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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Системи захисту об'єкту інформаційної діяльності від витоку конфіденційних даних технічними каналами передачі інформації»

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
_____ Ярослав ІВАНЦОВ

Виконав: здобувач вищої освіти групи СЗДМ 61
Ярослав ІВАНЦОВ

Керівник: _____ТУРОВСЬКИЙ Олександр___
д.т.н. , професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2025

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

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___125-Кібербезпека та захист інформації_____
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСК
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Іванцову Ярославу Васильовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Системи захисту об'єкту інформаційної діяльності від витоку конфіденційних даних технічними каналами передачі інформації»
керівник кваліфікаційної роботи ТУРОВСЬКИЙ Олександр, д.т.н., професор

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

2. Строк подання кваліфікаційної роботи 20.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи: опорний об'єкт інформаційної діяльності, технічні канали витоку інформації, вимоги до захисту інформації з обмеженим доступом, сучасні засоби захисту інформації від витоку технічними каналами, технічні засоби захисту та технічної системи охорони.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1 Провести аналіз сутності, властивостей та шляхів утворення технічних каналів витоку інформації, що утворюються основними технічними засобами та системами на об'єкті інформаційної діяльності;
4.2 Здійснити дослідження напрямків розробки та удосконалення єдиної моделі комплексної системи захисту з посиленими заходами від витоку інформації технічними каналами;
4.3. Розробити комплексну системи 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 _____20.10.2024 ___ _____

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 _____ Ярослав ІВАНЦОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Олександр ТУРОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

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

Метою кваліфікаційної роботи є підвищення ефективності функціонування системи захисту інформації від витоку технічними каналами 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.

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

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

Апробація:

О.В. Іванцов, О.В. Таров, Н.О. Левчук, Аналіз загроз несанкціонованого доступу до технічних каналів передачі інформації з обмеженим доступом. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.90 - 91.

https://duikt.edu.ua/uploads/p_2661_93669247.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 information protection system against leakage through technical channels at the object of information activity.

The following tasks were solved in the qualification work. 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, were reviewed. 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 of protection of the object of information activity with increased requirements for protection against information leakage through technical channels was developed.

Object of research. System of technical protection of the object of information activity.

Subject of research. System of information protection from leakage through technical data transmission channels.

Approbation:

O.V. Ivantsov, O.V. Tarov, N.O. Levchuk, Analysis of threats of unauthorized access to technical channels of information transmission with limited access. All-Ukrainian scientific and practical conference: Current problems of security of information and telecommunication systems. Kyiv, November 3, 2024, Kyiv: RVC DUICT. – 024. P.90 - 91.

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

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

ВИСНОВКИ……..…… ..49
ПЕРЕЛІК ПОСИЛАНЬ ……..…….. ..51
ДОДАТОК А ……..……... ..54

СПИСОК УМОВНИХ СКОРОЧЕНЬ

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

ВСТУП

Характерною та важливою проблемою сьогодення стало питання забезпечення безпеки функціонування державних установ, підприємств, загальнонаціональних систем та мереж забезпечення життєдіяльності населення які кваліфікуються як об’єкти інформаційної діяльності. Тобто об’єкти, неналежне функціонування чи вихід зі строю яких можуть значною мірою вплинути на якість управління життєдіяльності населення цілих регіонів. Виходячи з важливих змін в розвитку науки та техніки, ускладнення процесів економічного життя та суспільних відноси, розвитку різноманітних технологій, на основі яких функціонують вказані об’єкти можна зробити висновок про те, що одним з факторів, який забезпечує якість функціонування є різноманітна інформація. Забезпечення ефективного функціонування системи захисту інформації від витоку технічними каналами на об’єкті інформаційної діяльності є актуальним заданням, вирішенню якого присвячена дана робота.

Метою кваліфікаційної роботи є підвищення ефективності функціонування системи захисту інформації від витоку технічними каналами 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 встановлення вимог та організації захисту інформації від витоку технічними каналами здійснена їх класифікація за певними ознаками. Зокрема відокремлені типи ТКВІ за такими ознаками [1,2]:

- за видом інформаційної діяльності на ОІД,
- за принципом (фізичним ефектом, процесом) формування небезпечного сигналу (носія інформації),
- за середовищем поширення небезпечного сигналу,
- за способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника.

За видом інформаційної діяльності на ОІД відокремлюються такі типи ТКВІ [1,2]:

a) технічні канали витоку мовної інформації,
b) технічні канали витоку інформації, що обробляється в ОТЗС,
c) технічні канали витоку візуальної інформації,
d) матеріально-речовинні канали витоку інформації.

Класифікацію ТКВІ за принципом (фізичним ефектом, процесом) формування небезпечного сигналу, середовищем поширення небезпечного сигналу та способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника доцільно розглянути у межах визначених вище типів ТКВІ.[17]

Технічні канали витоку мовної інформації за цими ознаками поділяються на такі [1,2]:

a) Акустичні канали.

b) Акустовібраційні (віброакустичні) канали.

c) Акустооптоелектронні (лазерні акустичні) канали.

d) Акустоелектричні канали.

e) Відеоакустичні канали.

f) Канали ВЧ нав’язування (для зняття мовної інформації).

g) Канали витоку мовної інформації на основі закладних пристроїв.

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

1. Канали побічних електромагнітних випромінювань.
2. Канали побічних електромагнітних наведень.
3. Канали “паразитної” модуляції сигналів ВЧ генераторів.
4. Канали “паразитної” ВЧ генерації підсилювачів.
5. Канали перехоплення (зняття) інформації з волоконно-оптичних ліній передачі даних.
6. Канали перехоплення (зняття) інформації з каналів зв’язку.
7. Канали ВЧ нав’язування (для зняття інформації, що обробляється в ОТЗС).
8. Канали витоку інформації, що обробляється в ОТЗС, на основі закладних пристроїв.

Технічні канали витоку візуальної інформації поділяються на такі:

1. Візуальні канали.
2. Візуально оптичні канали.
3. Канали витоку візуальної інформації на основі закладних пристроїв.

Матеріально-речовинні канали витоку інформації:

1. Добування інформації з магнітних та інших носіїв інформації засобів ЕОТ, що вийшли з ладу.
2. Добування інформації з чернеток документів, з відходів виробництва, видавницької діяльності, діловодства тощо.

3. Хімічні канали. [17]

За носієм інформації та принципом формування небезпечного сигналу відокремлюються такі ТКВІ [2,3]:

електромагнітні канали витоку інформації, до яких відносяться канали побічних електромагнітних випромінювань, канали “паразитної” ВЧ генерації підсилювачів, канали “паразитної” модуляції ВЧ генераторів, канали перехоплення інформації з ліній радіо- (радіорелейного, стільникового, мобільного) зв’язку та тому подібні;

електричні канали витоку інформації, до яких відносяться канали побічних електромагнітних наведень на комунікації, канали зняття інформації з ліній провідного зв’язку та тому подібні;

параметричні канали витоку інформації, до яких відносяться, канали ВЧ нав’язування, канали “паразитної” модуляціїтатому подібні.

За місцем перехоплення інформації засобами технічної розвідки противника відокремлюються такі типи ТКВІ [2,3,4]:

1) канали перехоплення (зняття) інформації за межами КЗ,

2) канали перехоплення (зняття) інформації за межами КЗ з активним впливом на параметри технічного каналу витоку інформації (наприклад, канал ВЧ нав’язування),

3) канали зняття інформації засобами технічної розвідки, встановленими на ОІД (наприклад, технічні канали витоку інформації закладними пристроями).

Розглянута класифікація технічних каналів витоку інформації дозволяє систематизувати уявлення про них та встановити вимоги і заходи щодо захисту інформації від витоку відповідними ТКВІ/

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

Розглянемо сутність та шляхи (фізичні основи, принципи та порядок) утворення технічних каналів витоку інформації, що обробляється основними технічними засобами та системами. Найнебезпечнішими для витоку інформації, що обробляється в ОТЗС, є канали побічних електромагнітних випромінювань та наведень (канали ПЕМВН) [4,5]

Канал побічних електромагнітних випромінювань ОТЗС

Канал побічних електромагнітних випромінювань ОТЗС (канал ПЕМВ ОТЗС) утворюється шляхом перехоплення приймачами засобів технічної розвідки побічних електромагнітних полів, які формуються навколо електронних елементів та провідників (шлейфів) ОТЗС при проходженні ними інформаційних сигналів та поширення цих полів за межі контрольованої зони.

Інформаційними сигналами у даному випадку є електричні струми, що несуть інформацію.

Обробка та передача інформації в ОТЗС здійснюється за допомогою електричних струмів провідності, що представляють собою спрямований потік заряджених частинок - електронів. Як відомо з фізики, навколо нерухомих електронів чи групи електронів завжди присутнє електростатичне поле. Якщо ж цей заряд привести до руху, то в полі виникає магнітна складова і воно стає електромагнітним. Електромагнітне поле розповсюджується в просторі [4,5].

Навколо ОТЗС, як системи електронних елементів та провідників (шлейфів), в яких відповідно з принципом основної дії ОТЗС циркулюють електричні струми, що несуть інформацію, завжди присутні поля випромінювання. Оскілки ці випромінювання небажані та носять паразитичний (побічний) характер, їх називають побічними електромагнітними випромінюваннями (ПЕМВ). Побічні електромагнітні випромінювання

поширюються у вільному просторі і можуть бути перехоплені за межами КЗ приймачами засобів технічної розвідки противника, таким чином утворюється канал ПЕМВ ОТЗС (рис. 1.1) [4,5,6]:

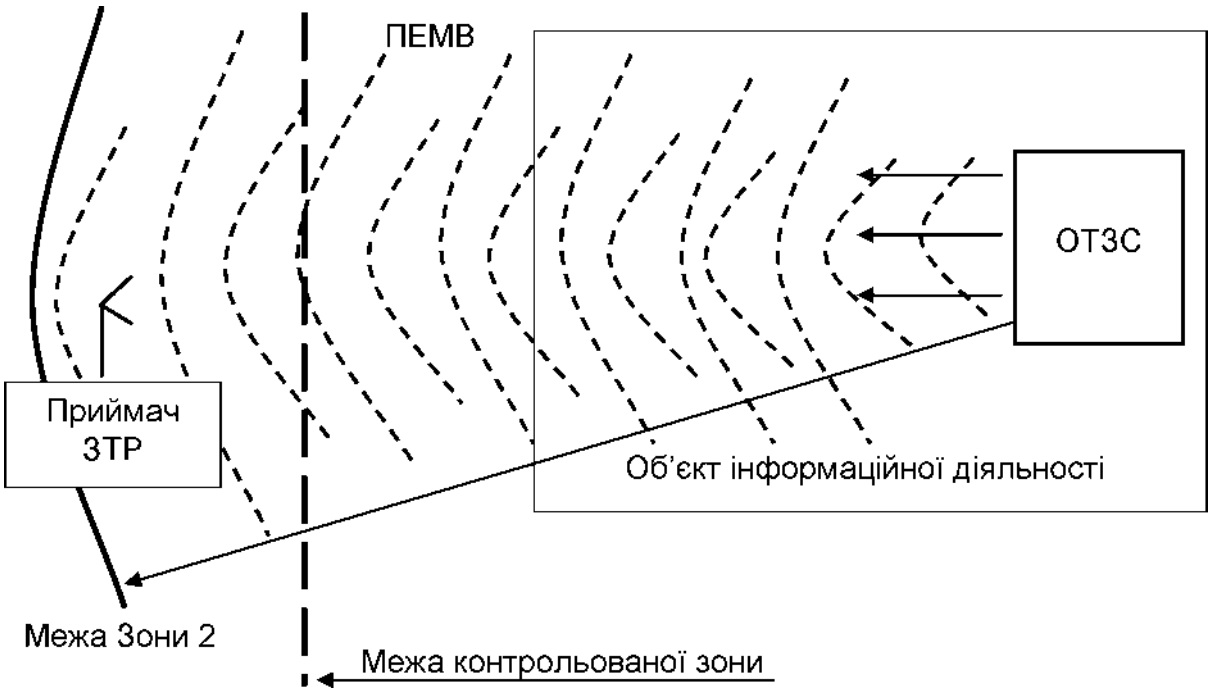


Рис. 1.1. Канал побічних електромагнітних випромінювань ОТЗС.

З фізики також відомо, що при поширенні електромагнітного поля воно загасає. Тому є така відстань від джерела випромінювання - ОТЗС, на якій поле випромінювання згасне до рівня, при якому стає неможливим його приймання (виявлення та вимірювання його параметрів). При цьому небезпечний сигнал, що несеться цим полем, буде, практично, зруйнований звичайними завадами та шумами. Як вже відмічалося раніше, простір, за межами якого відношення сигналу до завади не перевищує допустиму норму, є Зоною 2 даного ОТЗС. Розташування приймачів ЗТР противника за межами Зони 2 не дасть можливості перехоплення інформації [4,5,6].

Канал побічних електромагнітних випромінювань ДТЗС.

Канал побічних електромагнітних випромінювань ДТЗС, як різновид каналів ПЕМВ, утворюється шляхом перехоплення приймачами засобів

технічної розвідки за межами КЗ небезпечних сигналів у вигляді побічних електромагнітних полів ОТЗС, які перевипромінюються допоміжними технічними засобами та системами, а також сторонніми провідниками.

Допоміжні технічні засоби та системи, а також сторонні провідники, якщо вони знаходяться в зоні 1 ОТЗС або мають спільні пробіги з лініями, якими поширюються небезпечні сигнали (в тому числі сигнали побічних електромагнітних наведень) ОТЗС, є випадковими антенами і можуть призвести до витоку інформації небезпечними сигналами, наведеними на них побічними електромагнітними випромінюваннями основних технічних засобів та систем [4,5,6].

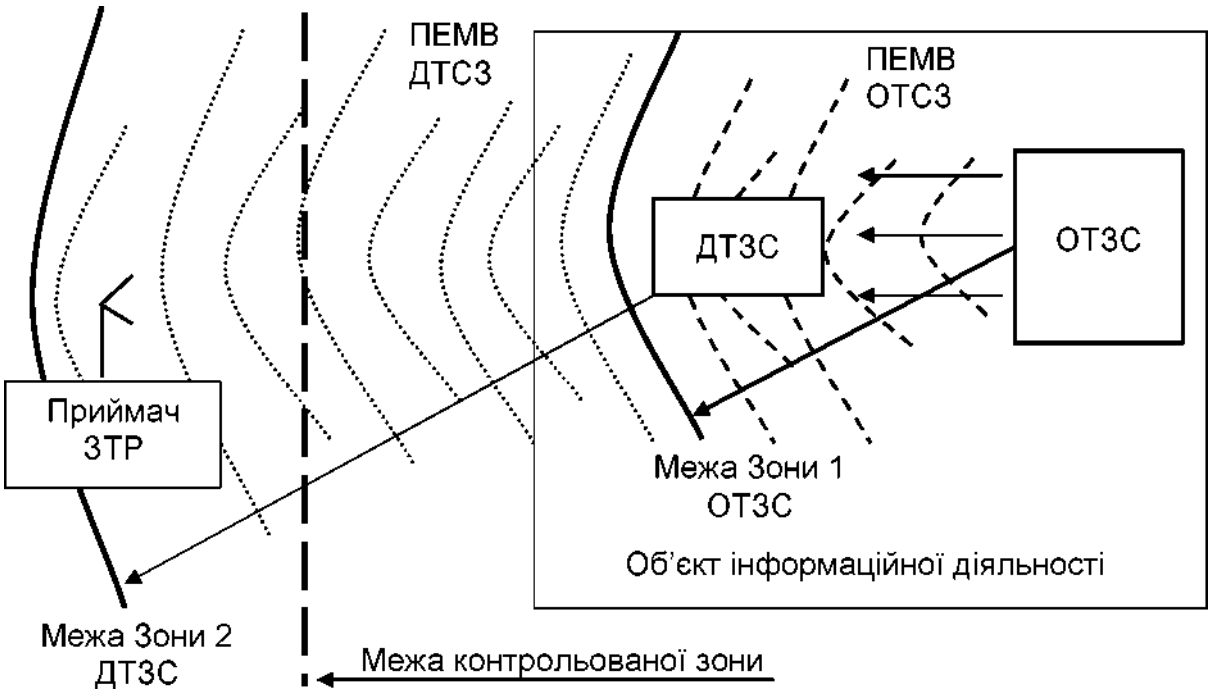


Рис. 1.2. Канал побічних електромагнітних випромінювань ДТЗС.

Канал "паразитної" модуляції сигналів ВЧ генераторів

Канал "паразитної" модуляції сигналів ВЧ генераторів, як різновид каналів ПЕМВ, утворюється шляхом модуляції небезпечним сигналом високочастотних сигналів ВЧ генераторів ОТЗС, випромінювання модульованих ВЧ коливань у вільний простір та перехоплення таких коливань радіоприймальними

пристроями засобів технічної розвідки за межами КЗ (рис. 1.3) [4,5,6].

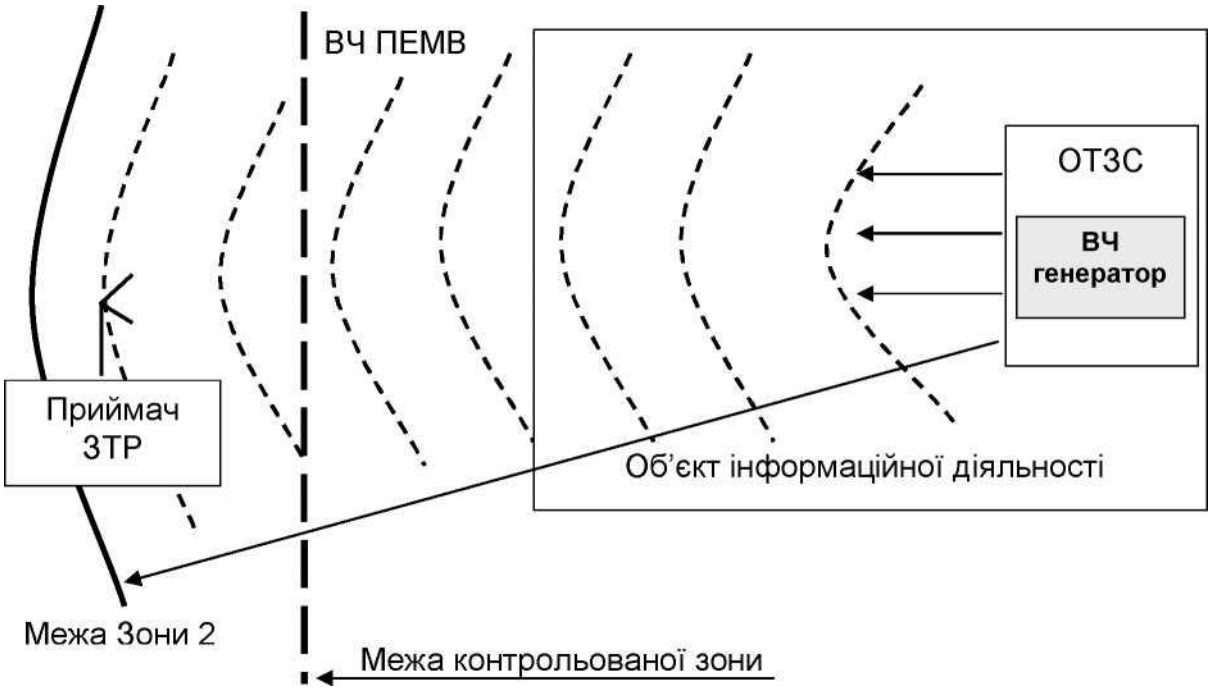


Рис. 1.3. Канал "паразитної" модуляції сигналів ВЧ генераторів.

Основні технічні засоби та системи в своєму складі мають генератори високих частот (ВЧ генератори). Практично всі засоби ЕОТ в своєму складі мають генератори тактових частот, гетеродини та інші ВЧ генератори. Високочастотний сигнал ВЧ генератора модулюється низькочастотними небезпечними сигналами, що циркулюють в ОТЗС, та випромінюється у вигляді електромагнітного поля у вільний простір. Оскільки згасання електромагнітного поля на високих частотах менше ніж на низьких, то поле розповсюджується дальше. А це, в свою чергу, дає можливість перехоплення інформації засобами технічної розвідки за межами Зони 2, розрахованої для сигналу без модуляції. Слід відмітити, що модуляція розширює спектр частот сигналу, підвищує його потужність і завадостійкість. Тому Зона 2 має розраховуватись з врахуванням модульованого випромінювання на частотах ВЧ генераторів ОТЗС [6,7,8].

Канал "паразитної" ВЧ генерації підсилювачів

Канал "паразитної" ВЧ генерації підсилювачів, як різновид каналів ПЕМВ,

утворюється шляхом самозбудження підсилювачів низької частоти (НЧ) ОТЗС на гармоніках, кратних небезпечному сигналу, поширення їх у вигляді поля електромагнітного випромінювання за межі КЗ та перехоплення цього поля радіоприймальними пристроями засобів технічної розвідки (рис. 1.4) [6,7,8].

Сучасні технічні засоби обробки інформації в своєму складі часто мають підсилювачі низької частоти (НЧ). Як правило, буд-який підсилювач складається безпосередньо з підсилювального (напівпровідникового) елементу та негативного зворотного зв’язку.

Нелінійність характеристик напівпровідникових елементів при підсиленні сигналів обумовлює наявність в суміші вихідного підсиленого сигналу кратних гармонік, тобто небезпечного сигналу на подвоєних, потроєних і так далі частотах. Якщо підсилювач з його негативним зворотнім зв’язком правильно розрахований, і підсилення здійснюється на лінійній ділянці характеристики підсилення, то сам сигнал підсилюється практично без спотворень і його кратні гармоніки мінімальні [6,7,8].

У результаті старіння чи інших причин параметри електронних елементів та характеристики негативного зворотного зв'язку можуть змінитись і призвести до порушення режиму роботи самого підсилювача в цілому. Негативний зворотній зв'язок може змінюватися в бік позитивного, коефіцієнт підсилення збільшується і, разом з цим, зростає нелінійність підсилення, підсилювальний елемент переходить в режим насичення. Зворотній зв’язок на деяких частотах стає позитивним, і підсилювач перетворюється в генератор. При цьому в режимі насичення кратні гармоніки сигналу можуть суттєво зростати, а їх поле електромагнітного випромінювання може досягти значного рівня. А це, в свою чергу, може дати можливість перехоплення інформації засобами технічної розвідки за межами Зони 2, розрахованої без врахування “паразитної” генерації [6,7,8].

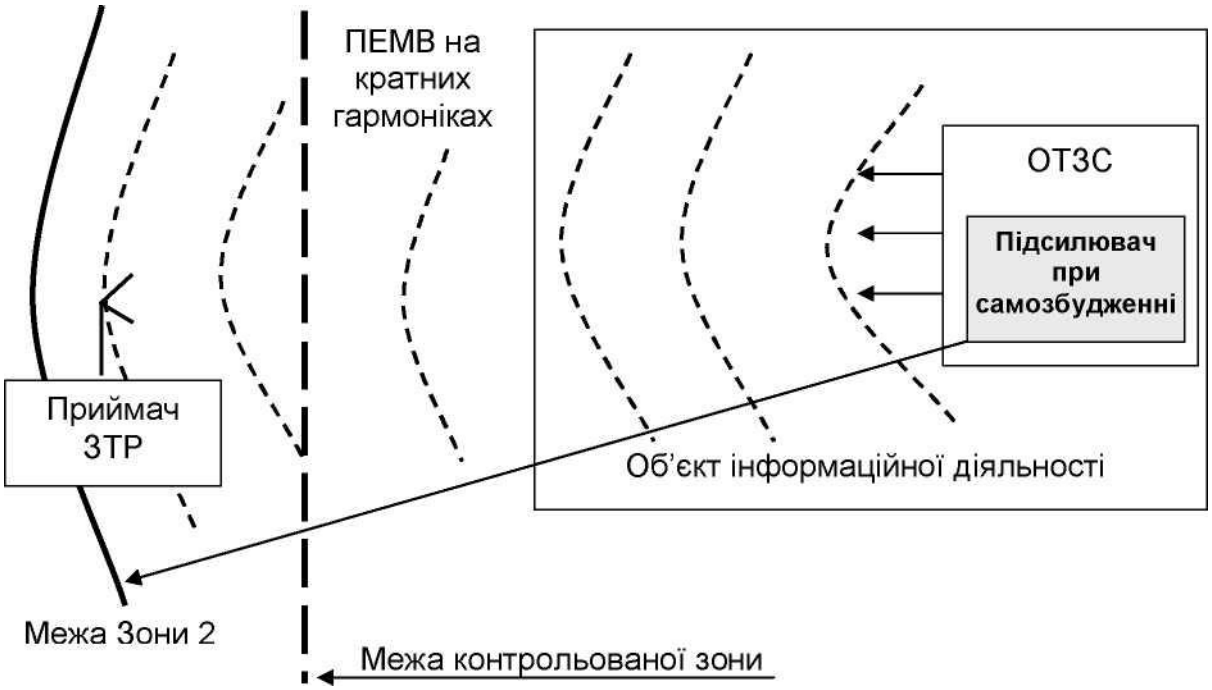


Рис. 1.4. Канал "паразитної" ВЧ генерації підсилювачів.

Ефект "паразитної" генерації характеризується нерегулярністю появи, тому одним із способів запобігання витоку інформації таким каналом є своєчасне виявлення (індикація) сигналів "паразитної" генерації та блокування роботи ОТЗС.

Запобігання витоку інформації каналом "паразитної" ВЧ генерації підсилювачів (унеможливлення створення такого ТКВІ) досягається шляхом [6,7,8]:

- створення КЗ не меншої за Зону 2, яка розраховується з врахуванням небезпечного сигналу на кратних гармоніках підсилювачів, організації режиму доступу до КЗ на ОІД;

- екранування ОТЗС, унеможливлення "паразитної" ВЧ генерації підсилювачів ОТЗС (локального екранування підсилювачів, оцінювання випромінювань та блокування роботи ОТЗС у разі виявлення "паразитної" ВЧ генерації, оцінювання, індикації та сигналізації відхилення параметрів підсилювачів та блокування роботи ОТЗС при виявленні позитивного зворотного зв'язку тощо);

- просторового електромагнітного зашумлення на об’єкті ЕОТ [8,9]

Канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС

Канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС, як різновид каналів побічних електромагнітних наведень (каналів ПЕМН), утворюється шляхом безпосереднього зняття з ліній електроживлення (заземлення) ОТЗС засобами технічної розвідки за межами КЗ небезпечних електричних сигналів, що наводяться в цих лініях побічними електромагнітними полями ОТЗС та/або просочуються (стікають) в ці лінії (або виникають в лінії електроживлення через нерівномірність споживання електроенергії) при функціонуванні ОТЗС (рис. 1.5) [6,7,8].

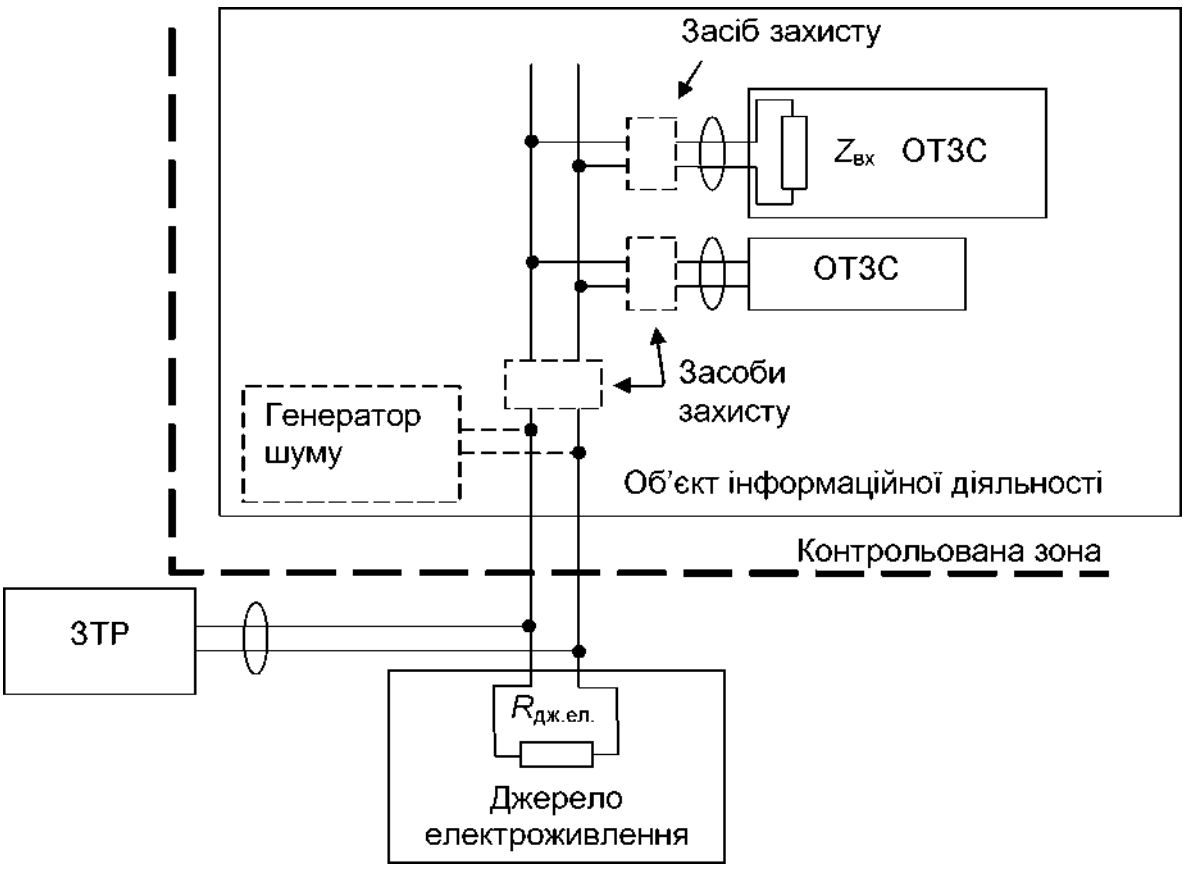


Рис. 1.5. Канал побічних електромагнітних наведень на лінії електроживлення ОТЗС.

Практично всі технічні засоби та системи обробки та передачі інформації живляться електричною енергією. Лінії електроживлення (заземлення) даних ОТЗС знаходяться в Зоні 1 ОТЗС, тому на них може наводитися за принципом електромагнітної індукції електричний струм, якій змінюється аналогічно небезпечному електромагнітному сигналу, і поширюється лініями електроживлення (заземлення).

Також під час обробки інформації вхідний опір ОТЗС може змінюватись за законом сигналів, що обробляються в них. Так, наприклад, підсилювачі (ключові схеми) працюють так, що вхідний (управляючий) сигнал управляє в схемі опором напівпровідника, який формує від джерела живлення підсилений сигнал.

В результаті коливання вхідного опору ОТЗС в ланцюгу електроживлення з’явиться змінна складова небезпечного сигналу по струму, яка на власному опорі джерела електроживлення створюватиме змінну складову напруги. Остання може стати доступною всім абонентам цієї мережі електроживлення, а якщо джерело електроживлення знаходиться за межами КЗ (лінії електроживлення виходять за межи КЗ), то противник може зняти інформацію шляхом безпосереднього підключення засобів технічної розвідки до лінії електроживлення [6,7,8]/

Крім побічних електромагнітних наведень на лінію заземлення ОТЗС має місце просочування небезпечних сигналів в ланцюги заземлення.

Під час роботи технічних засобів обробки інформації в наслідок ємнісних та інших зв'язків на корпусах цих засобів може накопичуватися небезпечний для життя потенціал. Цей потенціал може змінюватися за законом небезпечного сигналу, і небезпечний сигнал просочується в ланцюги заземлення.

Для забезпечення безпеки життєдіяльності персоналу всі технічні засоби заземлюються [8,9].

Сутність заземлення полягає у тому, що корпус технічного засобу

гальванічно зв’язується з ґрунтом "Землі" і потенціал, який накопився на корпусі, ланцюгами заземлення стікає в ґрунт, приймаючи його нульовий потенціал. Якщо система заземлення надійна і опір її досить малий, то стікання буде проходити швидше і корпус технічного засобу обробки інформації практично постійно буде нейтрально зарядженим [8,9].

Однак на практиці система заземлення не завжди може мати потрібний опір і противник може цим скористатися. Технічний канал витоку інформації ланцюгами заземлення ОТЗС наведений на рис. 1.6. [6,7,8]

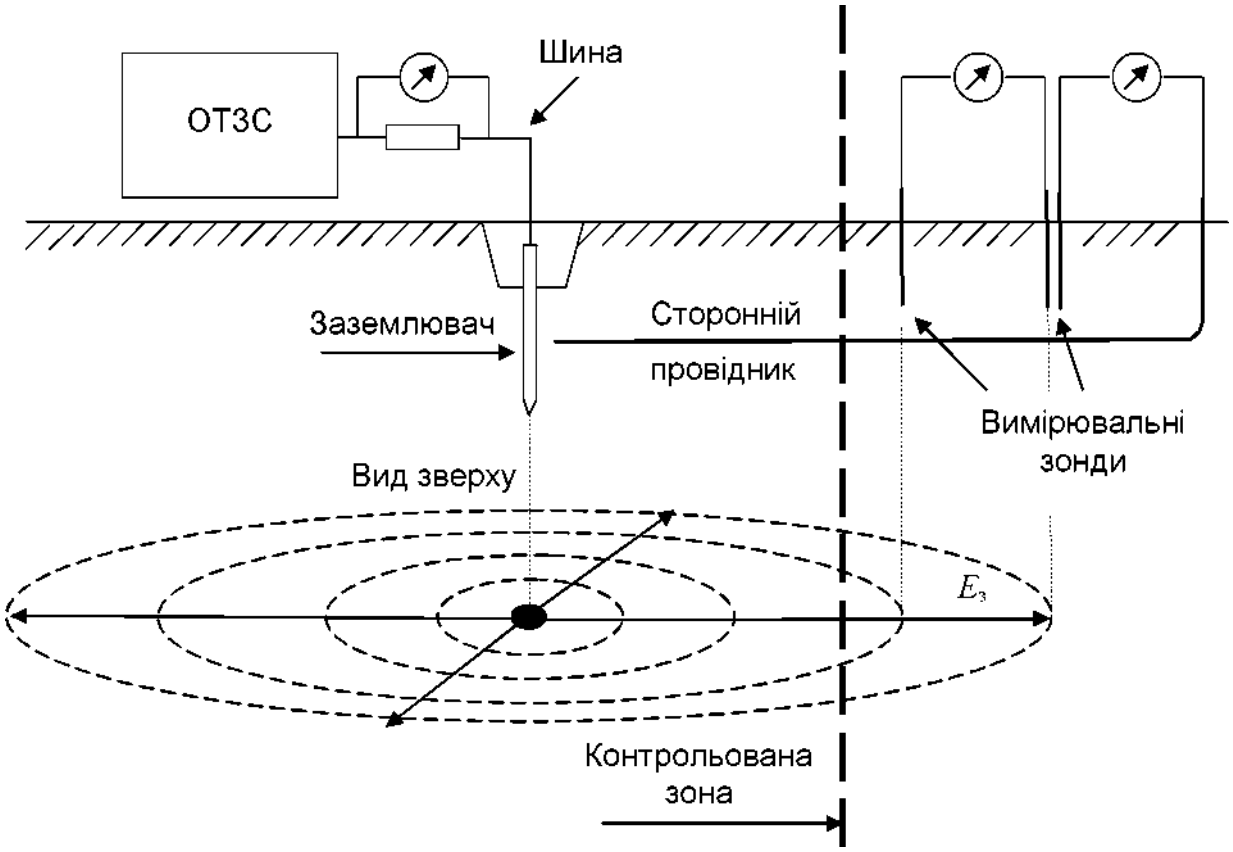


Рис. 1.6. Технічний канал витоку інформації ланцюгами заземлення ОТЗС.

Основні способи перехоплення небезпечних сигналів в ланцюгах заземлення [8,9]:

1. Перехоплення небезпечного сигналу з низькоомних ділянок ланцюга заземлення. Наприклад, слабко зварювальний шов, окислення контактів, мала

площа перетину шини заземлення, тощо.

2. Зняття різниці потенціалів ґрунту по віддаленню від заземлювача - джерела небезпечного сигналу, що можливе у разі великого опору заземлення.

3. Зняття потенціалу зі сторонніх провідників, що близько розташовані з заземлювачем та мають з ним ємнісний зв'язок.

4. Запобігання витоку інформації каналами побічних електромагнітних наведень на лінії електроживлення ОТЗС (унеможливлення створення таких ТКВІ) досягається шляхом Основні способи перехоплення небезпечних сигналів в ланцюгах заземлення:

5. Перехоплення небезпечного сигналу з низькоомних ділянок ланцюга заземлення. Наприклад, слабко зварювальний шов, окислення контактів, мала площа перетину шини заземлення, тощо.

6. Зняття різниці потенціалів ґрунту по віддаленню від заземлювача - джерела небезпечного сигналу, що можливе у разі великого опору заземлення.

7. Зняття потенціалу зі сторонніх провідників, що близько розташовані з заземлювачем та мають з ним ємнісний зв'язок [8,9,10]:

- створення КЗ та організації режиму доступу до КЗ на ОІД;
- електроживлення ОТЗС від автономних електричних джерел: електростанцій, акумуляторів, тощо, що розташовані у межах КЗ та не мають сторонніх споживачів;
- використання в лінії електроживлення ОТЗС технічних засобів захисту, що затримують сигнали низького рівня, мережевих фільтрів, систем двигун-генератор;
- використання лінійного зашумлення ліній електроживлення ОТЗС. [17]

Запобігання витоку інформації каналами побічних електромагнітних наведень на лінії заземлення ОТЗС, включаючи просочування небезпечних сигналів в ланцюги заземлення, (унеможливлення створення таких ТКВІ) досягається шляхом [8,9,10]:

- створення КЗ не меншої за Зону 2 та організації режиму доступу до КЗ

на ОІД;

- автономного від ДТЗС заземлення ОТЗС;
- забезпечення вимог щодо монтажу та опору заземлення ОТЗС;
- розташовування заземлювача з шинами заземлення в межах контрольованої зони на максимальній відстані від границі КЗ та сторонніх провідників;
- використання лінійного зашумлення ліній заземлення ОТЗС.

Канал побічних електромагнітних наведень на комунікації ДТЗС

Канали побічних електромагнітних наведень на комунікації ДТЗС, як різновид каналів ПЕМН, утворюється шляхом безпосереднього зняття з комунікацій ДТЗС (ліній електроживлення, заземлення та передачі даних ДТЗС, ліній зв'язку, ліній охоронних, протипожежних чи загальних систем безпеки, систем енергопостачання та інших систем) небезпечних електричних сигналів, що наводяться в цих комунікаціях побічними електромагнітними полями ОТЗС, полями комунікацій ОТЗС при їх спільному пробігу з комунікаціями ДТЗС (рис. 1.7) [8,9,10].

Якщо ДТЗС та їх лінії електроживлення, заземлення та передачі даних знаходяться в Зоні 1 ОТЗС, то на них може наводитися за принципом електромагнітної індукції електричний струм, якій змінюється аналогічно небезпечному сигналу, і поширюється лініями електроживлення, заземлення та передачі даних ДТЗС. Також, якщо ці лінії мають спільні пробіги з лініями, якими поширюються небезпечні сигнали, то можливі перенаведення небезпечних сигналів на лінії ДТЗС. Крім того, небезпечні сигнали через ланцюги живлення ДТЗС можуть просочуватися в лінії живлення ДТЗС. Якщо такі лінії електроживлення, заземлення або передачі даних ДТЗС виходять за межі КЗ, то противник може зняти інформацію шляхом безпосереднього підключення засобів технічної розвідки до цих ліній [8,9,10].

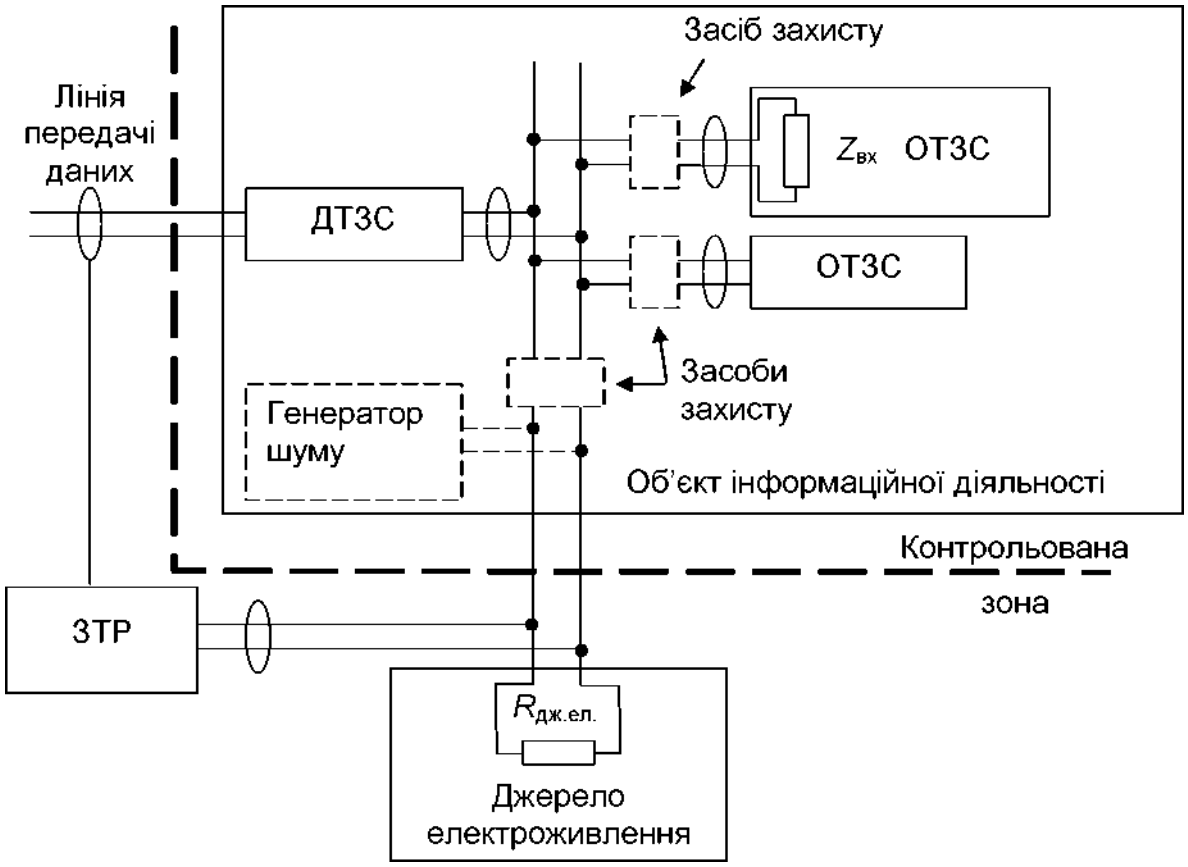


Рис. 1.7. Канали побічних електромагнітних наведень на комунікації ДТЗС.

Запобігання витоку інформації каналами побічних електромагнітних наведень на комунікації ДТЗС (унеможливлення створення таких ТКВІ) досягається шляхом [8,9,10]:

- створення КЗ та організації режиму доступу до КЗ на ОІД;
- розташування ДТЗС та їх комунікацій за межами Зони 1 ОТЗС;
- електроживлення ДТЗС від автономних електричних джерел: електростанцій, акумуляторів, тощо, що розташовані у межах КЗ;
- використання в лінії електроживлення ДТЗС технічних засобів захисту, що затримують сигнали низького рівня, мережевих фільтрів, систем двигун-генератор;
- використання лінійного зашумлення ліній електроживлення ДТЗС;
- забезпечення вимог щодо монтажу та опору заземлення ДТЗС;
- розташовування заземлювача з шинами заземлення в межах

контрольованої зони на максимальній відстані від границі КЗ та сторонніх провідників;

- використання лінійного зашумлення ліній заземлення ДТЗС.

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

Канал ВЧ нав'язування (для зняття інформації, що обробляється технічними засобами), як різновид параметричних каналів, утворюється шляхом введення ("нав'язування") спеціально створеного високочастотного сигналу (ВЧ-сигналу) в основні та/або допоміжні технічні засоби та системи їх комунікаціями з-за меж контрольованої зони, модуляції цього ВЧ-сигналу небезпечним сигналом на нелінійних елементах ОТЗС та/або ДТЗС та [9,11]:

- або відбиття цього ВЧ-сигналу від неузгоджених навантажень в ОТЗС та/або ДТЗС, поширення такого модульованого ВЧ-сигналу комунікаціями ОТЗС та/або ДТЗС за межі КЗ та його зняття засобами технічної розвідки при безпосередньому їх підключенні до комунікацій ОТЗС та/або ДТЗС за межами КЗ;

- або випромінювання такого модульованого ВЧ-сигналу у вільний простір та перехоплення такого випромінювання радіоприймальними засобами технічної розвідки за межами КЗ (рис. 1.8) [9,11].

Майже всі технічні засоби обробки інформації використовують напівпровідникові електронні елементи, провідність (опір) яких залежить від різниці потенціалів на їх полюсах. Якщо опромінити технічні засоби обробки інформації електромагнітним полем високої частоти (в мегагерцевому діапазоні), то в його ланцюгах, де циркулює небезпечний сигнал, з'являться наведені ВЧ струми, які, в свою чергу, впливатимуть на опори напівпровідників та інші параметри схем ТЗС [9,11].

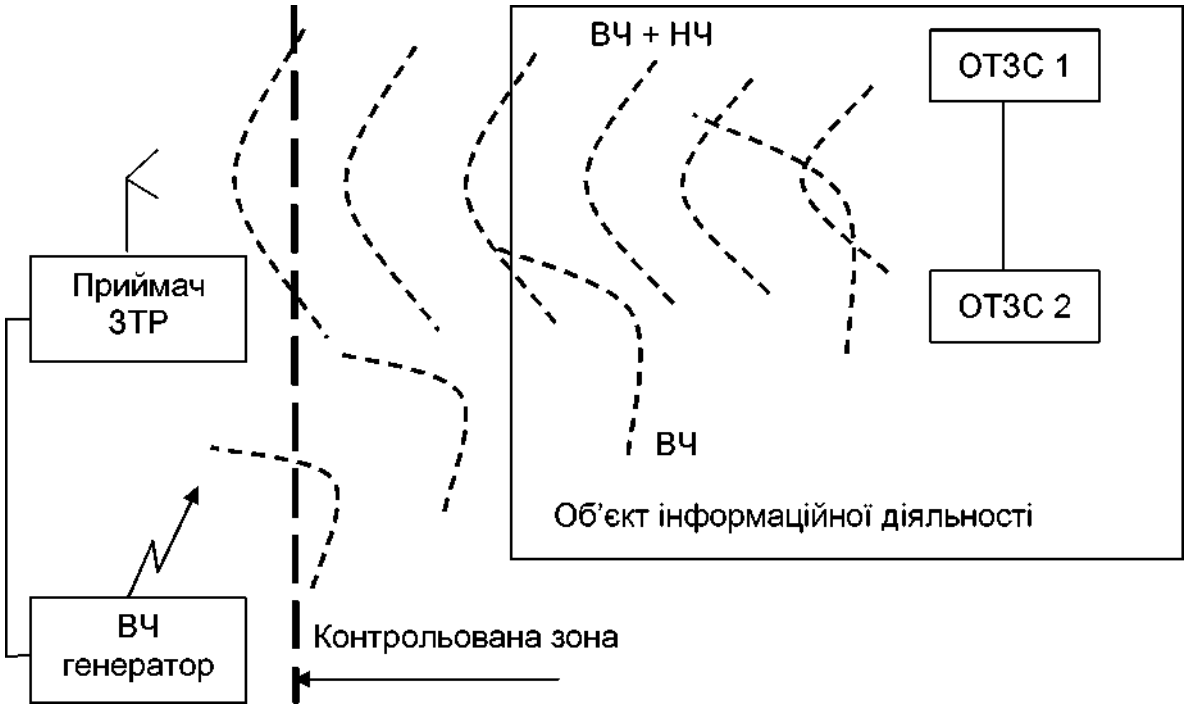


Рис. 3.7. Канал ВЧ нав'язування (для зняття інформації, що обробляється в ОТЗС).

В результаті в схемах здійсниться паразитна модуляція небезпечного сигналу з переносом його спектру ВЧ область. Перевипромінювання такого модульованого ВЧ сигналу може спричинити витік інформації [8,9,10].

Слід відмітити, що при цьому досить просто реалізувати перехоплення такого модульованого ВЧ сигналу, використавши когерентний прийомом, який забезпечує максимум завадостійкості.

Запобігання витоку інформації каналом ВЧ нав'язування (унеможливлення створення такого ТКВІ) досягається шляхомv:

- створення КЗ не меншої за Зону 2, яку розраховують з врахуванням можливого ВЧ нав'язування, та організації режиму доступу до КЗ на ОІД;
- екранування ОТЗС;
- просторового електромагнітного зашумлення на об'єкті ЕОТ;
- індикації, сигналізації поля ВЧ опромінення та блокування роботи ОТЗС.

Таким чином у пункті розглянуті основні різновиди технічних каналів

витоку інформації, які утворюються при її обробці в ОТЗС та основні заходи щодо запобігання витоку інформації цими каналами (унеможливлення створення таких ТКВІ).

1.3 Висновки по розділу

В розділі проведено аналіз основних технічних каналів витоку інформації на об’єкті інформаційної діяльності.

Подана класифікація технічних каналів витоку інформації на об’єкті інформаційної діяльності.

Розкрита сутність, властивості та шляхи утворення каналів витоку інформації, що обробляється основними технічними засобами та системами на об’єкті 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

Узагальнимо перелік можливих технічних каналів витоку інформації на об’єкті інформаційної діяльності:

1. канал побічних електромагнітних випромінювань (ПЕМВ) ОТЗС;
2. каналу побічних електромагнітних випромінювань ДТЗС;
3. канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС;
4. канал побічних електромагнітних наведень на комунікації ДТЗС;
5. канал ВЧ нав’язування;
6. оптичний канал витоку інформації;
7. встановлення закладних пристроїв.

Захист від вказаних технічних каналів витоку інформації має забезпечуватися наступними вимогами [11,12]**:**

- *канал побічних електромагнітних випромінювань ОТЗС шляхом* екранування ОТЗС або локального екранування електронних елементів.
- *канал побічних електромагнітних випромінювань ДТЗС* шляхом визначення R1 зони випромінювання та з подальшими рекомендаціями щодо розміщення ноутбука за межами цієї зони.
- *канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС* шляхом використання лінійного зашумлення ліній електроживлення ОТЗС.

- *канал побічних електромагнітних наведень на комунікації ДТЗС* вирішується електроживленням ДТЗС від автономних електричних джерел: електростанцій, акумуляторів, використання в лінії електроживлення ДТЗС технічних засобів захисту, що затримують сигнали низького рівня, мережевих фільтрів.

Другий варіант вирішення – це встановлення в блок живлення технічних засобів лінійного зашумлення [9,11]:

- *канал ВЧ нав'язування* шляхом екранування ОТЗС.

- *оптичний канал витоку інформації* має забезпечуватись самим співробітником шляхом оцінки оточуючого середовища.

- *встановлення закладних* пристроїв має вирішуватись організаційними методами недопущення сторонніх осіб в приміщення або, за потреби, шляхом перевірки приміщення пошуковою технікою.

В цілому способами запобігання витоку інформації, що обробляється в ОТЗС, та унеможливлення створення ТКВІ з врахуванням розглянутих ефектів є [9,11]:

- 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;

- живлення ОТЗС від автономних електричних джерел: електростанцій, акумуляторів;
- використання в ланцюгу живлення ОТЗС технічних засобів захисту, що затримують сигнали низького рівня, мережевих фільтрів;
- використання в ланцюгу живлення ОТЗС лінійного зашумлення;
- автономне заземлення ОТЗС;
- забезпечення вимог щодо монтажу на опору заземлення ОТЗС;
- розташовування заземлювача з шинами заземлення в межах контрольованої зони на максимальній відстані від границі КЗ та сторонніх провідників;
- зашумлення ліній заземлення ОТЗС та ДТЗС.

2.2. Вектори захисту інформації від витоку технічними каналами

Створення КСЗІ на об’єкті інформаційної діяльності, що спрямована на запобігання витоку інформації технічними каналами має базуватися на трьох векторах захисту інформації [9,11,12]:

1. Технічний захист інформації
2. Програмний захист інформації
3. Організаційно-технічний захист інформації

Етапи створення КСЗІ, що спрямована на запобігання витоку інформації технічними каналами

1 етап. Забезпечення технічного захисту АС при умові запобігання витоку інформації технічними каналами [12,13]. На першому етапі має бути впроваджений базовий технічний захист та проведення досліджень з метою виявлення ПЕВМН. Зокрема повинно бути реалізоване екранування технічних каналів, встановлення лінійного зашумлення в блок живлення електронних пристроїв та виявлення можливих випромінювань і наведень з метою подальшої розбудови експлуатаційної документації [12,13].

Проводиться атестація впровадженого комплексу технічного захисту інформації від витоку технічними каналами, що базується на основі пасивного засобу захисту та лінійного зашумлення за результатами якого видається документ: «Акт атестації автоматизованої системи» [12,13,14].

2 етап. Обстеження ІТС та підготовка вихідних даних для формування вимог до КСЗІ

На цьому етапі в загальному випадку виконується [12,13,14]:

- аналіз нормативно-правових актів, на підставі яких можуть встановлюватися обмеження доступу до певних видів інформації або заборона такого обмеження, визначається необхідність забезпечення захисту інформації згідно з іншими критеріями;
- визначаються переліки інформації, що підлягає автоматизованій обробці, і здійснюється її класифікація щодо рівня обмеження доступу до неї, вимог щодо забезпечення цілісності та вимог щодо забезпечення доступності відповідно до нормативно-правових актів [8,12,14]

Обстеження має враховувати такі аспекти як:

- технічна система;
- програмна частина;
- оброблювана інформація;
- користувачі;
- доступ до приміщення.

3 етап. Формування політики безпеки

На цьому етапі здійснюється [12,13,14]:

- аналіз ризиків (вивчення моделі загроз та моделі порушника, можливих наслідків від реалізації потенційних загроз);
- визначення вимог до заходів, методів і засобів захисту інформації;
- вибір основних рішень з протидії всім суттєвим загрозам, формування вимог, правил, обмежень, рекомендацій, які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів

і засобів захисту інформації, а також регламентують діяльність користувачів всіх категорій;

- документальне оформлення політики безпеки інформації [12,13,14]

Політика ІБ має враховувати всі особливості середовища обробки інформації та може бути цілком змінена співробітником захисту інформації організації-замовника. Нижче наведених розробником АС вимог політика бути не може.

Політика має бути оформлена у вигляді окремої системи, яка має включати [12,13,14]:

- інструкцію користувача;
- інструкцію системного адміністратора;
- інструкцію адміністратора безпеки.

В інструкції користувача мають бути вказані методи обробки інформації та правили, нехтування якими може призвести до реалізації загроз та витоку інформації [12,13,14].

4 етап. Розробка технічного завдання (далі — ТЗ) на створення КСЗІ

Технічне завдання на створення КСЗІ в ІТС є вихідним організаційно-технічним документом, в якому визначаються вимоги щодо захисту оброблюваної в ІТС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію в складі ІТС.

Технічне завдання на створення КСЗІ розробляється з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об’єднання в єдину систему всіх необхідних заходів і засобів захисту від різноманітних загроз безпеки інформації на всіх етапах життєвого циклу ІТС [14,15].

ТЗ на КСЗІ може розроблятися для вперше створюваних ІТС, а також під час модернізації вже існуючих ІТС.

ТЗ на КСЗІ може бути оформлений [16,17]:

- у вигляді окремого розділу загальної технічної задачі на створення ІТС;

- у вигляді окремого (часткового) ТЗ;
- у вигляді доповнення до загального ТЗ на створення ІТС.

Для інтегрованих ІТС (що складаються з декількох окремих інформаційних чи телекомунікаційних систем, які можуть функціонувати як самостійно, так і взаємодіяти між собою) рекомендується для кожної із складових частин ІТС створювати окремі КСЗІ і оформляти вимоги окремими ТЗ. Можлива розробка одного ТЗ на кілька однотипних складових частин ІТС, вказавши існуючі між ними відмінності або особливості [10,12,16]

5 етап. Розробка і реалізація проекту КСЗІ в ІТС.

Проект КСЗІ розробляється на підставі та у відповідності з Технічним завданням на створення ІТС і виконується на таких стадіях створення ІТС: ескізний проект, технічний проект, робоча документація.

При розробці проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають можливість забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і засобів захисту інформації [15,16].

Виконується розробка спільних рішень, необхідних для реалізації вимог ТЗ на КСЗІ, щодо організаційної структури КСЗІ, структури технічних і програмних засобів, алгоритмів функціонування та умов використання засобів захисту, реалізації визначених функціональним профілем захищеності послуг безпеки інформації.

6 етап. Введення КСЗІ від витоку технічними каналами передачі даних.

На цьому етапі повинна бути завершена розробка КСЗІ, підлаштування системи під середовище функціонування і затверджені документи, які входять до Плану захисту [15,16].

Проводиться навчання користувачів ІТС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів) основним положенням та процедурами документів Плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації.[13,15,16]/

Здійснюється інсталяція та перевірка програмних продуктів необхідних

для обробки інформації та засобів програмного захисту інформації залежно від способів обробки та передачі інформації.

Під час інсталяції повинні бути задіяні всі механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, механізми контролю за діями користувачів, а також контролю цілісності програмного забезпечення та бази даних захисту [16,17]

До засобів захисту вносяться відомості про користувачів АС, встановлюються їх повноваження щодо доступу до захищених ресурсів та середовища обробки/передачі інформації.

7 етап. Попередні випробування АС

Під час попередніх випробувань визначається працездатність системи шляхом опрацювання інформації в ролі користувача. Особою, що впроваджувала систему роблять спроби спричинити на неї вплив шляхом проведення спроб атак на комп'ютерну систему. Системі ставиться оцінка з урахуванням ЦКДС [17]. Виявлені недоліки та зауваження усуваються.

8 етап. Державна експертиза АС

Комплексна система захисту інформації, що є власністю держави, або інформації з обмеженим доступом, або іншої інформації, захист якої гарантується державою, повинна мати атестат відповідності вимогам захисту інформації, який видається ДССЗЗІ України за результатами державної експертизи.[17,18,19]

Державна експертиза КСЗІ проводиться з метою визначення її відповідності технічному завданню, вимогам нормативно-правових актів і нормативних документів щодо захисту інформації та з метою визначення можливості введення КСЗІ в експлуатацію в складі ІТС.

Державна експертиза КСЗІ є етапом приймальних випробувань ІТС та проводиться у відповідності до Положення про державну експертизу в сфері технічного захисту інформації.[17,18,19]

9 етап. Супровід КСЗІ

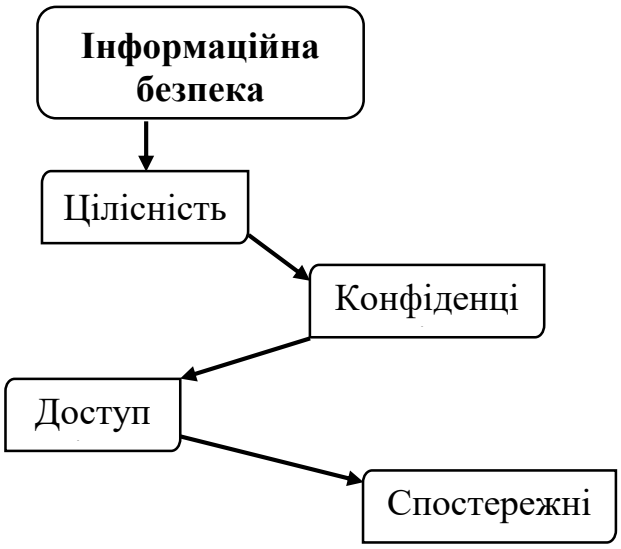
На цьому етапі виконуються роботи з організаційного забезпечення функціонування КСЗІ, її планової модернізації та з управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ [17,18,19]

Усі дії пов’язані з модернізацією та ремонтом АС не повинні заперечувати нормам прописаним в експлуатаційній документації та мають відповідати політиці захисту інформації.

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

КСЗІ побудується на основі портативної переносної електронно-обчислювальної машини, що дозволить гнучко та мобільно використовувати апаратно-програмну частину. Особливість системи полягає в тому, що швидкість розгортання в декілька разів скорочує час порівняно із звичайною процедурою побудови КСЗІ на основі персонального комп’ютера.

Захист інформації на основі КСЗІ має враховувати та гарантувати забезпечення цілісності, конфіденційності, доступності інформації та давати можливість спостережності за діями користувача та функціонуванням системи [18,19,20].



Цілісність інформації (information integrity) — властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом [19,20].

Конфіденційність інформації (information confidentiality) — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом [19,20].

Доступність (availability) — властивість ресурсу системи (КС, послуги, об'єкта КС, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний [19,20].

Спостереженість (accountability) — властивість КС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії [17,20].

Побудова КСЗІ має відбуватися за чіткою схемою-шаблоном відхилень від якої бути не повинно. Задля спрощення часу на розгортання КСЗІ уся документація має поділятися на дві частини [18,19,20]:

- експлуатаційна документація, яка виготовляється що спрямована на запобігання витоку інформації технічними каналами під час його виготовлення, та є засадничою документацією для розробки організаційної документації;

- організаційна документація, це документація, яка має надавати первинні вимоги для визначення потреби підвиду захищеного ноутбука та після введення ноутбука в експлуатацію включати політики інформаційної безпеки та розпорядження для користувачів щодо роботи за ноутбуком.

Базові політики щодо захисту інформації мають надаватися разом з ноутбуком на основі визначення його класу, можливостей та технічної захищеності інформації. При взятті АС на облік мають бути розроблені внутрішні політики в основу яких покладені базові.

Окрім забезпечення системи ЦКДС під час роботи за ноутбуком має забезпечуватися забезпечення захисту інформації від витоку технічними каналами. Основні технічні канали витоку інформації наведені в п. 1.1.

2.4. Висновки по розділу

В розділі подано результати дослідження напрямків удосконалення єдиної моделі комплексної системи захисту від витоку інформації технічними каналами.

Сформовані вимоги до захисту технічних каналів від несанкціонованого витоку інформації.

Визначені вектори захисту інформації від витоку технічними каналами.

Подано загальний опис єдиної моделі комплексної системи захисту від витоку технічними каналами.

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

Побудова КСЗІ відбувається згідно з НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Порядок створення КСЗІ в ІТС є єдиним незалежно від того, створюється КСЗІ в ІТС, яка проектується, чи в діючій ІТС, якщо виникла необхідність забезпечення захисту інформації або модернізації вже створеної КСЗІ[13,14]/

Процес створення комплексних систем захисту інформації полягає в реалізації комплексу взаємопогоджених заходів, спрямованих на розробку та впровадження інформаційних технологій, що забезпечує обробку інформації в ІТС відповідно до вимог, встановлених нормативно-правовими актами та НД у галузі захисту інформації. Порядок створення комплексних систем захисту інформації в ІТС розглядається цим НД як сукупність впорядкованих за часом, взаємопов'язаних, об'єднаних в окремі етапи робіт, виконання яких є необхідним і достатнім для створеної КСЗІ [18,19,20].

Послідовність виконання та типовий зміст робіт кожного з етапів створення КСЗІ повинні узгоджуватися з відповідними стадіями і етапами робіт зі створення ІТС, визначеними ГОСТ 34.601 [18,19,20].

Етапи робіт, які виконуються під час створення КСЗІ в конкретній ІТС, їх зміст та результати, терміни виконання визначаються ТЗ на створення КСЗІ. [13]/

Дозволяється виключати окремі етапи робіт або поєднувати декілька етапів, а також включати нові етапи робіт. За необхідністю дозволяється змінювати послідовність виконання окремих етапів - виконувати одночасно

декілька етапів робіт, окремі етапи виконувати до завершення попередніх і т.п., якщо це не призводить до зниження якості робіт і не суперечить цілям їх виконання [18,19,20].

Якщо у галузі впроваджені в установленому порядку і діють НД ТЗІ відомчого рівня або існують відповідні нормативні документи, чинність яких поширюється на організацію-власника ІТС або саму ІТС, то вони мають вищу силу і в першу чергу необхідно керуватися ними.

Якщо певний вид робіт не нормовано національною нормативною базою з технічного захисту інформації будь-якого з наведених рівнів, то допускається використання рекомендацій міжнародних стандартів в частині, що не суперечить нормативно – правовим актам та нормативним документам України. [13].

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

До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від [18,19,20]:

- витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;

- несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм, використання комп’ютерних вірусів та ін;

- спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту [13,14]

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС.

У випадках, визначених законодавством, роботи з проектування, розроблення, виготовлення, випробування, експлуатації ІТС мають виконуватись у комплексі із заходами, щодо забезпечення режиму секретності, протидії технічним розвідкам, а також з організаційними заходами щодо охорони інформації з обмеженим доступом, яка не є державною таємницею. [13]

Відповдно до п. 5.8 НД ТЗІ 3.7-003-2005, створення комплексів технічного захисту інформації від витоку технічними каналами здійснюється, якщо в ІТС обробляється інформація, що становить державну таємницю, або коли необхідність цього визначено власником інформації. В цьому пункті особливу увагу потрібно звернути саме власникам інформації. Можливо сам комплекс технічного захисту інформації і не знадобиться, але приділити увагу технічному захисту потрібно обов’язково.

Створення КЗЗ здійснюється в усіх ІТС, де обробляється інформація, що є власністю держави, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІТС, де така необхідність визначена власником інформації. Рішення щодо необхідності вжиття заходів захисту від спеціальних впливів на інформацію приймається власником інформації в кожному випадку окремо [18,19,20]/

Для організації робіт зі створення КСЗІ в ІТС створюється служба захисту інформації, порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000.

СЗІ створюється після прийняття рішення про необхідність створення КСЗІ. Як виняток СЗІ може створюватися на більш пізніх етапах робіт, але не пізніше етапу підготовки КСЗІ до введення в дію [13,16,19]

Служба захисту інформації є невідємною частиною будь якої системи, яка потребує захисту. Залежно від розмірів підприємства та кількості співробітників потрібно орієнтуватися на саму структуру служби захисту інформації.

Для маленького підприємства може бути достатньо призначити 1-2 відповідальних за захист інформації співробітників та покласти на них обов'язки служби захисту інформації, а для великого має бути створено як мінімум відділ з інформаційної безпеки.

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

1 етап. Обстеження ІТС та підготовка вихідних даних для формування вимог до КСЗІ. На цьому етапі в загальному випадку виконується [18,19,20]:

− аналіз нормативно-правових актів, на підставі яких можуть встановлюватися обмеження доступу до певних видів інформації або заборона такого обмеження, визначається необхідність забезпечення захисту інформації згідно з іншими критеріями;

− визначаються переліки інформації, що під-лягає автоматизованій обробці, і здійснюється її класифікація щодо рівня обмеження доступу до неї, вимог щодо забезпечення цілісності та вимог щодо забезпечення доступності відповідно до нормативно-правових актів.

При обстеженні ІТС розглядається як організаційно – технічна система, яка поєднує обчислювальну систему, фізичне середовище, середо-вище користувачів, оброблювану інформацію і технологію її обробки (далі – середовища функціонування ІТС) [18,19,20].

Метою обстеження є опис кожного середо-вища функціонування ІТС та виявлення в них елементів, які безпосередньо або опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних

середовищ, документування результатів обстеження для використання на наступних етапах робіт [18,19,20].

2 етап. Формування політики безпеки. На цьому етапі здійснюється:

− аналіз ризиків (вивчення моделі загроз та моделі порушника, можливих наслідків від реалі-зації потенційних загроз);

− визначення вимог до заходів, методів і засобів захисту інформації;

− вибір основних рішень з протидії всім суттєвим загрозам, формування вимог, правил, обмежень, рекомендацій, які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, а також регламентують діяльність користувачів всіх категорій;

− документальне оформлення політики безпеки інформації.

Політика безпеки повинна враховувати особливості окремих компонентів КСЗІ та може розроблятися для ІТС в цілому, для окремих складових компонента, для окремої функціональної задачі, для окремої технології обробки інформації. Політика безпеки оформляється у вигляді окремого документа Плану захисту [18,19,20]

3 етап. Розробка технічного завдання (далі – ТЗ) на створення КСЗІ. Технічне завдання на створення КСЗІ в ІТС є вихідним організаційно-технічним документом, в якому визначаються вимоги щодо захисту оброблюваної в ІТС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробу-вань КСЗІ та введення її в експлуатацію в складі ІТС [18,19,20].

Технічне завдання на створення КСЗІ розробляється з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об’єднання в єдину систему всіх необхідних заходів і засобів за-хисту від різноманітних загроз безпеки інформації на всіх етапах життєвого циклу ІТС. ТЗ на КСЗІ може розроблятися для вперше створюваних ІТС, а також під час модернізації вже існуючих ІТС.

ТЗ на КСЗІ може бути оформлений [18,19,20]:

− у вигляді окремого розділу загальної технічної задачі на створення ІТС;

− у вигляді окремого (часткового) ТЗ;

− у вигляді доповнення до загального ТЗ на створення ІТС.

Для інтегрованих ІТС (що складаються з декількох окремих інформаційних чи телекомунікаційних систем, які можуть функціонувати як самостійно, так і взаємодіяти між собою) рекомендується для кожної із складових частин ІТС створювати окремі КСЗІ і оформляти вимоги окремими ТЗ. Можлива розробка одного ТЗ на кіль-ка однотипних складових частин ІТС, вказавши існуючі між ними відмінності або особливості.[11]

4 етап. Розробка і реалізація проекту КСЗІ в ІТС.

Проект КСЗІ розробляється на підставі та у відповідності з Технічним завданням на створення ІТС і виконується на таких стадіях створення ІТС: ескізний проект, технічний проект, робоча документація.

При розробці проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають можливість забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і засобів захисту інформації.

Виконується розробка спільних рішень, необхідних для реалізації вимог ТЗ на КСЗІ, щодо організаційної структури КСЗІ, структури технічних і програмних засобів, алгоритмів функціонування та умов використання засобів захисту, реалізації визначених функціональним профілем захищеності послуг безпеки інформації.

5 етап. Введення КСЗІ в дію.

На цьому етапі повинна бути завершена розробка КСЗІ і затверджені документи, які входять до Плану захисту.

Проводиться навчання користувачів ІТС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів) основним положенням та процедурами документів Плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації.

Проводиться атестація впровадженого комплексу технічного захисту інформації від витоку технічними каналами, за результатами якого видається документ: «Акт атестації комплексу технічного захисту інформації».

Здійснюється згідно з документацією робо-чого проекту інсталяція, ініціалізація та перевірка працездатності комплексу засобів захисту інформації від НСД. Під час інсталяції повинні бути задіяні всі механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, механізми контролю за діями користувачів, а також контролю цілісності програмного забезпечення та бази даних захисту.

До бази даних захисту вносяться відомості про користувачів ІТС, встановлюються їх повноваження щодо доступу до захищених об’єктах ІТС, їх створення, модифікації, архівування, знищення, експорту / імпорту із системи.

6 етап. Попередні випробування.

Метою попередніх випробувань є перевірка працездатності КСЗІ, її відповідності технічним завданням і визначення можливості прийняття КСЗІ в дослідну експлуатацію. Попередні випробування проводяться у відповідності з програмою і методиками випробувань. Їх організовує замовник ІТС, а проводить – розробник КСЗІ спільно із замовником.

7 етап. Дослідна експлуатація. Під час дослідної експлуатації КСЗІ:

− відпрацьовуються технології захисту оброблюваної інформації, оббіг машинних носіїв інформації, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;

− співробітники системи захисту інформації та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань забезпечення режиму доступу;

− здійснюється доопрацювання програмного забезпечення, додаткове налаштування та конфігурування КЗЗ від НСД;

− здійснюється коригування робочої та експлуатаційної документації.

Дослідна експлуатація ІТС повинна здійснюватися без використання інформації, що становить державну таємницю. У разі використання в складі КСЗІ комплексу засобів захисту інформації від НСД, який не має експертного висновку про відповідність вимогам НД ТЗІ, необхідно здійснити комплекс робіт з підготовки до проведення оцінки відповідності цього комплексу засобів захисту інформації вимогам НД ТЗІ під час проведення державної експертизи КСЗІ.

8 етап. Державна експертиза КСЗІ. Комплексна система захисту інформації, що є власністю держави, або інформації з обмеженим доступом, або іншої інформації, захист якої гарантується державою, повинна мати атестат відповідності вимогам захисту інформації, який видається ДССЗЗІ України за результатами державної експертизи. Державна експертиза КСЗІ проводиться з метою визначення її відповідності технічному завданню, вимогам нормативно-правових актів і нормативних документів щодо захисту інформації та з метою визначення можливості введення КСЗІ в експлуатацію в складі ІТС. Державна експертиза КСЗІ є етапом приймальних випробувань ІТС та проводиться у відповідності до Положення про державну експертизу в сфері технічного захисту інформації. Якщо в ІТС обробляється інформація, яка є власністю держави, або інформація, захист якої гарантується державою, то дозвіл на експлуатацію ІТС дається наказом керівника організації тільки за наявності атестату відповідності КСЗІ.[12]

10 етап. Супровід КСЗІ. На цьому етапі виконуються роботи з організаційного забезпечення функціонування КСЗІ, її планової модернізації та з управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ. [10,17].

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

На цьому етапі розробник КСЗІ проводить детальне вивчення об’єкта, на якому створюється КСЗІ, керуючись моделлю загроз, моделлю потенційного порушника та результатами аналізу можливих ризиків. За результатами дослідження має розроблятися політика інформаційної безпеки як для ІТС так і для ОІД.

Далі на цьому етапі здійснюється:

- вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій і т.п., які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій;

- документальне оформлення політики безпеки інформації.[13]

Політика безпеки має розроблятись системи захисту в цілому під час виготовлення та удосконалюватись службою захисту інформації під час введення її в експлуатацію на підприємстві.

Створення комплексу ТЗІ передбачає три етапи:

- розроблення комплексу ТЗІ (І етап);
- упровадження комплексу ТЗІ (ІІ етап);
- атестацію комплексу ТЗІ (ІІІ етап).

Зміст та порядок робіт на етапах створення комплексу ТЗІ визначається нормативними документами системи ТЗІ.[10]

Вимоги до захищеності інформації від витоку технічними каналами та норми захищеності інформації визначаються нормативно-правовими актами та нормативними документами системи ТЗІ.

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

Засоби захисту інформації від витоку через технічні канали мають різноманітні характеристики та функціонал:

Блокіратор бездротового зв’язку «СБ ТЗІ 7-1»: Ефективність поданого засобу залежить від різних чинників, включаючи відстань до джерела випромінювання, відстань до приймача, рівень випромінювання та коефіцієнт спрямованості антен [17,19]

Колонка акустична захищена «МАРС-АКЗ. Призначена для захисту приміщень від витоку інформації через акустичні канали. Вона включає акустичний випромінювач і комутатор, який відключає акустичний випромінювач від лінії, коли відсутній сигнал від генератора шуму, що унеможливлює використання колонки як мікрофону. Рівень чутливості (83±2) дБ; Номінальний опір 10 Ом; Номінальна електрична потужність, не більше 5 ВА [17,19].

Протизавадний Фільтр ФЗП-110-2 Має специфікації щодо робочої напруги, струму споживання, струму витоку та діапазону частот. Номінальна робоча напруга - 220 В (50 Гц), номінальний струм споживання - 10 А, струм витоку не більше 15 мА, діапазон частот - 10 кГц ... 18000 МГ [19].

Вібровипромінювачі МАРКИ ВІ Ці вібровипромінювачі працюють у діапазоні від 180 Гц до 5600 Гц з опором обмотки 50 Ом.

Генератор шуму марки „Базальт-5”. Призначений для захисту об'єктів від витоку інформації через побічні електромагнітні випромінювання. Цей генератор створює потужне просторове електромагнітне поле шуму у широкому діапазоні частот від 0,1 до 1000 МГц.[18,19].

Засоби захисту інформації стають все більш важливими в умовах постійного розвитку технологій. Одним із надійних рішень для промисловості є **мережевий завадозахисний фільтр типу ФЗП103-2.** Ці фільтри, відповідно до

стандарту ТУ У 31.1-31731859-001-2003, гарантують захист інформації від витоку через кола електроживлення основних та допоміжних засобів обробки інформації.

ФЗП103-2 працюють у широкому діапазоні частот, від звукових до надвисоких, запобігаючи впливу високовольтних імпульсів. Ці фільтри є безпечними в експлуатації, навіть при обриві або відсутності заземлення, що робить їх надійними засобами захисту. Вони відповідають усім вимогам вітчизняного стандарту ДСТУ 3639-97 "ФІЛЬТРИ ПРОТИЗАВАДНІ".

Особливістю цих фільтрів є компактні габарити та невелика вага, що дозволяє їх ефективно використовувати в різних системах. Наприклад, такий фільтр займає об’єм лише 0,42 дм³ та важить не більше 0,85 кг, що робить їх зручними для використання в різних умовах та ситуаціях**.** [30-33].

Засіб активного захисту автоматизованих систем "DELTA-7" є важливим елементом захисту інформації на об'єктах електронно-обчислювальної техніки, спеціального зв'язку та інших сферах інформаційної діяльності. Цей засіб призначений для гарантованого перекриття інформаційних сигналів побічних електромагнітних випромінювань і наведень, що виникають внаслідок дії різноманітних технічних пристроїв, включаючи комп'ютери, копіювальну техніку, мережеве обладнання та засоби зв'язку.

Спеціальний інформаційно-телекомунікаційний термінал (СІТ) - це електронно-обчислювальний пристрій, розроблений для захисту від витоку інформації через побічні електромагнітні випромінювання та наведення. Цей пристрій використовується для обробки конфіденційних даних, що становлять державну таємницю, і може застосовуватися на об'єктах різних категорій інформаційної діяльності.

Обидва засоби, "DELTA-7" та СІТ, є критичними для забезпечення безпеки та конфіденційності інформації в сфері технологій, де захист від побічних електромагнітних випромінювань є ключовим аспектом забезпечення інформаційної безпеки..

Генератор шумових сигналів МАРС-ТЗО-4-2 - це ефективний пристрій, спроектований для створення шумових сигналів у широкому діапазоні частот від 180 до 5600 Гц. Він забезпечує стале ефективне значення вихідної напруги на опорі навантаження, що становить не менше 3,5 В, при цьому передає віброприскорення у всій смузі шумового сигналу не менше 50 дБ, завдяки використанню вібровипромінювача ВИ4.

Акустичні колонки "МАРС-АК", що входять до складу системи, створюють звуковий тиск у великому діапазоні робочих частот, що не менше 80 дБ на відстані 1 метра. Засіб також має широкий діапазон регулювання рівнів шумових сигналів на виходах, що становить не менше 20 дБ, та витрачає невелику потужність, не перевищуючи 40 ВА.

Цей генератор є лише одним із широкого спектру засобів, які можна використовувати в різних областях, де створення шумових сигналів або регулювання їх параметрів є важливим аспектом роботи обладнання чи систем. [33]. А також інші засоби.

3.6. Висновки по розділу

В розділі подана комплексна системи захисту об’єкту інформаційної діяльності від витоку інформації технічними каналами.

Визначено нормативно-правове забезпечення розробки комплексної системи захисту інформації на об’єкті інформаційної діяльності. Подано заходи та засоби комплексної системи технічного захисту інформації на об’єкті інформаційної діяльності. Окреслено етапи створення комплексної системи технічного захисту інформації на об’єкті інформаційної діяльності.

Розроблено та оформлено політику безпеки інформації від витоку технічними каналами витоку на об’єкті інформаційної діяльності

Запропоновано технічні засоби запобігання витоку інформації та об’єкті інформаційної діяльності.

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.

– Розглянуто питання охорони навколишнього природнього середовища.

1. У першому розділі кваліфікаційної роботи проведено аналіз основних технічних каналів витоку інформації на об’єкті інформаційної діяльності. Подана класифікація технічних каналів витоку інформації на об’єкті інформаційної діяльності. Розкрита сутність, властивості та шляхи утворення каналів витоку інформації, що обробляється основними технічними засобами та системами на об’єкті інформаційної діяльності.

2. У другому розділі кваліфікаційної роботи подано результати дослідження напрямків удосконалення єдиної моделі комплексної системи захисту від витоку інформації технічними каналами. Сформовані вимоги до захисту технічних каналів від несанкціонованого витоку інформації. Визначені вектори захисту інформації від витоку технічними каналами. Подано загальний опис єдиної моделі комплексної системи захисту від витоку технічними каналами.

3. У третьому розділі кваліфікаційної роботи подана комплексна системи захисту об’єкту інформаційної діяльності від витоку інформації технічними каналами. Визначено нормативно-правове забезпечення розробки комплексної

системи захисту інформації на об’єкті інформаційної діяльності. Подано заходи та засоби комплексної системи технічного захисту інформації на об’єкті інформаційної діяльності. Окреслено етапи створення комплексної системи технічного захисту інформації на об’єкті інформаційної діяльності. Розроблено та оформлено політику безпеки інформації від витоку технічними каналами витоку на об’єкті інформаційної діяльності

ПЕРЕЛІК ПОСИЛАНЬ

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 інтер, 1997. — 704 с.

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

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

Ярослав ІВАНЦОВ

Кваліфікаційна робота
здобувача освітнього ступеня «МАГІСТР»

Тема:

СИСТЕМИ ЗАХИСТУ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ВІД ВИТОКУ КОНФІДЕНЦІЙНИХ ДАНИХ ТЕХНІЧНИМИ КАНАЛАМИ ПЕРЕДАЧІ ІНФОРМАЦІЇ

125 – Кібербезпека та захист інформації

Керівник: д.т.н., професор Олександр ТУРОВСЬКИЙ

Київ - 2025

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

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: Комплексна системи захисту об'єкту інформаційної діяльності з підвищеними вимогами до захисту від витоку інформації технічними каналами

4. ВИСНОВКИ: Узагальнено одержані результати

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)

3. За середовищем поширення небезпечного сигналу

1. За видом інформаційної діяльності на ОКІ

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

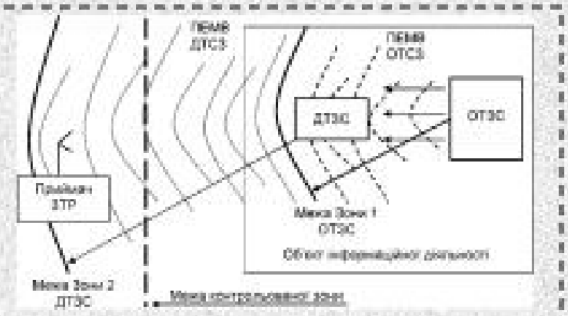
ПЕРШИЙ РЕЗУЛЬТАТ

ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

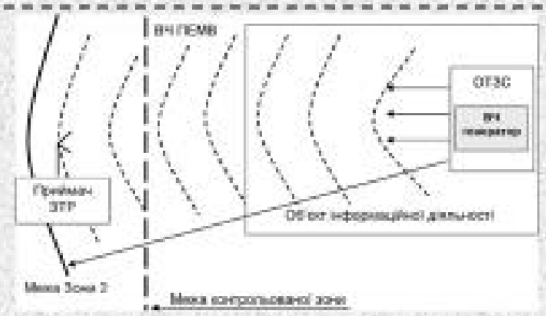
СТРУКТУРА ТЕХНІЧНОГО КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ

ПЕРШИЙ РЕЗУЛЬТАТ

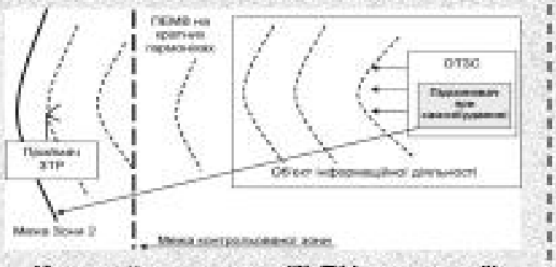
ХАРАКТЕРИСТИКА ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ



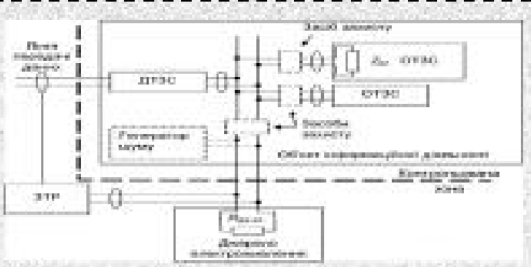
Канал побічних електромагнітних випромінювань



Канал "паразитної" модуляції сигналів ВЧ генераторів



Канал "паразитної" ВЧ генерації підсилювачів



Канали побічних електромагнітних наведень на комунікаціях

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*

ВЕКТОРИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ:

Технічний захист інформації.

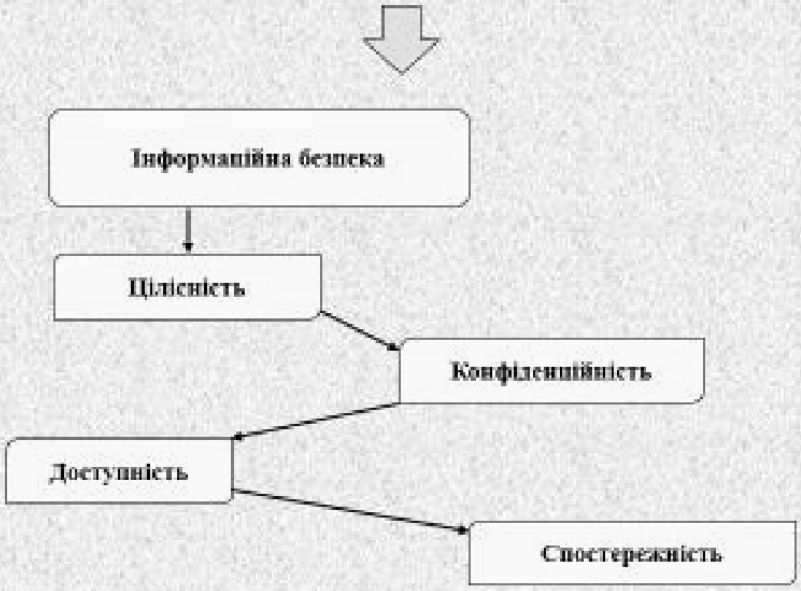
Програмний захист інформації.

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;**

ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ КСЗІ: ВИМОГИ



ТРЕТІЙ РЕЗУЛЬТАТ

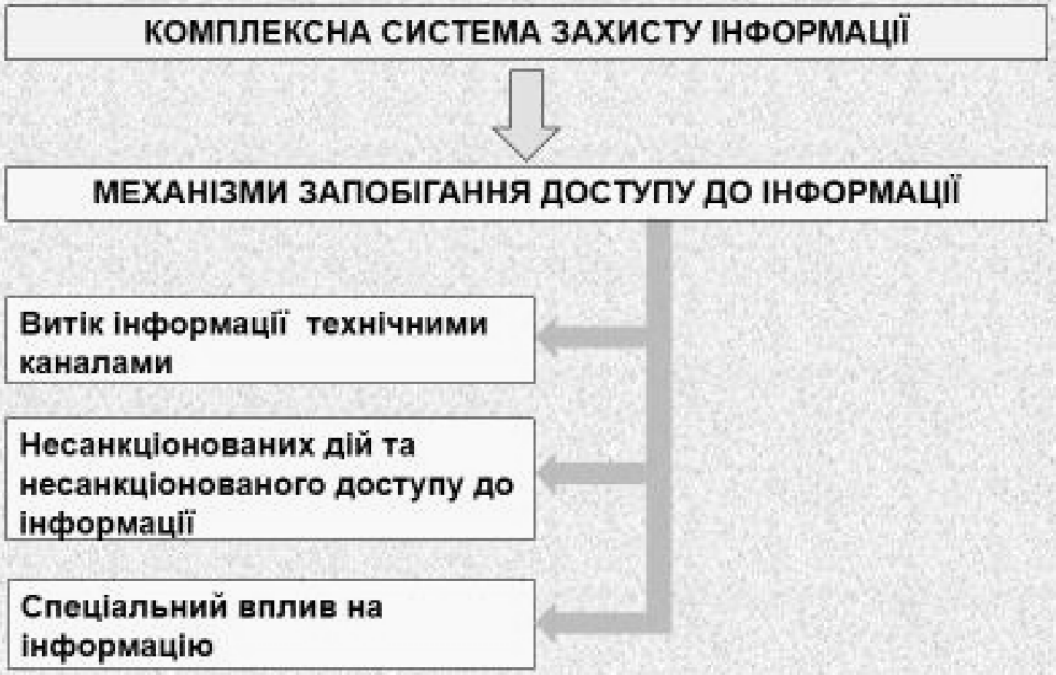
НД ТЗІ 3.7-003-05

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

ТРЕТІЙ РЕЗУЛЬТАТ

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



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.**

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.

Апробація:

О.В. Іванцов, О.В. Таров, Н.О. Левчук, **Аналіз загроз несанкціонованого доступу до технічних каналів передачі інформації з обмеженим доступом.** *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.90 - 91.

ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ПІДВИЩЕННЯ ЗАХИСТУ

- провести інвентаризацію ОТЗС, ДТЗС, ліній електроживлення, заземлення та комунікацій, які можуть утворювати технічні канали витоку інформації;
- визначити межі контрольованої зони, Зони 1 та Зони 2 для основних технічних засобів і систем обробки інформації;
- застосувати екранування, фільтрацію, заземлення, просторове електромагнітне зашумлення та контроль побічних електромагнітних випромінювань;
- регламентувати доступ до приміщень, носіїв інформації, технічних засобів і документації з питань технічного захисту інформації;
- організувати періодичний контроль ефективності КСЗІ та оновлення політики безпеки відповідно до змін у складі ОІД.

ДЯКУЮ ЗА УВАГУ !