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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Метод протидії витоку інформації матеріально-речовим каналом за рахунок використання сучасних систем контролю доступу»

на здобуття освітнього ступеня магістра
зі спеціальності __125 Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Єгор ВАСІН

Виконав: здобувач вищої освіти групи СЗДМ 61
Єгор ВАСІН

Керівник: КОТЕНКО Андрій
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2026

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

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

_____Васіну Єгору Олександровичу_____
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Метод протидії витоку інформації матеріально-речовим каналом за рахунок використання сучасних систем контролю доступу»
керівник кваліфікаційної роботи _____Андрій КОТЕНКО 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.
Зміст пояснювальної записки (перелік питань, що підлягають розробці):
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 _____ Єгор ВАСІН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Андрій КОТЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 68 сторінок, має 9 рисунків, 4 таблиць. Список використаних джерел містить 26 найменувань і займає 3 сторінки.

Метою кваліфікаційної роботи є підвищення ефективності функціонування системи протидії витоку інформації матеріально-речовим каналом на об’єкті інформаційної діяльності.

В кваліфікаційній роботі вирішено наступні завдання. Проведено огляд 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. Проведено розробку комплексної систему захисту об’єкту інформаційної діяльності з підвищеними вимогами до захисту від витоку інформації технічними каналами.

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-телекомунікаційних 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 efficiency of the functioning of the system for countering information leakage through a material channel at the object of information activity.

The following tasks were solved in the qualification work. A review of the essence, properties and ways of forming technical channels of information leakage, formed by the main technical means and systems at the object of information activity, was conducted. The directions of development and improvement of a single model of a comprehensive protection system with enhanced measures against information leakage through technical channels were investigated. A comprehensive system for protecting the object of information activity with increased requirements for protection against information leakage through technical channels was developed.

Approbation:

N.A. Andrienko, I.S. Volkovetsky, E. O. Vasin. 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 security of information and telecommunication systems. Kyiv, November 05, 2025, Kyiv: RVC DUIKT. – 2025. P.29-30. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

OBJECT OF INFORMATION ACTIVITY, COMPREHENSIVE INFORMATION PROTECTION SYSTEM, TECHNICAL CHANNELS OF INFORMATION LEAKAGE.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ ……. …7
ВСТУП……..…….. …8
РОЗДІЛ 1. АНАЛІЗ ОСНОВНИХ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ……. …9
1.1. Класифікація технічних каналів витоку інформації на об'єкті інформаційної діяльності ……. …9
1.2. Сутність та шляхи утворення каналів витоку інформації, що обробляється основними технічними засобами та системами на об'єкті інформаційної діяльності ……...……. ..12
1.3 Висновки по розділу …….……... ..26

РОЗДІЛ 2. ДОСЛІДЖЕННЯ НАПРЯМКІВ УДОСКОНАЛЕННЯ ЄДИНОЇ МОДЕЛІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ВІД ВИТОКУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ КАНАЛАМИ ……... ..27
2.1. Формування вимог до захисту технічних каналів від несанкціонованого витоку інформації ……... ..27
2.2. Вектори захисту інформації від витоку технічними каналами ….. ..29
2.3.Загальний опис єдиної моделі комплексної системи захисту від витоку технічними каналами ……..……. ..34
2.4. Висновки по розділу…… ..36

РОЗДІЛ 3. КОМПЛЕКСНА СИСТЕМИ ЗАХИСТУ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ВІД ВИТОКУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ КАНАЛАМИ ……..... ..37
3.1 Нормативно-правове забезпечення розробки комплексної системи захисту інформації на об'єкті інформаційної діяльності ……... ..37
3.2 Заходи та засоби комплексної системи технічного захисту

інформації на об’єкті інформаційної діяльності ……..... ..38
3.3 Етапи створення комплексної системи технічного захисту інформації на об’єкті інформаційної діяльності ……... ..40
3.4. Розробка та оформлення політики безпеки інформації від витоку технічними каналами витоку на об’єкті інформаційної діяльності …… ..45
3.5 Рекомендації по застосуванню технічних засобів запобігання витоку інформації на об’єкті інформаційної діяльності ……... ..46
3.6. Висновки по розділу ……... ..48

РОЗДІЛ 4. ОХОРОНА ПРИРОДНЬОГО СЕРЕДОВИЩА…… ..50
4.1. Біологічне забруднення довкілля ……... ..50
4.2. Наслідки забруднень ……..…..…….. ..51
4.3 Якість довкілля ……..…… ..52
4.4. Висновок по розділу …… ..54

ВИСНОВКИ……..……. ..55
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ …….. ..57
ДОДАТОК А ……..……... ..57

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

Найважливішим питанням сьогодення є захист безпеки установ, підприємств, систем та мереж, що відповідають за життєдіяльність населення, адже всі вони вважаються об'єктами інформаційної діяльності. Тобто об'єкти, що неналежним чином функціонують або не виконують необхідних функцій, можуть суттєво впливати на якість життя населення цілих регіонів. Виходячи зі значного прогресу в науково-технічному розвитку, ускладнення економічних процесів та соціальних відносин, а також розвитку різноманітних технологій, що базуються на цих принципах, можна зробити висновок, що одним із факторів, що впливає на якість функціонування, є різноманітність інформації. Запобігання ефективному функціонуванню системи захисту інформації за допомогою технічних засобів у центрі інформаційної діяльності є серйозним завданням, вирішенню якого присвячено цю справу.

Метою кваліфікаційної роботи є підвищення ефективності функціонування системи протидії витоку інформації матеріально-речовим каналом на об’єкті 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 технічних каналів витоку інформації на об'єкті інформаційної діяльності

Для категоризації вимог до захисту інформації та технічних каналів, через які відбувається її витік, інформацію було класифіковано за певними ознаками. Зокрема, різновиди ТКВІ класифікуються за такими ознаками [1,2]:

- за специфічною активністю інформації на ІЗ,

- за принципом (кінетичний ефект, процедура) створення шкідливого сигналу (інформаційне середовище),

- за середовищем передачі небезпечного повідомлення,

- за процесом переривання (видалення) небезпечного сигналу за допомогою технічних знань противника.

За типом обробки інформації на ІЗ розрізняють такі типи ТКВІ [1,2]:

а) засоби технічного зв'язку, що сприяють витоку мовних даних,

технічні засоби витоку інформації в ІЗС,

технічні способи інформування населення про небезпеку сонця,

d) матеріальні та інформаційні канали, що дозволяють здійснювати витік.

Рекомендується розглянути класифікацію ТКВІ за принципом (фізичним ефектом, процесом) створення небезпечного сигналу, середовищем, через яке передається сигнал, та методом його переривання (знищення).[17]

Технічні способи отримання та поширення мовленнєвої інформації відповідно до цих властивостей поділяються на такі категорії [1, 2]

Акустичні волокна.

b) Канали акустичних коливань (віброакустичні).

c) Оптичні канали, що використовують звукові хвилі.

Акустоелектричні канали.

e) Відеоканали, що мають справу зі звуком.

f) Використання радіочастотних каналів для стягнення податків (для усунення мовлення).

g) Канали, через які витікає мовленнєва інформація на основі вбудованих пристроїв.

Технічні канали інформації, що обробляється в ОТЗС, поділяються на такі категорії [1, 2]

1. Канали побічного випромінювання.

2. Канали побічних емоційних перешкод.

3. Канали «паразитної» зміни радіочастотних сигналів, що надсилаються генераторами.

4. Канали генераторів паразитного радіочастотного випромінювання.

5. Канали перехоплення (видалення) у волоконно-оптичних лініях передачі даних.

6. Канали перехоплення (видалення) інформації, що передається через канали зв'язку.

7. Канали радіочастотної потужності (для усунення обробки інформації в ОТЗС).

8. Канали, через які відбувається витік інформації ОТЗС, на основі вбудованих пристроїв.

Технічні канали витоку візуальної інформації класифікуються на:

1. Візуальні носії.

2. Оптико-оптичні канали.

3. Канали, через які може відбуватися витік візуальної інформації, на основі вбудованих пристроїв.

Витік інформації через матеріальні канали:

1. Вилучення інформації з несправних пристроїв ЕОТ.

2. Збір інформації з попередньо написаних документів, виробничих відходів, видавничих відходів тощо.

3. Хімічні речовини, що проходять через канал.[17]

Відправник інформації та принцип створення небезпечного сигналу є важливими для розпізнавання наступних TCVI [2,3]:

Канали витоку інформації електромагнітними засобами, включаючи засоби побічного електромагнітного випромінювання, засоби «паразитної» генерації енергії, засоби «паразитної» зміни потужності, засоби перехоплення інформації з радіо («радіорелейних», «стільникових», «мобільних») ліній зв'язку та інші подібні канали;

канали, що витікають електричну інформацію, включаючи канали, що мають побічний вплив на зв'язок, канали, що витягують інформацію з дротового зв'язку та інші канали;

канали, що витікають інформацію про параметричну конструкцію, включаючи канали, через які передається радіочастотна потужність, канали, що мають «паразитну» природу, та інші подібні канали.

За місцем розташування джерела інформації розрізняють такі типи ТКВІ [2,3,4]:

1) канали перехоплення (видалення) інформації за межами КІ,

2) канали запобігання (видалення) інформації з-за меж КІ, що активно впливають на параметри каналу витоку технічної інформації (наприклад, канал КІ),

3) методи вилучення інформації за допомогою технічного інтелекту, встановленого на ІВ (наприклад, канали витоку інформації з вбудованими пристроями).

Категоризована класифікація каналів витоку технічної інформації сприяє їх систематичному розумінню та встановленню вимог і заходів щодо запобігання витоку інформації пов'язаними з ними ТКВІ.

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

Обговоримо фундаментальні концепції та методи (фізичні основи, принципи та процедури), що використовуються для створення технічних каналів передачі інформації, що обробляється основними технічними засобами та системами. Найбільш шкідливими для опромінення інформації, що обробляється в ОТЗС, є канали побічного випромінювання та перешкод (канали ПЕМВН) [4,5].

Канал побічного електромагнітного випромінювання ОТЗС.

Канал побічного емоційного випромінювання ОТЗС (канал ПЕМВ ОТЗС) утворюється внаслідок взаємодії між інформаційними сигналами та побічними емоційними полями, що створюються електронними компонентами та провідниками (петлями) ОТЗС. Ці поля потім передаються до цільової аудиторії.

Інформаційні сигнали в цьому випадку є електричними потоками, що несуть знання.

Обробка інформації та передача в ОТЗС здійснюється за допомогою струмів електричної провідності, які є формою спрямованого потоку частинок, заряджених електронами. Як загальновідомо з фізики, навколо нерухомих електронів або кластера електронів завжди присутнє електростатичне поле. Якщо цей струм змінити на протилежний, у полі з'явиться магнітна складова, отже, ця складова є електромагнітною. Електромагнітне поле поширюється по простору.

Навколо ОТЗС, як системи електронних компонентів та провідників (петль), в яких, згідно з принципом первинної дії ОТЗС, поширюються електричні струми, що несуть інформацію, завжди існує поле випромінювання. Оскільки ці випромінювання є шкідливими та мають паразитний (побічний)

характер, їх називають побічними електромагнітними випромінюваннями (ПЕВ). Побічне випромінювання поширюється у вільному просторі та може бути перервано розвідувальними приймачами противника, що утворює канал технічної інформації ОТЗС (рис. 1.1) [4,5,6]:

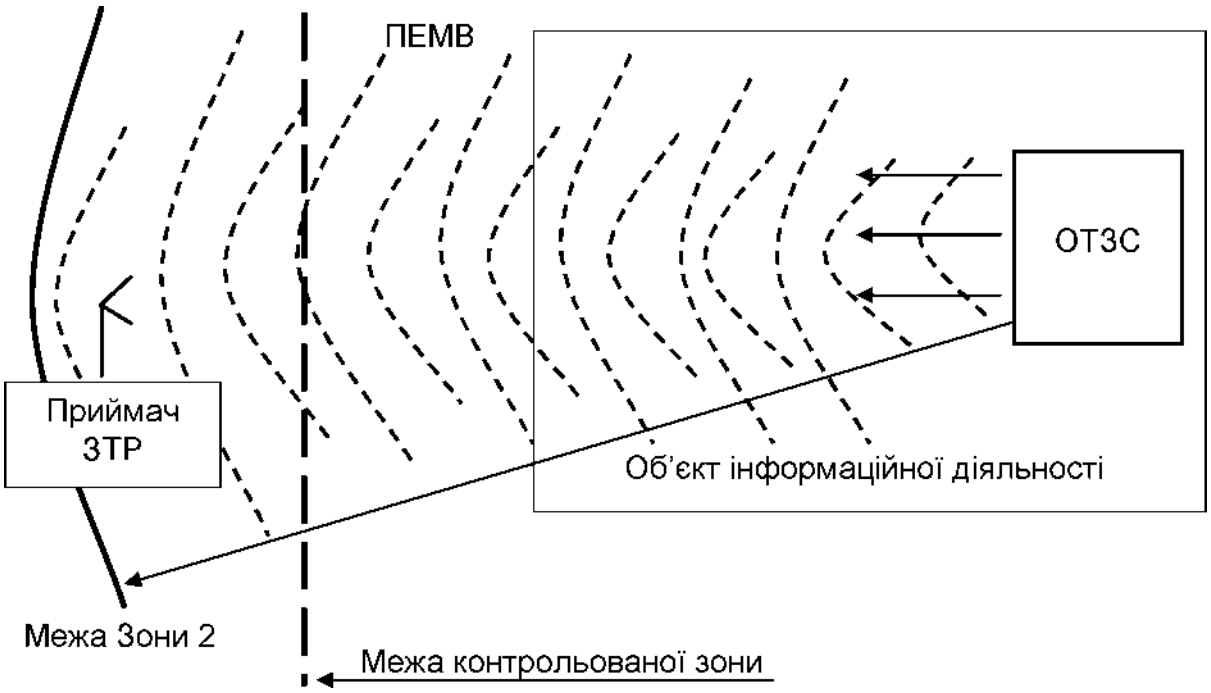


Рис. 1.1. Канал побічних електромагнітних випромінювань ОТЗС.

Також з фізики відомо, що за наявності електромагнітного поля воно розсіюється. В результаті існує відстань від джерела випромінювання – ОТЗС, на якій поле випромінювання зменшується до такої міри, що його вже неможливо приймати (вимірювати його властивості). У цьому випадку небезпечне повідомлення, що передається цим полем, буде майже повністю знищено звичайними перешкодами та шумом. Як зазначалося раніше, зона, за межами якої співвідношення сигнал/перешкода не перевищує допустиму межу, вважається Зоною 2 ОТЗС. Положення прийому ЗТР противника поза Зоною 2 не сприятиме захопленню інформації.

Канал непрямого випромінювання ДТЗС.

Канал бокового електромагнітного випромінювання від ДТЗС, подібний до типу каналу ПЕМВ, утворюється взаємодією приймачів технічної розвідки з небезпечними сигналами, що присутні у вигляді зовнішніх полів ОТЗС. Ці поля потім перевипромінюються за допомогою допоміжної техніки та систем, а також зовнішніх провідників.

Допоміжні технічні засоби та системи, а також зовнішні трубопроводи, якщо вони розташовані в першій зоні ОТЗС або мають спільні з'єднання з лініями, що переносять небезпечну інформацію (включаючи інформацію щодо побічного електромагнітного випромінювання), вважаються випадковими та можуть призвести до витоку інформації через основні технічні засоби та системи. Це шкідливо для безпеки системи.

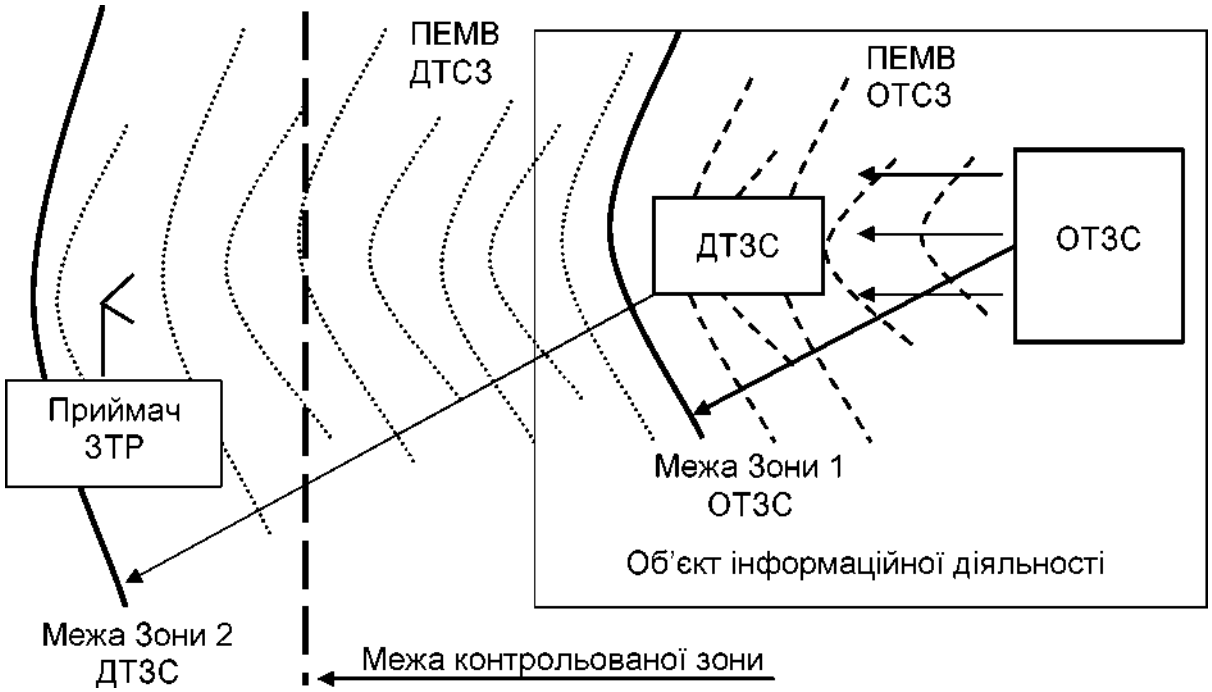


Рис. 1.2. Канал побічних електромагнітних випромінювань ДТЗС.

Канал паразитного впливу генераторів радіочастотних сигналів.

Канал «паразитного» впливу сигналів генераторів радіочастотних сигналів, як форма каналів PEMV, створюється шляхом зміни високочастотних

сигналів генераторів радіочастотних сигналів OTZS небезпечним сигналом, цей сигнал потім випромінюється у вільний простір і, нарешті, приймається за допомогою радіотехнологій за межами KZ (рис. 1.3) [4,5,6].

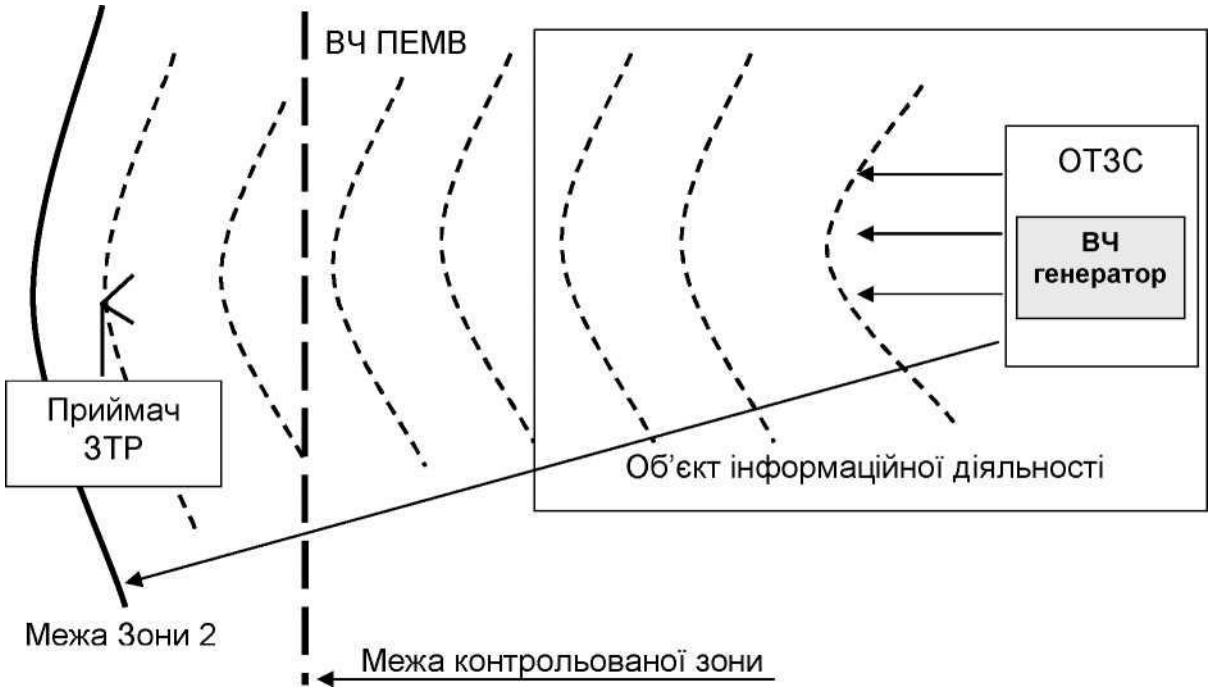


Рис. 1.3. Канал "паразитної" модуляції сигналів ВЧ генераторів.

Основні технічні засоби та системи включають високочастотні генератори (ВЧ-генератори). Майже всі ЕОТ мають генератори, що здійснюють тактову частоту, генератори, що виробляють інші форми енергії тощо. Потужний сигнал ВЧ-генератора змінюється малопотужними небезпечними сигналами, що циркулюють в ЕОТ та проектуються у вільний простір. Оскільки амплітуда електромагнітного поля на високих частотах менша, ніж на низьких частотах, поле поширюється далі. Це, теоретично, дозволяє виявляти інформацію за допомогою технічної експертизи поза Зоною 2, яка розраховується для сигналу без модуляції. Важливо визнати, що спектр сигналу розширюється, його потужність збільшується, а шум посилюється. Як наслідок, Зону 2 слід розраховувати з урахуванням частотно-специфічних діаграм випромінювання ВЧ-генераторів ЕОТ на частотах 6, 7, 8.

Канал паразитної РЧ-генерації підсилювачів потужності.

Канал «паразитної» генерації радіочастот у підсилювачах, як форма каналів ПЕМВ, створюється шляхом самозбудження низькочастотних (НЧ) підсилювачів ОТЗС на гармоніках, кратних небезпечному сигналу, їх поширення через канал електромагнітного випромінювального поля, що поширюється повз коротке замикання, та прийому цього поля радіопристроями технологічного інтелекту (рис. 1.4) [6,7,8].

Сучасні технічні методи обробки інформації часто використовують низькочастотні (НЧ) підсилювачі. Як правило, будь-який підсилювач складається з напівпровідникового елемента, який підсилює сигнал, та негативного зворотного зв'язку.

Нелінійність властивостей напівпровідникових компонентів при роботі з сигналами зумовлює наявність кількох гармонік у складі вихідного підсиленого сигналу, наприклад, небезпечне повідомлення на подвоєних, потроєних та інших частотах. Якщо підсилювач з його негативним зворотним зв'язком точно розрахований, а процес посилення сигналу здійснюється в лінійній частині підсилювальної функції характеристики, то сигнал переважно посилюється без спотворень, а його кратні гармоніки мінімізуються.

Внаслідок старіння або інших причин параметри електронних компонентів та властивості негативного зворотного зв'язку можуть змінюватися, що призводить до порушення режиму роботи підсилювача в цілому. Негативний зворотний зв'язок може переходити в позитивний, коефіцієнт посилення збільшується, а нелінійність збільшення також збільшується, підсилювальний елемент досягає своєї максимальної потужності. Зворотний зв'язок на певних частотах є позитивним, що призводить до того, що підсилювач перетворюється на генератор. Крім того, в режимі насичення кратні гармоніки сигналу значно збільшуються, а також значно збільшується їх електромагнітне поле. Це, теоретично, може полегшити отримання інформації

за допомогою технічної експертизи поза Зоною 2, яка розраховується без урахування "паразитної" генерації.

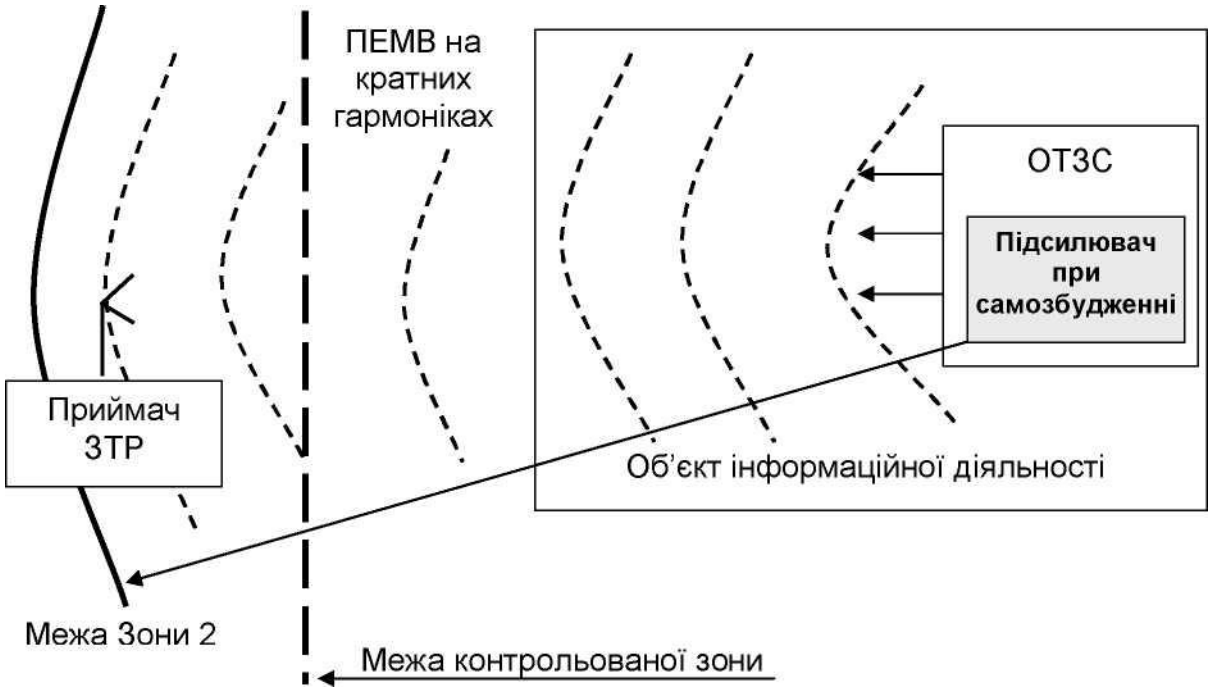


Рис. 1.4. Канал “паразитної” ВЧ генерації підсилювачів.

Основні технічні засоби та системи включають високочастотні генератори (ВЧ-генератори). Майже всі ЕОТ мають генератори, що здійснюють тактову частоту, генератори, що виробляють інші форми енергії тощо. Потужний сигнал ВЧ-генератора змінюється малопотужними небезпечними сигналами, що циркулюють в ЕОТ та проектуються у вільний простір. Оскільки амплітуда електромагнітного поля на високих частотах менша, ніж на низьких частотах, поле поширюється далі. Це, теоретично, дозволяє виявляти інформацію за допомогою технічної експертизи поза Зоною 2, яка розраховується для сигналу без модуляції. Важливо визнати, що спектр сигналу розширюється, його потужність збільшується, а шум посилюється. Як наслідок, Зону 2 слід розраховувати з урахуванням частотно-специфічних діаграм випромінювання ВЧ-генераторів ЕОТ на частотах 6, 7, 8.

Канал паразитної РЧ-генерації підсилювачів потужності.

Канал «паразитної» генерації радіочастот у підсилювачах, як форма каналів ПЕМВ, створюється шляхом самозбудження низькочастотних (НЧ) підсилювачів ОТЗС на гармоніках, кратних небезпечному сигналу, їх поширення через канал електромагнітного випромінювального поля, що поширюється повз коротке замикання, та прийому цього поля радіопристроями технологічного інтелекту (рис. 1.4) [6,7,8].

Сучасні технічні методи обробки інформації часто використовують низькочастотні (НЧ) підсилювачі. Як правило, будь-який підсилювач складається з напівпровідникового елемента, який підсилює сигнал, та негативного зворотного зв'язку.

Нелінійність властивостей напівпровідникових компонентів при роботі з сигналами зумовлює наявність кількох гармонік у складі вихідного підсиленого сигналу, наприклад, небезпечне повідомлення на подвоєних, потроєних та інших частотах. Якщо підсилювач з його негативним зворотним зв'язком точно розрахований, а процес посилення сигналу здійснюється в лінійній частині підсилювальної функції характеристики, то сигнал переважно посилюється без спотворень, а його кратні гармоніки мінімізуються.

Внаслідок старіння або інших причин параметри електронних компонентів та властивості негативного зворотного зв'язку можуть змінюватися, що призводить до порушення режиму роботи підсилювача в цілому. Негативний зворотний зв'язок може переходити в позитивний, коефіцієнт посилення збільшується, а нелінійність збільшення також збільшується, підсилювальний елемент досягає своєї максимальної потужності. Зворотний зв'язок на певних частотах є позитивним, що призводить до того, що підсилювач перетворюється на генератор. Крім того, в режимі насичення кратні гармоніки сигналу значно збільшуються, а також значно збільшується їх електромагнітне поле. Це, теоретично, може полегшити отримання інформації за допомогою технічної експертизи поза Зоною 2, яка розраховується без

урахування "паразитної" генерації.

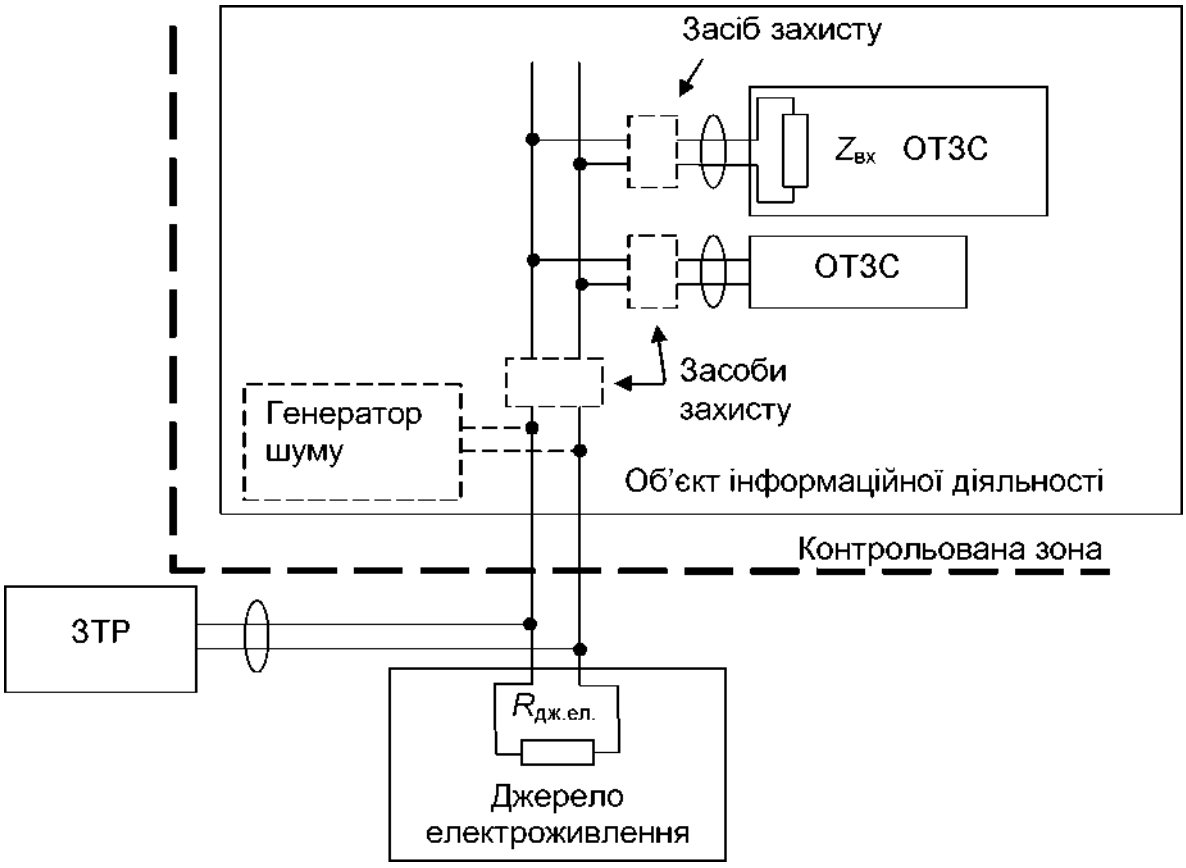


Рис. 1.5. Канал побічних електромагнітних наведень на лінії електроживлення ОТЗС.

Майже всі технологічні методи та системи обробки та передачі інформації залежать від електроенергії. Лінії живлення (заземлення) ОТЗ даних розташовані в Зоні 1 ОТЗ, тому на них може індукуватися електричний струм за принципом електромагнітної індукції, який змінюється подібно до небезпечного електричного сигналу та поширюється по лініях живлення (заземлення).

Крім того, під час обробки інформації вхідний опір ОТЗ, ймовірно, змінюватиметься відповідно до закону сигналів, що беруть участь в обробці. Наприклад, підсилювачі (ключові компоненти) мають можливість керувати опором напівпровідника в колі, що формує посилений сигнал від джерела живлення.

Зі зміною вхідного опору ОТЗ у колі живлення з'являтиметься небезпечний сигнал зі змінною складовою струму. Це створить змінну складову напруги на опорі джерела живлення. Останні можуть бути доступні всім абонентам мережі електропостачання. Якщо джерело живлення знаходиться поза зоною короткого замикання (лінії живлення проходять повз зону короткого замикання), противник може безпосередньо підключити засоби технічної розвідки до лінії живлення з метою вилучення інформації.

Окрім побічних ефектів електромагнітних перешкод із заземлювальною лінією ОТЗС, відбувається викид шкідливих сигналів у заземлювальні кола.

Під час роботи технологічних процесів обробки інформації, в результаті ємнісних та інших з'єднань, на корпусах цих процесів може накопичуватися смертельний потенціал. Цей потенціал залежить від закону небезпечного сигналу, якщо небезпечний сигнал присутній, він просочується в заземлювальні кола.

Для забезпечення безпеки персоналу спрямовуються всі технічні ресурси [8,9].

Концепція заземлення полягає в тому, що корпус технічного засобу гальванічно з'єднаний з ґрунтом Землі, а потенціал, що накопичується на корпусі, передається в землю через заземлювальні кола, приймаючи нульовий потенціал. Якщо система заземлення надійна, а її опір достатньо низький, то потік буде швидшим, і корпус технічних засобів обробки інформації майже завжди буде мати нейтральний заряд.

Однак, з практичного боку, система заземлення може не мати необхідної міцності, і цим може скористатися опонент. Технічний канал витоку інформації через заземлюючі кола ОТЗС проілюстровано на рис. 1.6.[6,7,8]

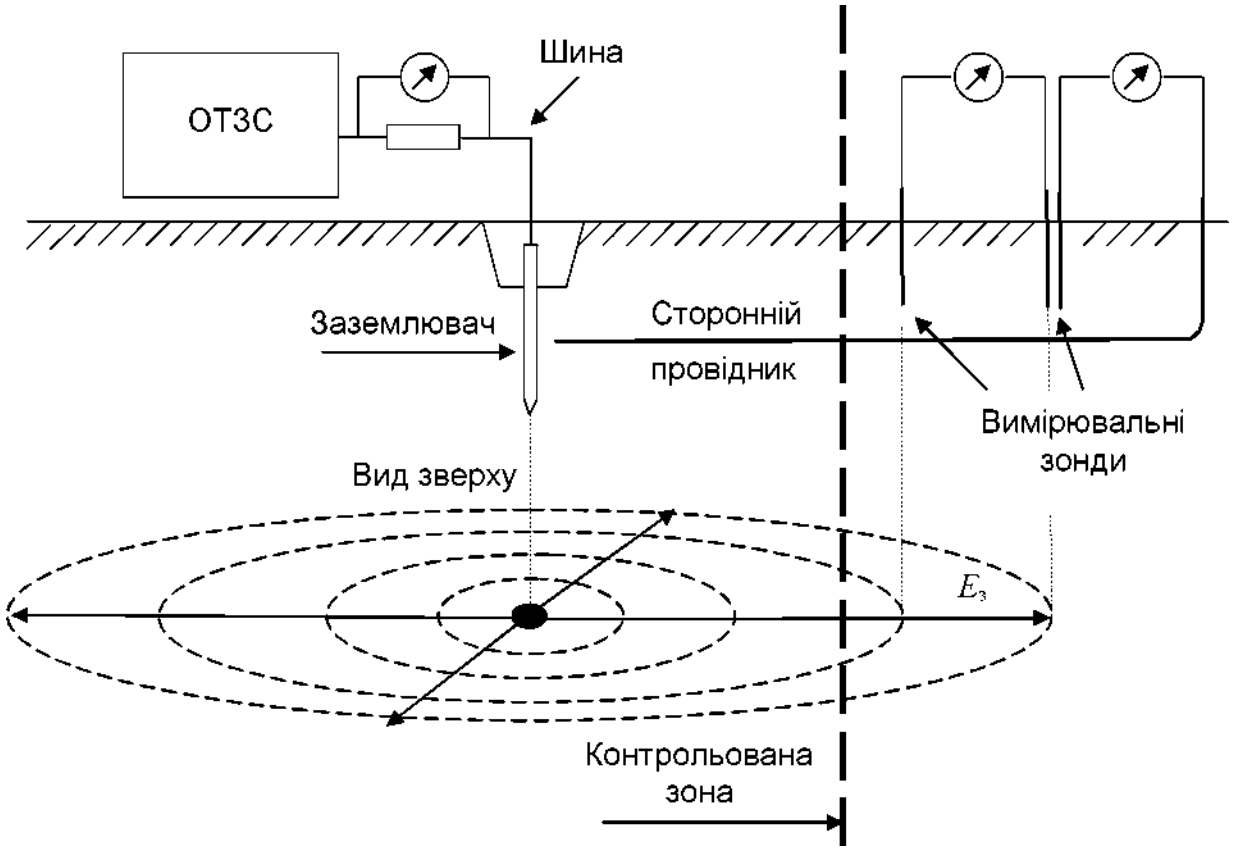


Рис. 1.6. Технічний канал витоку інформації ланцюгами заземлення ОТЗС.

Основними методами запобігання небезпечним сигналам у заземлювальних колах є [8,9]:

1. Блокування шкідливого сигналу з вразливих ділянок системи заземлення. Наприклад, слабкий зварний шов, окислені контакти, невелика площа заземлення, обмежена своїми розмірами тощо.

2. Усунення різниці потенціалів між ґрунтом та заземлювачем – причини виникнення небезпечного сигналу, що можливо при великій величині заземлювача.

3. Знищення напруги з сусідніх сторонніх провідників, які з'єднані із заземлювачем та мають з ним ємність.

4. Основні методи запобігання витоку інформації через канали непрямих електромагнітних перешкод на лінії живлення ОТЗС (для запобігання створенню цих ТКВІ) досягаються наступними методами:

5. Блокування шкідливого сигналу з вразливих ділянок системи заземлення. Наприклад, слабка лінія зварювання, окислені контакти, невелика площа заземлення, обмежена своїми розмірами тощо.

6. Усунення різниці потенціалів між ґрунтом та заземлювачем – це небезпечне джерело сигналу, яке може виникнути, коли заземлювач має великий опір.

7. Знищення напруги від сусідніх зовнішніх провідників, які з'єднані із заземлювачем та мають з ним ємнісний зв'язок.

- Було виконано створення короткого замикання та організацію доступу до нього.

- Живлення ОТЗС здійснюється від автономних джерел електроенергії: електростанцій, акумуляторів тощо, що знаходяться в зоні короткого замикання та не мають зовнішніх споживачів.

- Використання в лінії живлення ОТЗС технічних захисних пристроїв, що затримують низькорівневий зв'язок, мережевих фільтрів та генераторів двигунів.

- Придушення лінійних перешкод у лініях живлення ОТЗС.[17] Запобігання витоку інформації через канали непрямих електромагнітних перешкод на лінії заземлення ОТЗС, включаючи витік небезпечних сигналів у заземлюючі кола (неможливість створення таких ТКВІ) досягається [8,9,10].

- Створення короткого замикання, коротшого за Зону 2, та організація режиму доступу до короткого замикання на ВРЗ;

- незалежне регулювання ОТЗС від ДТЗС.

- забезпечення виконання вимог до монтажу та опору заземлення ОТЗС;

- Розміщення заземлювача відносно контрольованої зони та максимальної відстані від межі короткого замикання та сторонніх провідників;

- Використання лінійного шумозаглушення на лініях заземлення ОТЗС.

Бічні електромагнітні перешкоди на каналі зв'язку ДТЗС.

Бічні електромагнітні поля в середовищі комунікацій DTZS, які класифікуються як канали PEMN, створюються шляхом видалення небезпечних електричних сигналів із системи (живлення, заземлення та лінії передачі даних DTZS, лінії зв'язку, лінії безпеки, пожежної або загальної безпеки, системи енергопостачання та інші компоненти). Ці компоненти потім підключаються до системи (рис. 1.7) [8,9,10].

Якщо DTZS та їх джерело живлення, лінії передачі заземлення та даних розташовані в Зоні 1 OTZS, то електричний струм може бути індукований до них за принципом електромагнітної індукції, подібний до небезпечного сигналу, і проходить через джерело живлення, лінії передачі заземлення та даних DTZS. Крім того, якщо ці лінії мають спільні діаграми спрямованості з лініями, що поширюють небезпечні сигнали, то можливе перенаправлення цих сигналів на лінії DTZS. Крім того, небезпечні сигнали через кола живлення DTZS можуть мігрувати в лінії живлення DTZS. Якщо це обладнання живлення, заземлення або передачі даних ДТЗС виходить за межі ЗК, то зловмисник може безпосередньо підключити ці елементи обладнання до цих ліній зв'язку, інформація може бути видалена[8,9,10].

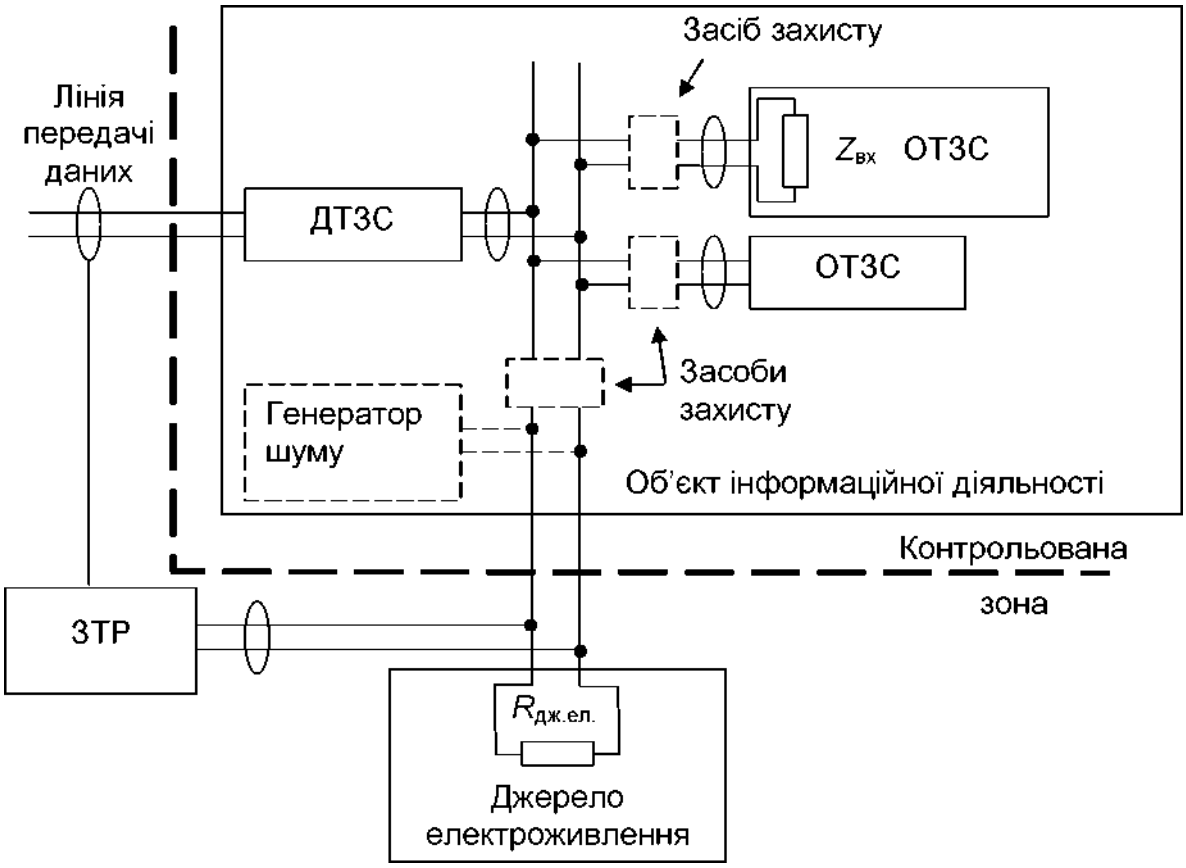


Рис. 1.7. Канали побічних електромагнітних наведень на комунікації ДТЗС.

Запобігання витоку інформації через непрямі канали зв'язку DTZS (неможливість створення такого TCVI) досягається за допомогою [8,9,10].

- Створення короткого замикання та організація режиму доступу до короткого замикання на OID;

- розташування DTZS та їх зв'язок із зовнішніми сторонами в Зоні 1 OTZS.

- живлення DTZS від автономних джерел живлення: електростанцій, акумуляторів тощо, розташованих поблизу входу короткого замикання;

- використання технічних засобів захисту в лінії живлення DTZS, що затримують низькорівневий зв'язок, мережевих фільтрів та систем двигун-генератор.

- використання лінійного шумозаглушення на лініях живлення DTZS;

- забезпечення виконання вимог до монтажу та опору заземлення DTZS;

- розташування вимикача, який контролює відстань між коротким замиканням та зовнішнім середовищем, цей вимикач розташований на максимальній відстані від межі короткого замикання та інших провідників;

Використання лінійних методів зменшення шуму на лініях заземлення ДТЗС.

Радіочастотний канал для видалення інформації (наприклад, для обробки інформації в ОТЗС).

Процес видалення інформації з технічних засобів через радіочастотний канал (для видалення інформації, що обробляється технічними засобами), як різновид параметричних каналів, здійснюється шляхом вставки («нав'язування)» спеціального високочастотного сигналу в основні та допоміжні технічні засоби та системи. Цей сигнал є небезпечним для зовнішнього світу та складається з технічного сигналу, який не є лінійним. Цей процес призводить до видалення сигналу з зони.

- модулювання цього радіочастотного сигналу від різнорідних навантажень в ОТЗС та/або ДТЗС, поширення цього сигналу по комунікаціях ОТЗС та/або ДТЗС за межі КС, а потім видалення сигналу за допомогою технічної експертизи при безпосередньому підключенні до зовнішніх комунікацій.

- або випромінювання модульованого радіочастотного сигналу в простір та прийом цього сигналу засобами технічної розвідки за межами КЗ (рис. 1.8) [9,11].

Майже всі технологічні методи обробки інформації використовують напівпровідникові електронні компоненти, провідність (опір) яких залежить від різниці напруг між їх полюсами. Якщо технічні засоби обробки інформації піддати впливу високочастотного електромагнітного поля (в мегагерцовому діапазоні), то в колах ТСК виникатиме небезпечний сигнал, що вплине на провідність напівпровідників та інші властивості ТСК.

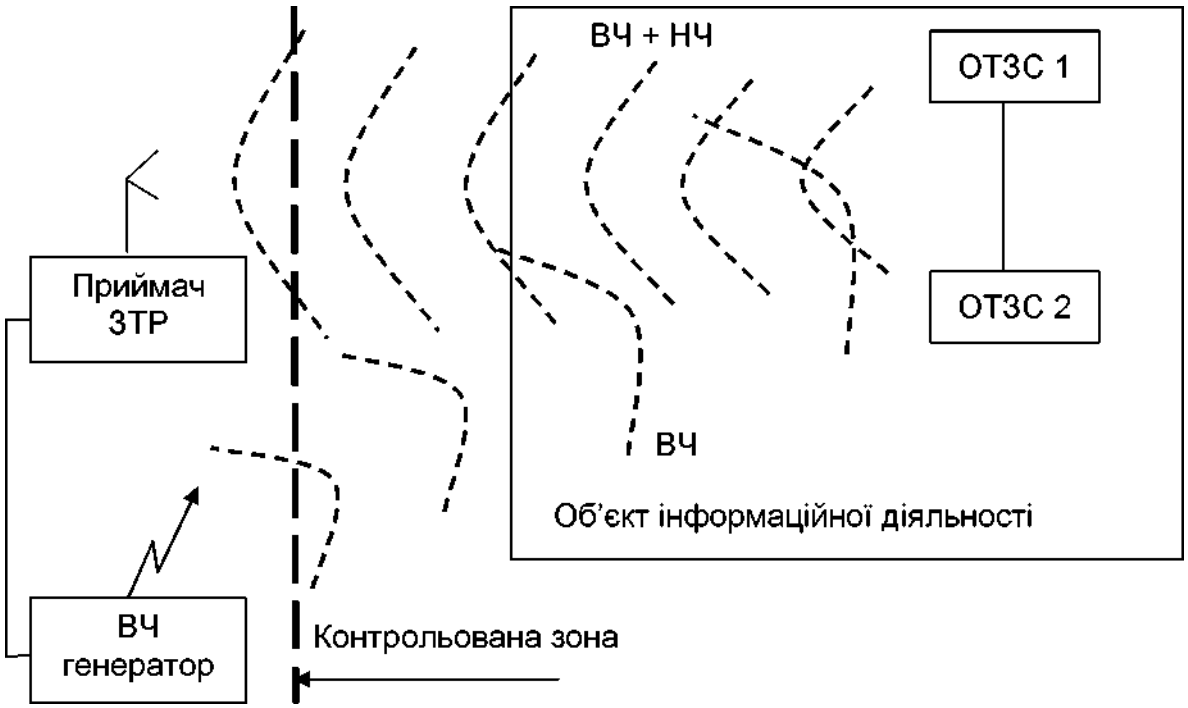


Рис. 3.7. Канал ВЧ нав'язування (для зняття інформації, що обробляється в ОТЗС).

Таким чином, ці схеми слугуватимуть паразитним фільтром для небезпечного сигналу, що призведе до його передачі в радіочастотну область. Повторне випромінювання цього модульованого радіочастотного сигналу може призвести до витоку інформації [8,9,10].

Важливо визнати, що в цьому випадку легко реалізувати прийом цього модульованого радіочастотного сигналу за допомогою когерентного детектування, цей метод забезпечує найбільший ступінь завадостійкості.

Виникнення радіочастотного каналу для передачі інформації (неможливість створення aTCVI) запобігається:

- створенням короткого замикання довжиною щонайменше 2 зони, це розраховується з урахуванням потенційного впливу радіочастот та організації доступу до короткого замикання на OID;

- захистом OTZ;

- просторовим електромагнітним шумом, пов'язаним з об'єктом ЕОТ;

- індикацією, сигналом радіочастотного поля випромінювання та перешкодами роботі OTZ.

Як наслідок, у розділі основна увага приділяється основним типам каналів витоку технічної інформації, що формуються під час обробки інформації в ОТЗС, та основним заходам щодо запобігання витоку інформації через ці канали (насамперед, запобіганню створенню таких каналів витоку інформації).

1.3 Висновки по розділу

У розділі розглядаються основні технічні методи витоку інформації на об'єкті інформаційної діяльності.

Обговорюється категоризація технічних каналів витоку інформації на ціль інформаційної діяльності.

Висвітлено фундаментальні принципи, властивості та методи обробки витоків інформації, а також об'єкт інформаційної діяльності.

РОЗДІЛ 2.
ДОСЛІДЖЕННЯ НАПРЯМКІВ УДОСКОНАЛЕННЯ ЄДИНОЇ МОДЕЛІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ВІД ВИТОКУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ КАНАЛАМИ

2.1. Формування вимог до захисту технічних каналів від несанкціонованого витоку

Підсумуємо потенційні канали витоку технічної інформації від об'єктів інформаційної діяльності:

1. Канали бічного електромагнітного випромінювання (SEM) від OTZS;

2. Канали бічного електромагнітного випромінювання від DTZS;

3. Канали бічних електромагнітних перешкод на лінії електропередачі OTZS (земля);

4. Канали бічних електромагнітних перешкод на зв'язку DTZS;

5. Канали радіочастотних перешкод;

6. Канали витоку оптичної інформації;

7. Встановлення вбудованих пристроїв.

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

- Запобігання каналам бічного електромагнітного випромінювання від OTZS шляхом екранування OTZS або часткового екранування електронних компонентів.

- Запобігання каналам бічного електромагнітного випромінювання від DTZS шляхом визначення зони випромінювання R1 та пропозиції розміщення ноутбука поза цією зоною.

- Бічні канали електромагнітних перешкод на лінії електропередачі OTZS (земля) можуть бути усунені шляхом лінійного придушення шумів лінії електропередачі OTZS.

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

Другим рішенням є встановлення лінійних пристроїв придушення перешкод у 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 вирішувати 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 ЕОТ 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 ЕОТ);

- Оптимізація методів доступу для коротких замикань та саморобних вибухових пристроїв;

- Екранування ЕОТ;

- Встановити просторовий електромагнітний шум на об'єкті ЕОТ;

- Індикувати відхилення параметрів підсилювача та запобігати роботі ЕОТ;

- Розмістити DTZ подалі від Зони 1 ЕОТ та розмістити ЕОТ поблизу його Зони 1, де можуть бути присутні зовнішні провідники;

- Використовувати пристрої технічного захисту в лінії DTZS для затримки сигналів низького рівня;

- Використовувати лінійний шум в лінії DTZS та зовнішніх провідниках;

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

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

- Використовувати лінійний шум у ланцюзі живлення OTZS;

- Незалежне заземлення OTZS;

- Переконатися, що встановлення кронштейна заземлення OTZS відповідає вимогам;

- Розмістіть заземлювальний вимикач та його заземлювальну шину в контрольованій зоні та дотримуйтесь максимальної відстані від меж короткого замикання та зовнішніх провідників;

- Придушіть шум у заземлювальних лініях OTZS та DTZS.

2.2. Вектори захисту інформації від витоку технічними каналами

Створення КСЗІ (Системи контролю інформаційної безпеки) в об'єктах інформаційної діяльності для запобігання витоку інформації через технічні канали повинно базуватися на трьох вимірах захисту інформації [9,11,12]:

1. Захист технічної інформації

2. Процедурний захист інформації

3. Організаційно-технічний захист інформації

Етап 1 створення КСЗІ для запобігання витоку інформації через технічні канали

Етап 1: Забезпечення технічного захисту Системи автоматизації (АС) з одночасним запобіганням витоку інформації через технічні канали [12,13]. На першому етапі слід впровадити основні заходи технічного захисту та провести тестові дослідження ПЕВМН (Мережі процедур, програм та інформації). Зокрема, слід впровадити екранування технічних каналів, встановити лінійні пристрої для придушення перешкод у блоках живлення електронного

обладнання, а також виявляти потенційні випромінювання та перешкоди для подальшого покращення експлуатаційної документації [12,13].

На основі пасивного захисту та лінійних заходів придушення шуму, впроваджена система технічного захисту для запобігання витоку інформації через технічні канали повинна бути сертифікована, а за результатами сертифікації має бути виданий "Сертифікат сертифікації системи автоматизації" [12,13,14]. Фаза друга: Дослідження ІТС та підготовка початкових даних для формулювання вимог KSIZ

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

- Аналіз відповідних нормативних актів та правових документів для визначення обмежень або заборон доступу до певних типів інформації та визначення необхідності забезпечення захисту інформації відповідно до інших стандартів;

- Визначення переліку інформації, яка підлягає обробці автоматично, та її класифікація за рівнями обмеження доступу, вимогами до забезпечення цілісності та вимогами до забезпечення доступності відповідно до нормативних актів та правових документів [8,12,14]

Дослідження повинно враховувати такі аспекти:

- Технічні системи;

- Програмні компоненти;

- Інформація, що обробляється;

- Користувачі;

- Дозволи на доступ до місцезнаходження.

Фаза 3: Розробка політики безпеки

На цій фазі виконуються такі завдання [12,13,14]:

- Аналіз ризиків (вивчення моделей загроз та зловмисників, а також можливих 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 технологій інформаційної безпеки в інтелектуальних транспортних системах (ІТС) для безпечної обробки інформації, а також конкретних заходів та засобів захисту інформації та регулювання діяльності різних груп користувачів;

- Політика інформаційної безпеки повинна враховувати всі характеристики середовища обробки інформації та бути повністю модифікованою відповідальним за захист інформації в організації клієнта. Ця політика не повинна відповідати вимогам, встановленим розробником системи автоматизації (АС).

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

- Посібник користувача;

- Посібник системного адміністратора;

- Посібник адміністратора безпеки.

Посібники користувача повинні чітко визначати методи та правила обробки інформації; нехтування цими методами та правилами може призвести до реалізації загроз та витоків інформації [12,13,14].

Фаза четверта: Розробка Технічного завдання на створення інфраструктури інформаційної безпеки (ІІБ) (далі – ТЗ)

Технічне завдання на створення інфраструктури інформаційної безпеки (ТЗБ) – це документ, що визначає вимоги до захисту інформації в інфраструктурі інформаційної безпеки (ІІБ), процес створення ІІБ, різні процеси тестування ІІБ, а також початкову організаційно-технічну документацію для її впровадження в ІІБ.

Розробка Технічного завдання на створення ІІБ повинна враховувати комплексний підхід до побудови ІІБ, який передбачає інтеграцію всіх необхідних заходів та засобів на кожному етапі життєвого циклу ІІБ в єдину систему для вирішення різних загроз інформаційній безпеці [14,15].

ТЗБ ІІБ може бути використане як для початкового створення ІІБ, так і для модернізації існуючих ІІБ.

ТЗБ KSZI може бути розроблено такими способами [16,17]:

- Як окремий розділ загального технічного завдання на ІІБ;

- Як окремий (частковий) ТЗ;

- Як доповнення до загального ТЗ ІТС.

Для інтегрованих ІТС (що складаються з кількох незалежних інформаційних або комунікаційних систем, які можуть працювати незалежно та взаємодіяти одна з одною) рекомендується розробляти окремий ТЗ для кожного компонента ІТС, з вимогами, визначеними як окремі ТЗ. Як варіант, можна розробити один ТЗ для кількох подібних компонентів ІТС, окресливши їхні відмінності або характеристики [10,12,16].

Фаза 5: Розробка та впровадження проектів ТЗ в ІТС.

Проекти ТЗ розробляються та впроваджуються на основі загальної технічної місії ІТС та виконуються відповідно до цієї місії протягом таких фаз створення ІТС: проектні проекти, технічні проекти та робочі документи.

Під час розробки проектів ЗЗІ необхідні проектні рішення для забезпечення сумісності та взаємодії між різними компонентами ЗЗІ, а також ефективності різних заходів та засобів захисту інформації [15,16].

Для реалізації вимог Специфікації управління проектами (TOR) CSI необхідні спільні рішення. Ці рішення стосуються організаційної структури CSI, структури технологій та програмних засобів, умов використання операційних алгоритмів та засобів захисту, а також впровадження послуг інформаційної безпеки, визначених відповідно до функціонального профілю безпеки.

6 етап. Впровадження KSIZ для запобігання витокам через технічні канали передачі даних.

На цьому етапі розробка KSIZ має бути завершена, система адаптована до середовища експлуатації, а документація, що входить до плану захисту, має бути затверджена [15,16].

Усі категорії користувачів ІТС (персонал технічної служби, звичайні користувачі) повинні пройти навчання з основних умов та процедур документації плану захисту, щоб забезпечити їх дотримання правил політики інформаційної безпеки та заходів захисту інформації. [13,15,16]

Встановлення та тестування програмних продуктів, необхідних для обробки інформації, та програмних заходів захисту інформації відповідно до методів обробки та передачі інформації.

Під час встановлення необхідно включити всі механізми обмеження доступу користувачів до інформаційних та апаратних ресурсів ІТС, механізми контролю поведінки користувачів, а також механізми контролю цілісності програмного забезпечення та бази даних [16,17].

Введення інформації про користувачів АС до засобу захисту та встановлення їхніх прав доступу до захищених ресурсів та середовища обробки/передачі інформації.

Фаза 1: Попереднє тестування АС

На етапі попереднього тестування працездатність системи визначається шляхом моделювання обробки інформації користувачами. Розробник системи намагатиметься вплинути на її роботу шляхом атаки на комп'ютерну систему. Оцінка системи буде проведена з посиланням на CCDS [17]. Будь-які виявлені недоліки та проблеми будуть розглянуті.

Другий етап: Національна акредитація АС

Будь-яка інтегрована система захисту інформації, що перебуває у національній власності, інформація з обмеженим доступом або інша інформація, що охороняється державою, повинна мати сертифікат відповідності вимогам захисту інформації. Цей сертифікат видається Державною службою

захисту інформації та комунікаційних технологій України за результатами національної акредитації. [17,18,19]

Національна акредитація КСІЗ полягає у визначенні її відповідності вимогам технічних завдань, відповідним законам та нормативним актам щодо захисту інформації, а також у визначенні можливості введення КСІЗ в експлуатацію як частини ІТС.

Національна акредитація КСІЗ є етапом приймальних випробувань ІТС та проводиться відповідно до «Положення про національну акредитацію у сфері технічного захисту інформації». [17,18,19]

Третій етап: Підтримка CSI

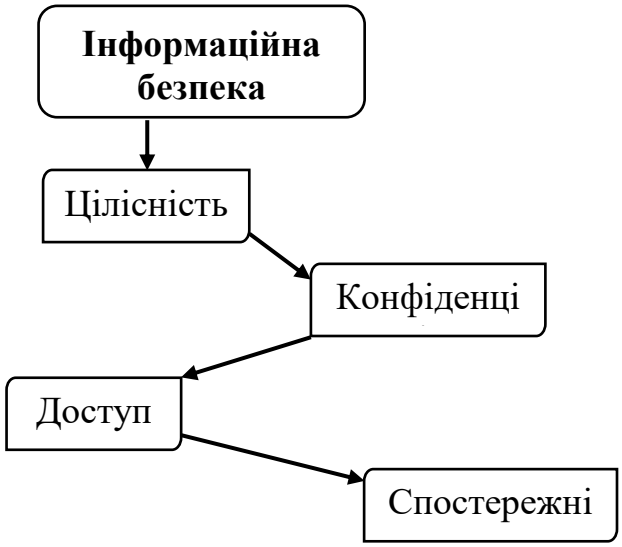
Під час цього етапу проводиться робота із забезпечення організації та функціонування CSI, а також управління модернізацією її планів та заходів захисту інформації відповідно до планів захисту та експлуатаційної документації компонентів CSI. [17,18,19]

Усі дії, пов'язані з модернізацією та обслуговуванням AS, не повинні порушувати специфікації, викладені в експлуатаційній документації, та повинні відповідати політиці захисту інформації.

2.3. Загальний опис єдиної моделі комплексної системи захисту від витоку технічними каналами

CSI буде побудовано на портативному електронному комп'ютері, що забезпечить гнучке та мобільне використання як апаратних, так і програмних компонентів. Система характеризується швидкістю розгортання, яка в кілька разів перевищує звичайні розгортання CSI на основі персональних комп'ютерів.

Захист інформації на основі CSI повинен враховувати та гарантувати цілісність, конфіденційність та доступність інформації, а також забезпечувати можливість моніторингу 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 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, яка використовується для надання початкових вимог до визначення потреб захищених підмоделей ноутбуків та включає політики інформаційної безпеки та інструкції з експлуатації ноутбуків після їх введення в експлуатацію.

Разом з ноутбуками повинні надаватися основні політики захисту інформації, виходячи з їх категорії, функціональності та визначень технічної інформаційної безпеки. Внутрішні політики повинні бути розроблені на основі цих основних політик під час реєстрації AS.

Окрім забезпечення системи CCDS, також необхідно запобігати витоку інформації через технічні канали під час використання ноутбуків. Основні технічні канали витоку інформації перелічені на сторінці 1.1.

2.4. Висновки по розділу

У цьому розділі представлено результати дослідження комплексної системи захисту, розробленої для вдосконалення єдиної моделі запобігання витокам інформації через технічні канали.

У розділі окреслено вимоги до захисту технічних каналів від несанкціонованих витоків інформації.

Визначено заходи захисту інформації для запобігання витокам через технічні канали.

Також наведено загальний опис єдиної моделі.

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

3.1 Нормативно-правове забезпечення розробки комплексної системи захисту інформації на об'єкті інформаційної діяльності

КСЗІ будується відповідно до НД ТЗІ 3.7-003-05 «Порядок створення інтегрованої системи захисту інформації в інформаційно-комунікаційних системах». Незалежно від того, чи створюється КСЗІ в ІТС на стадії проектування, чи в існуючій ІТС, процедура створення КСЗІ в рамках ІТС однакова, якщо потрібно забезпечити захист інформації або модернізувати існуючу КСЗІ [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 рамках ІТС відповідним нормативним актам у сфері захисту інформації та вимогам НД. НД розглядає процедуру створення складної системи захисту інформації в рамках ІТС як низку хронологічно впорядкованих, взаємопов'язаних та об'єднаних незалежних робочих фаз, реалізація яких є необхідною та достатньою для створення КСЗІ [18,19,20]. Послідовність виконання та типовий зміст робіт кожного етапу створення KSIZ повинні узгоджуватися з відповідними фазами та кроками робіт для створення ITS, як визначено в ГОСТ 34.601 [18,19,20].

Фази робіт, їх зміст, результати та терміни виконання під час створення KSIZ у конкретній ITS визначаються ТЗ [13] на створення KSIZ.

Окремі фази робіт можуть бути пропущені або кілька фаз можуть бути об'єднані, а також можуть бути додані нові фази робіт. За необхідності послідовність виконання окремих фаз може бути змінена, наприклад,

виконання кількох фаз робіт одночасно або виконання певних фаз перед завершенням попередніх фаз, за умови, що це не призведе до зниження якості робіт або конфлікту з цілями реалізації [18,19,20].

Якщо в галузі вже запроваджено галузевий Національний регламент захисту технічної інформації (НД ТЗІ) відповідно до встановлених процедур, або якщо існують відповідні нормативні документи, і їхня дія поширюється на організацію-власника ІТС або на саму ІТС, ці регламенти мають вищу силу та повинні дотримуватися в першу чергу. Якщо певний вид робіт не підпадає під дію жодного з вищезазначених рівнів національних нормативних актів щодо захисту технічної інформації, тоді можуть бути прийняті рекомендації щодо міжнародних стандартів, за умови, що вони не суперечать українським нормативним актам, положенням та документам. [13].

3.2 Заходи та засоби комплексної системи технічного захисту інформації на об’єкті інформаційної діяльності

Системи інформаційної безпеки (СІБ) охоплюють заходи та засоби захисту інформації від наступного [18,19,20]:

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

- Несанкціоновані операції та несанкціонований доступ до інформації, наприклад, через підключення пристроїв та ліній зв'язку, видавання себе за зареєстрованих користувачів, обхід заходів захисту для використання інформації або поширення неправдивої інформації, використання вбудованих пристроїв або програм, використання комп'ютерних вірусів тощо;

- Специфічний вплив на інформацію, такий як порушення цілісності інформації або пошкодження систем захисту шляхом формування полів та сигналів [13,14].

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

Там, де це дозволено законом, проектування, розробка, виробництво, випробування та експлуатація інтелектуальних транспортних систем (ІТС) повинні поєднуватися із заходами щодо забезпечення конфіденційності, контррозвідки та організаційними заходами щодо захисту інформації, яка не є державною таємницею та має обмежений доступ. [13]

Згідно зі статтею 5.8 Декрету № НД ТЗІ 3.7-003-2005, якщо інтелектуальна технологічна система обробляє інформацію, що становить державну таємницю, або якщо власник інформації вважає це за необхідне, має бути створена система захисту інформаційних технологій, щоб запобігти витоку інформації через технічні канали. У цій статті особливо наголошується на інтересах власника інформації. Сама система захисту інформаційних технологій може бути не обов'язковою, але необхідно наголосити на технічному захисті.

У всіх системах інформаційно-технологічного обслуговування (ІТС) має бути створено Управління захисту інформації (УЗІ) для інформації, яка є державною власністю, становить державну чи іншу таємницю або належить до певних специфічних видів (необхідність її захисту визначається законом), а також для інформації, яку власник інформації вважає за необхідне захистити. Власник інформації повинен індивідуально, виходячи з конкретних обставин, вирішувати, чи потрібні заходи для запобігання особливому впливу на інформацію [18,19,20].

Для організації створення Управління інформаційної безпеки (УІБ) у системі інформаційно-технологічного обслуговування створюється служба захисту інформації. Процедури її створення, завдання, функції, структура та повноваження визначені в НД 1.4-001-2000.

Після прийняття рішення про створення Управління інформаційної безпеки (УІБ) згодом створюється Інформаційна система інформаційної безпеки (ІСБ). Як виняток, ІСБ може бути створена пізніше, але не пізніше етапу підготовки до впровадження УІБ [13,16,19].

Служби захисту інформації є невід'ємною частиною будь-якої системи, яка потребує захисту. Залежно від розміру бізнесу та кількості співробітників, архітектура самої служби захисту інформації потребує ретельного розгляду.

Для малого бізнесу може бути достатньо призначення 1-2 співробітників з інформаційної безпеки. Покладання обов'язків щодо захисту інформації на співробітників є надзвичайно важливим; більші компанії повинні принаймні створити відділ інформаційної безпеки.

3.3 Етапи створення комплексної системи технічного захисту інформації на об’єкті інформаційної діяльності

Фаза 1: Підготовка вхідних даних для опитування Інтелектуальних транспортних систем (ІТС) та формулювання вимог до Зони спільного використання інформації (ЗСІЗ). Ця фаза зазвичай включає такі операції [18,19,20]:

− Аналіз відповідних нормативних актів та правових документів для визначення обмежень або заборон доступу до певних типів інформації та визначення необхідності забезпечення захисту інформації відповідно до інших стандартів;

− Визначення переліку інформації, що потребує автоматизованої обробки, та її категоризація відповідно до рівнів обмеження доступу, вимог до забезпечення цілісності та вимог до забезпечення доступності відповідно до нормативних актів та правових документів.

В опитуванні Інтелектуальна транспортна система 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 цього опитування є опис операційного середовища кожної Інтелектуальної транспортної системи (ІТС), визначення елементів, які можуть прямо чи опосередковано впливати на інформаційну безпеку, визначення взаємодії між різними елементами середовища та запис результатів опитування для використання на наступних етапах роботи [18,19,20].

Фаза 2: Розробка стратегій безпеки. Під час цієї фази будуть виконані такі роботи:

− Аналіз ризиків (вивчення моделей загроз та зловмисників, а також можливих 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 безпечних технологій обробки інформації в 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) і може бути розроблена для всієї ІТС, окремих компонентів компонента, конкретних функціональних завдань або конкретних технологій обробки інформації. Політика безпеки розробляється як окремий документ від плану захисту [18,19,20].

Фаза 3: Розробка технічних специфікацій (ТЗ) для створення СІБ. Технічні специфікації, що використовуються для створення СІБ в рамках ІТС, є початковими організаційно-технічними документами. Вони визначають вимоги до захисту інформації, що обробляється в рамках ІТС, процедури створення ІПС, процедури виконання всіх типів тестів ІПС та процедури її розгортання як частини ІТС [18,19,20].

Розробка технічних специфікацій ІПС враховує комплексний підхід до побудови ІПС, який передбачає інтеграцію всіх необхідних заходів та засобів захисту від різних загроз інформаційній безпеці на кожному етапі життєвого циклу ІТС в єдину систему. Загальні вимоги ІПС можуть бути розроблені для новоствореної ІТС або під час модернізації існуючої ІТС.

Загальні вимоги КСЗІ можуть бути опубліковані [18,19,20]:

- Як окремий розділ при створенні загального технічного завдання для інтелектуальних транспортних систем (ІТС);

- Як окремий (частковий) збірник технічних завдань (ЗТЗ);

- Як доповнення до створення загального збірника технічних завдань для інтелектуальних транспортних систем (ІТС).

Для інтегрованих інтелектуальних транспортних систем (що складаються з кількох незалежно працюючих та інтерактивних інформаційних або комунікаційних систем) рекомендується створювати окремі критичні системні вимоги (КСВ) для кожного компонента інтелектуальної транспортної системи та формалізувати вимоги в окремі збірники технічних завдань (ЗТЗ). Як варіант, можна розробити єдиний збірник технічних завдань (ЗТЗ) для кількох ідентичних компонентів інтелектуальної транспортної системи із зазначенням відмінностей або характеристик між ними. [11]

Етап 4: Розробка та впровадження проектів критичних системних вимог (КСВ) в інтелектуальних транспортних системах (ІТС).

Проекти критичних системних вимог (КСВ) розробляються на основі створення технічного завдання на інтелектуальні транспортні системи (ІТС) та відповідно до його вимог, і реалізуються на таких етапах створення інтелектуальної транспортної системи (ІТС): попереднє проектування, технічне проектування та підготовка робочої документації. Під час розробки проекту КЗІ були перевірені та сформульовані проектні рішення, що забезпечують сумісність та взаємодію всіх компонентів КЗІ та різних заходів і методів захисту інформації.

Розробляються необхідні спільні рішення для реалізації вимог Обсягу повноважень (ТЗ) проекту КЗІ, включаючи організаційну структуру КЗІ, структуру технологій та програмних засобів, алгоритми роботи та умови використання засобів захисту, а також реалізацію послуг інформаційної безпеки, визначених у профілі функціональної безпеки.

П'ятий етап: Розгортання КЗІ.

На цьому етапі розробка КЗІ 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 для розуміння основних термінів та процедур документів плану захисту з метою дотримання політики інформаційної безпеки та правил експлуатації засобів захисту інформації.

Впроваджена система технічного захисту інформації для запобігання порушенням даних буде сертифікована технічними каналами, а за результатами сертифікації буде видано «Сертифікат сертифікації системи технічного захисту інформації».

Комплекс засобів захисту інформації для запобігання порушенням національної безпеки даних (NSD) буде встановлено, ініціалізовано та валідовано в операційній діяльності відповідно до робочих документів проекту. Під час встановлення мають бути ввімкнені всі механізми, що обмежують доступ користувачів до інформаційних та апаратних ресурсів Інтелектуальної транспортної системи (ІТС), механізми контролю роботи користувачів, а також механізми моніторингу цілісності програмного забезпечення та бази даних.

Інформація про користувачів ІТС вноситься до бази даних захисту, а також встановлюються права доступу до захищених об'єктів ІТС, включаючи створення, модифікацію, архівування, знищення та експорт/імпорт цих об'єктів із системи.

Фаза шоста: Попереднє випробування

Метою попереднього випробування є перевірка роботи KSIZ та її відповідності технічним характеристикам, а також визначення можливості введення KSIZ у дослідну експлуатацію. Попереднє випробування проводитиметься відповідно до процедур та методів випробувань. Ці завдання організовуються клієнтом ITS та спільно виконуються розробниками KSIZ та клієнтом.

Фаза 7: Пілотна експлуатація. Під час пілотної експлуатації KSIZ:

- Розробка технологій для обробки захисту інформації, обігу машинних носіїв даних, обмеження доступу користувачів до ресурсів ITS та автоматизованого керування операціями користувачів;

- Забезпечення отримання персоналом системи захисту інформації та користувачами ITS практичних операційних навичок у сфері технологій захисту інформації, програмного та апаратного забезпечення, а також розуміння вимог до контролю доступу, викладених в організаційних та управлінських документах;

- Завершення розробки програмного забезпечення та виконання додаткового налаштування та конфігурації для KPP Агентства національної безпеки (NSD);

- Коригування робочої та експлуатаційної документації.

Інформація, що становить державну таємницю, не повинна використовуватися під час пілотної експлуатації ITS. Якщо пакет заходів захисту інформації, наданий Національним агентством з питань інформаційної безпеки (НАБЗ), включено до Інфраструктури інформаційної безпеки (ІІБ), і цей пакет ще не отримав експертного висновку щодо його відповідності Національним правилам технологічної безпеки (НД ТЗІ), необхідно виконати низку завдань для підготовки до оцінки відповідності пакету заходів захисту інформації вимогам НД ТЗІ під час процесу національної експертизи ІІБ.

Етап 8: Державна експертиза ІІБ. Системи захисту інформації, що належать державі, інформація з обмеженим доступом або інша інформація, що охороняється державою, повинні мати сертифікат відповідності вимогам захисту інформації, виданий Державною службою інформаційної безпеки України за результатами державної експертизи. Метою державної експертизи ІІБ є визначення того, чи відповідає вона вимогам технічних завдань, законодавства та нормативних актів щодо захисту інформації, а також чи може ІІБ бути введена в експлуатацію як частина Інформаційно-технологічної системи (ІТС). Державна оцінка ІІБ є етапом приймально-здавальних випробувань ІТС та проводиться відповідно до «Положення про державну експертизу у сфері технічного захисту інформації». Якщо інформація, що обробляється ІТС, є державною або охоронюваною державою, керівник організації може наказати про затвердження експлуатації ІТС лише після отримання сертифіката відповідності від KSIZ. [12]

Фаза 1: Підтримка KSIZ. На цій фазі буде проведено роботу щодо забезпечення організаційної роботи KSIZ, модернізації її планів та управління заходами захисту інформації відповідно до планів захисту та експлуатаційних документів компонентів KSIZ. [10,17]

3.4. Розробка та оформлення політики безпеки інформації від витоку технічними каналами на об’єкті інформаційної діяльності

Фаза 1: Підготовка вхідних даних для опитування Інтелектуальних транспортних систем (ІТС) та визначення вимог до Зони обміну інформацією (ЗОБІ). Ця фаза зазвичай включає такі операції [18,19,20]:

− Аналіз відповідних нормативних актів та правових документів для виявлення обмежень або заборон доступу до певних типів інформації та визначення необхідності забезпечення захисту інформації відповідно до інших стандартів;

− На основі нормативних актів та правових документів, визначення переліку інформації, що потребує автоматизованої обробки, та її категоризація відповідно до рівнів обмеження доступу, вимог цілісності та вимог доступності.

В опитуванні Інтелектуальні транспортні системи розглядаються як організаційно-технологічна система, що поєднує обчислювальні системи, фізичні середовища, середовища користувачів, обробку інформації та технології обробки (далі – операційне середовище ІТС) [18,19,20].

Це опитування має на меті описати операційне середовище кожної Інтелектуальної транспортної системи (ІТС), визначити фактори, які можуть прямо чи опосередковано впливати на інформаційну безпеку, визначити взаємодію між різними факторами в середовищі та зафіксувати результати опитування для використання на наступних етапах роботи [18,19,20].

Фаза 2: Розробка стратегій безпеки. Під час цієї фази будуть виконані такі роботи:

− Аналіз ризиків (вивчення моделей загроз та зловмисників, а також можливих 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 безпечних технологій обробки інформації в ІТС, а також конкретних заходів та засобів захисту інформації та специфікацій діяльності для різних груп користувачів;

− Складання документа політики інформаційної безпеки.

Політика безпеки повинна враховувати характеристики кожного компонента Системи інформаційної безпеки (СІБ) і може бути розроблена для всієї ІТС, окремих компонентів компонента, конкретних функціональних завдань або конкретних технологій обробки інформації. Політика безпеки розробляється як документ, незалежний від плану захисту [18,19,20].

Фаза третій: Розробка технічної специфікації (ТС) Системи інформаційної безпеки (СІБ). Технічна специфікація, яка використовується для

створення Системи інформаційної безпеки (СІБ) в рамках Інтелектуальної транспортної системи (ІТС), є початковим організаційно-технічним документом. Ці специфікації визначають вимоги до захисту інформації, що обробляється в рамках Інтелектуальних транспортних систем (ІТС), процес створення Систем інформаційної безпеки (СІБ), процедури проведення різних тестів СІБ та процес їх розгортання як частини СІБ [18,19,20].

Розробка технічних специфікацій СІБ враховує комплексний підхід до побудови СІБ, інтегруючи всі необхідні заходи та механізми захисту на кожному етапі життєвого циклу СІБ в єдину систему для вирішення різних загроз інформаційній безпеці. Загальні вимоги до інтелектуальних транспортних систем (ІТС) можуть бути розроблені для нових ІТС або для модернізації існуючих ІТС.

Загальні вимоги до КСЗІ можуть бути опубліковані такими способами [18,19,20]:

- як окремий розділ під час створення загальних технічних завдань для інтелектуальних транспортних систем (ІТС);

- як окремий (частковий) комплект технічних завдань (ЧТЗ);

- як доповнення до створення загального комплекту технічних завдань для інтелектуальних транспортних систем (ІТС).

Для інтегрованих інтелектуальних транспортних систем (що складаються з кількох незалежно працюючих та інтерактивних інформаційних або комунікаційних систем) рекомендується створювати окремі критичні системні вимоги (КВВ) для кожного компонента інтелектуальної транспортної системи та формалізувати ці вимоги як окремі комплекти технічних завдань (КТЗ). Як варіант, можна розробити єдиний комплект технічних завдань (КВВ) для кількох ідентичних компонентів інтелектуальної транспортної системи, вказавши відмінності або характеристики між ними. [11]

Фаза 4: Розробка та впровадження проекту критичних системних вимог (КВВ) для інтелектуальних транспортних систем (ІТС). Проект критичних

системних вимог (КВВ) розробляється на основі та відповідно до технічних специфікацій Інтелектуальних транспортних систем (ІТС) та реалізується на таких етапах створення ІТС: попереднє проектування, технічне проектування та робоча документація. Під час розробки проекту КВВ тестуються та вдосконалюються схеми проектування для забезпечення сумісності та взаємодії всіх компонентів КВВ, а також різних заходів та методів захисту інформації.

Розробляються необхідні загальні рішення для задоволення вимог Обсягу повноважень (ТО) проекту КВВ, включаючи організаційну структуру КВВ, технічну та програмну архітектуру, алгоритми роботи та умови використання засобів захисту, а також впровадження послуг інформаційної безпеки, визначених у профілі функціональної безпеки.

П'ятий етап: Розгортання КВВ

На цьому етапі має бути завершена розробка критичної інформаційної інфраструктури (КІІ) та затверджені документи, що входять до плану захисту.

Усі користувачі ІТС (персонал технічної служби та загальні користувачі) повинні пройти навчання для розуміння основної термінології та процедур документів плану захисту інформації, тим самим дотримуючись політик інформаційної безпеки та правил експлуатації засобів захисту інформації.

Системи технічного захисту інформації, впроваджені для запобігання порушенням даних, будуть сертифіковані технічними каналами, а за результатами сертифікації буде видано «Сертифікат сертифікації системи технічного захисту інформації».

Набори інструментів захисту інформації, розгорнуті для запобігання порушенням даних національної безпеки (NSD), будуть встановлені, ініціалізовані та перевірені відповідно до робочої документації проекту, а також будуть валідовані під час операційної діяльності. Під час встановлення мають бути ввімкнені всі механізми, що обмежують доступ користувачів до інформаційних та апаратних ресурсів Інтелектуальної транспортної системи

(ІТС), механізми контролю операцій користувачів, а також механізми моніторингу цілісності програмного забезпечення та баз даних.

Інформація про користувачів ІТС буде внесена до захищеної бази даних, а також будуть встановлені дозволи доступу до захищених об'єктів ІТС, включаючи створення, модифікацію, архівування, знищення та експорт/імпорт цих об'єктів із системи.

Фаза шоста: Попереднє тестування

Метою попереднього тестування є перевірка роботи КСІЗ та її відповідності технічним характеристикам, а також визначення можливості введення КСІЗ у дослідну експлуатацію. Попереднє тестування буде проведено відповідно до процедур та методів тестування. Ці завдання організовуються замовником ІТС та спільно виконуються розробниками КСІЗ та замовником.

Фаза сьома: Пілотна експлуатація. Під час пілотної експлуатації КСІЗ:

- Розробка технологій обробки інформаційної безпеки, обробки машинних носіїв даних, обмеження доступу користувачів до ресурсів ІТС та автоматизації управління операціями користувачів;

- Забезпечити, щоб персонал системи інформаційної безпеки та користувачі інформаційно-технологічних систем (ІТС) мали практичні навички роботи з технологіями інформаційної безпеки, програмним та апаратним забезпеченням, а також розуміли вимоги до контролю доступу, зазначені в організаційних та управлінських документах;

- Завершити розробку програмного забезпечення та додаткову конфігурацію налаштувань для Агентства національної безпеки (АНБ) та Бюро національної безпеки (БНБ);

- Коригувати робочу та експлуатаційну документацію.

Під час пілотної експлуатації ІТС інформація, що становить державну таємницю, не повинна використовуватися. Якщо Інфраструктура інформаційної безпеки (ІББ) включає пакет захисту інформації, наданий Національним агентством інформаційної безпеки (НАІБ), і цей пакет ще не отримав

експертного висновку щодо його відповідності Національним правилам технологічної безпеки (НПР), необхідно виконати низку завдань для оцінки відповідності пакета захисту інформації НПР під час процесу перевірки Національної інфраструктури інформаційної безпеки (НІІБ).

Фаза 8: Перевірка Національної інфраструктури інформаційної безпеки (НІІБ). Державні системи захисту інформації, інформація з обмеженим доступом або інша інформація, що охороняється державою, повинні мати сертифікат відповідності вимогам захисту інформації, виданий Державною службою інформаційної безпеки України за результатами державної перевірки. Метою державної експертизи систем інформаційної безпеки є визначення їх відповідності вимогам технічних умов, законів, нормативних актів та правил щодо захисту інформації, а також можливості введення системи інформаційної безпеки в експлуатацію як частини інформаційно-технологічної системи (ІТС). Державна оцінка систем інформаційної безпеки є частиною етапу приймально-здавальних випробувань інформаційно-технологічної системи та проводиться відповідно до таких нормативних актів:Національні правила оцінки у сфері технічного захисту інформації. Якщо інформація, що обробляється службою інформаційних технологій (ІТС), є національною інформацією або захищена державою, керівник організації може схвалити експлуатацію ІТС лише після отримання кваліфікаційного сертифіката від Державного бюро інформаційних технологій (ДБІТ). [12]

Фаза 1: Підтримка ДБІТ. Ця фаза включатиме забезпечення функціонування організації ДБІТ, оновлення її планів та управління заходами захисту інформації відповідно до планів захисту та операційних документів різних компонентів ДБІТ. [10,17]

3.5 Рекомендації по застосуванню технічних засобів запобігання витоку інформації на об’єкті інформаційної діяльності

Методи захисту інформації від розголошення за допомогою технічних засобів мають різні властивості та можливості:

Блокатор бездротового зв'язку "СБ ТЗІ 7-1": Ефективність представлених методів залежить від різних факторів, включаючи відстань до джерела випромінювання, відстань до приймача, рівень випромінювання та спрямованість антен.

Акустичний екранований гучномовець "МАРС-АКЗ". Розроблений з метою захисту приміщення від витоків інформації, пов'язаних зі звуком. Він включає акустичний випромінювач та вимикач, який відключає акустичний випромінювач від лінії, коли генератор шуму не має сигналу, що запобігає роботі гучномовця як мікрофона. Рівень чутливості (83±2) дБ; Номінальний опір становить 10 Ом, а максимальна потужність, яку можна подати, становить 5 ВА.

Завадостійкий фільтр ФЗП-110-2 має властивості щодо робочої напруги, споживаного струму, струму витоку та діапазону частот. Номінальна напруга, на яку розрахований робочий механізм, становить 220 В (50 Гц), споживаний струм під час роботи – 10 А, а струм витоку – не більше 15 мА. Діапазон частот – 10 кГц... 18000 МГц.

Частотні випромінювачі марки VI. Ці частотні випромінювачі працюють у діапазоні від 180 Гц до 5600 Гц з опором обмотки 50 Ом.

Генератор шуму цієї марки називається «Базальт-5». Призначений для екранування об'єктів від витоку інформації через побічну електрику. Цей генератор створює потужне шумове поле з широким діапазоном частот від 0,1 до 1000 МГц.[18,19].

Інформаційна безпека стає все більш актуальною з постійним розвитком технологій. Одним з ефективних рішень для промисловості є мережевий фільтр перешкод типу FZP103-2. Ці фільтри відповідають стандарту ТУ У 31.1-31731859-001-2003 та призначені для запобігання витоку інформації з основних та додаткових пристроїв обробки інформації через систему живлення.

ФЗП103-2 працює на різних частотах, від звукових до високих, що запобігає впливу високої напруги. Ці фільтри безпечні у використанні, навіть якщо є обрив або відсутність фундаменту, що робить їх надійними засобами захисту. Вони відповідають усім вимогам вітчизняного стандарту ДСТУ 3639-97 «ФІЛЬТРИ ПРОТИ ПЕРЕКЛЮЧЕННЯ».

Унікальною особливістю цих фільтрів є їх компактний розмір та легка конструкція, що дозволяє ефективно інтегрувати їх у різні системи. Наприклад, цей тип фільтра має об'єм 0,42 дм³ та вагу 0,85 кг, що робить його ідеальним для різних сценаріїв та умов.[30-33].

Пристрій активного захисту для автоматизованих систем "ДЕЛЬТА-7" є невід'ємною частиною захисту інформації в електронно-обчислювальних машинах, засобах спеціального зв'язку та інших сферах інформаційної діяльності. Цей пристрій призначений для запобігання блокуванню інформаційних сигналів, спричиненому побічним електромагнітним випромінюванням та перешкодами технічних пристроїв, включаючи комп'ютери, копіювальну техніку, мережеве обладнання та засоби зв'язку.

Спеціальний інформаційно-телекомунікаційний пристрій (СІТ) - це електронний пристрій, призначений для захисту від витоку інформації через побічні електронні випромінювання та наведення. Цей пристрій використовується для обробки персональних даних, що вважаються секретними, і може використовуватися на об'єктах різних інформаційних категорій.

Обидва методи, "ДЕЛЬТА-7" та СІТ, є важливими для забезпечення безпеки та конфіденційності інформації щодо технологій, захист цієї інформації має першорядне значення для безпеки та конфіденційності самої інформації.

Шумогенератор МАРС-ТЗО-4-2 - це успішний пристрій, який створює шум у широкому діапазоні частот від 180 до 5600 Гц. Він гарантує стабільне значення вихідної напруги на опорі навантаження, яке не менше 3,5 В, а також

передає прискорення, яке відчувається у всьому діапазоні шуму, не менше 50 дБ, завдяки використанню вібратора VI4.

Гучномовці в системі MARS-AK мали звуковий тиск, достатній для роботи системи на відстані 1 метра, з мінімумом 80 дБ. Діапазон регулювання пристрою для рівня шуму на виходах становить не менше 20 дБ, і він споживає мало енергії, не більше 40 ВА.

Цей генератор є лише одним з багатьох різних пристроїв, які можна використовувати в різних сферах, де створення шуму або регулювання параметрів має вирішальне значення для роботи обладнання або систем.[33] Поряд з іншими технологіями.

3.6. Висновки по розділу

У розділі описано комплексний підхід до захисту об'єкта інформаційної діяльності від витоку через технічні засоби.

Розглянуто ступінь нормативно-правового забезпечення розробки комплексної системи захисту інформації щодо об'єкта інформаційної діяльності.

Описано компоненти та методи комплексної системи технічного захисту інформації, призначеної для інформаційної діяльності.

Описано етапи створення комплексної системи технічного захисту інформації у цільового об'єкта інформаційного забезпечення.

Сформульовано та формалізовано політику безпеки від витоку даних через технічні засоби витоку даних у місці призначення інформації.

Обговорено технічні методи запобігання витоку інформації та мету інформаційної діяльності.

ВИСНОВКИ

У процесі підготовки кваліфікаційного завдання було виконано такі дії:

- Проведено дослідження фундаментальних принципів, властивостей та методів технічних каналів витоку інформації, утворених основними технічними засобами та інформаційними системами у фокусі інформаційної діяльності.

- Досліджено шляхи розробки та вдосконалення єдиної моделі комплексної системи безпеки з підвищеним захистом від витоку інформації через технічні засоби.

- Створено комплексну систему захисту об'єкта інформаційної діяльності, яка потребує підвищеного захисту від втрати інформації через технічні засоби.

- Розглянуто суперечки щодо захисту навколишнього середовища.

1. У першій частині кваліфікації проведено дослідження основних технічних методів витоку інформації у об'єкта інформаційної діяльності. Наведено категоризацію технічних методів розкриття інформації у фокусі інформаційної діяльності. Виявлено фундаментальні принципи, властивості та методи витоку інформації. Розкрито основні технічні засоби та функціональні можливості інформаційних систем.

2. У другій частині кваліфікаційного завдання представлено результати дослідження напрямків вдосконалення єдиної моделі комплексної системи запобігання витоку інформації через технічні засоби. Встановлено необхідні правила захисту технічних каналів від незаконного розголошення інформації. Визначено вектори захисту від витоку інформації через технічні засоби. Наведено загальний опис єдиної моделі комплексної системи, призначеної для запобігання витоку через технічні засоби.

3. Третя частина кваліфікаційного завдання – це комплексна система захисту об’єкта інформаційної діяльності від витоку через технічні засоби. Розглянуто ступінь нормативно-правового забезпечення розробки комплексної системи захисту інформації у фокусі інформаційної діяльності. Описано методи та заходи комплексної технічної системи захисту інформації щодо об’єкта інформаційної діяльності. Описано етапи створення комплексної технічної системи захисту інформації про об’єкти інформаційної діяльності. Формульовано та формалізовано політику безпеки від витоку даних через технічні засоби доступу до даних на об’єкті інформації.

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.

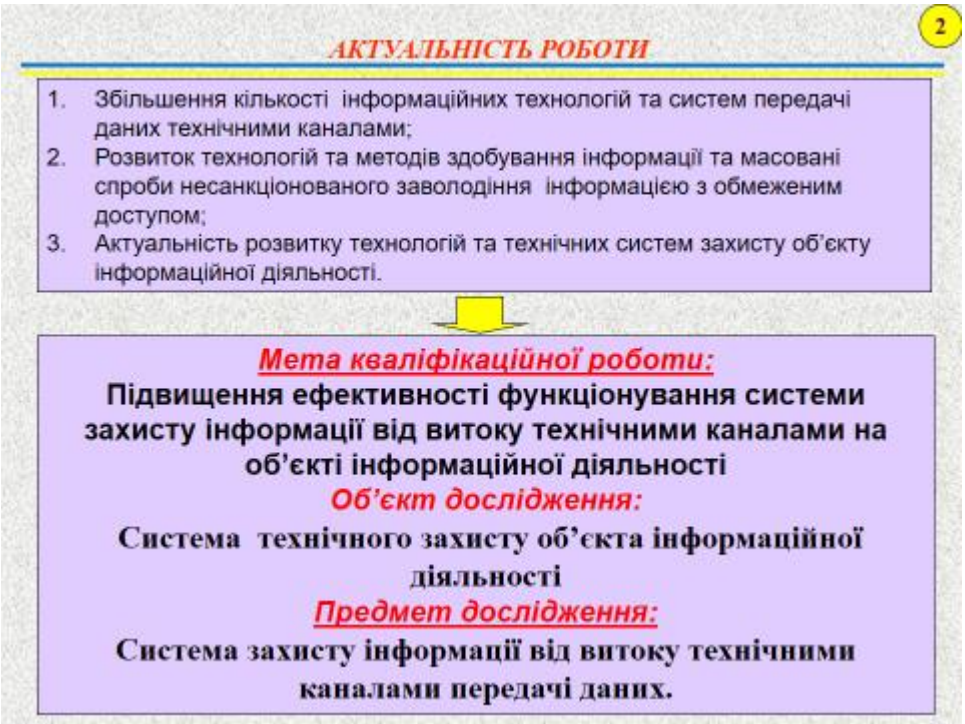
22. Волошин І. М. Методика дослідження проблем природокористування. — Львів: ЛДУ, 1994. — 160 с.

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

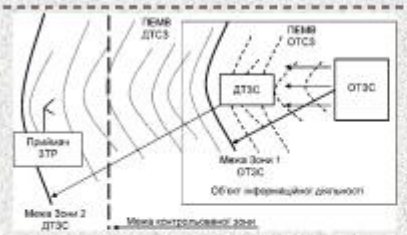
ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

СТРУКТУРА ТЕХНІЧНОГО КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ

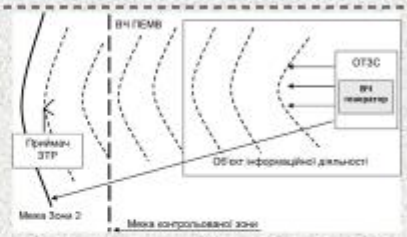
6

ПЕРШИЙ РЕЗУЛЬТАТ

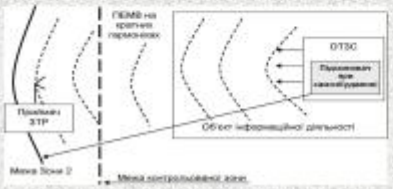
ХАРАКТЕРИСТИКА ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ



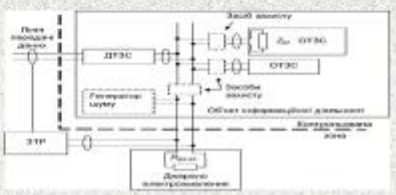
Канал побічних електромагнітних випромінювань



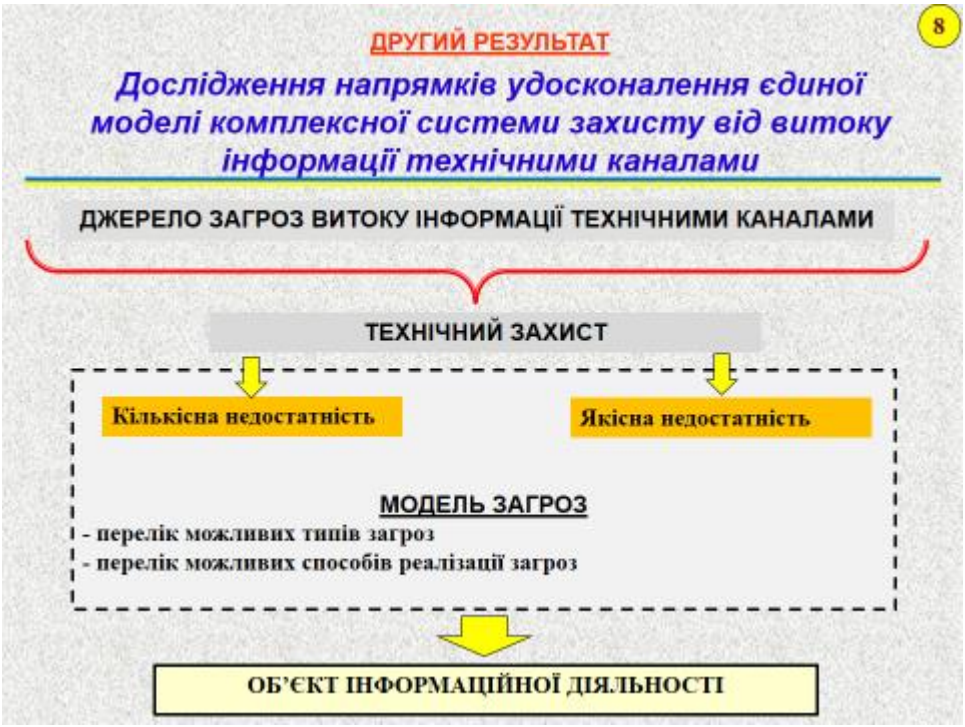
Канал "паразитної" модуляції сигналів ВЧ генераторів



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.

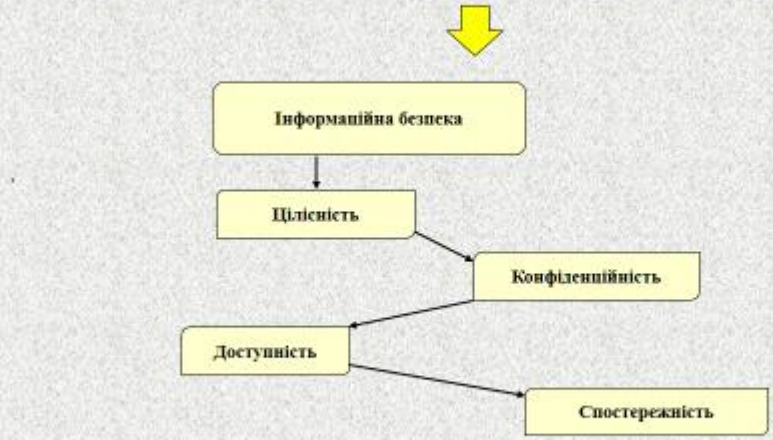
ШЛЯХИ ЗАХИСТУ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ:

- 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 !