочим крокам створення ІТС, визначеним у ГОСТ 34.601 [18,19,20].

Етапи робіт, що виконуються під час створення КСЗІ в конкретній ІТС, їх зміст, результати та терміни виконання визначаються Планом робіт зі створення КСЗІ (ТЗ). [13]

Окремі етапи робіт можуть бути пропущені або кілька етапів можуть бути об'єднані, а також можуть бути додані нові етапи робіт. За необхідності порядок виконання етапів може бути змінений — наприклад, виконання кількох етапів одночасно, або виконання етапу до завершення попереднього етапу тощо — за умови, що це не призведе до зниження якості робіт або не суперечитиме цілям реалізації [18,19,20].

Якщо в галузі вже впроваджено встановлені процедури, а також діють відомчі Правила захисту технічної інформації (НД ТЗІ) або існують відповідні нормативні документи, що поширюються на організацію-власника Інтелектуальної транспортної системи (ІТС) або на саму ІТС, ці правила мають вищу чинність і повинні дотримуватися в першу чергу. Якщо певний вид робіт не підпадає під дію жодного з вищезазначених рівнів національних нормативних баз захисту технічної інформації, то допускається прийняття рекомендацій міжнародних стандартів за умови, що це не суперечить українським нормативним актам та правовим документам.[13]

3.2 Процедури та пристрої комплексної системи захисту технічної інформації об'єктів інформаційної діяльності

КСЗІ включає засоби реалізації наступних методів, механізмів та заходів для захисту інформації від наступних шкідливих наслідків [18,19,20]:

- Витік через технічні канали, включаючи канали бічного електромагнітного випромінювання та перешкод, акустичні та електричні канали та інші канали;

- Несанкціоновані операції та несанкціонований доступ до інформації, наприклад, шляхом підключення до обладнання та ліній зв'язку, видавання себе за зареєстрованих користувачів, обхід заходів захисту тощо. Використання інформації або нав'язування неправдивої інформації, використання вбудованих пристроїв чи програм, використання комп'ютерних вірусів тощо;

- Здійснення спеціального впливу на інформацію, наприклад, шляхом формування полів та сигналів для порушення цілісності інформації або для компрометації систем захисту [13,14].

Для кожної конкретної Інтелектуальної транспортної системи (ІТС) склад, структура та вимоги до Інформаційної системи безпеки інформації (ІСБІ) залежать від характеристик інформації, що обробляється, типу автоматизованої системи та умов експлуатації ІТС.

Там, де це дозволено законом, проектування, розробка, виготовлення, випробування та експлуатація ІТС повинні поєднуватися із заходами щодо забезпечення конфіденційності, запобігання поширенню технічної інформації та організації заходів щодо захисту інформації, яка не є державною таємницею та має обмежений доступ. [13]

Відповідно до статті 5.8 Декрету № НД ТЗІ 3.7-003-2005, якщо інформаційно-технологічна система (ІТС) обробляє інформацію, що становить державну таємницю, або якщо власник інформації вважає це необхідним, має бути створена система технічного захисту, щоб запобігти витоку інформації через технічні канали. У цій статті особливо підкреслюється важливість власника інформації. Сама система технічного захисту може бути не обов'язковою, але до заходів технічного захисту необхідно ставитися серйозно. У всіх інформаційно-технологічних системах (ІТС) має бути створена система захисту державної таємниці (СЗДТ), якщо інформація, що обробляється, є державною власністю, становить державну чи іншу таємницю, або належить до певних видів інформації, що потребує захисту згідно з певними законами, або якщо власник інформації вважає за необхідне захистити інформацію. Рішення про необхідність вжиття заходів для захисту інформації від спеціального впливу приймається власником інформації індивідуально виходячи з конкретних обставин [18,19,20].

Для організації створення інфраструктури інформаційної безпеки (ІІБ) в рамках інформаційно-технологічної системи (ІТС) створюється служба захисту

інформації (СЗІ). Процедури, завдання, функції, структура та повноваження цієї служби визначені в НД 1.4-001-2000.

СІС створюється після прийняття рішення про створення ІЗІ. Як виняток, СІС може бути створена на наступному етапі, але не пізніше етапу підготовки до впровадження ІЗІ [13,16,19].

Служба захисту інформації є невід'ємною частиною будь-якої системи, що потребує захисту. Структура самої Служби захисту інформації повинна бути ретельно розглянута, виходячи з розміру організації та кількості співробітників.

Для малих підприємств достатньо призначити 1-2 співробітників, відповідальних за захист інформації, та доручити їм виконання обов'язків служби захисту інформації; тоді як для великих підприємств слід створити щонайменше відділ інформаційної безпеки.

3.3 Етап побудови комплексної системи захисту інформації для інформаційної діяльності

Етап 1: Початкова підготовка даних для обстеження інформаційно-технологічних послуг (ІТС) та збір вимог до Системи інформаційної безпеки (КСЗІ). На цьому етапі зазвичай необхідно виконати такі завдання [18,19,20]:

- Проаналізувати нормативно-правові документи, які можуть нав'язувати або забороняти певні види доступу до інформації, та визначити необхідність забезпечення захисту інформації відповідно до інших стандартів;

- Визначити перелік інформації, що підлягає автоматизованій обробці, та класифікувати її відповідно до рівня обмеження доступу, вимог до забезпечення цілісності та вимог до забезпечення доступності відповідно до нормативно-правових документів.

Під час огляду Інтелектуальної транспортної системи (ІТС) вона розглядається як організаційно-технічна система, що поєднує обчислювальні

системи, фізичні середовища, середовища користувачів, оброблювану інформацію та технології обробки (далі - операційне середовище ІТС) [18,19,20].

Метою огляду є опис кожного операційного середовища ІТС, визначення елементів, які можуть прямо чи опосередковано впливати на інформаційну безпеку, визначення взаємодії між різними елементами середовища та документування результатів огляду для використання на наступних етапах роботи [18,19,20].

Етап другий: Розробка стратегії безпеки. Під час цього етапу будуть виконані такі роботи:

− Аналіз ризиків (вивчення моделей загроз та зловмисників, а також потенційних наслідків реалізації потенційних загроз);

− Визначення вимог до заходів, методів та засобів захисту інформації;

− Вибір основних рішень для усунення всіх основних загроз, розробка вимог, правил, обмежень та рекомендацій щодо використання захищених технологій обробки інформації в Інтелектуальній транспортній системі (ІТС), а також конкретних заходів та засобів захисту інформації та регулювання діяльності різних груп користувачів;

− Складання документів політики інформаційної безпеки.

Політика безпеки повинна враховувати характеристики кожного компонента Системи інформаційної безпеки (СІБ) та може бути розроблена для всієї ІТС, окремих компонентів компонента, конкретних функціональних завдань або конкретних технологій обробки інформації. Політика безпеки пишеться у вигляді окремого документа плану захисту [18,19,20].

Фаза третя: Розробка Технічного завдання на створення Системи інформаційної безпеки (СІБ) (далі – ТЗ). Технічне завдання створення КСЗІ в ІТС полягає у написанні початкових організаційно-технічних документів, що визначають вимоги до захисту інформації, що обробляється в ІТС.

Процедури створення інформаційно-ізольованих зон безпеки знань (ЗІЗЗ), проведення різних тестів ЗІЗЗ та їх розгортання як частини інтелектуальних транспортних систем (ІТС) [18,19,20].

Розробка технічного завдання (ТЗ) на створення ЗІЗЗ враховує комплексний підхід до побудови ЗІЗЗЗ, інтегруючи всі необхідні заходи та засоби в єдину систему на кожному етапі життєвого циклу ІТС для вирішення різних загроз інформаційній безпеці. ТЗЗЗЗ може бути розроблено для новостворених ІТС або під час модернізації існуючих ІТС.

ТЗЗ може бути розроблено такими способами [18,19,20]:

− Як окремий розділ у загальному технічному завданні на створення ЗІЗЗЗ;

− Як окреме (часткове) ТЗЗЗ;

− Як доповнення до загального ТЗЗЗЗЗЗ.

Для Інтегрованих інтелектуальних транспортних систем (ІТС, що складаються з кількох незалежно працюючих та інтерактивних інформаційних або комунікаційних систем) рекомендується створити окрему Систему знань, безпеки та інформації (СЗБІ) для кожного компонента ІТС та формалізувати вимоги в окремі Технічні специфікації (ТС). Як варіант, можна розробити одну СЗБ для кількох ідентичних компонентів ІТС, вказавши їхні відмінності або характеристики. [11]

Фаза 4: Розробка та впровадження проектів СЗБІ в рамках ІТС

Розробка проектів СЗБІ базується та реалізується відповідно до технічних специфікацій, створених для ІТС, і відбувається протягом таких фаз створення ІТС: попереднє проектування, технічне проектування та робоча документація.

Під час розробки проектів СЗБІ необхідно перевірити та сформулювати проектні рішення, щоб забезпечити сумісність та взаємодію між різними компонентами СЗБІ, а також різні заходи та засоби захисту інформації.

Для реалізації вимог ТЗ KSIZ розробляються необхідні спільні рішення, включаючи організаційну структуру KSIZ, архітектуру апаратного та програмного забезпечення, алгоритми роботи та умови використання засобів захисту, а також впровадження послуг інформаційної безпеки відповідно до функціональних профілів безпеки.

Фаза 5: Експлуатація KSIZ.

На цьому етапі розробка KSIZ має бути завершена, а документи, що входять до плану захисту, мають бути затверджені.

Усі категорії користувачів ІТС (персонал технічної служби та звичайні користувачі) повинні пройти навчання з ключових термінів та процедур документів плану захисту для забезпечення дотримання політики інформаційної безпеки та правил експлуатації засобів захисту інформації.

Впроваджена система технічного захисту інформації для запобігання витокам через технічні канали проходить сертифікацію, після завершення якої буде видано «Сертифікат сертифікації системи технічного захисту інформації».

Згідно з робочою документацією проекту, система засобів захисту інформації для запобігання НРД буде встановлена, ініціалізована та валідована в операційній діяльності. Під час встановлення необхідно враховувати механізми доступу всіх ізольованих користувачів до інформації та апаратних ресурсів ITS, механізми контролю операцій користувачів, а також засоби контролю цілісності програмного забезпечення та бази даних. Захист.

Внести інформацію користувачів Інтелектуальної транспортної системи (ІТС) до бази даних захисту та визначити їхні дозволи на доступ до об'єктів ІТС, що захищаються, включаючи створення, модифікацію, архівування, знищення та експорт/імпорт об'єктів із системи.

Фаза 6: Попереднє тестування.

Метою попереднього тестування є перевірка працездатності КСЗІ, її відповідності технічним характеристикам та визначення можливості введення КСЗІ в дослідну експлуатацію. Попереднє тестування проводиться відповідно до встановлених процедур та методів тестування. Тестування організовується замовником ІТС та спільно виконується розробником КСЗІ та замовником.

Фаза 7: Дослідна експлуатація. Під час дослідної роботи КСЗІ:

- Тестування технологій, що використовуються для захисту оброблюваної інформації, потоку машинних носіїв інформації, обмеження доступу користувачів до ресурсів ІТС та автоматичного керування операціями користувачів;

- Персонал системи захисту інформації та користувачі ІТС отримують практичні навички використання технологій захисту інформації, програмних та апаратних засобів, а також опановують вимоги щодо забезпечення режимів доступу, викладені в організаційних та нормативних документах;

- Фіналізація програмного забезпечення та завершення інших налаштувань та конфігурацій КПП НСД;

- Завершено розробку робочої та експлуатаційної документації.

Пробний запуск ІТС має бути проведений без використання інформації, що становить державну таємницю. Якщо КСІЗ використовує інструментарій захисту інформації НСД, і цей комплекс ще не отримав експертного висновку щодо його відповідності вимогам НД ТЗІ, під час національної експертизи КСІЗ необхідно виконати низку завдань для оцінки його відповідності вимогам НД ТЗІ.

Фаза 8: Національна експертиза КСІЗ. Інформаційні системи, що перебувають у державній власності, інформація з обмеженим доступом або інша інформація, що охороняється державою, повинні мати сертифікат

відповідності вимогам захисту інформації, виданий Державною службою захисту інформації України за результатами державної експертизи. Державна експертиза системи захисту інформації (СЗІ) має на меті визначити, чи відповідає вона вимогам технічних завдань, законодавства та нормативних актів щодо захисту інформації, а також чи може СЗІ бути введена в експлуатацію як частина системи інформаційних технологій (СІТ). Державна експертиза ЦБІ є етапом приймально-здавальних випробувань ІТС та проводиться відповідно до Положення про державну експертизу у сфері захисту технічної інформації. Якщо ІТС обробляє інформацію, що перебуває у державній власності, або інформацію, що охороняється державою, керівник організації може наказати ІТС ввести її в експлуатацію лише після отримання сертифіката відповідності ЦБІ. [12] Фаза 1: Підтримка ЦБІ. На цьому етапі будуть проводитися роботи щодо забезпечення організації та функціонування Центру безпеки інформаційних систем (ЦБІ), планової модернізації та управління ресурсами. Захист інформації здійснюється відповідно до плану захисту та експлуатаційної документації компонента Управління інформаційними системами (ІСУ). [10,17]

3.4. Розробити та зареєструвати стратегії інформаційної безпеки для запобігання витоку через технічні канали для об'єктів інформаційної діяльності.

На цьому етапі розробники ІСУ проведуть детальне дослідження об'єктів, що будуть створені в ІСУ, на основі моделей загроз, моделей потенційних зловмисників та результатів аналізу потенційних ризиків. На основі результатів дослідження мають бути розроблені стратегії інформаційної безпеки для Системи інформаційних технологій (ІТС) та Об'єктів інформаційної діяльності (ОІД).

Крім того, на цьому етапі будуть виконані такі роботи:

- Вибір основних рішень для усунення всіх основних загроз, розробка рекомендацій щодо використання захищених технологій обробки інформації в ІТС, конкретних заходів та засобів захисту інформації, а також загальних вимог, правил, обмежень та рекомендацій для різних видів діяльності користувачів;

- Написання документів політики інформаційної безпеки. [13]

Політика безпеки повинна розроблятися під час виробничого процесу всієї системи захисту та уточнюватися відділом захисту інформації під час процесу введення підприємства в експлуатацію. Створення системи TZI поділяється на три фази:

- Розробка системи TZI (Фаза 1);
- Впровадження системи TZI (Фаза 2);
- Сертифікація системи TZI (Фаза 3).

Конкретний зміст робіт та процедури для кожного етапу створення системи TZI зазначені в положенні про систему TZI. [10]

Вимоги до запобігання витоку інформації через технічні канали та стандарти інформаційної безпеки зазначені в положенні та нормативних актах про систему TZI.

3.5 Рекомендації щодо використання технічних засобів для запобігання витоку інформації від цілей інформаційної діяльності

Методи запобігання витоку інформації через технічні канали мають різні характеристики та функції:

Бездротовий комунікаційний екран «SB TZI 7-1»: Ефективність цього засобу залежить від різних факторів, включаючи відстань до джерела

випромінювання, відстань до приймача, інтенсивність випромінювання та коефіцієнт спрямованості антени [17,19].

Акустичний екран «МАРС-АКЗ»: Призначений для запобігання витоку інформації з місць розташування через акустичні канали. Включає акустичний випромінювач та вимикач для відключення акустичного випромінювача від лінії.

Коли генератор шуму не має вихідного сигналу, динамік не може використовуватися як мікрофон. Чутливість: (83±2) дБ; Номінальний імпеданс: 10 Ом; Номінальна потужність: не більше 5 ВА [17,19].

Протиперешкодний фільтр FZP-110-2 має характеристики щодо робочої напруги, струму розсіювання потужності, струму витоку та діапазону частот. Номінальна робоча напруга: 220 В (50 Гц), номінальний струм розсіювання потужності: 10 А, струм витоку не більше 15 мА, діапазон частот: від 10 кГц до 18000 кГц [19].

Вібраційні випромінювачі марки VI: Ці вібраційні випромінювачі працюють у діапазоні частот від 180 Гц до 5600 Гц та мають опір обмотки 50 Ом.

Генератор шуму марки «Базальт-5»: Призначений для запобігання витоку інформації з об'єктів через бічне електромагнітне випромінювання. Цей генератор створює потужне просторове електромагнітне шумове поле в широкому діапазоні частот від 0,1 до 1000 МГц. [18,19]

З безперервним розвитком технологій заходи захисту інформації стають все більш важливими. Фільтр захисту від мережевих перешкод типу FZP103-2 є одним із надійних рішень у промисловій сфері. Ці фільтри відповідають стандартам ТУ У 31.1-31731859-001-2003, забезпечуючи інформаційну безпеку та запобігаючи витоку через ланцюги живлення основного та допоміжного обладнання для обробки інформації.

FZP103-2 працює в широкому діапазоні частот, від чутних до надвисокочастотних, запобігаючи впливу імпульсів високої напруги. Ці

фільтри безпечно працюють навіть в умовах розімкнутих ланцюгів або поганого заземлення, що робить їх надійним засобом захисту. Вони відповідають усім вимогам вітчизняного стандарту ДСТУ 3639-97 «Фільтри протиперешкодні».

Ці фільтри характеризуються компактними розмірами та малою вагою, що робить їх ефективними в різних системах. Наприклад, цей фільтр має об'єм лише 0,42 дм³ та важить не більше 0,85 кг, що робить його зручним у використанні в різних умовах та ситуаціях. [30-33]

Пристрій активного захисту "ДЕЛЬТА-7" для автоматизованих систем є важливим компонентом захисту інформації в сферах електронно-обчислювальних засобів, спеціалізованого зв'язку та іншої інформаційної діяльності. Цей пристрій призначений для захисту інформаційних сигналів шляхом блокування бічного електромагнітного випромінювання та перешкод від різних технічних пристроїв, включаючи комп'ютери, копіювальні апарати, мережеве обладнання та засоби зв'язку.

Спеціалізований інформаційно-комунікаційний термінал (СІТ) - це електронно-обчислювальний пристрій, призначений для запобігання витоку інформації через бічне електромагнітне випромінювання та наведення. Цей пристрій використовується для обробки секретних даних, що становлять державну таємницю, і може використовуватися в різних умовах інформаційної діяльності.

Як "ДЕЛЬТА-7", так і СІТ є важливими для забезпечення безпеки та конфіденційності інформації в технічній галузі, оскільки запобігання бічному електромагнітному випромінюванню є ключовим аспектом забезпечення інформаційної безпеки.

Генератор шуму MARS-TZO-4-2 – це високоефективний пристрій, призначений для генерації широкосмугового шумового сигналу в діапазоні частот від 180 до 5600 Гц. У ньому використовується вібраційний випромінювач VI4, який забезпечує постійну ефективну вихідну напругу не

менше 3,5 В на резисторі навантаження та забезпечує вібраційне прискорення не менше 50 дБ по всій смузі шумового сигналу.

Система включає акустичний гучномовець MARS-AK, який генерує рівні звукового тиску в широкому робочому діапазоні частот, з рівнем звукового тиску не менше 80 дБ на відстані 1 метра. Пристрій також має широкий діапазон регулювання рівня вихідного шумового сигналу, не менше 20 дБ, та низьке енергоспоживання, що не перевищує 40 ВА.

Цей генератор – лише один із багатьох пристроїв, що застосовуються в різних галузях, де генерація шумового сигналу або регулювання параметрів є важливим аспектом роботи пристрою або системи. [33] та інші методи.

3.6. Висновок по третьому розділу

У цьому розділі представлено комплексну систему інформаційної безпеки об'єктів інформаційної діяльності, призначену для запобігання витоку інформації через технічні канали.

У цьому розділі визначено нормативно-правове забезпечення побудови систем інформаційної безпеки для суб'єктів інформаційної діяльності.

У цьому розділі представлено конкретні заходи та засоби для систем технологій інформаційної безпеки суб'єктів інформаційної діяльності.

У цьому розділі окреслено різні етапи побудови систем технологій інформаційної безпеки для суб'єктів інформаційної діяльності.

У цьому розділі сформульовано та офіційно встановлено стратегії інформаційної безпеки для суб'єктів інформаційної діяльності з метою запобігання витоку інформації через технічні канали.

У цьому розділі запропоновано технічні засоби для запобігання витоку інформації від суб'єктів інформаційної діяльності.

ВИСНОВОК

Під час підготовки роботи було виконано наступні завдання:

– Проведено аналіз сутності, характеристик та методів формування технічних каналів витоку інформації, що утворюються основними технічними засобами та системами об'єктів інформаційної діяльності.

– Досліджено напрямки розвитку та вдосконалення єдиної моделі комплексної системи захисту для посилення заходів запобігання витоку інформації через технічні канали.

– Розроблено комплексну систему захисту об'єктів інформаційної діяльності, яка ставить підвищені вимоги до запобігання витоку інформації через технічні канали.

– Розглянуто питання охорони навколишнього середовища.

1. У першій частині звіту про перевірку кваліфікації проаналізовано основні технічні канали витоку інформації об'єктів інформаційної діяльності. Проведено класифікацію технічних каналів витоку інформації об'єктів інформаційної діяльності. Розкрито сутність, характеристики та методи формування каналів витоку інформації, що обробляються основними технічними засобами та системами об'єктів інформаційної діяльності.

2. У другій частині звіту про перевірку кваліфікації представлено результати дослідження в галузі вдосконалення єдиної моделі комплексної системи захисту для запобігання витоку інформації через технічні канали. Сформульовано вимоги до захисту для запобігання несанкціонованому витоку інформації через технічні канали. Було визначено заходи захисту інформації для запобігання витоку інформації через технічні канали. Надано загальний опис моделі комплексної системи захисту інформації від витоку інформації через технічні канали.

3. У частині третій кваліфікаційної роботи представлено комплексну систему захисту об'єктів інформаційної діяльності для запобігання витоку

інформації через технічні канали. Визначено нормативно-правове забезпечення розробки комплексної системи захисту інформації для об'єктів інформаційної діяльності. Представлено заходи та засоби комплексної системи захисту інформаційних технологій для об'єктів інформаційної діяльності. Окреслено етапи створення комплексної системи захисту інформаційних технологій для об'єктів інформаційної діяльності. Формульовано та офіційно встановлено стратегію інформаційної безпеки для запобігання витоку інформації через технічні канали для об'єктів інформаційної діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

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

3. Юдін О. Критеріальний аналіз сучасних операційних систем у задачах захисту інформаційних ресурсів / О. Юдін, О. Весельська // Наукоємні технології. — 2012. — Т. 14. — №. 2. — С. 74-79.

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

5. Класифікація загроз державним інформаційним ресурсам інженерно-технічного спрямування. Методологія побудови класифікатора / О. К. Юдін, С. С. Бучик // Наукоємні технології. - 2015. - № 2. - С. 188-195

6. Аналіз та класифікація систем контролю та управління доступом на підприємстві О. К. Юдін, д-р техн. наук, проф. Національний авіаційний університет orcid.org/0000-0001-5098-7796; О. М. Весельська Національний авіаційний університет orcid.org/0000-0002-4914-2187.

7. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу – Київ, 1999. – 20 с.

8. Принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних системах / Ю.В. Землянко, О.А. Замула, О.О. Ткач, Н.І. Литвинова, Я.А. Пересічанська.]., 2010.

9. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.]–Вінниця : ВНТУ, 2017.– 120 с.

10. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення – Київ, 2007. – 6 с.

11. НД ТЗІ 3.1-001-07. Захист інформації на об’єктах інформаційної діяль-ності. Створення комплексу технічного захисту інформації. Передпроектні роботи – Київ, 2007. – 5 с.

12. Принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних систем [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: http://openarchive.nure.ua/bitstream/document/861/1/460-469.pdf.

13. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі – Київ, 2005. – 20 с.

14. Засоби створення шкідливого програмного забезпечення [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://studfile.net/preview/5206321/page:17/.

15. Безпека інформаційно-комунікаційнихсистем. Шкідливе програмне забезпечення [Електронний ресурс] – Режим доступу до ресурсу: http://virt.ldubgd.edu.ua/pluginfile.php/39805/mod_resource/content/3/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%201.4.pdf.

16. ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО УРЯДУВАННЯ Навчальний посібник у 15 частинах Загальна редакціяАндрій Іванович Семенченко, Валерій Михайлович Дрешпак Формат 60×90/16.Папір офс. 80 г/м2. Гарн. Таймс. Друк офс.Ум. друк. арк. 4,5. Авт. арк. 3,0. Наклад 500 прим. Видавець та друк: ФОП Москаленко О. М.

17. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації [Електронний ресурс] : навчальний посібник / С. О. Іванченко, О. В. Гавриленко, О. А. Липський [та ін.] ; НТУУ «КПІ». – Електронні текстові дані (1 файл: 615 Кбайт). – Київ : НТУУ «КПІ», 2016. – 104 с. – Назва з екрана.

18. Безпека систем підтримки прийняття рішень [Текст] : навч. посіб. / Ковтунець В. В., Нестеренко О. В., Савенков О. І. ; Нац. акад. упр. - Київ : Нац. акад. упр., 2016. - 189 с. : рис., табл. - Бібліогр.: с. 183-184. - 300 прим. - ISBN 978-617-7386-00-0

19. ЗАКОН УКРАЇНИ Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

20. Білявський Г. О., Падун М. М., Фурдуй Р. С. Основи загальної екології. — К.: Либідь. 1995 — 368 с.

21. Білявський Г. О., Фурдуй Р. С. Практикум із загальної екології. // Навч. посібн.— К.:Либідь, 1997.—160с.

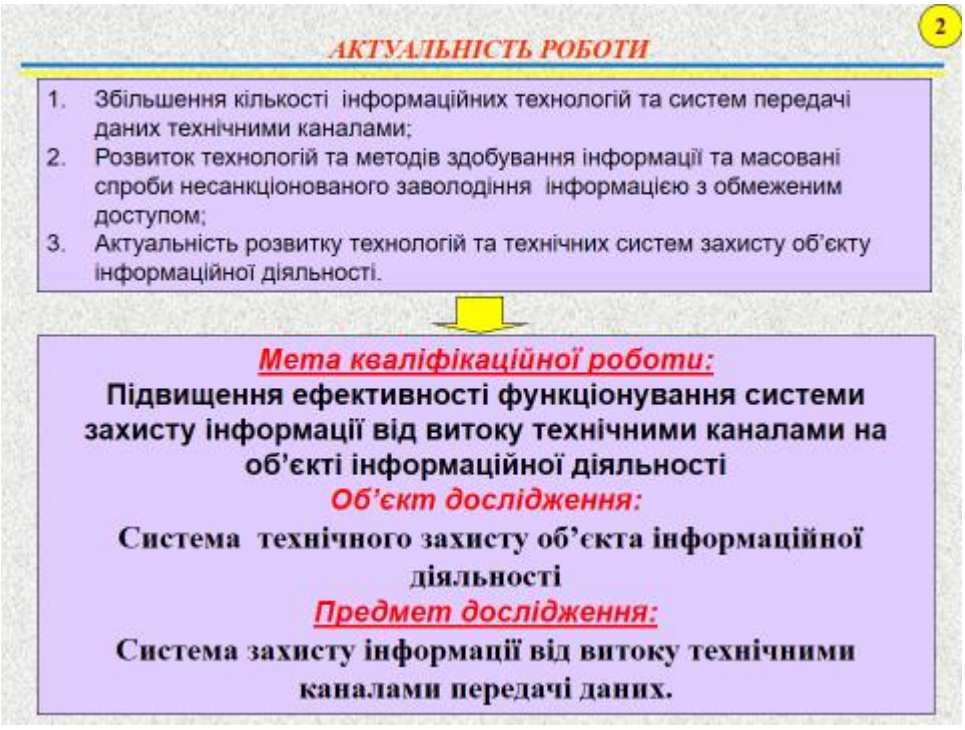
22. Волошин І. М. Методика дослідження проблем природокористування. — Львів: ЛДУ, 1994. — 160 с.

23. Екологічний словник: Навч. посібник /В.В.Прежко та ін. – Харків: ХДАМГ, 1999. – 416 с.

24. Екологія і закон: Екологічне законодавство України. У 2-х кн./ Відповідальний редактор док. юрид. наук, професор, акад. Андрейцев В. А. — К.: Юрінком їнтер, 1997. — 704 с.

25. Злобін Ю.А. Основи екології.- К.: Лібра, 1998. – 249.

ДОДАТОК А


2
АКТУАЛЬНІСТЬ РОБОТИ
1. Збільшення кількості інформаційних технологій та систем передачі даних технічними каналами;
2. Розвиток технологій та методів здобування інформації та масовані спроби несанкціонованого заволодіння інформацією з обмеженим доступом;
3. Актуальність розвитку технологій та технічних систем захисту об'єкту інформаційної діяльності.
Мета кваліфікаційної роботи:
Підвищення ефективності функціонування системи захисту інформації від витоку технічними каналами на об'єкті інформаційної діяльності
Об'єкт дослідження:
Система технічного захисту об'єкта інформаційної діяльності
Предмет дослідження:
Система захисту інформації від витоку технічними каналами передачі даних.

СТРУКТУРА РОБОТИ

3

1. РОЗДІЛ 1: **Аналіз основних технічних каналів витоку інформації на об'єкті інформаційної діяльності**
2. РОЗДІЛ 2: **Дослідження напрямків удосконалення єдиної моделі комплексної системи захисту від витоку інформації технічними каналами**
3. РОЗДІЛ 3: **Дослідження напрямків удосконалення єдиної моделі комплексної системи захисту від витоку інформації технічними каналами**
4. РОЗДІЛ 4: **Охорона природнього середовища**
5. ВИСНОВКИ: **Узагальнено одержані результати**

4

ПЕРШИЙ РЕЗУЛЬТАТ

Аналіз основних технічних каналів витоку інформації на об'єкті інформаційної діяльності

ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

ОСНОВНІ ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

1. РАДІОКАНАЛ; 2. ЕЛЕКТРИЧНИЙ;
3. АКУСТИЧНИЙ; 4. ОПТИЧНИЙ; 5. МАТЕРІАЛЬНО-РЕЧОВИЙ.

КЛАСИФІКАЦІЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

2. За принципом (фізичним ефектом, процесом) формування небезпечного сигналу (носія інформації)

1. За видом інформаційної діяльності на ОКІ

3. За середовищем поширення небезпечного сигналу

4. За способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника

5

ПЕРШИЙ РЕЗУЛЬТАТ

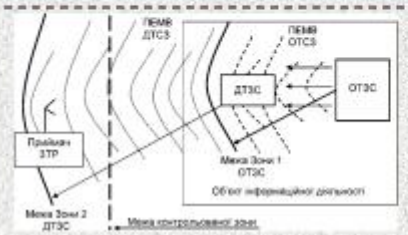
ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

СТРУКТУРА ТЕХНІЧНОГО КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ

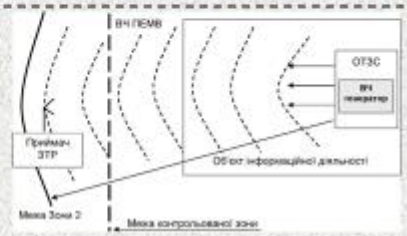
6

ПЕРШИЙ РЕЗУЛЬТАТ

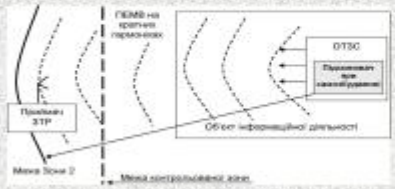
ХАРАКТЕРИСТИКА ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ



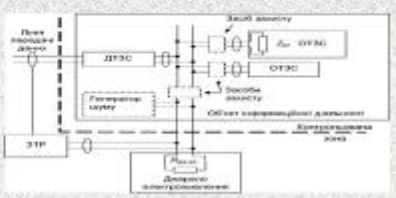
Канал побічних електромагнітних випромінювань



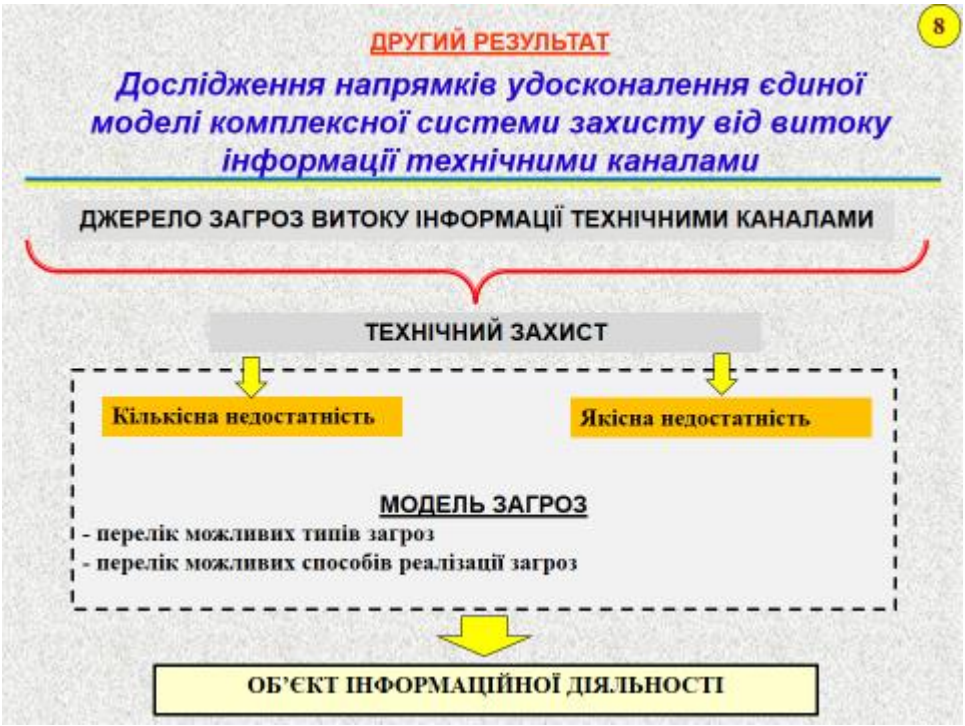
Канал "паразитної" модуляції сигналів ВЧ генераторів



Канал "паразитної" ВЧ генерації підсилювачів



Канали побічних електромагнітних наведень на комунікаціях


8
ДРУГИЙ РЕЗУЛЬТАТ
Дослідження напрямків удосконалення єдиної моделі комплексної системи захисту від витоку інформації технічними каналами
ДЖЕРЕЛО ЗАГРОЗ ВИТОКУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ КАНАЛАМИ
ТЕХНІЧНИЙ ЗАХИСТ
Кількісна недостатність
Якісна недостатність
МОДЕЛЬ ЗАГРОЗ
- перелік можливих типів загроз
- перелік можливих способів реалізації загроз
ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ


8
ДРУГИЙ РЕЗУЛЬТАТ
ЗАХИСТ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ
Канал побічних електромагнітних випромінювань
Локальне екранування електронних елементів
Канал побічних електромагнітних наведень на лінії електроживлення (заземлення)
Лінійне зашумлення ліній електроживлення
Канал ВЧ нав'язування
Екранування
Оптичний канал витоку інформації
Перекриття оптичних каналів

9

ДРУГИЙ РЕЗУЛЬТАТ

ВЕКТОРИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ:

Технічний захист інформації.
Програмний захист інформації.
Організаційно-технічний захист інформації.

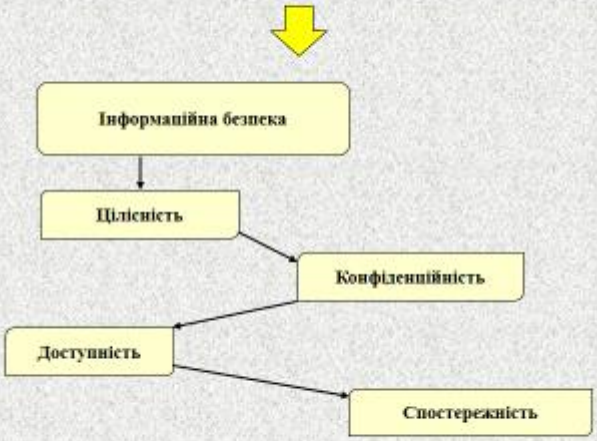
ШЛЯХИ ЗАХИСТУ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ:

- **Створення КЗ не меншої за найбільшу Зону 2, яку розраховують з врахуванням усіх властивих об'єкту ЕОТ технічних каналів витоку інформаці;**
- **Організація режиму доступу до КЗ та ОІД;**
- **Екранування ОТЗС;**
- **Просторове електромагнітне зашумлення на об'єкті ЕОТ;**
- **Індикація відхилення параметрів підсилювачів та блокування роботи ОТЗС;**
- **Розміщення ДТЗС не ближче Зони 1 ОТЗС, а ОТЗС - на ближче своєї Зони 1 до можливих сторонніх провідників;**
- **Використання в лініях ДТЗС технічних засобів захисту, що затримують сигнали низького рівня;**
- **Використання в лініях ДТЗС та сторонніх провідниках лінійного зашумлення;**

10

ДРУГИЙ РЕЗУЛЬТАТ

ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ КСЗІ: ВИМОГИ



11

ТРЕТІЙ РЕЗУЛЬТАТ

НД ТЗІ 3.7-003-05

ЕТАПИ СТВОРЕННЯ КСЗІ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ:

1. Забезпечення технічного захисту ІТС;
2. . Обстеження ІТС та підготовка вихідних даних для формування вимог до КСЗІ
3. Формування політики безпеки КСЗІ в ІТС
4. Розробка технічного завдання КСЗІ в ІТС
5. Розробка і реалізація проекту КСЗІ в ІТС
6. Введення КСЗІ від витоку технічними каналами
7. Попередні випробування АС
8. Державна експертиза АС
9. Супровід КСЗІ

12

ТРЕТІЙ РЕЗУЛЬТАТ

Дослідження напрямків удосконалення єдиної моделі комплексної системи захисту від витоку інформації технічними каналами

13

ТРЕТІЙ РЕЗУЛЬТАТ

РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ:

4 етап. Розробка і реалізація проекту КСЗІ в ІТС:
-Способи запобігання витоку інформації технічними каналами:
-Вибір технічного обладнання, призначеного для реалізації запобігання витоку інформації технічними каналами.

ТЕХНІЧНЕ ОБЛАДНАННЯ :

Блокіратор бездротового зв'язку **«СБ ТЗІ 7-1**
Протизавадний фільтр **«ФЗП-110-2»**
Вібровипромінювачі **«ВІ»**
Генератор шуму марки **„Базальт-5".**
Мережевий завадозахисний фільтр **«ФЗП103-2»**
Колонка акустична захищена **«МАРС-АКЗ.**

14

ВИСНОВКИ:

У ПРОЦЕСІ ПІДГОТОВКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ були виконані наступні задачі:

– Проведено аналіз сутності, властивостей та шляхів утворення технічних каналів витоку інформації, що утворюються основними технічними засобами та системами на об'єкті інформаційної діяльності.

– Досліджено напрямки розробки та удосконалення єдиної моделі комплексної системи захисту з посиленими заходами від витоку інформації технічними каналами.

– Розроблено комплексну систему захисту об'єкту інформаційної діяльності з підвищеними вимогами до захисту від витоку інформації технічними каналами.

ДЯКУЮ ЗА УВАГУ !