КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет автоматизації і інформаційних технологій

Кафедра кібербезпеки та комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

на тему:

«ЗАХИСТ ІНФРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ КЛАСУ 1 ВІД ВИТОКУ ЕЛЕКТРИЧНИМ КАНАЛОМ»

Гелетухи Артема Васильовича

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет автоматизації і інформаційних технологій

Кафедра кібербезпеки та комп'ютерної інженерії

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____
«_____»_____20____року

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР
ЗАХИСТ ІНФРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ КЛАСУ 1 ВІД ВИТОКУ ЕЛЕКТРИЧНИМ КАНАЛОМ

Я, як здобувач вищої освіти КНУБА, розумію і підтримую політику закладу з академічної доброчесності. Я не надавав і не одержував недозволену допомогу під час підготовки цієї роботи. Використання результатів і ідей, текстів інших авторів мають посилання на відповідне джерело.

Здобувач: Гелетуха Артем Васильович

125 «Кібербезпека»
(спеціальність)
Безпека інформаційних і комунікаційних систем
Група: БІКСс-23

Керівник: Котенко А. М.

Кандидат технічних наук, доцент
(вчене звання, науковий ступінь)
Рецензент: Терентьєв О.О.

Ідентичність підтверджую

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: автоматизації і інформаційних технологій

Випускова кафедра: кібербезпеки та комп'ютерної інженерії

Ступінь вищої освіти: бакалавр

Спеціальність: 125 «Кібербезпека»

Освітня програма: Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ

Завідувач кафедри
Делембовський М.М
«____»_____20__ року

З А В Д А Н Н Я
ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР
Гелетухи Артема Васильовича

1. Тема роботи: **«Захист інформації в автоматизованій системі класу 1 від витоку електричним каналом»** затверджена наказом ректора КНУБА №576/52-15/13.2/26 від 14 травня 2026 року.

2. Керівник роботи: Котенко Андрій Миколайович, кандидат технічних наук, доцент.

3. Термін подання здобувачем роботи до захисту _____

4. Зміст пояснювальної записки за розділами:

Р. 1. Аналіз нормативних вимог, основи технічного захисту та електричного каналу.

Р. 2. Аналіз серидовища функціонування ас ксласу 1 та оцінювання захищеності.

Р. 3. Система захисту інформації в ас класу 1 від витоку електричним каналом.

5. Графічний матеріал за розділами:

Р. 1. Актуальність, мета, завдання, об’єкт і предмет дослідження, нормативно-правова база технічного захисту інформації, класифікація інформації з обмеженим доступом, класифікація автоматизованих систем за НД ТЗІ 2.5-005-99, загрози інформаційній безпеці, технічні канали витоку інформації, електричний канал витоку інформації.

Р. 2. Загальна характеристика об’єкта інформаційної діяльності, структура об’єкта інформатизації як об’єкта розвідки, основні та допоміжні технічні засоби, контрольована зона, джерела небезпечних сигналів, схема електричного каналу витоку через лінії електроживлення, схема електричного каналу витоку через ланцюги заземлення, модель загроз, модель порушника, вибір контрольних точок для оцінювання захищеності.

Р. 3. Архітектура комплексної системи захисту інформації в АС класу 1, організаційні та режимні заходи захисту, схема захисту ланцюгів електроживлення, мережеві фільтри, розділовий трансформатор, гальванічна розв’язка зовнішніх ліній, екранування кабельних трас, локальний контур заземлення, засоби просторового та лінійного зашумлення, комплексна схема підключення засобів захисту, розрахунок ефективності захисних рішень, зведена оцінка залишкового ризику, порядок контролю ефективності та експлуатаційного моніторингу

6. Консультанти розділів кваліфікаційної випускної роботи

Розділ	Прізвище, ініціали та посада консультанта	Перевірив	
		дата	підпис
Розділ 1.			
Розділ 2.			
Розділ 3.			

7. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1. Аналіз нормативних вимог, основи технічного захисту та електричного каналу	Травень 2026
Розділ 2. Аналіз серидовища функціонування ас ксласу 1 та оцінювання захищеності	Травень 2026
Розділ 3. Система захисту інформації в ас класу 1від витоку електричним каналом	Травень 2026
Остаточне оформлення роботи	Травень 2026
Направлення роботи для перевірки на плагіат	Червень 2026
Попередній захист роботи на випусковій кафедрі	Червень 2026
Направлення роботи на рецензування	Червень 2026

8. Дата видачі завдання _____

Керівник _____ _____
(підпис) *(прізвище та ініціали)*

Здобувач _____ _____
(підпис) *(прізвище та ініціали)*

РЕЗЮМЕ (SUMMARY) *до кваліфікаційної випускної роботи здобувача:*	Гелетуха Артем Васильович Heletukha Artem Vasylovych

ЗВО	Київський національний університет будівництва і архітектури		
Тема (українською та англійською)	Захист інформації в автоматизованій системі класу 1 від витоку електричним каналом / Development of a Technical Information Protection System for a Class 1 Automated System Against Leakage Through an Electrical Channel		
Освітній ступінь	Бакалавр		
Факультет	Автоматизації і інформаційних технологій		
Випускова кафедра	Кібербезпеки та комп'ютерної інженерії		
Спеціальність	125 «Кібербезпека та захист інформації»		
Освітня програма	Безпека інформаційних і комунікаційних систем		
Керівник	к.т.н., доцент Котенко Андрій Миколайович		
Обсяг роботи:	*пояснювальна записка, стор.*	*Розділів*	*Презентація, кількість слайдів*
	≈88	*Три*	≈16
Розділ 1	Аналіз нормативних вимог, Основи технічного захисту та електричного каналу		
Розділ 2	Аналіз серидовища функціонування ас ксласу 1 та оцінювання захищеності		
Розділ 3	Система захисту інформації в ас класу 1від витоку електричним каналом		

Висновки по роботі:	У роботі проаналізовано нормативно-правову базу технічного захисту інформації, визначено основні загрози та канали витоку інформації в автоматизованій системі класу 1. Розглянуто фізичні передумови формування електричного каналу витоку через ланцюги електроживлення, заземлення, сигнальні та комунікаційні лінії. Розроблено модель загроз і модель порушника, обґрунтовано вибір організаційних та технічних заходів захисту. Запропоновано комплексну систему захисту, що включає фільтрацію електроживлення, екранування кабельних трас, гальванічну розв'язку зовнішніх ліній, удосконалення системи заземлення, застосування засобів лінійного і просторового зашумлення. Виконано розрахункову оцінку ефективності запропонованих рішень та визначено рівень залишкового ризику. Отримані результати можуть бути використані під час проєктування, модернізації та експлуатаційного контролю КСЗІ на об'єктах, де обробляється інформація з обмеженим доступом.
Ключові слова: Keywords:	Автоматизована система класу 1, технічний захист інформації, інформація з обмеженим доступом, електричний канал витоку, технічні канали витоку інформації, КСЗІ, модель загроз, модель порушника, ПЕМВН, мережевий фільтр, екранування, заземлення, гальванічна розв'язка, лінійне зашумлення, просторове зашумлення, залишковий ризик.

"____" _____ 2026р.

Здобувач: _____ /_____ /

Керівник: _____/ _____ /

"___" _____ 2026 р.

АНОТАЦІЯ

Основна текстова частина бакалаврської кваліфікаційної роботи налічує орієнтовно 80 сторінок без урахування додатків, ілюстративних матеріалів та таблиць.

Об'єкт дослідження - процес технічного захисту інформації з обмеженим доступом в умовах функціонування автоматизованої системи класу 1.

Предмет дослідження – електричний канал витоку інформації в АС класу 1

Мета роботи - сформувати та обґрунтувати комплекс заходів захисту інформації в автоматизованій системі класу 1 від витоку електричним каналом, а також оцінити ступінь ефективності запропонованих рішень.

Методи дослідження - аналіз нормативно-правових документів, системний аналіз, чисельні розрахункові методи.

У роботі впорядковано нормативну базу та узагальнено теоретичні засади технічного захисту інформації. Досліджено умови функціонування типової автоматизованої системи класу 1, розроблено модель загроз і модель порушника, обґрунтовано застосування мережевих фільтрів, екранування кабельних трас, гальванічної розв'язки зовнішніх ліній, вдосконаленого заземлення та організаційного режиму контролю.

Практичне значення одержаних результатів полягає в можливості безпосереднього впровадження запропонованого комплексу рішень під час проєктування або модернізації КСЗІ на об'єктах, де здійснюється обробка інформації з обмеженим доступом.

Ключові слова: АС класу 1, технічний захист інформації, електричний канал витоку, КСЗІ, модель загроз, мережевий фільтр, заземлення, гальванічна розв'язка, спеціальні дослідження

ABSTRACT

The main textual part of the bachelor's qualification thesis comprises approximately 80 pages, excluding appendices, illustrative materials, and tables.

The object of the study is the process of technical protection of restricted access information under the operating conditions of a class 1 automated system.

The subject of the study is the methods, models, and engineering-technical means that prevent information leakage through power supply circuits, grounding circuits, signal lines, and communication conductors.

The purpose of the thesis is to develop and substantiate a set of measures for protecting information in a class 1 automated system against leakage through an electrical channel, as well as to assess the effectiveness of the proposed solutions.

The research methods include the analysis of regulatory and legal documents, system analysis, and numerical calculation methods.

The thesis systematizes the regulatory framework and summarizes the theoretical foundations of technical information protection. The operating conditions of a typical class 1 automated system are analyzed. A threat model and an intruder model are developed. The use of power line filters, shielding of cable routes, galvanic isolation of external lines, improved grounding, and an organizational control regime is substantiated.

The practical significance of the obtained results lies in the possibility of direct implementation of the proposed set of solutions during the design or modernization of an integrated information protection system at facilities where restricted access information is processed.

Keywords: class 1 automated system, technical information protection, electrical leakage channel, integrated information protection system, threat model, power line filter, grounding, galvanic isolation, special research.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

Скорочення	***Розшифрування***
АС	автоматизована система
АС-1	автоматизована система класу 1
ІзОД	інформація з обмеженим доступом
ІТС	інформаційно-телекомунікаційна система
КЗ	контрольована зона
КСЗІ	комплексна система захисту інформації
КТЗІ	комплекс технічного захисту інформації
НСД	несанкціонований доступ
ОІД	об’єкт інформаційної діяльності
ПЕМВН	побічні електромагнітні випромінювання і наводки
ПЕОМ	персональна електронно-обчислювальна машина
СШ	співвідношення сигнал/шум
ТЗІ	технічний захист інформації
ТКВІ	технічні канали витоку інформації
ТЗОІ	технічні засоби обробки інформації
ДТЗС	допоміжні технічні засоби і системи
LC-фільтр	фільтр на основі індуктивності та ємності

ЗМІСТ

ВСТУП

Питання захисту інформації набувають дедалі більшої ваги у зв’язку з тим, що сучасні автоматизовані системи стали основним середовищем накопичення, обробки та передавання інформації з обмеженим доступом. Підвищення продуктивності технічних засобів, розширення мережевої інфраструктури і збільшення кількості супутніх допоміжних систем паралельно збільшують ймовірність реалізації технічних каналів витоку інформації.

Серед усіх технічних каналів витоку особливу позицію займає електричний канал. Його специфічна небезпека полягає в тому, що він виникає на базі штатної інженерної інфраструктури об’єкта: силових ліній, контурів заземлення, телефонних, сигнальних і мережевих провідників. Інформативні сигнали здатні проникати в ці кола як через паразитні зв’язки всередині самого обладнання, так і внаслідок наведень від побічних електромагнітних випромінювань.

Ефективний захист від витоку електричним каналом неможливий без комплексного підходу. Встановлення окремих фільтрів чи екранів саме по собі недостатнє: необхідне поєднання нормативного обґрунтування, організаційного режиму, спеціальних вимірювань, документального супроводу та інженерно-технічних рішень.

Об’єкт дослідження - процес технічного захисту інформації з обмеженим доступом в автоматизованій системі класу 1.

Предмет дослідження - методи, моделі та інженерно-технічні засоби, що перешкоджають витоку інформації через ланцюги живлення, заземлення, сигнальні та комунікаційні провідники.

Мета роботи - розробити комплекс організаційних та технічних рішень для захисту інформації в автоматизованій системі класу 1 від витоку електричним каналом і обґрунтувати ефективність запропонованих заходів.

Для реалізації поставленої мети необхідно: вивчити нормативно-правові засади захисту інформації; дослідити фізичну природу електричного каналу витоку;

побудувати модель загроз і модель порушника; обґрунтувати підбір технічних засобів захисту; виконати практичне проєктування; визначити порядок введення системи захисту в експлуатацію та подальшого регламентного контролю.

Методи дослідження: аналіз нормативних документів, системний аналіз структури ОІД, розрахункові методи оцінки співвідношення сигнал/шум, порівняльний аналіз технічних засобів захисту.

Практичне значення отриманих результатів полягає у формуванні готового до впровадження комплексу рішень, який може бути адаптований до конкретного об’єкта інформаційної діяльності та застосований при розробленні або вдосконаленні КСЗІ.

РОЗДІЛ І. АНАЛІЗ НОРМАТИВНИХ ВИМОГ, ОСНОВ ТЕХНІЧНОГО ЗАХИСТУ ТА ЕЛЕКТРИЧНОГО КАНАЛУ ВИТОКУ

1.1 Нормативно-правова база захисту інформації з обмеженим доступом та вимоги до її безпеки

Відповідно до Закону України «Про Інформацію», порядок отримання, використання та зберігання інформації визначається правовим режимом доступу, на підставі якого здійснюється її класифікація . Залежно від цього режиму інформація поділяється на:

- відкриту, що перебуває у власності фізичної особи;
- відкриту, що належить державі;
- конфіденційну, яка перебуває у власності фізичних або юридичних осіб;
- конфіденційну державну;
- інформацію, що становить державну таємницю;
- службову.

Поняття інформаційної безпеки трактується як такий стан інформації, за якого гарантується збереження її властивостей відповідно до чинної політики безпеки - згідно з НД ТЗІ 1.1-003-99 «Термінологія у сфері захисту інформації комп’ютерних систем від несанкціонованого доступу».

Для характеристики стану захищеності інформації застосовується модель CIA, що охоплює конфіденційність, цілісність та доступність. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу» передбачає можливість урахування й інших параметрів захищеності.

За загальним принципом уся інформація визнається відкритою, крім тієї, що належить до категорії з обмеженим доступом. Інформація з обмеженим доступом за правовим режимом поділяється на конфіденційну та таку, що містить державну таємницю.

Конфіденційна інформація - це відомості, якими фізичні або юридичні особи володіють, користуються чи розпоряджаються, і поширення яких відбувається за їхнім власним волевиявленням на визначених ними умовах.

Таємна інформація охоплює відомості у сферах оборони, економіки, науково-технічного розвитку, зовнішньополітичної діяльності, державної безпеки та охорони правопорядку, розголошення яких здатне завдати шкоди національній безпеці держави. Такі відомості підлягають державній охороні і відносяться до державної таємниці у встановленому законодавством порядку. Їх поділяють на відомості особливої важливості (ОВ), цілком таємні (ЦТ) та таємні (Т).

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» встановлює, що під час обробки відкрита інформація повинна зберігати цілісність, яка забезпечується захистом від дій, здатних призвести до її ненавмисної або навмисної зміни чи знищення .

При обробці конфіденційної або таємної інформації необхідно гарантувати її захист від несанкціонованого або неконтрольованого ознайомлення, модифікації, знищення, копіювання та поширення.

Знання нормативно-правової бази необхідне не лише для формального дотримання вимог законодавства, а й для коректного визначення критеріїв оцінки захищеності. Нормативні документи встановлюють допустимі значення параметрів сигналу у контрольних точках, перелік обов’язкових етапів при створенні КСЗІ та документальний супровід системи протягом усього терміну її функціонування.

1.2 Загрози інформації та шляхи її витоку в АС класу 1

Для підтримання конфіденційності, цілісності та доступності інформації, а також ефективного управління інформаційною системою слід вживати заходів, що захищають не лише від витоку через електричні канали, але й від будь-якого втручання у процес обробки та від порушення функціонування системи або об’єкта.

До найчастіше зустрічуваних потенційно небезпечних загроз відносяться ненавмисні помилки користувачів, операторів, системних адміністраторів та інших

осіб, залучених до експлуатації й технічного обслуговування інформаційних систем. Такі помилки можуть або безпосередньо породжувати загрозу (зокрема, хибне введення даних чи помилка у коді, що спричиняє збій системи), або утворювати умови, якими можуть скористатися зловмисники.

За даними досліджень у галузі інформаційної безпеки, людський фактор є причиною понад 65% збитків, завданих інформаційним ресурсам, тоді як природні катастрофи (пожежі, землетруси тощо) трапляються значно рідше.

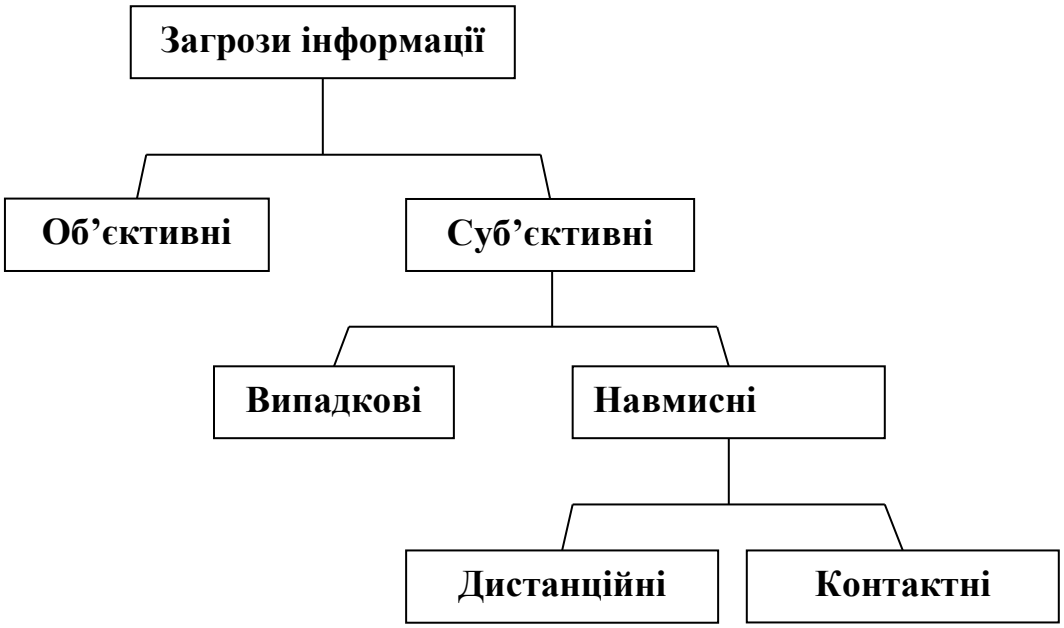

Рисунок 1.1 - Класифікація загроз

За мотивами виникнення суб’єктивні загрози поділяються на випадкові та навмисні.

Випадкові загрози є наслідком проєктних помилок у автоматизованих системах та засобах захисту, дефектів програмного забезпечення, відмов апаратури та інфраструктурних систем, а також помилок персоналу в процесі експлуатації.

Навмисні загрози породжуються свідомими і цілеспрямованими діями осіб, які прагнуть порушити інформаційну безпеку або незаконно заволодіти даними.

За місцем знаходження джерела щодо автоматизованої системи навмисні загрози поділяються на:

- дистанційні - джерело загрози розміщене за межами контрольованої зони;

- контактні - реалізуються всередині контрольованої зони, зазвичай пов’язані з фізичним проникненням до місць обробки або зберігання інформації.

За типом задіяного засобу впливу джерела загроз поділяються на: людину, апаратне забезпечення, програмне забезпечення, фізичне середовище.

Відповідно до НД ТЗІ 1.1-002-99 і НД ТЗІ 2.5-004-99, загрози класифікуються за чотирма класами :

- *Порушення конфіденційності* - несанкціоноване ознайомлення з інформацією на противагу встановленим правилам доступу;
- *Порушення цілісності* - повне або часткове знищення, модифікація даних чи нав’язування фальшивої інформації;
- *Порушення доступності* - блокування доступу або виведення з ладу системи чи її складових;
- *Втрата спостережуваності та керованості* - порушення механізмів ідентифікації й автентифікації, розподілу повноважень, аудиту або відмова від передавання/прийняття повідомлень.

До потенційних загроз в АС класу 1 належать: відключення засобів забезпечення функціонування, дезорганізація роботи, впровадження сторонніх осіб до складу персоналу, перехоплення ПЕМВН, викрадення носіїв, несанкціоноване отримання реквізитів доступу, ненавмисні помилки персоналу, несанкціоноване ввімкнення технічних засобів, запровадження шкідливого ПЗ, навмисне видалення або спотворення даних.

Особливе місце серед джерел технічних каналів витоку посідають ПЕОМ, через які можуть проходити практично всі основні канали витоку - від радіоканалів до матеріально-речових. Захищені дані можуть зберігатися в оперативній або постійній пам’яті, на змінних носіях, в пам’яті пристроїв введення/виведення та в каналах з’єднання мережі.

Канали витоку формуються як при активній роботі системи, так і в режимі очікування. Їх основними джерелами є: електромагнітні поля, наведення в

ланцюгах живлення та заземлення, паразитні випромінювання елементів ЕОМ, випромінювання на частотах КВА.

Технічному контролю ПЕМВН підлягають: побічні електромагнітні випромінювання у діапазоні 10 Гц–100 МГц, наведення в ланцюгах живлення та заземлення, електроакустичні перетворення (300 Гц–3,4 кГц) та високочастотні ЕМП (20 кГц–100 МГц).

Для АС класу 1 характерне те, що значна частина загроз реалізується не через програмне середовище, а через фізичну інфраструктуру об’єкта. Навіть за наявності коректно налаштованої ОС і криптографічних засобів безпека не гарантована, якщо за межі контрольованої зони виходять провідники живлення, заземлення або зв’язку з інформативними наведеннями.

1.3 Напрями захисту інформації в АС класу 1 від витоку технічними каналами

Комплексна система захисту інформації (КСЗІ) являє собою підхід до побудови інформаційної безпеки, що передбачає вбудовування захисних механізмів у всі компоненти системи, яка обробляє інформацію. Вона реалізує проактивні, активні та реактивні моделі захисту з використанням різних напрямів забезпечення безпеки .

КСЗІ розроблена для захисту інформації як в ізольованих комп’ютерах, так і в корпоративних мережах, дозволяє нейтралізувати відомі та потенційні загрози шляхом усунення архітектурних вразливостей і є ефективним засобом боротьби зі шкідливим програмним забезпеченням.

Організаційний захист є системою заходів, що ґрунтується на нормативно-правовому регулюванні виробничої діяльності та взаємовідносин персоналу з метою запобігання несанкціонованому доступу і нейтралізації внутрішніх та зовнішніх загроз. Його завдання охоплюють: стабільне функціонування підприємства, запобігання загрозам безпеці, захист законних інтересів, протидію

розкраданню ресурсів та розголошенню службової інформації, запобігання порушенням у роботі технічних засобів.

Засоби криптографічного захисту інформації (СКЗІ) - апаратні, програмні або комбіновані засоби шифрування та розшифрування інформації, що застосовуються для захисту від несанкціонованого доступу, а також для створення та перевірки електронного підпису . Основні методи криптографічного перетворення включають перестановку, заміщення, аналітичне перетворення та гамування. Функціонування СКЗІ базується на асиметричній криптографії з використанням ЕЦП .

Інженерний захист передбачає застосування фізичних конструкцій (стін, дверей, сейфів, блокувальних пристроїв) та охоронної і пожежної сигналізації для запобігання знищенню або пошкодженню носіїв інформації.

Технічний захист реалізує захист від НСД і від витоку через технічні канали . Для цього створюється КТЗІ, що є невід'ємною частиною КСЗІ. НСД може здійснюватися за допомогою штатних засобів системи або шляхом підключення сторонніх засобів. Захист на рівні програмного забезпечення включає системи розмежування доступу, ідентифікацію та автентифікацію, аудит, антивірусні засоби.

На апаратному рівні застосовуються апаратні ключі та сигналізаційні пристрої. На мережевому рівні - міжмережеві екрани, системи виявлення вторгнень, засоби VPN та аналізу захищеності.

До технічних заходів захисту відносяться також резервування критичних підсистем, побудова стійких обчислювальних мереж, системи пожежогасіння, резервне енергозабезпечення та фізичне блокування доступу до приміщень.

1.4 Інформаційна безпека та місце технічного захисту інформації

Технічний захист інформації як елемент загальної інформаційної безпеки будується через поєднання організаційних заходів та інженерно-технічних засобів.

Організаційні рішення регламентують права доступу, порядок роботи з носіями і проведення сервісних робіт, а інженерно-технічні засоби - фільтри, екрани, розв’язувальні пристрої - безпосередньо знижують рівень інформативних сигналів у каналах витоку. Взаємне доповнення цих напрямів є фундаментом системного захисту АС класу 1.

Фізичне середовище, в якому функціонує автоматизована система, - планування приміщень, розташування обладнання, прокладання кабельних трас - суттєво визначає характер і кількість потенційних каналів витоку. Стан системи заземлення, якість екранування, наявність суміжних зон із нижчим рівнем контролю формують перелік актуальних загроз для конкретного об’єкта. Саме тому аналіз фізичного середовища є обов’язковим першим кроком при проєктуванні системи захисту.

Спеціальні дослідження та контрольні вимірювання є основним інструментом кількісної оцінки захищеності від витоку технічними каналами. Вимірювання рівнів інформативного сигналу та шуму у вводах живлення, вузлах заземлення і місцях виходу комунікацій дозволяють встановити фактичний стан захисту та перевірити його відповідність нормативним вимогам.

Технічний захист від витоку електричним каналом доповнює, але не замінює криптографічні та програмні засоби. Шифрування захищає зміст даних, але не перешкоджає витоку неопрацьованого інформативного сигналу через провідники живлення чи заземлення. Системний підхід передбачає узгоджене застосування технічних, програмних і криптографічних заходів на всіх рівнях обробки інформації.

Захищеність АС класу 1 потребує забезпечення не тільки на момент введення в дію, а й протягом усього терміну експлуатації. Кожна зміна конфігурації, прокладання нових кабелів або ремонтні роботи можуть утворити нові канали витоку, що вимагає регулярних перевірок, актуалізації моделі загроз і повторних спеціальних досліджень.

Контрольована зона є фізичним периметром, у межах якого здійснюється контроль доступу персоналу та обладнання. Точне визначення меж КЗ є відправною точкою для формування переліку каналів витоку і вибору контрольних точок для вимірювань.

1.5 Класифікація інформації та особливості автоматизованих систем класу 1

АС класу 1 характеризується тим, що в ній функціонує один користувач або чітко визначена група з однаковим рівнем доступу до захищеної інформації. Фіксований склад користувачів дає змогу точніше окреслити межі контрольованої зони та побудувати реалістичну модель порушника, хоча й не скасовує вимог до технічного захисту від витоку.

Межі КЗ для АС класу 1 визначаються відповідно до фізичного розміщення обладнання, конфігурації приміщення та схем прокладання ліній живлення, заземлення і комунікацій. Будь-який вихід провідника за межі КЗ є потенційною точкою витоку.

Перелік потенційних каналів витоку прямо залежить від складу технічних засобів системи. Комп’ютерна техніка з імпульсними блоками живлення, принтери, сканери і мережеве обладнання генерують інформативні наведення у мережі живлення та кабельних трасах. Телефонні апарати, охоронна сигналізація та кліматична техніка можуть виступати провідниками для виносу інформації за межі КЗ.

Документальне забезпечення КСЗІ є обов’язковою умовою її легітимності. Акт обстеження, акт категоріювання, технічне завдання, протоколи спеціальних досліджень формують доказову базу відповідності системи вимогам нормативних документів.

Сервісне обслуговування і технічне супроводження - один із найбільш вразливих режимів з точки зору витоку. Тимчасове підключення стороннього обладнання або вимкнення захисних пристроїв під час ремонту може утворити

новий канал витоку, тому такі роботи виконуються лише уповноваженим персоналом з веденням журналу і подальшим відновленням захисту.

1.6 Технічні канали витоку інформації

Перехоплення інформації технічними каналами може здійснюватися як контактними (підключення до ліній), так і безконтактними методами (індукційне знімання сигналів). Безконтактні методи не потребують фізичного порушення цілісності кабельних трас і можуть застосовуватися на відстані кількох сантиметрів або більше залежно від рівня сигналу.

Інформативні сигнали здатні поширюватися всередині КЗ у полях обладнання, кабельних трасах та системі заземлення, а також виходити за межі через мережу живлення, телефонні та мережеві лінії - саме ці точки є основними місцями потенційного перехоплення.

Найбільш актуальними для АС класу 1, як правило, є загрози через мережу живлення та систему заземлення, оскільки ці канали найлегше доступні для зовнішнього порушника.

Конкретний перелік технічних каналів витоку визначається архітектурою об’єкта - плануванням приміщень, розміщенням обладнання та конфігурацією інженерних мереж. Об’єкт зі спільними шинами заземлення і загальними вводами живлення має більший потенційний периметр витоку порівняно з ізольованим об’єктом із власними системами.

Допоміжні технічні засоби - обладнання, що функціонує в тому самому приміщенні або пов’язане з ним інженерними мережами, - здатні ненавмисно переносити інформативні наведення за межі КЗ. Режим роботи обладнання суттєво впливає на ступінь небезпеки: під час штатної роботи наведення максимальні, а у період сервісних робіт виникають додаткові несанкціоновані канали.

1.7 Електричний канал витоку інформації: джерела та фізичні передумови

Мережа електроживлення є одним із головних шляхів виходу інформативних сигналів за межі КЗ. Струм споживання обчислювальної техніки синхронно

змінюється з оброблюваними даними, утворюючи інформативні складові у напрузі мережі, які можуть бути зняті спеціальною вимірювальною апаратурою в будь-якій доступній точці тієї самої мережі будівлі.

Система заземлення, первинно призначена для захисту персоналу від ураження електричним струмом, може одночасно слугувати провідником інформативних сигналів. Паразитні струми від нерівномірного навантаження або ємнісних зв'язків між обладнанням розповсюджуються всіма металевими конструкціями, з'єднаними з шиною заземлення.

Телефонні та сигнальні лінії, що виходять за межі КЗ, є каналами витоку при контактному підключенні засобів перехоплення: навіть без активної передачі вони можуть нести наведений сигнал від обладнання, що обробляє інформацію.

Безконтактне індукційне перехоплення не залишає фізичних слідів і може здійснюватися навіть через будівельні конструкції при достатньому рівні сигналу. ПЕМВН є невід'ємним наслідком роботи цифрової техніки, тому при визначенні меж захисних заходів для АС класу 1 їхня загроза обов'язково враховується.

Імпульсні джерела живлення сучасних ПЕОМ вносять у мережу кондуктивні завади, промодульовані потоком оброблюваних даних. Сервісні роботи і тимчасові підключення стороннього обладнання є одним із найнебезпечніших моментів: захисні пристрої часто тимчасово відключаються, а підключуване обладнання може мати дефектну ізоляцію.

Електричний канал не є ізольованим - він взаємодіє з іншими технічними каналами, формуючи комбіновані загрози (кондуктивно-акустичні, кондуктивно-електромагнітні), які значно складніше виявити і нейтралізувати.

1.8 Нормативно-правова база технічного захисту інформації

Нормативно-правова база ТЗІ в Україні включає закони, нормативні документи ТЗІ та державні стандарти, що встановлюють вимоги до організації захисту і до технічних рішень. Тільки дотримання всього комплексу вимог -

правових і технічних - дозволяє легітимно ввести систему в експлуатацію і пройти державну експертизу.

НД ТЗІ, зокрема НД ТЗІ 3.7-003-23, визначають послідовність етапів зі створення КСЗІ, склад обов'язкової документації та вимоги до спеціальних досліджень.

Дотримання цих стандартів є не лише юридичним зобов'язанням, а й гарантією методичної правильності виконаних робіт.

Категоріювання ОІД - обов'язкова процедура, що передує проєктуванню КСЗІ: вона встановлює клас системи і перелік обов'язкових захисних заходів. Для АС класу 1 рівень вимог до технічного захисту відповідає категорії об'єкта та грифу оброблюваної інформації.

Технічне завдання є провідним проектним документом, що визначає склад і характеристики засобів захисту, а також порядок їх впровадження. Політика безпеки встановлює правила роботи з інформацією, права та обов'язки персоналу і порядок реагування на інциденти. Обидва документи розробляються на підставі моделі загроз і затверджуються до початку проєктних робіт.

Приймальні випробування КСЗІ підтверджують відповідність реалізованої системи вимогам технічного завдання і нормативним значенням допустимих рівнів сигналу. Протоколи вимірювань, акти обстежень та висновки про відповідність НД ТЗІ є доказовою базою при перевірках контролюючих органів.

ВИСНОВКИ ДО РОЗДІЛУ І:

У розділі систематизовано нормативні засади захисту інформації, визначено місце технічного захисту в загальній системі інформаційної безпеки та розкрито фізичні передумови утворення електричного каналу витоку. Для АС класу 1 ключове значення мають правильне окреслення КЗ, документальне оформлення КСЗІ та поєднання організаційних і технічних рішень.

РОЗДІЛ ІІ. Аналіз середовища функціонування АС класу 1 та оцінювання захищеності від витоку електричним каналом

2.1 Об'єкт інформаційної діяльності

Правову й організаційну основу технічного захисту інформації в Україні утворює система нормативних актів, серед яких ключову роль відіграє Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.1999 № 1229/99. Цей документ встановлює правові й організаційні засади виконання заходів із захисту інформації з обмеженим доступом в органах державної влади, військових формуваннях, підприємствах та установах незалежно від форм власності.

Серед галузевих нормативних документів у сфері інформаційної безпеки визначну роль займають Тимчасові рекомендації з технічного захисту інформації від витоку через побічні електромагнітні випромінювання і наводки (ТР ПЕМВН-95). Цей документ є невід'ємною складовою системи ТЗІ і регламентує технічні вимоги та заходи з виявлення й нейтралізації ПЕМВН, що можуть утворювати канали витоку конфіденційних відомостей. Дія документа поширюється на всі категорії організацій і осіб, які опрацьовують інформацію з обмеженим доступом: органи виконавчої влади, військові підрозділи, підприємства всіх форм власності та дипломатичні установи України за кордоном.

У сфері технічного захисту інформації прийнято використовувати низку ключових понять:

- *Конфіденційність* - властивість інформації, що забезпечує її недоступність для осіб, які не мають відповідного дозволу;
- *Цілісність* - збереження повноти, достовірності та незмінності інформації у процесі її обробки або передачі;
- *Доступність* - своєчасний та безперешкодний доступ до інформаційного ресурсу для суб’єктів, які володіють необхідними повноваженнями, відповідно до встановлених правил політики безпеки.

- Технічний захист інформації - сукупність інженерно-технічних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації в умовах функціонування автоматизованих систем та комп’ютерних мереж .

Інформаційна система у цьому контексті розуміється як об'єднання програмних, апаратних і комунікаційних засобів, що забезпечують збір, оброблення, передавання та зберігання інформації.

Для виконання робіт із технічного захисту інформації необхідним є дозвільний документ, що підтверджує право організації або фізичної особи на здійснення таких робіт у межах чинного законодавства. Забезпечення захисту інформації в межах певного об’єкта або системи реалізується через комплекс технічного захисту інформації, що включає сукупність організаційних заходів, технічних засобів і регламентних процедур, спрямованих на зведення до мінімуму ризиків витоку чи компрометації інформації з обмеженим доступом.

У контексті інформаційної безпеки особливу увагу приділяють сигналам як фізичним носіям інформації, що використовуються для передавання повідомлень у системах зв'язку. *Сигнал* - це абстрактний об’єкт, який дозволяє описувати інформаційні процеси без прив’язки до конкретної фізичної реалізації (на відміну від повідомлення, не обов’язково має бути отриманим). У загальному випадку сигнал являє собою змінний фізичний процес, параметри якого можуть змінюватися в часі відповідно до змісту переданої інформації. Математична модель сигналу дозволяє формалізувати процес його аналізу та виявлення інформаційного навантаження.

Запис сигналів на матеріальний носій формує так звані дані, які, для набуття змісту, повинні бути оброблені спеціальними методами. Фізичні об’єкти, здатні генерувати сигнали, слугують джерелами цих сигналів. Якщо джерело створено та використовується з метою легітимного інформаційного обміну, його класифікують як функціональне. До таких джерел належать технічні засоби зв’язку,

радіопередавальні пристрої, акустичні випромінювачі, а також людина як суб’єкт мовлення.

Водночас ті самі сигнали, що є необхідними для нормальної роботи систем, за відсутності належного технічного захисту здатні перетворитися на загрозу інформаційній безпеці. У такому разі функціональні сигнали набувають статусу небезпечних, оскільки стають потенційними каналами витоку захищеної інформації.

Крім того, існують джерела сигналів, які виникають випадково або створюються навмисно зловмисниками. Такі сигнали зазвичай генеруються незалежно від волі власника інформації, і їх виявлення часто вимагає проведення спеціальних технічних досліджень. Сигнали, які виникають як побічний ефект функціонування електронних або електричних пристроїв, за наявності в них захищеної інформації, визнаються небезпечними.

Головними джерелами небезпечних сигналів є електричні та радіоелектронні компоненти - фактично будь-які елементи сучасних електронних систем. Вони здатні випромінювати сигнали в різних частотних діапазонах або зазнавати впливу паразитних зв’язків і наведень з інформативним навантаженням. Як наслідок, навіть ненавмисно сформовані сигнали можуть використовуватися для несанкціонованого отримання конфіденційних відомостей.

З огляду на викладене, технічному захисту підлягає інформація з обмеженим доступом, що існує у вигляді сигналів і полів, які виникають у процесі функціонування засобів передавання, обробки, зберігання й відображення даних. До цих засобів відносяться як основні (ТЗПІ), так і допоміжні технічні пристрої та системи (ДТЗС). Попри значні матеріальні витрати, впровадження засобів ТЗІ є безумовно необхідною умовою підтримання належного рівня інформаційної безпеки.

Класифікація джерел небезпечних сигналів може бути здійснена за фізичною природою сигналу:

- Акустоелектричні перетворювачі;
- Генератори низько та високочастотних сигналів;
- Елементи та ланцюги, що утворюють паразитні електромагнітні зв’язки та наведення.

Своєчасне виявлення та нейтралізація зазначених джерел є першочерговим завданням системи технічного захисту інформації.

Технічні засоби пересилання, оброблення, зберігання та відображення інформації (ТЗПІ) поділяються на основні й допоміжні. Основні засоби (ОСЗ) безпосередньо працюють із захищеною інформацією, тоді як допоміжні (ОСС) обробляють інші дані, але можуть стати джерелами витоку через побічні сигнали чи наведення. Обидва типи потребують заходів технічного захисту.

Основні технічні засоби (ОТЗ) - це технічні засоби пересилання, оброблення, зберігання та відображення інформації (ТЗПІ), що застосовуються для роботи з інформацією з обмеженим доступом. До них належать як безпосередньо засоби та системи обробки інформації, так і засоби зв’язку, через які здійснюється передача даних.

До складу технічних засобів пересилання, оброблення, зберігання та відображення інформації (ТЗПІ), що використовуються в інформаційно-комунікаційних системах, входять різні категорії апаратних засобів, які класифікуються за функціональним призначенням та характером опрацьованої інформації.

У науково-технічному контексті до ТЗПІ відносяться такі групи засобів:

- Системи зв’язку різного типу, що включають телефонний, телеграфний, директорський, гучномовний, диспетчерський, внутрішній, службовий та технологічний зв’язок. Ці засоби забезпечують передачу мовної та службової інформації між абонентами інформаційної системи;
- Засоби обчислювальної техніки (ЗОТ), до яких належать як цілісні інформаційно-телекомунікаційні системи (ІТС), електронно-обчислювальні

машини (ЕОМ), так і їх окремі компоненти. Вони призначені для автоматизованої обробки, зберігання та аналізу інформації, у тому числі з обмеженим доступом;

- Аудіоапаратура, що включає системи підсилення звуку, звукозапису та звуковідтворення, які використовуються для фіксації, трансляції або програвання мовного та акустичного контенту в межах інформаційних об’єктів;
- Технічні засоби, що формують дискретні канали зв’язку, включаючи абонентську апаратуру з пристроями відображення та сигналізації, а також обладнання для підвищення достовірності передачі інформації й каналоутворювальну апаратуру. Вони забезпечують розмежування та керування цифровими потоками даних між абонентами;
- Апаратура для передачі відеоінформації, що включає пристрої для перетворення, обробки, передачі та приймання відеосигналів, зокрема таких, що містять факсимільну або аналогову графічну інформацію;
- Системи внутрішнього телебачення (СВТ), які реалізують замкнені відеоканали спостереження та контролю в межах підприємств, організацій або спеціалізованих об’єктів;
- Системи відеозапису та відеовідтворення, що забезпечують збереження та відтворення відеоматеріалів, зокрема тих, що містять конфіденційну або службову інформацію.

Ці технічні засоби є об'єктами потенційного ризику витоку інформації і, відповідно, підлягають обов’язковому аналізу та впровадженню відповідних заходів технічного захисту інформації (ТЗІ).

Допоміжні технічні засоби і системи (ДТЗС) є складовою частиною загальної інформаційно-технічної інфраструктури об'єкта, але не призначені безпосередньо для обробки інформації з обмеженим доступом. Водночас їхня наявність у контрольованих зонах створює потенційну загрозу витоку інформації технічними каналами. ДТЗС можуть бути як захищеними, так і незахищеними, залежно від специфіки об'єкта і реалізованих заходів захисту.

До типових представників ДТЗС належать:

- системи спеціальної охоронної та пожежної сигналізації;
- дзвінкова сигналізація;
- контрольно-вимірювальна апаратура (КВА);
- засоби кондиціонування повітря та системи клімат-контролю;
- технічні засоби приймання програм радіомовлення і телебачення, а також обладнання радіотрансляційних мереж;
- системи годинофікації.

У практичному середовищі нерідко відбувається функціональне перетинання основних технічних засобів (ОТЗ) та ДТЗС. Наприклад, у межах одного приміщення можуть бути встановлені однотипні комп’ютери, що мають різний функціональний статус: один використовується для обробки захищеної інформації (ОТЗ), інший виконує допоміжні функції (ДТЗС), зокрема для доступу до мережі Інтернет.

До конструктивних елементів, які можуть виступати як потенційні канали витоку інформації, належать:

- кінцеві пристрої та апаратура;
- кабельні мережі, що з'єднують технічні засоби між собою;
- комутаційне обладнання, включаючи кроси, розподільні бокси, комутатори;
- елементи систем заземлення та електроживлення.

З особливою увагою слід розглядати ті компоненти ДТЗС, що виходять за межі контрольованої зони. Саме вони здатні перетворитися на ефективні канали витоку інформації, зокрема у вигляді побічних інформаційних наведень. Крім того, окремі складові ТЗПІ та ДТЗС можуть діяти як випадкові антени, як зосередженого типу (обладнання та блоки), так і розподіленого (кабелі, дроти), що підвищує ризики компрометації інформації.

Отже, попри другорядну роль ДТЗС в обробці захищеної інформації, вони вимагають не менш ретельного контролю і мають неодмінно включатися до комплексної системи технічного захисту інформації на рівних засадах з ОТЗ.

Об'єкт інформатизації (ОІ) - сукупність елементів, у тому числі інформаційних ресурсів, які містять відомості з обмеженим доступом, технічних засобів оброблення інформації (ТЗОІ), допоміжних технічних засобів і систем (ДТЗС), а також приміщень або будівель, де ці засоби розміщуються.

Виділені приміщення - це окремі приміщення, призначені для ведення закритих переговорів або виконання робіт з інформацією з обмеженим доступом. У свою чергу, приміщення, що захищаються, передбачені для проведення конфіденційних переговорів, не обов'язково пов'язаних із державною таємницею.

Засоби обчислювальної техніки (ЗОТ) - категорія об'єктів інформатизації, в яких обробка інформації здійснюється з використанням комп'ютерних систем та мереж.

Інформаційні об'єкти підлягають сертифікації відповідно до чинних вимог у сфері інформаційної безпеки. Сертифікації підлягають також спеціалізовані засоби та захищені об'єкти, що використовуються в інфраструктурі захисту інформації .

З позиції потенційного зловмисника об'єкт інформатизації постає як об'єкт розвідки (рис. 2.1), несанкціонований доступ до якого реалізується через наявні або потенційні канали витоку інформації.

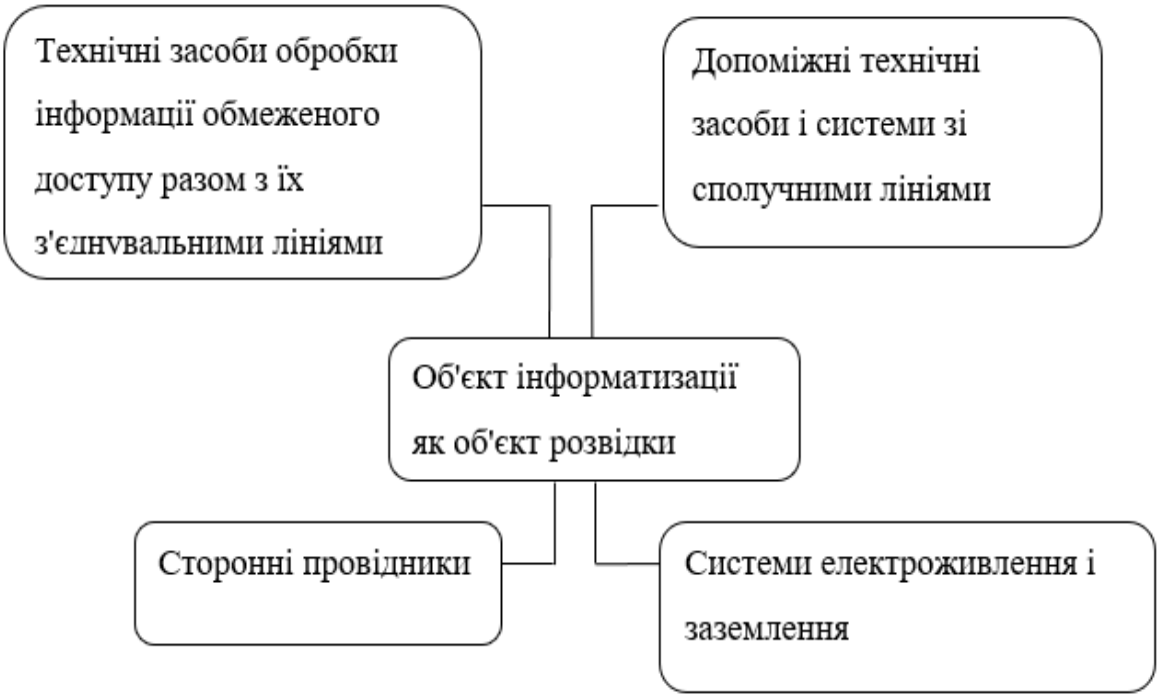

Рисунок 2.1 - Об’єкт інформатизації, як об’єкт розвідки

Для забезпечення ефективного захисту інформації важливе значення має поняття контрольованої зони (КЗ). Контрольована зона - це простір, у межах якого унеможливлено перебування осіб чи транспортних засобів без відповідного допуску. Межа КЗ визначається периметром охоронюваної території, а в разі часткового захисту - межами охоронюваних будівель або їх частин. Визначення КЗ здійснюється керівництвом організації з урахуванням реальних умов розміщення об’єкта та потенційної загрози перехоплення технічними засобами розвідки.

Суттєвими джерелами витоку інформації електричним каналом є зовнішні провідники - дроти, кабелі, металеві труби та інші електропровідні конструкції, які не належать до ТЗОІ чи ДТЗС, але фізично перетинають приміщення, де розміщене технічне обладнання, що обробляє інформацію з обмеженим доступом.

Природа потенційних джерел небезпечних сигналів, що здатні викликати витік інформації, дозволяє класифікувати їх на такі категорії:

- акустоелектричні перетворювачі;
- випромінювачі побічних низькочастотних сигналів;

- випромінювачі побічних високочастотних сигналів;
- паразитні зв'язки і наведення.

КСЗІ на об'єктах інформатизації зобов'язана враховувати всю сукупність перерахованих компонентів і чинників, забезпечуючи надійну недоступність захищеної інформації для сторонніх осіб і засобів технічної розвідки.

2.2 Електричний канал витоку інформації

Для розуміння природи загрози необхідно розглянути сутність, форми та фізичні засади формування електричних каналів витоку інформації, що обробляється основними технічними засобами та системами. При цьому особлива увага приділяється принципам утворення ЕКВІ та типовому порядку їх реалізації.

У низці технічних засобів обробки інформації (ТЗОІ), зокрема в системах підсилення звуку, носієм інформації виступає електричний струм, параметри якого (сила струму, напруга, частота та фаза) змінюються відповідно до закону зміни інформаційного (голосового) сигналу.

Електричний канал витоку інформації (ЕКВІ) - це канал несанкціонованої передачі захищеної інформації, який формується через електропровідні елементи системи (лінії електроживлення, заземлення, сигнальні та комунікаційні дроти), внаслідок виникнення паразитних електричних зв’язків або наведень.

Такий канал формується тоді, коли інформаційні сигнали, що обробляються технічними засобами, індукують електричні величини (струм або напругу) у суміжних електричних колах і можуть бути перехоплені спеціальними технічними засобами за межами контрольованої зони.

Передача інформативного сигналу відбувається через провідникові канали, які не призначені для цього функціонально.

Джерелами інформативних сигналів у таких каналах є електричні струми та напруги, що виникають у струмопровідних елементах під впливом зовнішніх електромагнітних полів або за рахунок внутрішніх ємнісних та індуктивних зв’язків у структурі електронних схем.

Наведені інформативні сигнали можуть виникати:

- у лініях живлення ТЗОІ;
- у лініях живлення й з’єднаннях ДТЗС;
- у заземлювальних ланцюгах ТЗОІ та ДТЗС;
- у зовнішніх провідниках (трубопроводах, металевих конструкціях, екранах кабелів тощо).

Інформативні сигнали можуть потрапляти в коло живлення ТЗОІ як внаслідок впливу паразитних електромагнітних випромінювань, так і через внутрішні паразитні ємнісні або індуктивні з’єднання випрямного модуля. У підсилювальних пристроях сигнали можуть замикатися через джерело живлення, що створює падіння напруги на внутрішньому опорі. При недостатньому згладжуванні у фільтрах ці сигнали можуть бути виявлені в мережі живлення.

Крім заземлюючих провідників, призначених для підключення ТЗОІ до заземлення, гальванічне заземлення може включати інші провідникові елементи, які виходять за межі контрольованої зони, включаючи нульовий провід електромережі, металеві оболонки з'єднувальних кабелів, трубопроводи водопостачання, опалення та елементи будівельної арматури. У сукупності ці елементи формують систему провідників, яка здатна передавати інформативні сигнали.

Технічні засоби, з’єднувальні лінії, лінії електроживлення, зовнішні провідники та елементи заземлення можуть функціонувати як випадкові антени, до яких за допомогою струмоприймачів або індукційних датчиків можливо підключити засоби технічної розвідки для перехоплення інформаційного сигналу.

Залежно від механізму виникнення наведених інформативних сигналів, їх ділять на такі типи:

- наведення в електричних колах ТЗОІ, спричинене побічними або паразитними електромагнітними випромінюваннями;

- наведення в з'єднувальних лініях ДТЗС і сторонніх провідниках, спричинене аналогічними джерелами ПЕМВ;

- наведення, спричинене внутрішніми паразитними ємнісними або індуктивними зв'язками;

- наведення у заземлювальних ланцюгах, спричинене впливом ПЕМВ, а також гальванічними зв'язками між схемною землею та конструктивними елементами системи.

Основою виникнення випадкових небезпечних сигналів у приміщеннях, де використовуються радіоелектронні та електротехнічні пристрої, є вторинне та направлене електромагнітне випромінювання (СЕМВН). Одним із проявів такого впливу є перешкоди, що виникають унаслідок небажаного перенесення електричної напруги з одного радіоелемента до іншого.

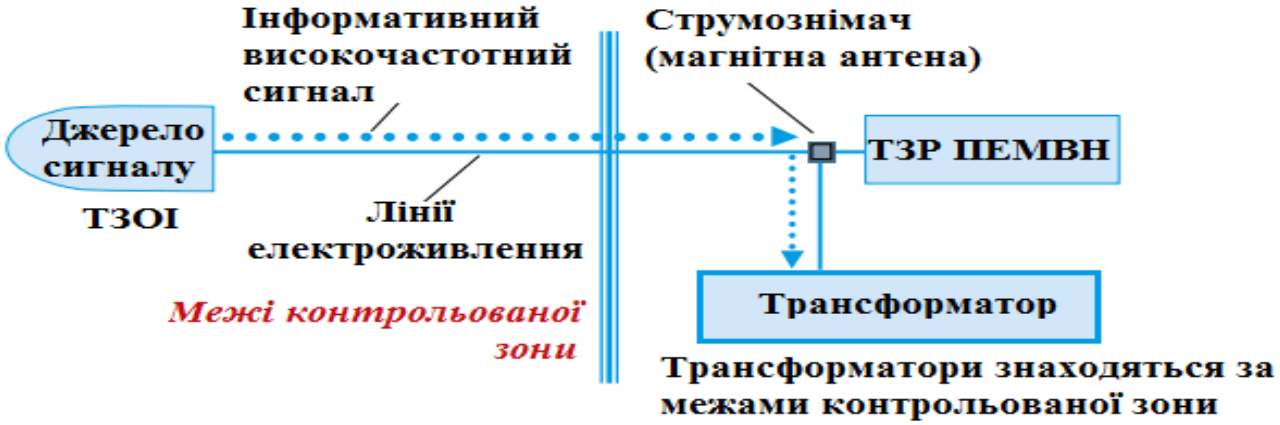

Рисунок 2.2 - Електричний канал витоку інформації за рахунок наведень інформативних сигналів у лініях електроживлення ТЗОІ

Такі явища є наслідком паразитних зв'язків між окремими елементами системи, які виникають через електричні наведення (ємнісні, індуктивні, гальванічні).

Паразитне наведення зумовлює появу на виході елементів сигналів (напруги або струму), що не відповідають їх функціональному призначенню. В деяких

випадках паразитні зворотні зв’язки можуть викликати самозбудження підсилювача, а також суттєво змінювати його амплітудно-частотні характеристики.

Явища пов’язані із паразитними наведеннями мають три складові:

- Джерело наведеної напруги (елемент, що випромінює сигнал);
- Приймач наведеної напруги (елемент, що приймає сигнал);
- Паразитний зв’язок між ними (випадковий небажаний канал передачі).

Процес усунення паразитних наведень полягає у виявленні та локалізації всіх трьох зазначених елементів. Це завдання є надзвичайно складним, оскільки в більшості випадків у системі діє одночасно кілька паразитних каналів зв’язку з різними джерелами наведень. Виявити слабкіші джерела та зв’язки можливо лише після усунення сильніших джерел впливу.

У будь-якому електронному пристрої, крім передбачених схемотехнікою основних провідників струму (дротів, струмопровідних доріжок друкованих плат), присутні також численні побічні шляхи поширення електричних сигналів. Ці шляхи виникають унаслідок паразитних зв’язків та електромагнітного втручання, що є неминучим явищем. Через них можуть передаватися небезпечні сигнали від акустико-електричних перетворювачів та інших джерел.

Основною причиною утворення паразитних каналів є електричні та магнітні поля, що створюються електричними зарядами і струмами, які протікають у колах електронних елементів. Постійні струми та заряди формують електричні та магнітні поля. Змінні струми породжують електромагнітні поля, які можуть поширюватися в просторі й впливати на інші елементи та компоненти електронної системи.

Крім впливу полів, гальванічні з’єднання між компонентами пристрою створюють додаткові шляхи поширення сигналів, тобто електричні сигнали можуть передаватися від одних блоків до інших навіть через спільні електричні кола. У результаті цього виникають як паразитні, так і керовані зв’язки, що призводить до взаємного впливу функціональних вузлів як всередині одного пристрою, так і між суміжними електронними модулями.

Такі зв’язки негативно впливають на точність, стабільність та функціональність електронних компонентів, вузлів і систем. Тому в процесі проєктування електронних пристроїв важливим завданням є зменшення рівня паразитних впливів до допустимих значень.

Чим вищі вимоги до технічних характеристик електронного обладнання, тим більший обсяг витрат спрямовується на нейтралізацію паразитних зв’язків та перешкод. У високоточних вимірювальних приладах значна частка їх вартості припадає саме на системи усунення паразитних сигналів, що забезпечує їхню надійність та відповідність прийнятим стандартам.

Усі електронні та електричні пристрої, а також кабелі, що з’єднують їх між собою, є джерелами паразитних зв’язків і наведень, які є невід’ємною частиною будь-якого електронного середовища. Кожен такий пристрій слід розглядати як потенційне джерело загроз інформаційній безпеці.

Існує три основні типи паразитних зв’язків:

- Ємнісні;
- Індуктивні;
- Гальванічні

Ємнісний паразитний зв’язок виникає внаслідок утворення електричного поля між провідними елементами або деталями, що знаходиться під потенціалом. Така паразитна ємність створюється між близько розташованими елементами радіоелектронного чи електричного пристрою (рис 2.2).

Оскільки опір ємності ($Xc = 1/\omega C$) зменшується зі зростанням частоти, то при високочастотному сигналі енергія, що передається через паразитну ємність, зростає. Унаслідок цього можливе самозбудження підсилювальних каскадів на частотах, які перевищують номінальну робочу смугу, що призводить до нестабільної роботи пристрою.

У разі близькості об’єкта технічного захисту інформації (ОТЗІ) до джерела технічних загроз (ДТЗС) можливе формування паразитного ємнісного зв’язку,

через який інформаційні сигнали можуть передаватися від ОТЗІ до ДТЗС, порушуючи конфіденційність інформації.

Оцінювання рівня паразитної ємнісної наводки вимагає знання ємності елементів пристрою яка визначається експериментальними методами, оскільки її точний розрахунок у складних конструкціях є досить складним.

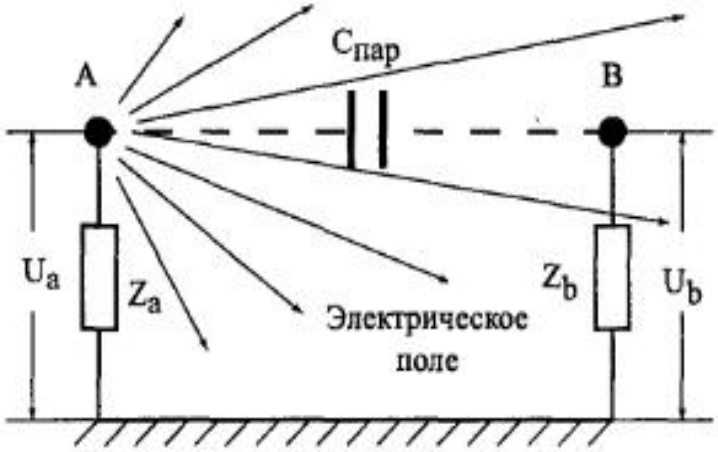

Рисунок 2.3 - Схема ємнісного паразитного зв'язку

На наведеному рис. 2.3 Ua позначає потенціал заряду в точці А відносно загального корпусу пристрою, який створює електричне поле. Під впливом цього поля в точці В індукується заряд протилежного знаку, що призводить до появи наведеної напруги Ub відносно корпусу.

Величина потенціалу Ub визначається взаємодією паразитної ємності Ср між точками А і В та повних опорів у ланцюзі Zb. При цьому ємнісний опір розраховується так: $Z = 1/(j\omega C)$.

(ω - кругова частота зміни потенціалу в точці А, j - уявна одиниця, С - ємність між точками)

Таким чином, паразитна ємність створює ємнісний зв’язок, що дозволяє передачу сигналу між електричними точками без прямого з’єднання.

Паразитні індуктивні зв’язки виникають через взаємну індукцію між провідниками елементів електричного кола, зокрема між трансформаторами. Такі

зв’язки можуть створювати зворотні зв’язки, які здатні викликати самозбудження підсилювальних каскадів у межах робочих частот (рис 2.4).

Критичною є ситуація, коли вхідний трансформатор підсилювача, що працює з низькорівневими сигналами, розташований поблизу джерел змінного магнітного поля (наприклад, силових трансформаторів). У таких умовах на вторинній обмотці трансформатора може виникнути електрорушійна сила (ЕРС), яка досягає кількох мілівольт, що в десятки або сотні разів перевищує допустимий рівень для вхідного сигналу.

Ефективність паразитного індуктивного зв’язку залежить від розмірів трансформаторів (чим менші розміри, тим слабший паразитний зв’язок).

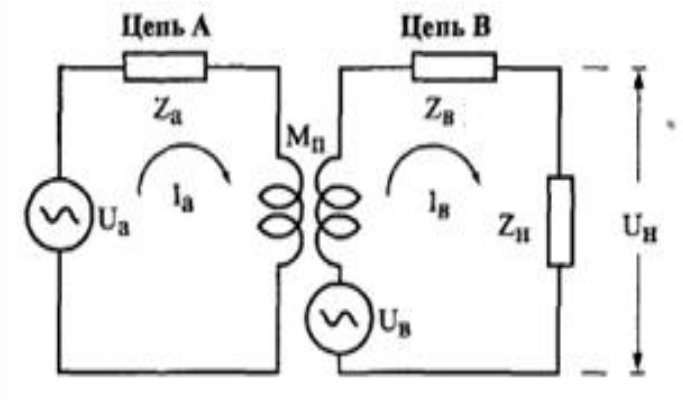

Рисунок 2.4 - Схема паразитного індуктивного зв'язку

Змінний струм, який протікає через ланцюг А, генерує змінне магнітне поле, яке може перетинати провідники іншого ланцюга В, створюючи в ньому електрорушійну силу (ЕРС) індукції. Це явище є основою взаємної індуктивності, рівень якої залежить від просторового розташування контурів, конфігурації провідників, ступеня проникнення магнітного потоку одного кола через інше.

Чим більша частка магнітного потоку першого ланцюга проникає у площу другого тим вищим є коефіцієнт взаємної індукції, тобто паразитний зв’язок стає сильнішим.

Гальванічні паразитні зв’язки виникають унаслідок наявності активного опору, через який проходять струми кількох незалежних електричних кіл. Такими елементами часто виступають спільні опори з’єднувальних кабелів, внутрішні опори джерел живлення та систем керування.

Прикладом може бути ситуація, коли кілька інформаційно-обчислювальних модулів комп’ютера підключені до одного джерела живлення (наприклад, +5 В). У момент подачі керуючого сигналу на входи тригерів 0 від одного з вузлів через спільні опори протікає струм, який спричиняє появу наведеної напруги на елементах іншого вузла, викликаючи небажаний вплив на його роботу.

Приклад спрощеної електричної схеми:

- вузол 1 і вузол 2 підключені до джерела живлення через спільні опори Z01, Z02, Z03;
- під час проходження сигналу з напругою Ui на вузлі 1 виникають струми Iц1 та Iц2;
- унаслідок цього на еквівалентному опорі Zн вузла 2 індукується наведена напруга Uh.

Коефіцієнт гальванічного паразитного зв’язку розраховується так:

$\beta = U_н / U_i$

(Uн - наведена напруга у другому вузлі, Ui - вхідна напруга першого вузла)

У ситуації, коли побічні електромагнітні поля та струми містять конфіденційні дані, паразитні з’єднання та наведення можуть стати каналами витоку захищеної інформації. Такі явища є вторинними фізичними процесами, які здатні спричинити несанкціоноване поширення інформаційного сигналу за межі контрольованого середовища.

Імовірність витоку інформації через паразитні провідники зумовлюється:

- геометричною конфігурацією провідних елементів;
- їх розмірами та взаємним розташуванням;
- електромагнітними властивостями середовища.

На відміну від функціональних антен, які проєктуються з урахуванням визначених характеристик передачі чи приймання сигналів, випадкові антени виникають спонтанно та неконтрольовано. До них можуть належати:

- монтажні провідники;
- патч-корди;
- друковані плати;
- електронні компоненти;
- металеві корпуси та інші струмопровідні частини.

Хоча електричні властивості випадкових антен значно поступаються параметрам штатних антен, мала відстань між джерелом сигналу та місцем його можливого приймання значно підвищує ризик інформаційного витоку.

Через складну та невизначену просторову конфігурацію точне моделювання таких антен є складним. Тому для аналізу використовують спрощені моделі (наприклад):

- зосереджені випадкові антени (телефони, гучномовці, датчики розташовані поза межами контрольованої зони);
- розподілені випадкові антени (кабелі, дроти, металеві труби та інші комунікації, що виходять за межі захищеної території).

Рівень сигналу, який наводиться у випадковій антені, залежить не лише від потужності електромагнітного випромінювання, але й від:

- відстані між ТЗПІ (технічними засобами передачі інформації) та ДТЗС (джерелами технічного зчитування сигналу);
- довжини паралельного прокладання провідників;
- спільного шляху поширення сигналу.

Таким чином, випадкові антени є реальними каналами створення електричних каналів витоку інформації, і їх ідентифікація та нейтралізація є важливим аспектом забезпечення інформаційної безпеки.

Отже, формування ЕКВІ можливе за наявності одночасного виконання таких умов:

- вихід провідників за межі контрольованої зони (КЗ) (сполучні лінії допоміжних технічних засобів і систем (ДТЗС), лінії електроживлення, заземлення та сторонні провідники повинні виходити за межі КЗ об’єкта, виконуючи функції випадкових антен);
- зосереджена випадкова антена повинна бути розташована так, щоб її частина або точка підключення виходила за межі контрольованої зони;
- можливість фізичного підключення до антен (має існувати можливість безпосереднього підключення засобів технічної розвідки до згаданих антен за межами КЗ);
- доступ до провідників живлення та заземлення (поза межою КЗ має бути технічна можливість підключення до ліній живлення, заземлення та сторонніх провідників для зняття наведеного сигналу).

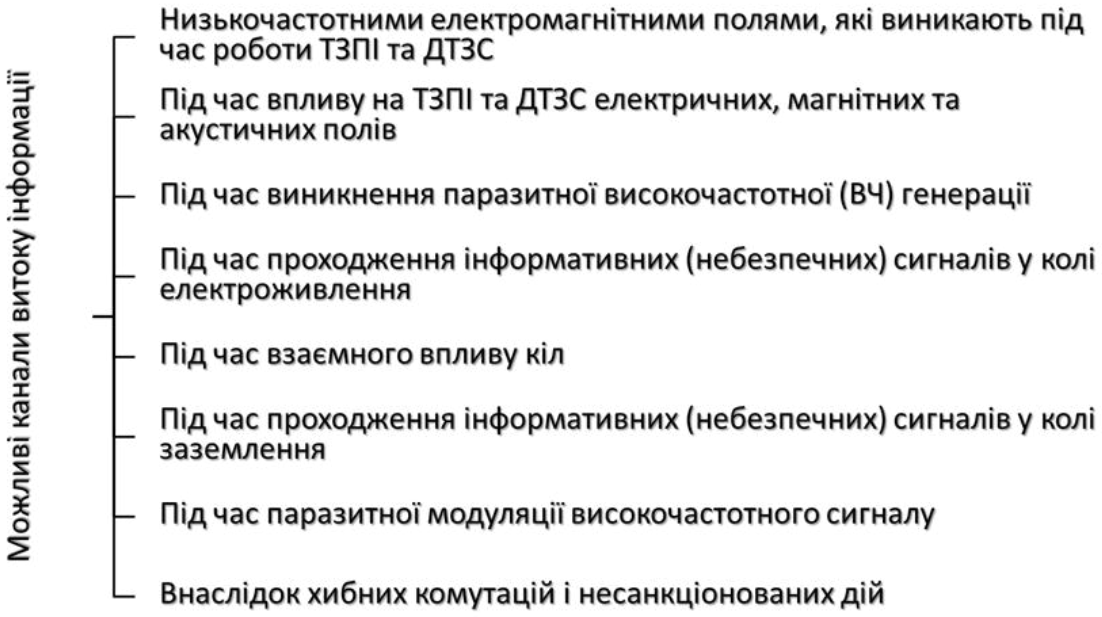

Рисунок 2.5 - Приклади сигналів каналу витоку інформації

2.3 Шляхи захисту інформації від витоку електричним каналом

Роботи із захисту інформації на об’єктах ТЗОІ включають категоріювання об'єктів згідно з вимогами ТПКО-95, а також передбачають обов’язкове внесення розділу з технічного захисту інформації до технічного завдання на монтаж. Монтаж таких об’єктів виконується відповідно до рекомендацій ТР ЕОТ-95. Після монтажу здійснюється обстеження об’єкта, включаючи технічний контроль, встановлення (у разі потреби) атестованих засобів захисту і подальша оцінка ефективності реалізованих заходів.

Обстеження об’єкта інформатизації включає:

- аналіз потоків інформації, що потребують захисту;
- ідентифікацію складу основних та допоміжних технічних засобів;
- виявлення кабельних ліній, які виходять за межі контрольованої зони та мають паралельний пробіг з іншими комунікаціями.

Додатково виконується виявлення комунікацій, що проходять через об'єкт і виходять за межі зони контролю, вимірювання побічних електромагнітних

випромінювань і наведень, а також оцінка відповідності рівнів сигналів нормативним вимогам.

Результати обстеження фіксуються в акті, що включає:

- ситуаційний та генеральний плани;
- перелік технічних засобів, зокрема тих, що мають вихід за межі контрольованої зони;
- пропозиції щодо додаткових захисних заходів (при необхідності).

До акта додаються схема розміщення обладнання та комунікацій, а також протоколи вимірювань.

Організаційний етап включає:

- перелік інформації з обмеженим доступом, що підлягає технічному захисту;
- встановлення необхідності впровадження захисних заходів з урахуванням потенційної шкоди в разі порушення цілісності або витоку інформації;
- встановлення приміщень, у яких обробляється інформація з обмеженим доступом;
- визначення переліку технічних засобів, які підлягають використанню або демонтажу, а також кабельних мереж, що виходять за межі контрольованої зони;
- Ідентифікація систем, які потребують переобладнання, демонтажу або оснащення захисними пристроями.

Засоби технічного захисту умовно поділяються на дві категорії (рис. 2.6).

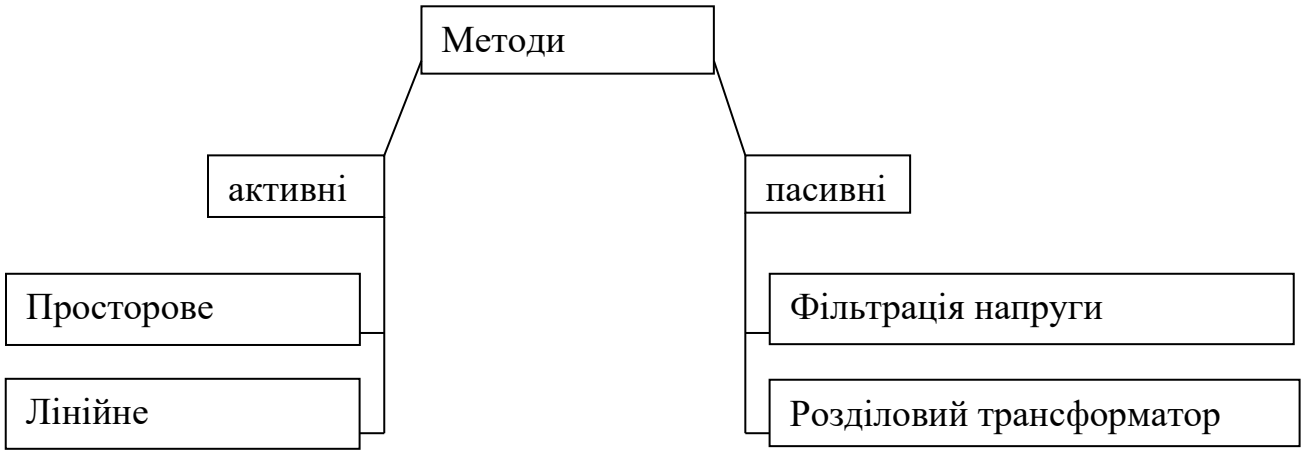

Рисунок 2.6 - Методи захисту інформації від витоку електричним каналом

Первинні технічні заходи також включають блокування акустоелектричних перетворювачів і ліній зв’язку, що виходять за межі контрольованої зони.

Це реалізується шляхом:

- відключення ліній зв’язку або встановлення простих схем захисту;
- демонтаж кабелів і обладнання;
- видалення потенційно небезпечних елементів за межами КЗ.

У системах телефонного зв’язку застосовується відключення викличних ліній, використання розеток для тимчасового відключення і встановлення простих захисних пристроїв. Для запобігання витоку інформації через системи гучномовного зв’язку впроваджуються вимикачі у викличних колах і на входах гучномовців, забезпечується можливість відключення мікрофонних підсилювачів. У провідних мережах мовлення відключаються гучномовці і використовуються найпростіші захисні пристрої.

Служби оповіщення повинні використовувати спеціально призначені абонентські пристрої з окремим прокладанням кабелів. Для систем годинофікації передбачається відключення електрогодинників на час проведення закритих заходів.

Аналогічно, в системах пожежної та охоронної сигналізації дозволено відключення датчиків або використання таких, що не потребують спеціального захисту. Під час функціонування телевізорів, радіоприймачів, звукопідсилювальної та звуковідтворювальної апаратури в період обробки захищеної інформації необхідно забезпечити їх відключення від електроживлення, ліній зв'язку та антенних кабелів.

Системи електронної оргтехніки і кондиціонування повинні бути розміщені в межах КЗ з живленням від внутрішніх трансформаторних підстанцій; у разі порушення цієї вимоги вони повинні бути відключені. Аналогічний підхід застосовується до побутової техніки, вона має живитися від окремого фідера або бути відключена.

Технічні заходи передбачають забезпечення основних і допоміжних технічних засобів пристроями захисту. Розміщення обладнання рекомендується здійснювати ближче до центру будівлі або з боку основної частини контрольованої зони. У разі неможливості дотримання цієї вимоги слід застосовувати екранування обладнання або приміщення, встановлення фільтрів у незахищені канали зв'язку, прокладання кабелів в екранованих конструкціях, скорочення довжини паралельного прокладання різних ліній та захист кіл заземлення і живлення.

Засоби технічного захисту включають:

- мережеві фільтри;
- пристрої блокування електричних каналів;
- засоби екранування;
- засоби заземлення та вирівнювання потенціалів;
- генератори лінійного та просторового зашумлення;
- спеціалізовані екрановані приміщення.

У випадку технічних засобів, які проявляють мікрофонний ефект, захисні дії залежать від вхідного опору. Для низькоомних елементів рекомендовано

відключення по двох проводах або використання фільтрів із високим опором, для високорезистивних рекомендовано замикання на низький опір.

Пристрої з активними компонентами, як-от автогенератори, мікрофонні або гучномовні підсилювачі, у неробочому стані повинні бути переведені в режим очікування. Підключення засобів захисту має виконуватися без порушення електричної схеми обладнання. Кабелі мають бути прокладені з урахуванням екранування і без утворення петель. Перехрещення трас слід здійснювати під прямим кутом. Живлення обладнання повинно бути стабілізоване і проходити через низькочастотні фільтри. Всі металеві конструкції повинні бути заземлені, а система заземлення має бути побудована за радіальною схемою, без утворення контурів.

Екрани кабельних ліній, що виходять за межі контрольованої зони, мають заземлюватися в одній точці, уникати контактів з конструкціями будівлі й не використовуватись як сигнальні чи живильні провідники. У довгих лініях екрани ділять на секції з одностороннім заземленням для зниження високочастотного опору.

Для запобігання витоку інформації за межі КЗ необхідно забезпечити, щоб рівень співвідношення «інформативний сигнал/шум» за її межами не перевищував нормативно допустимих значень. З цією метою розміщення ОТЗ рекомендується здійснювати у внутрішніх приміщеннях об’єкта, переважно на нижніх поверхах. До додаткових заходів належать:

- екранування ОТЗ або приміщень;
- впровадження систем просторового зашумлення;
- заміна незахищених технічних засобів на сертифіковані захищені аналоги;
- встановлення мережевих фільтрів.

Особливої уваги потребують високочастотні ОТЗ (зокрема, процесори, модулі пам’яті, дисплеї), які рекомендується розміщувати виключно в екранованих приміщеннях. Для кабелів, ліній і проводів, що мають вихід за межі КЗ,

передбачено застосування фільтрів, які пригнічують високочастотні завади. Прокладка кабелів повинна здійснюватися в екранувальних конструкціях, з дотриманням вимог симетричності та ізоляції від інших мереж.

Кабелі ОТЗ та ДТЗС прокладаються окремими пакетами. Заборонено утворення замкнених петель. Перехрещення кабелів, що мають вихід за межі контрольованої зони, повинно відбуватись під прямим кутом з обов'язковим уникненням електричного контакту між екрануючими оболонками. Неактивні або резервні лінії демонтуються або заземлюються.

Для забезпечення гальванічної та електромагнітної розв'язки електроживлення рекомендується застосовувати розділові системи типу «електродвигун-генератор». Дозволяється також використання завадоподавляючих фільтрів. При цьому живлення має здійснюватися через екрановані кабелі. Ділянки між технічним засобом і фільтрами або роздільними системами повинні прокладатися в жорстких екранованих конструкціях.

У жодному разі не допускається спільна прокладка в одному екранованому каналі кабелів живлення, розв'язаних від промислової мережі, з іншими кабелями, що мають вихід за межі КЗ. Заборонено також підключення незахищених засобів, які виходять за межі КЗ, до захищених джерел живлення без проміжного фільтра.

У випадках, коли пасивні засоби не забезпечують необхідного рівня захисту, застосовуються системи просторового зашумлення. Їх склад включає широкосмугові генератори шуму, рамкові антени та пульти контролю працездатності. Монтаж та обслуговування таких систем здійснюється організаціями, що мають відповідну ліцензію. Живлення генераторів шуму повинно надходити від того самого джерела, що і живлення основних технічних засобів.

Ефективність зашумлення визначається відповідністю характеристик завадових сигналів параметрам інформативного сигналу. Ідеальний шум має рівномірний розподіл ймовірності, максимальну ентропію, а також спектр, що повторює частотну структуру захищуваного сигналу. Використання шумів із

нормованим розподілом, адаптованих до рядкової структури відеосигналів, забезпечує значне підвищення ефективності маскування у порівнянні з квазібілими сигналами. Це дозволяє досягти оптимального захисту при мінімальних енергетичних витратах, особливо у випадку витоку інформації через провідні електричні канали.

Екранувальні кабельні конструкції в поєднанні з екранувальними конструкціями технічних засобів електронно-обчислювальної техніки (ЕОТ) повинні формувати замкнений електромагнітно ізольований об’єм. Прокладання кабелів до та з таких конструкцій здійснюється виключно через завадоподавляючі фільтри.

Екранувальні конструкції поділяються на жорсткі та гнучкі. Основу жорстких конструкцій становлять сталеві труби та металеві короби й коробки. Гнучкі конструкції виконуються з металорукавів або сітчастих елементів. Для екранування кабельних ліній також використовуються водогазопровідні труби, переважно тонкостінні оцинковані або електрозварні сталеві. Нерознімні з’єднання труб виконуються шляхом зварювання, рознімні - за допомогою муфт і контргайок.

Короби прямокутного перетину виготовляються з листової сталі. Вони забезпечують зручність прокладання кабелів і можливість їх роз’єдуваного підключення. На торцях секцій передбачені фланці для електричного з’єднання з іншими елементами конструкцій. Для забезпечення надійного струмопровідного контакту поверхня фланців повинна мати антикорозійне провідне покриття. Рекомендовано використовувати комбіновані екрани, що поєднують мідні та сталеві шари, з метою підвищення ефективності екранування.

Оцінка ефективності впроваджених заходів технічного захисту здійснюється на підставі результатів інструментального контролю.

У контексті безпеки електромагнітного випромінювання кабелів передачі даних слід зазначити, що однією з основних причин неконтрольованих випромінювань є незадовільний технічний стан з’єднувачів. У теоретично

ідеальному випадку, за відсутності дефектів в оболонці кабелю, рознімних з'єднувачах та інших елементах системи, ефективність екранування може перевищувати 100 дБ, що фактично унеможливлює витік інформації через кабельне випромінювання.

Однак у практичних умовах неповне або пошкоджене екранування, а також корозійні ушкодження з’єднувачів можуть призводити до суттєвих витоків електромагнітної енергії. У такому випадку можливе використання спеціалізованих технічних засобів для виявлення місць випромінювання, аналогічних тим, що застосовуються в кабельному телебаченні.

Найбільш ефективним способом усунення описаних недоліків є заміна електричних кабелів на волоконно-оптичні. Такий підхід забезпечує повне усунення електромагнітних випромінювань, однак вимагає впровадження оптичних і оптико-електричних перетворювачів на обох кінцях лінії зв'язку. Доцільність переходу на оптичні канали визначається на основі оцінки рівня випромінювань самих перетворювачів, особливо в локальних обчислювальних мережах.

Узагальнення до підрозділів 2.1–2.3

Захист інформації від витоку електричними каналами в системах ЕОТ вимагає комплексного підходу, що включає організаційні, первинні та технічні заходи. Основними засобами протидії витоку є екранування, просторове зашумлення, використання фільтрів та раціональна організація електроживлення і заземлення. Особливу увагу приділяють усуненню небезпечних випромінювань у кабельних мережах, що реалізується шляхом застосування екранованих конструкцій, контролю стану з'єднувачів та, за можливості, заміни електричних ліній на волоконно-оптичні. Ефективність реалізованих заходів підтверджується результатами інструментального контролю.

2.4 Обстеження середовища функціонування системи

Обстеження об'єкта інформаційної діяльності є першим і визначальним практичним кроком у процесі створення КСЗІ. Його мета - отримати вичерпні

відомості про фізичне середовище функціонування АС класу 1, необхідні для подальшого формування моделі загроз і технічного завдання. Обстеження проводиться спеціалізованою організацією з відповідною ліцензією Держспецзв'язку і оформляється актом, що є первинним документом у складі КСЗІ.

Аналіз приміщення починається з фіксації його конструктивних параметрів: матеріалу зовнішніх і внутрішніх стін, стелі та підлоги, наявності суміжних приміщень, а також розташування вікон і дверей. Особлива увага приділяється суміжним зонам - приміщенням, де можуть перебувати особи без відповідного допуску. Наявність спільних будівельних конструкцій (перегородок, стелі, підлоги) між захищеним приміщенням і суміжними зонами є чинником підвищеного ризику для акустоелектричного і акустичного каналів. Встановлюється також перелік усіх точок, де інженерні комунікації перетинають периметр контрольованої зони.

Аналіз системи електроживлення включає визначення конфігурації розподільчих щитів, схем прокладання силових кабелів і розташування точок підключення обладнання. Критично важливим є питання про те, чи є живлення об'єкта виділеним або спільним з іншими споживачами будівлі. За відсутності виділеного живлення розподільчий щит є потенційним місцем відбору інформативного сигналу зловмисником. Фіксується також місце введення кабелю живлення до приміщення, доступність електрощита для сторонніх осіб та наявність або відсутність мережевих фільтрів на вводі.

Система заземлення перевіряється на тип заземлювача (виділений або природний), опір контуру розтікання, наявність зв'язків між заземленням обладнання і будівельними металоконструкціями. Особливою небезпекою є так звані природні заземлювачі - металеві трубопроводи систем водопостачання й опалення, залізобетонна арматура будівлі, які мають численні неконтрольовані зв'язки з зовнішньою інфраструктурою. Для АС класу 1 рекомендується виділений контур заземлення без гальванічного зв'язку з системою заземлення будівлі. Опір

контуру вимірюється методом амперметра-вольтметра або спеціалізованим приладом.

Схема кабельних трас є одним із найважливіших результатів обстеження. Вона відображає маршрути всіх кабелів - живлення, заземлення, мережевих, телефонних і сигнальних ліній - від обладнання до точок виходу з КЗ. Особливо важливо фіксувати ділянки паралельного прокладання кабелів різного призначення, де можливе ємнісне та індуктивне наведення. На схемі позначаються всі місця, де кабелі перетинають стіни, підлогу або стелю приміщення.

Аналіз системи допуску персоналу дозволяє оцінити реалістичність загроз з боку різних категорій порушників. Встановлюється перелік осіб, що мають легальний доступ до приміщення і технічного обладнання, порядок проведення сервісних робіт і допуск зовнішніх технічних фахівців. Доступність суміжних технічних приміщень - серверних, електрощитових, кабельних шахт - для технічного персоналу будівлі є чинником підвищеного ризику.

Системи охоронної та пожежної сигналізації самі можуть бути каналами витоку, якщо їх лінії проходять через захищені приміщення і виходять за межі КЗ без гальванічної розв'язки. Під час обстеження встановлюється тип і конфігурація сигналізаційних систем, схеми прокладання ліній і наявність розв'язувальних пристроїв на виходах з КЗ. Допоміжні технічні засоби, що не є необхідними для виконання завдань АС, рекомендується виключити або ізолювати від захищеного середовища.

За результатами обстеження складається акт, до якого додаються: ситуаційний і генеральний плани об'єкта, схема розміщення обладнання, схема кабельних трас, схеми живлення і заземлення, протоколи первинних вимірювань у контрольних точках, а також перелік виявлених невідповідностей і рекомендації щодо їх усунення. Акт обстеження є підставою для розроблення моделі загроз і технічного завдання на створення КСЗІ.

2.5 Модель загроз

Модель загроз є нормативним документом, що визначає перелік актуальних загроз безпеці інформації для конкретного об'єкта з урахуванням результатів обстеження. Відповідно до НД ТЗІ 1.6-005-2013, модель загроз розробляється на підставі аналізу середовища функціонування і включає опис кожної загрози: механізм реалізації, потенційний вплив на безпеку, ймовірність реалізації і методи нейтралізації. Для АС класу 1 модель загроз зосереджується переважно на технічних каналах витоку і загрозах несанкціонованого доступу.

Загроза витоку по мережі електроживлення є актуальною, якщо живлення об'єкта є спільним з іншими споживачами будівлі і розподільчий щит доступний для сторонніх осіб. Механізм реалізації: зловмисник підключає спеціалізований аналізатор до розподільчої мережі будівлі поза межами КЗ і реєструє коливання напруги в мережі, що корелюють з оброблюваними даними. Ця загроза є пасивною - жодних активних впливів на систему не здійснюється, що унеможливлює її виявлення штатними засобами аудиту. Заходи нейтралізації: встановлення виділеного контуру живлення і мережевого фільтра на вводі класу не нижче FP3 за ТР ПЕМВН-95.

Загроза витоку по системі заземлення є особливо небезпечною, оскільки шина заземлення в будівлі з'єднана з усіма металоконструкціями і доступна в багатьох місцях. Інформативні струми в шині заземлення можуть бути зняті кліщами струму без порушення цілісності провідника. Рівень цієї загрози підвищується при використанні природних заземлювачів, що мають виходи за межі КЗ через водопровідні і опалювальні системи. Заходи нейтралізації: виділений контур захисного заземлення за радіальною схемою, ізоляція від природних заземлювачів.

Загроза контактного підключення до телефонної або сигнальної лінії реалізується через пасивне прослуховування лінії в доступній точці за межами КЗ. Пристрій перехоплення підключається паралельно до лінії; наявна в ній

інформативна складова знімається через узгоджувальний трансформатор і аналізується. Навіть якщо лінія не активна для основного призначення, вона може нести наведений сигнал від суміжних активних кабелів. Заходи нейтралізації: встановлення пристрою гальванічної розв'язки (оптрон або трансформатор) на виході лінії з КЗ.

Загроза безконтактного індукційного перехоплення реалізується шляхом підведення індукційної котушки або кліщів до кабельної траси без фізичного порушення ізоляції. Змінний струм у кабелі формує магнітне поле, що наводить ЕРС у котушці-перехоплювачі. Ця загроза є найбільш прихованою: засіб перехоплення не залишає жодних фізичних слідів і може встановлюватися навіть через будівельні конструкції при достатньому рівні сигналу. Заходи нейтралізації: прокладання кабелів у металевих коробах або трубах з надійним заземленням екрана.

Загроза несанкціонованого підключення під час сервісних робіт реалізується в момент, коли захисні засоби частково вимкнені, а сторонній персонал має легальний доступ до технічних вузлів. Зловмисник може встановити прихований провідник між захищеним і незахищеним сегментом мережі або закладний пристрій у корпусі обладнання. Заходи нейтралізації: жорсткий регламент сервісних робіт, обов'язкова присутність відповідального представника замовника, пломбування критичних точок, контрольні вимірювання після кожного обслуговування.

Загроза від закладних пристроїв передбачає попереднє встановлення в обладнання або інфраструктуру мікроелектронних пристроїв перехоплення, що живляться від мережі і передають інформативний сигнал по лінії живлення або безпроводово. Закладний пристрій може бути введений як під час монтажу або ремонту, так і через ланцюг постачань. Заходи нейтралізації: спеціальні обстеження приміщень і обладнання виявляючою апаратурою, контроль ланцюга постачань, заборона несертифікованого обладнання.

Таблиця -2.1 Матриця ризиків

Загроза	Ймовірність (1–3)	Збиток (1–3)	Пріоритет
Витік по мережі живлення	3	3	Критичний
Витік по заземленню	2	3	Високий
Контактне підключення до тел. лінії	2	2	Середній
Безконтактне перехоплення	1	2	Низький
Закладний пристрій	1	3	Середній

Модель загроз у підсумковій формі представляється у вигляді таблиці або структурованого переліку, де для кожної загрози вказуються: найменування загрози, джерело, механізм реалізації, контрольна точка, нормативно допустиме значення параметра безпеки, виміряне значення до впровадження захисту, запропонований засіб нейтралізації і очікуване значення після впровадження. Модель загроз підлягає перегляду при будь-яких змінах конфігурації системи, складу обладнання або меж КЗ.

2.6 Модель порушника

Модель порушника є нормативним документом, що розробляється на підставі аналізу потенційних зловмисників, здатних реалізувати загрози, зафіксовані в моделі загроз. Відповідно до рекомендацій НД ТЗІ, модель порушника описує: категорії можливих порушників, їхні мотиви, рівень кваліфікації, доступні ресурси та рівень фізичного і логічного доступу до об'єкта. Саме модель порушника визначає, які загрози з переліку актуальних є реалістичними - тобто можуть бути реалізовані конкретним типом зловмисника в конкретних умовах.

За рівнем технічної підготовки і доступу до об'єкта виділяють три основні категорії порушників. Категорія 1 - непідготовлений сторонній: фізично перебуває поза КЗ, не має спеціального обладнання, здатний скористатися лише найпростішими загальнодоступними методами (наприклад, підключення до відкритої розетки в коридорі). Категорія 2 - кваліфікований технічний фахівець без

доступу до КЗ: має знання в галузі технічної розвідки, спеціалізоване обладнання (аналізатор спектра, індукційні датчики), здатний реалізувати пасивне перехоплення за межами КЗ. Категорія 3 - інсайдер або особа, що діє під виглядом технічного персоналу: має легальний тимчасовий доступ до КЗ і може встановлювати закладні пристрої або несанкціоновано змінювати конфігурацію.

Мотивація порушника визначає масштаб операції і готовність до ризику. Корисливий порушник прагне до максимально швидкого і безпечного результату при мінімальних витратах; він обирає найпростіший і найдешевший метод перехоплення. Порушник, що діє за завданням конкурента або спецслужби, готовий до тривалої і ретельно спланованої операції із залученням дорогого спеціалізованого обладнання. Внутрішній порушник (незадоволений співробітник або агент, впроваджений в організацію) є найнебезпечнішою категорією: він має легальний доступ і знання про конфігурацію системи.

Класифікація порушників за часом дії є важливою для оцінки ризиків у різні фази функціонування системи. На етапі проєктування і монтажу існує ризик закладання несанкціонованих елементів у схему живлення або заземлення. Під час нормальної експлуатації основну небезпеку становить зовнішнє пасивне перехоплення. У період сервісного обслуговування ризик максимальний через тимчасове розширення доступу і часткове вимкнення захисних засобів. Після виведення системи з експлуатації залишається загроза відновлення інформації з носіїв, що не пройшли процедуру гарантованого знищення.

Найнебезпечнішим сценарієм є скоординована дія внутрішнього і зовнішнього порушника. Внутрішній порушник у зручний момент тимчасово вимикає захисний засіб або встановлює прихований провідник, надаючи зовнішньому порушнику можливість зняти інформативний сигнал. Для нейтралізації такого сценарію необхідні одночасно технічні заходи (контроль цілісності - пломбування вузлів, сигналізація при порушенні) та організаційні

(принцип двох уповноважених осіб при сервісних роботах, відеофіксація в технічних приміщеннях).

За результатами аналізу для конкретного об'єкта визначається актуальна модель порушника - найбільш реалістична категорія з огляду на доступність об'єкта, наявність осіб із відповідними мотивами і рівень потенційних ресурсів зловмисника. Заходи захисту проєктуються з розрахунку на нейтралізацію загроз від порушника актуальної категорії, але з розумним запасом, що враховує можливість появи більш кваліфікованого зловмисника. Модель порушника є динамічним документом і переглядається при суттєвих змінах у персональному складі організації або у зовнішньому середовищі.

2.7 Вибір контрольних точок і методика оцінювання захищеності

Вибір контрольних точок для проведення спеціальних досліджень є прямим наслідком моделі загроз: для кожної актуальної загрози визначається конкретна точка на лінії поширення інформативного сигналу, де вимірюється його рівень. Контрольні точки вибираються з урахуванням принципу «найближча доступна точка перехоплення» - де сигнал ще несе максимальне інформативне навантаження, але вже знаходиться в місці, доступному для зловмисника (або хоча б принципово доступному з фізичних міркувань).

Для типової АС класу 1 перелік контрольних точок включає: ввід силової мережі до захищеного приміщення (канал по мережі живлення); вузол підключення до шини захисного заземлення (канал по системі заземлення); місце виходу телефонної лінії з приміщення (телефонний канал); місце виходу мережевого кабелю LAN з приміщення (мережевий канал); ділянки кабельних трас у суміжних технічних приміщеннях (канал безконтактного перехоплення). За результатами попереднього аналізу перелік може доповнюватися або скорочуватися залежно від конкретної конфігурації об'єкта.

Методика вимірювань базується на вимогах ТР ПЕМВН-95 і передбачає визначення співвідношення сигнал/шум (СШ) у кожній контрольній точці.

Вимірювання проводяться в двох режимах: при роботі обладнання з максимальним навантаженням (запущені тестові програми, що максимально завантажують процесор і систему пам'яті) та при вимкненому обладнанні (для визначення рівня власного шуму). Різниця між виміряними значеннями дає рівень інформативного сигналу. Вимірювання виконуються сертифікованим обладнанням, що пройшло метрологічну перевірку.

Рівень інформативного сигналу Uc вимірюється в дБмкВ відносно 1 мкВ. Рівень шуму Un вимірюється в тих самих одиницях при вимкненому обладнанні. Співвідношення сигнал/шум визначається як: СШ = Uc – Un (дБ). Нормативно допустиме значення СШ для відповідної категорії об'єкта визначається за таблицями ТР ПЕМВН-95 і становить, наприклад, 8 дБ для об'єктів 1-ї категорії. Якщо виміряне СШ перевищує нормативне значення, виконується розрахунок необхідного коефіцієнта ослаблення: K = СШвим – СШнорм + ΔK, де ΔK - запас захищеності (як правило, 6–10 дБ).

Коефіцієнт ослаблення засобу захисту перевіряється шляхом порівняльних вимірювань до і після його встановлення в тих самих умовах і при тій самій методиці. Ефективність засобу підтверджується, якщо виміряний коефіцієнт ослаблення перевищує розрахований необхідний коефіцієнт. Аналізатор спектра підключається до контрольної точки через узгоджувальний трансформатор або безпосередньо залежно від типу точки. Частотний діапазон сканування зазвичай охоплює від 10 кГц до 400 МГц, крок частотної розгортки - 1 кГц або менше.

Аналіз частотного складу інформативного сигналу дозволяє визначити, в яких частотних смугах він має найбільшу інтенсивність, і відповідно підібрати характеристики засобу захисту. Для цифрової обчислювальної техніки характерна наявність інформативних складових у широкому діапазоні від кількох кГц до кількох сотень МГц. При цьому на нижніх частотах (до 1 МГц) найбільш виражені складові від тактової частоти і шин даних, на середніх (1–100 МГц) - від процесора і відеосистеми, на верхніх (100+ МГц) - від компонентів, що працюють на

гармоніках тактової частоти. Знання цього розподілу дозволяє правильно обрати смугу мережевого фільтра і точки вимірювань.

За результатами вимірювань складається зведена таблиця, що містить для кожної контрольної точки: найменування точки, виміряне значення СШ до захисту, нормативно допустиме значення СШ, необхідний коефіцієнт ослаблення, обраний засіб захисту і виміряне значення СШ після впровадження захисту. Ця таблиця є основним кількісним підтвердженням ефективності КСЗІ і включається до протоколу спеціальних досліджень. Відповідність усіх виміряних значень нормативним є необхідною умовою для підписання акта приймальних випробувань.

2.8 Документальне забезпечення аналітичного етапу

Документальне забезпечення є обов'язковою умовою легітимності КСЗІ: без відповідних актів, протоколів і схем система не може вважатися такою, що відповідає вимогам нормативних документів ТЗІ, і не допускається до обробки інформації з обмеженим доступом. Склад документації аналітичного етапу визначається НД ТЗІ 3.7-003-23 і включає кілька обов'язкових документів.

Акт обстеження об'єкта інформаційної діяльності є первинним документом, що фіксує результати огляду об'єкта і містить вичерпну характеристику приміщення, системи живлення, заземлення та кабельних трас. Документ складається комісією з представників власника об'єкта та спеціалізованої організації з ліцензією на провадження діяльності у сфері ТЗІ. До акта обов'язково додаються ситуаційний план, схеми кабельних трас, живлення і заземлення, а також фотоматеріали критичних вузлів.

Акт категоріювання об'єкта інформаційної діяльності встановлює клас АС і відповідний рівень вимог до технічного захисту. Для АС класу 1 акт категоріювання підтверджує, що в системі функціонує один або чітко визначений склад користувачів з однаковими правами доступу. Категорія об'єкта встановлюється за максимальним грифом оброблюваної інформації відповідно до ТПКО-95 і безпосередньо визначає нормативне значення допустимого СШ за ТР ПЕМВН-95.

Модель загроз і модель порушника є ключовими аналітичними документами, що обґрунтовують необхідність конкретних захисних заходів. Вони розробляються на підставі акта обстеження і є вхідними даними для технічного завдання. Модель загроз визначає перелік актуальних загроз і механізми їх реалізації; модель порушника визначає реалістичний профіль зловмисника для кожної загрози. Обидва документи затверджуються власником об'єкта і є складовою частиною технічного завдання.

Технічне завдання на створення КСЗІ є провідним проектним документом. Для захисту від витоку електричним каналом воно містить: вимоги до виділеного живлення і мережевих фільтрів (клас, коефіцієнт ослаблення, частотний діапазон), вимоги до системи заземлення (схема підключення, опір контуру), вимоги до екранування кабельних трас, вимоги до гальванічної розв'язки зовнішніх ліній, нормативні значення параметрів, яких слід досягти після впровадження захисту. Технічне завдання є юридично значущим документом і підписується уповноваженими представниками замовника і виконавця.

Протоколи спеціальних досліджень складаються за результатами інструментальних вимірювань до і після впровадження захисту. Кожен протокол містить: дату і умови проведення вимірювань, відомості про застосоване метрологічно повірене обладнання, схему контрольних точок, зафіксовані значення у всіх точках і висновок про відповідність або невідповідність нормативним вимогам. Протоколи підписуються відповідальними особами - представником спеціалізованої організації і відповідальним за ТЗІ з боку замовника.

Схеми електроживлення і заземлення у складі документації КСЗІ відображають реалізовану конфігурацію захисних засобів: місця встановлення фільтрів, точки підключення заземлювачів, маршрути екранованих кабелів. Ці схеми є не лише документом, що описує поточний стан, але й робочими інструментами для технічного обслуговування і для перевірки стану системи під час планових і позапланових перевірок.

Журнал сервісних робіт і журнал змін конфігурації ведуться протягом усього терміну експлуатації АС і є основним документальним підтвердженням дотримання регламентів. Записи в журналі є доказовою базою при перевірках контролюючих органів і в разі розслідування інцидентів. Будь-яка зміна конфігурації обладнання, провідників або захисних засобів, не зафіксована в журналі, є підставою для призначення позапланових спеціальних досліджень.

2.9. Теоретичні засади захисту від витоку електричним каналом

2.9.1. Фізичні механізми утворення електричного каналу витоку

Будь-який електронний пристрій у процесі штатного функціонування генерує сукупність електромагнітних полів, що виходять далеко за межі корпусу і взаємодіють з навколишнім середовищем. Ці поля є неминучим наслідком протікання змінних струмів у схемотехнічних елементах і провідниках - від провідних доріжок друкованих плат до зовнішніх ліній живлення і зв’язку. Відповідно, технічне обладнання автоматизованої системи класу 1 постійно формує в навколишньому просторі фізичне середовище, що може переносити відомості про характер та зміст інформаційних процесів, які відбуваються всередині системи.

З фізичної точки зору електричний канал витоку інформації виникає тоді, коли струм або напруга, що виникають у лінії під впливом інформативного сигналу, стають доступними для вимірювання у точці, розташованій за межами контрольованої зони. Для цього необхідне одночасне виконання трьох умов: присутність у лінії інформативної складової, фізична доступність лінії для сторонньої особи і наявність технічних засобів, здатних зареєструвати та декодувати цю складову. Якщо хоча б одна з умов не виконується - канал не є актуальним, а отже, захист може бути обмежений нейтралізацією тієї умови, яку найпростіше усунути з технічної та економічної точки зору.

Механізм наведення інформативного сигналу на суміжні лінії реалізується через три фізичні явища, що можуть діяти одночасно або незалежно одне від одного. Перше явище - ємнісне наведення. Між двома паралельними провідниками

завжди існує паразитна ємність, величина якої залежить від відстані між ними, довжини паралельного прокладання і діелектричних властивостей ізоляції. Зміна напруги на інформативному провіднику через цю ємність наводить напругу на суміжному провіднику. Особливістю ємнісного наведення є зростання його рівня зі збільшенням частоти сигналу, оскільки опір ємності обернено пропорційний частоті. Для типових кабельних трас навіть на частотах 100 кГц - 1 МГц ємнісне наведення може сягати рівнів, що перевищують нормативно допустимі значення.

Друге явище - індуктивне наведення. Змінний струм у провіднику формує магнітне поле, силові лінії якого охоплюють суміжні провідники і наводять у них електрорушійну силу. Величина наведеної ЕРС пропорційна швидкості зміни магнітного потоку і визначається взаємною індуктивністю між провідниками. На відміну від ємнісного наведення, індуктивне характеризується тим, що його рівень залежить від геометрії контурів і взаємного розташування провідників. Екранування кабелів знижує індуктивне наведення, оскільки металевий екран концентрує і шунтує магнітне поле всередині себе, не даючи йому поширюватися на зовнішні провідники.

Третє явище - гальванічне наведення, або наведення через спільний опір. Якщо кілька кіл мають спільну ділянку з ненульовим активним опором - наприклад, спільну шину живлення або спільний провідник заземлення - то струм одного кола спричиняє падіння напруги на цій ділянці, яке сприймається іншими колами як втручання. Гальванічне наведення є найбільш небезпечним, оскільки діє незалежно від частоти, не ослаблюється відстанню між провідниками і практично не піддається екрануванню. Єдиним надійним засобом захисту від нього є роздільне живлення різних кіл або гальванічна ізоляція між захищеним обладнанням і зовнішньою інфраструктурою.

2.9.2. Побічні електромагнітні випромінювання і наводки: природа і небезпека

Побічні електромагнітні випромінювання і наводки (ПЕМВН) є неодмінним супутником роботи будь-якого цифрового пристрою. На відміну від корисного сигналу, що навмисно генерується для виконання функціональних задач, ПЕМВН виникають як небажаний побічний ефект роботи схемотехніки і характеризуються широким спектром частот, що охоплює від одиниць герц до сотень мегагерц.

Природа ПЕМВН пов’язана із наявністю в цифровій апаратурі струмів з крутими фронтами перемикання. Кожен логічний перехід у мікросхемі - переключення транзистора - супроводжується короткочасним імпульсом струму, спектр якого містить компоненти на частотах, що значно перевищують основну тактову частоту пристрою. Так, мікропроцесор із тактовою частотою 3 ГГц генерує ПЕМВН на частотах до кількох десятків гігагерц, а кожен перехід логіки «0»→«1» або «1»→«0» є окремим джерелом імпульсного випромінювання. Оскільки ці переключення відбуваються відповідно до коду, що обробляється, вони несуть у собі інформативну складову, яка може бути декодована зловмисником.

Найбільш небезпечними з точки зору витоку є три компоненти ПЕМВН. Перша - безпосереднє електромагнітне випромінювання корпусу пристрою і підключених до нього кабелів, що функціонують як антени. Друга - наводки в ланцюгах живлення: у момент перемикань мікросхем змінюється струм, що споживається пристроєм, і це відображається у вигляді мікроімпульсів напруги на лінії живлення. Третя - акустоелектричні наводки, коли механічна вібрація від трансформаторів, котушок індуктивності або капацитивних мікрофонів перетворюється на електричний сигнал.

Для автоматизованої системи класу 1, де весь обсяг оброблюваної інформації з обмеженим доступом сконцентрований в одному або кількох пристроях, рівень ПЕМВН є максимальним порівняно з розподіленими системами. Це пояснюється тим, що весь інформативний трафік проходить через одне фізичне місце, а відтак

сигнал у ланцюгах живлення і заземлення корелює безпосередньо зі змістом оброблюваних даних. Зловмисник, що підключився до мережі живлення навіть на значній відстані від захищеного об’єкта, може реєструвати ці кореляції і відновлювати оброблювані дані.

2.9.3. Класифікація методів і засобів захисту від витоку

Методи захисту від витоку через електричний канал поділяються на пасивні і активні залежно від того, чи вносять вони зміни в параметри середовища поширення сигналу.

Пасивні методи спрямовані на ослаблення або повне блокування інформативного сигналу в каналі поширення без введення додаткових сигналів. До них належать: мережеві фільтри, що ослаблюють завади у смузі частот, небезпечних для витоку; розділові трансформатори і гальванічна розв’язка, що повністю розривають провідниковий шлях поширення сигналу; екранування кабелів і корпусів, що блокує індуктивне і ємнісне наведення; вдосконалення системи заземлення за топологією «зірки», що виключає замкнені контури заземлення.

Активні методи полягають у формуванні завадового сигналу, який накладається на інформативний і робить неможливим його виокремлення. Найбільш поширеними є: генератори просторового зашумлення, що формують широкосмуговий електромагнітний шум у захищеному приміщенні; генератори лінійного зашумлення, що вводять шумовий сигнал безпосередньо в лінії живлення і заземлення. Вимоги до завадового сигналу визначаються критерієм максимальної ентропії: серед усіх сигналів з однаковою потужністю найбільшу ентропію має шум з рівномірним розподілом ймовірності, що унеможливлює його ідентифікацію і видалення зловмисником.

Організаційні заходи не є технічними засобами захисту, але відіграють критичну роль у забезпеченні їх ефективності. Жодна технічна система не може гарантувати захист, якщо сервісний персонал безконтрольно підключає стороннє

обладнання, пломби не перевіряються або зміни конфігурації не документуються. Саме тому нормативні документи ТЗІ вимагають документального підтвердження як технічних, так і організаційних складових КСЗІ.

2.10. Архітектура комплексної системи захисту інформації в АС класу 1

2.10.1. Принципи побудови КСЗІ

Комплексна система захисту інформації (КСЗІ) від витоку електричним каналом в автоматизованій системі класу 1 будується відповідно до сукупності принципів, що визначають її архітектуру, склад засобів і порядок функціонування. Ці принципи не є довільними - вони випливають з аналізу природи загроз і закріплені в нормативних документах технічного захисту інформації.

Принцип багаторівневого захисту є ключовим архітектурним рішенням. Він передбачає, що загроза, яка подолала один рівень захисту, зустрічає наступний, незалежно від першого. В контексті захисту від витоку електричним каналом перший рівень - організаційний: він обмежує фізичний доступ до критичних точок інфраструктури (електрощитів, кабельних стояків, телефонних кросів) і регламентує порядок сервісних робіт. Другий рівень - технічний пасивний: мережеві фільтри, виділене заземлення, гальванічна розв’язка і екранування кабельних трас фізично ослаблюють інформативний сигнал у всіх потенційних каналах витоку. Третій рівень - технічний активний: генератори зашумлення накладають на залишковий сигнал завадовий шум, що виключає його розшифровку навіть при успішному перехопленні. Четвертий рівень - контрольний: регулярні вимірювання підтверджують, що стан системи захисту відповідає нормативним вимогам і не деградував з часом.

Принцип адресності означає, що кожен засіб захисту встановлюється для нейтралізації конкретної загрози, зафіксованої в моделі загроз об’єкта. Це виключає формальний підхід, при якому засоби встановлюються «для галочки» без урахування реального переліку актуальних загроз. Наприклад, якщо на конкретному об’єкті відсутній телефонний зв’язок, встановлення пристрою

гальванічної розв’язки для телефонної лінії не є доцільним і не входить до складу КСЗІ. Водночас якщо аналіз показав, що система заземлення об’єкта має зв’язок з природними заземлювачами будівлі - виділений контур заземлення є обов’язковим засобом.

Принцип верифікованості вимагає, щоб кожен захисний захід мав вимірюваний критерій ефективності. Для мережевого фільтра таким критерієм є коефіцієнт ослаблення у визначеному частотному діапазоні, що вимірюється аналізатором спектра. Для виділеного контуру заземлення - опір розтікання, що вимірюється спеціалізованим приладом. Для гальванічної розв’язки - коефіцієнт передачі сигналу, що підтверджується вимірюванням рівня сигналу на виході лінії до і після встановлення пристрою. Без таких критеріїв неможливо об’єктивно підтвердити ефективність системи захисту при приймальних випробуваннях або при перевірках контролюючих органів.

Принцип нормативної обґрунтованості вимагає, щоб вибір кожного технічного рішення спирався на конкретний нормативний документ, що встановлює відповідну вимогу. Характеристики мережевого фільтра - клас захисту, коефіцієнт ослаблення, частотний діапазон - визначаються ТР ПЕМВН-95. Вимоги до системи заземлення - ДСТУ 3396.1-96 і ТР ЕОТ-95. Порядок документального оформлення - НД ТЗІ 3.7-003-23. Посилання на конкретні нормативні документи фіксуються в технічному завданні і є обов’язковими для підтвердження відповідності при приймальних випробуваннях.

Принцип сумісності з вимогами електробезпеки означає, що заходи ТЗІ не повинні суперечити вимогам безпеки персоналу і можуть реалізовуватися паралельно з заходами електробезпеки. На практиці вимоги ТЗІ і вимоги електробезпеки часто збігаються: виділений контур заземлення знижує і рівень паразитних струмів у системі заземлення (захист від витоку), і потенціал корпусів при пошкодженні ізоляції (захист персоналу). Мережевий фільтр захищає від

витоку інформативного сигналу в зовнішню мережу і водночас захищає чутливе обладнання від імпульсних перенапруг і завад з мережі.

2.10.2. Багаторівнева модель захисту: деталізація рівнів

Перший організаційний рівень включає: встановлення меж контрольованої зони (КЗ) і документальне фіксування всіх точок перетину інженерних комунікацій з межею КЗ; призначення відповідального за технічний захист інформації і розмежування ролей персоналу; розробку і затвердження регламенту допуску персоналу і сторонніх осіб; порядок проведення сервісних робіт на обладнанні і інженерних мережах; ведення журналу сервісних робіт і журналу змін конфігурації; інструктаж персоналу щодо ознак несанкціонованого технічного втручання.

Другий технічний пасивний рівень включає: встановлення мережевого фільтра на вводі живлення в КЗ і індивідуальних фільтрів на робочих місцях; організацію виділеного контуру заземлення за топологією «зірки»; прокладання кабелів в екранованих металевих коробах на ділянках виходу з КЗ; встановлення пристроїв гальванічної розв’язки на телефонних і сигнальних лініях; пломбування корпусів фільтрів, роз’ємів заземлення і кабельних гофрів.

Третій технічний активний рівень включає: встановлення генератора просторового зашумлення в приміщенні КЗ при недостатній ефективності пасивних засобів; підключення генератора лінійного зашумлення до ліній живлення і заземлення; налаштування параметрів шуму відповідно до спектральних характеристик інформативного сигналу об’єкта; забезпечення живлення генераторів від того самого джерела, що і захищуване обладнання.

Четвертий контрольний рівень включає: проведення планових спеціальних досліджень з вимірюванням рівнів сигналу в контрольних точках; позапланові дослідження після будь-яких змін конфігурації або сервісних подій; візуальний контроль пломб за встановленим графіком; аналіз журналів сервісних робіт на предмет несанкціонованих змін; архівування всіх протоколів і актів.

2.10.3. Взаємодія організаційних і технічних складових КСЗІ

Помилкою, що найчастіше зустрічається при побудові КСЗІ, є недооцінка організаційних складових на тлі розгорнутого переліку технічних засобів. Практика показує, що найдорожчий мережевий фільтр може бути нейтралізований, якщо сервісний технік безконтрольно підключає стороннє обладнання до тієї ж розетки під час обслуговування. Або якщо пломба на корпусі фільтра не перевіряється після кожного відвідування сервісного персоналу.

З іншого боку, виключно організаційні заходи без технічних рішень не здатні забезпечити захист від пасивного перехоплення. Навіть якщо доступ до приміщення строго регламентований, це не впливає на рівень інформативного сигналу в загальній мережі живлення будівлі, де зловмисник може підключитися без будь-якого проникнення на об’єкт.

Взаємодія двох складових реалізується через конкретні механізми. Технічні засоби захисту перебувають під організаційним контролем: стан мережевих фільтрів і пломб перевіряється за регламентом, зміни конфігурації фіксуються в журналі, доступ до технічних приміщень регламентований. Організаційні заходи підкріплюються технічними: пломби не лише фіксують факт несанкціонованого доступу, але й фізично ускладнюють його завдяки спеціальним конструктивним рішенням; контроль доступу до серверних і щитових кімнат реалізується замками і засобами контролю доступу.

2.11. Організаційні та режимні заходи захисту

Рисунок 3.1 – Організаційні заходи захисту інформації від витоку за рахунок електромагнітного випромінювання

2.11.1. Розмежування ролей і відповідальності

Ефективна організаційна складова КСЗІ починається з чіткого розмежування ролей між усіма учасниками процесу: власником (замовником) системи, адміністратором безпеки, користувачем і технічним персоналом. Кожна роль має строго визначені повноваження і зони відповідальності, що виключає як дублювання, так і прогалини в контролі.

Власник системи несе кінцеву відповідальність за стан захищеності і приймає рішення щодо складу та обсягу КСЗІ, затверджує технічне завдання, модель загроз і модель порушника, підписує акт введення системи в експлуатацію і звітні документи про стан захищеності. Власник також встановлює режим доступу до приміщення і визначає перелік осіб, уповноважених на прийняття рішень щодо зміни конфігурації системи.

Адміністратор безпеки здійснює поточний оперативний контроль стану КСЗІ. До його обов’язків належать: щомісячний огляд пломб і стану обладнання, ведення журналу контролю, погодження заявок на сервісні роботи, присутність при кожному відвідуванні сервісного персоналу, первинне розслідування виявлених інцидентів. Адміністратор безпеки не має права самостійно змінювати конфігурацію технічних засобів захисту - для цього потрібне рішення власника системи і залучення уповноваженого виконавця.

Користувач системи - оператор, що безпосередньо обробляє інформацію з обмеженим доступом - не має права вносити зміни в конфігурацію апаратного або програмного забезпечення, підключати зовнішні пристрої або носії без дозволу, залишати відкритими документи або виводити їх на екран у присутності неуповноважених осіб. Фіксований режим роботи оператора (строго визначений час початку і завершення роботи) дозволяє адміністратору безпеки ефективніше контролювати стан системи.

Технічний персонал, що здійснює обслуговування обладнання та інженерних систем, є найбільш ризиковою категорією з погляду технічного захисту. Кожен візит сервісного спеціаліста є потенційним вікном для встановлення закладного пристрою або несанкціонованої зміни конфігурації. Тому для технічного персоналу вводиться правило роботи лише за письмовою заявкою, у присутності адміністратора безпеки і з фіксацією всіх дій у журналі сервісних робіт.

2.11.2. Регламентування сервісних робіт

Регламент сервісних робіт є одним із найважливіших організаційних документів КСЗІ, оскільки саме у період проведення технічного обслуговування ризик реалізації загроз є максимальним. Типовий регламент включає такі елементи.

Порядок подачі і погодження заявки. Сервісна організація подає заявку на проведення робіт не пізніше, ніж за 24 години до запланованого візиту. Заявка містить: найменування і реєстраційні дані сервісної організації, прізвища і посади осіб, що проводитимуть роботи, перелік і номенклатуру обладнання, яке вноситься,

зміст і обсяг запланованих робіт, очікуваний час виконання. Заявка погоджується адміністратором безпеки і затверджується власником системи.

Процедура допуску. При прибутті сервісного персоналу адміністратор безпеки перевіряє документи і звіряє їх з переліком у заявці. Обладнання, що вноситься, реєструється в журналі доступу. Перед початком робіт адміністратор здійснює огляд поточного стану захисних засобів і фіксує показання в журналі контролю: стан пломб, відсутність нових або переставлених кабелів, цілісність корпусів обладнання.

Порядок проведення робіт. Сервісний персонал виконує роботи виключно в присутності адміністратора безпеки. Заборонено: залишати сервісний персонал наодинці в приміщенні, підключати принесене обладнання до мережі живлення або заземлення КЗ без дозволу адміністратора, виконувати роботи, що не передбачені погодженою заявкою. Будь-яка тимчасова зміна конфігурації (відключення фільтра, від’єднання заземлення) фіксується в журналі і обов’язково усувається до закінчення робіт.

Процедура завершення і відновлення. Після завершення сервісних робіт адміністратор безпеки перевіряє: відновлення всіх захисних засобів у вихідний стан, повернення конфігурації мережевих фільтрів і заземлення до вихідних значень, цілісність пломб (у разі необхідності - пломбування знову з фіксацією нових пломб у журналі), відсутність стороннього обладнання або провідників. За наявності сумнівів щодо стану системи адміністратор призначає позапланове вимірювання в контрольних точках.

2.11.3. Документальне забезпечення організаційних заходів

Документальне забезпечення організаційних заходів охоплює кілька обов’язкових документів, що разом утворюють доказову базу ефективності КСЗІ.

Журнал контролю стану КСЗІ ведеться адміністратором безпеки і містить записи про кожний огляд: дату, результати огляду пломб, виявлені невідповідності

і вжиті заходи. Журнал зберігається у захищеному від несанкціонованого доступу місці і передається наступному адміністратору безпеки при зміні посадової особи.

Журнал сервісних робіт фіксує кожне відвідування сервісного персоналу: дату і час, склад групи, реєстраційні дані сервісної організації, перелік виконаних робіт, стан системи до і після робіт, підписи адміністратора безпеки і старшого сервісного спеціаліста.

Журнал змін конфігурації ведеться при кожній зміні в схемах електроживлення, заземлення або кабельних трас: дата, опис зміни, причина зміни, виконавець, підтвердження уповноваженої особи. Будь-яка незафіксована зміна є підставою для позапланових спеціальних досліджень.

Журнал обліку і руху носіїв інформації фіксує всі дії з носіями, що містять інформацію з обмеженим доступом: реєстрацію нових носіїв, видачу в роботу і здавання, переміщення за межі КЗ і повернення, знищення носіїв з підтвердженням методу знищення.

Інструкції для персоналу розробляються для кожної ролі: оператора, адміністратора безпеки і технічного персоналу. Вони містять конкретний перелік дій у штатному режимі роботи і при виявленні нештатних ситуацій, включаючи порядок дій при виявленні ознак несанкціонованого технічного втручання.

ВИСНОВКИ ДО РОЗДІЛУ ІІ:

У другому розділі проведено аналіз середовища функціонування автоматизованої системи класу 1 та сформовано методологічні засади оцінювання її захищеності від витоку електричним каналом. На підставі розглянутого матеріалу можна зробити такі висновки.

По-перше, об'єкт інформаційної діяльності є складною сукупністю технічних засобів, інженерних мереж і організаційного середовища. Для коректного визначення загроз необхідно розглядати не лише основне обладнання (ТЗПІ), але й допоміжні технічні засоби (ДТЗС), а також усі провідники і конструкції, що виходять за межі контрольованої зони. Контрольована зона є визначальним

поняттям для вибору контрольних точок і для оцінки практичної реалістичності кожної загрози.

По-друге, електричний канал витоку формується через три основні механізми: ємнісні, індуктивні і гальванічні паразитні зв'язки. Розуміння цих механізмів є необхідною умовою для правильного вибору засобів захисту: ємнісні зв'язки усуваються просторовим розведенням кабелів і металевими коробами, індуктивні -перехрещенням трас і екрануванням, гальванічні - виділеними контурами заземлення і розділовими трансформаторами.

По-третє, ефективний захист від витоку передбачає обов'язкове обстеження об'єкта і проведення спеціальних досліджень з вимірюванням рівнів сигналів у контрольних точках. Лише кількісна оцінка захищеності на підставі інструментальних вимірювань і порівняння з нормативними значеннями ТР ПЕМВН-95 дозволяє обґрунтовано стверджувати, що система відповідає встановленим вимогам.

По-четверте, документальне забезпечення - акт обстеження, акт категоріювання, модель загроз, модель порушника, технічне завдання і протоколи спеціальних досліджень - є обов'язковою умовою легітимності КСЗІ. Відсутність або неповнота будь-якого з цих документів є підставою для відмови у введенні системи в штатну експлуатацію.

Результати аналізу, виконаного в другому розділі, є безпосередньою основою для проєктування системи захисту, що розглядається в третьому розділі роботи.

РОЗДІЛ ІІІ. СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ В АС КЛАСУ 1 ВІД ВИТОКУ ЕЛЕКТРИЧНИМ КАНАЛОМ

3.1. Фізична безпека і контроль доступу

Фізична безпека приміщення, де розміщена автоматизована система класу 1, є першою лінією захисту від будь-яких загроз, включаючи технічні канали витоку. Якщо зловмисник має фізичний доступ до приміщення або обладнання - жодна технічна система не може гарантувати повний захист.

Двері приміщення обладнуються замком підвищеної надійності або системою контролю доступу на основі ідентифікаційних карток. Список осіб, що мають право доступу, затверджується власником системи і регулярно переглядається. Вікна і технологічні отвори в зовнішніх стінах обладнуються відповідно до вимог фізичної безпеки.

Суміжні технічні приміщення - електрощитова, серверна кімната, кабельні шахти - мають власний режим доступу і не повинні бути доступні для персоналу, що не має відповідних повноважень. Навіть якщо ці приміщення знаходяться за межами КЗ, кабелі системи, що проходять через них, перебувають у зоні підвищеного ризику і потребують екранування в металевих коробах.

Охоронна сигналізація приміщення, якщо вона є, підключається таким чином, щоб її лінії не слугували потенційним каналом витоку. Для цього використовуються пристрої гальванічної розв’язки на виходах ліній сигналізації з КЗ або оптоволоконні лінії зв’язку замість металевих.

Особливу увагу слід приділити кутовим і транзитним кімнатам, через які проходять кабелі системи на шляху до електрощита або телефонного крос-боксу. Ці кімнати можуть мати нижчий рівень контролю доступу порівняно з основним приміщенням КЗ, що робить відрізки кабельних трас у них вразливими до безконтактного перехоплення. Металеві короби з пломбованими замками на таких ділянках є обов’язковими.

3.1. Технічні засоби захисту від витоку у ланцюгах електроживлення

3.1.1. Мережеві фільтри: принцип дії, класифікація і вибір

Мережевий фільтр є основним пасивним технічним засобом захисту від витоку інформативного сигналу у ланцюгах електроживлення. Він є LC-чотириполюсником, схема якого розрахована на максимальне ослаблення завад у заданому частотному діапазоні при мінімальному ослабленні напруги живлення промислової частоти 50 Гц. Основними елементами фільтра є індуктивності, що створюють високий опір для високочастотних складових, і ємності, що шунтують ці складові на корпус або землю.

Конструктивно мережевий фільтр для захисту від витоку ПЕМВН містить: синфазний дросель - двох- або чотирипровідну котушку, намотану на загальному феромагнітному осерді, що ефективно ослаблює синфазну завадову складову; конденсатори, підключені між кожним із провідників і корпусом (Y-конденсатори), що шунтують синфазну завадову складову на корпус; диференційні конденсатори, підключені між фазним і нульовим провідниками (X-конденсатори), що шунтують диференційну завадову складову; захисні варистори або розрядники для захисту від перенапруг.

Класифікація мережевих фільтрів для ТЗІ відповідно до ТР ПЕМВН-95 здійснюється за класами FP1 - FP3, де клас FP3 забезпечує найвищий рівень ослаблення. Вибір класу фільтра визначається результатами вимірювань рівня інформативного сигналу в контрольній точці і розраховується як різниця між виміряним і нормативно допустимим рівнями з урахуванням запасу захищеності.

При виборі мережевого фільтра, крім класу захисту, враховуються такі параметри: номінальний струм навантаження - фільтр повинен витримувати максимальний струм усіх підключених споживачів без перегріву і деградації характеристик; діапазон робочих частот - для сучасної цифрової техніки фільтр повинен ефективно ослаблювати завади в діапазоні від 10 кГц до не менше 300 МГц; допустима ємність між провідниками і корпусом - для систем з підвищеними

вимогами до витоку струму (медичне обладнання) Y-конденсатори обираються мінімальної ємності.

Встановлення мережевих фільтрів має свої вимоги щодо монтажу. Кабель від розподільчого щита до фільтра прокладається в металевому екранованому коробі або трубі, щоб виключити індуктивне наведення від цієї незахищеної ділянки. Корпус фільтра підключається до виділеного захисного заземлення через можливо коротший провідник великого перерізу. Відстань від фільтра до захищуваного обладнання також повинна бути мінімальною.

3.1.2. Розділові трансформатори і системи електродвигун-генератор

Розділовий трансформатор забезпечує гальванічне роз'єднання між захищеним і незахищеним сегментами мережі живлення. На відміну від мережевого фільтра, який ослаблює завади в певному частотному діапазоні, розділовий трансформатор повністю розриває постійний гальванічний шлях передачі сигналу між первинним і вторинним колами. Це означає, що будь-яка постійна складова і надзвичайно низькочастотні компоненти (нижче кількох герц) інформативного сигналу, що можуть «прослизати» крізь мережевий фільтр, повністю блокуються трансформатором.

Ємнісний зв'язок між обмотками трансформатора є обмежуючим чинником ефективності ізоляції на підвищених частотах. Для мінімізації цього ефекту застосовуються розділові трансформатори з екранованою обмоткою (екранований розділовий трансформатор, EPT): між первинною і вторинною обмотками розміщується заземлений металевий екран, що зменшує паразитну ємність між обмотками на порядок і більше.

Найбільш ефективною системою гальванічного роз'єднання є система «електродвигун-генератор». У ній живлення від зовнішньої мережі подається на електродвигун, який через механічне з'єднання приводить у рух генератор, що живить захищене обладнання. Оскільки вал між двигуном і генератором не є електричним провідником - будь-який сигнал, що є в мережі живлення двигуна, не

може безпосередньо проникнути в мережу генератора. На практиці залишається незначний акустичний і магнітний зв’язок через спільний корпус, але він суттєво менший за ємнісний зв’язок трансформатора. Система «електродвигун-генератор» є найкращим рішенням для об’єктів з максимальними вимогами до гальванічної ізоляції, проте потребує значних витрат на встановлення і обслуговування.

3.1.3. Фільтрація сигнальних і телефонних ліній

Телефонні та сигнальні лінії, що входять у приміщення КЗ, підлягають тому самому ретельному аналізу і захисту, що і лінії електроживлення. Ці лінії є потенційними каналами витоку з кількох причин: по-перше, вони можуть нести наведені інформативні сигнали від розташованого поруч обладнання; по-друге, при безпосередньому контактному підключенні зловмисника до лінії за межами КЗ він отримує доступ до всіх наведень у ній.

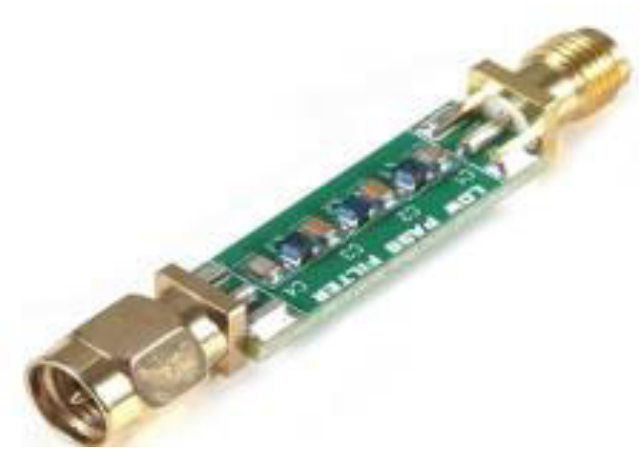

Рисунок 3.2 – Приклад фільтрувального модуля для захисту сигнальної лінії від інформативних наведень

Для захисту телефонних ліній застосовуються два підходи. Перший - встановлення спеціалізованих фільтрів у діапазоні частот, небезпечних для витоку ПЕМВН. Такий фільтр ослаблює всі складові вище певної граничної частоти (наприклад, 5–10 кГц), пропускаючи лише голосовий сигнал у смузі 300 Гц - 3,4 кГц. Другий підхід - встановлення трансформатора гальванічної розв’язки, що повністю ізолює лінію від обладнання по постійному струму і суттєво послаблює зв’язок на підвищених частотах.

Сигнальні лінії систем охоронної та пожежної сигналізації захищаються аналогічним чином, але з урахуванням того, що ці системи, як правило, передають цифрові або частотно-маніпульовані сигнали, а не голос. Для них застосовуються оптронні розв’язувачі, що забезпечують повну гальванічну ізоляцію і пропускають лише корисний сигнал у заданому форматі.

3.1.4. Генератори лінійного зашумлення

У випадках, коли пасивних засобів (фільтрів і гальванічної розв’язки) виявляється недостатньо для досягнення нормативного рівня захищеності в певній контрольній точці, застосовуються активні засоби - генератори лінійного зашумлення. Ці пристрої вводять широкосмуговий шумовий сигнал безпосередньо в лінію живлення або заземлення, знижуючи співвідношення сигнал/шум нижче нормативно допустимого рівня.

Принцип дії генератора лінійного зашумлення полягає у такому: генератор формує шумовий сигнал з рівномірним спектральним розподілом у заданому частотному діапазоні і через узгоджувальний трансформатор вводить його в лінію. Рівень введеного шуму підбирається таким чином, щоб він перевищував рівень інформативного сигналу на величину, достатню для невідтворюваності інформації.

Критично важливою є вимога синхронізації живлення генератора лінійного зашумлення з захищуваним обладнанням. Якщо генератор і обладнання живляться від різних джерел, завадовий сигнал і інформативний сигнал можуть мати різні фазові зсуви, що дозволить зловмиснику відфільтрувати завадовий сигнал. Тому живлення генератора підключається виключно після загального мережевого фільтра, з тієї самої виділеної групи, що і захищуване обладнання.

3.2. Захист за допомогою екранування і вдосконалення системи заземлення

3.2.1. Екранування кабельних трас і корпусів обладнання

Екранування є первинним методом захисту від ємнісного та індуктивного наведення на кабельні траси. Металевий екран навколо кабелю відповідно до теорії

електромагнітного екранування блокує електричне поле ззовні і відводить його в землю, а замкнений по периметру металевий екран ослаблює магнітне поле за рахунок наведення вихрових струмів.

Для кабельних трас, що виходять за межі КЗ або проходять через зони з нижчим рівнем контролю доступу, застосовуються металеві короби або труби зі суцільним заземленням. Металевий короб одночасно виконує дві функції: по-перше, він екранує кабелі, знижуючи рівень ПЕМВН від них; по-друге, він унеможливлює фізичний контакт сторонньої особи з кабелями без порушення цілісності короба, що виявляється при плановому огляді.

Вибір матеріалу і конструкції металевого короба залежить від вимог до рівня екранування. Для більшості об’єктів АС класу 1 достатньо сталевих листових коробів завтовшки 1,5–2 мм з фланцевими з’єднаннями між секціями, що забезпечують надійний електричний контакт. Для підвищених вимог застосовуються короби зі стальних листів, покритих міддю або латунню, або комбіновані конструкції з феромагнітного матеріалу зовні і немагнітного провідного матеріалу всередині - такі конструкції забезпечують ослаблення як електричного, так і магнітного поля.

Екранування корпусів обладнання є компетенцією виробника і зазвичай не може бути змінене в процесі експлуатації. Проте якщо специфікація обладнання не відповідає вимогам ТЗІ, воно може бути замінено на атестовані аналоги або розміщене в додатковому екрані. Для систем з максимальними вимогами до захисту використовуються спеціально розроблені або атестовані ЕОМ, що пройшли спеціальні дослідження на рівень ПЕМВН.

3.2.2. Гальванічна розв’язка зовнішніх ліній

Гальванічна розв’язка є найбільш ефективним засобом захисту від витоку через зовнішні лінії, оскільки вона повністю розриває провідниковий шлях між захищеним і незахищеним середовищем. Для її реалізації застосовуються два типи пристроїв: оптоелектронні розв’язувачі (оптрони) і трансформаторні розв’язувачі.

Оптоелектронний розв’язувач перетворює електричний сигнал на вході в оптичний, передає його оптичним каналом і знову перетворює на електричний на виході. Між вхідним і вихідним колами відсутній будь-який електричний зв’язок, а ємнісний зв’язок через оптичне середовище є ненабагато нижчим, ніж у трансформатора. Недоліком є обмеження смуги пропускання і необхідність живлення електронних елементів з обох боків розв’язки.

Трансформаторний розв’язувач передає сигнал через магнітний зв’язок між первинною і вторинною обмотками. Він добре підходить для аналогових сигналів (наприклад, телефонного голосового сигналу) і забезпечує природний частотний фільтр, ослаблюючи складові вище резонансної частоти трансформатора. Для підвищення ефективності ізоляції між обмотками розміщується заземлений електростатичний екран.

Рівень ослаблення пристрою гальванічної розв’язки вимірюється в тих самих одиницях, що і для мережевих фільтрів - у децибелах. Відповідно до вимог ТЗІ, для телефонних і сигнальних ліній необхідний рівень ослаблення зазвичай становить не менше 60 дБ у відповідному частотному діапазоні.

Після встановлення пристрою гальванічної розв’язки обов’язково перевіряється якість передачі корисного сигналу, щоб переконатися, що захисний пристрій не спотворює його до неприйнятного рівня. Для телефонної лінії - перевіряється якість голосового зв’язку, для ліній сигналізації - надійність передачі командних сигналів у всіх передбачених режимах роботи.

3.2.3. Побудова виділеного контуру заземлення

Система заземлення є однією з найбільш вразливих частин інфраструктури об’єкта з погляду витоку інформації. Причина полягає в тому, що шина заземлення в типовій будівлі з’єднана з великою кількістю металевих конструкцій (арматура, трубопроводи, елементи конструкцій кріплення) і доступна у багатьох точках за межами КЗ. Будь-які паразитні струми, що потрапляють у шину заземлення, розтікаються всією цією системою і можуть бути зняті в несподіваних місцях.

Виділений контур заземлення вирішує цю проблему, забезпечуючи окремий шлях заземлення для захищеного обладнання, що не має жодного електричного зв'язку з системою заземлення будівлі і природними заземлювачами. Виділений заземлювач - звичайно сталевий стрижень або сітка з сталевого дроту - вбивається або закопується в ґрунт на відстані від фундаменту будівлі, що виключає контакт між ним і арматурою фундаменту.

Провідники від виділеного заземлювача до шини заземлення обладнання прокладаються в металевих трубах або коробах, що додатково захищає їх від несанкціонованого підключення. Від шини заземлення до кожного елемента обладнання проводяться окремі провідники за топологією «зірки» - коли всі провідники з'єднуються в одній точці (шині). Ця топологія виключає замкнені контури заземлення, в яких можуть циркулювати паразитні струми.

Опір розтікання виділеного контуру заземлення вимірюється і підтверджується в протоколі спеціальних досліджень. Нормативне значення опору залежить від категорії об'єкта і, як правило, не перевищує 4-10 Ом для об'єктів першої і другої категорій. Якщо питомий опір ґрунту в місці встановлення заземлювача є надто високим, вживаються заходи для його зниження: збільшення площі заземлювача, застосування добавок для зниження опору ґрунту, горизонтальне прокладання смуг заземлення.

3.2.4. Просторове зашумлення: принципи і засоби

Система просторового зашумлення є активним засобом захисту, що доповнює пасивні засоби в тих випадках, коли вони не забезпечують нормативного рівня захищеності. Принцип її дії полягає в тому, що генератор шуму формує широкосмуговий електромагнітний шум у приміщенні КЗ, маскуючи ПЕМВН від обладнання і роблячи неможливим їх перехоплення ззовні.

Система просторового зашумлення складається з трьох основних компонентів. Генератор шуму - електронний пристрій, що формує широкосмуговий шумовий сигнал у визначеному частотному діапазоні. Система антен - рамкові

антени або відрізки дроту, що підключаються до генератора і випромінюють шумовий сигнал у приміщенні. Пульт контролю - пристрій, що дозволяє контролювати справність генератора і рівень шуму в приміщенні.

Ефективність системи просторового зашумлення суттєво залежить від рівномірності розподілу шумового поля в приміщенні. При встановленні антенної системи необхідно врахувати геометрію приміщення і розташування обладнання, щоб уникнути «мертвих зон» з недостатнім рівнем шуму. Для невеликих приміщень одна рамкова антена, встановлена в центрі, зазвичай забезпечує достатню рівномірність. Для більших приміщень або при складній геометрії може знадобитися кілька антен.

Вимоги до шумового сигналу визначаються критерієм максимальної ентропії: сигнал повинен мати рівномірний розподіл ймовірності амплітуди і плоский спектр у робочому діапазоні частот. Детермінований сигнал (наприклад, пилкоподібний або синусоїдальний) не підходить для зашумлення, оскільки може бути ідентифікований і відфільтрований. Оптимальним є гаусівський шум, що має максимальну ентропію при заданій потужності.

3.3. Практична реалізація системи захисту інформації в АС-1

3.3.1. Генератор просторового зашумлення БАЗАЛЬТ-5ГЕШ

Генератор просторового зашумлення БАЗАЛЬТ-5ГЕШ є сертифікованим вітчизняним засобом ТЗІ, призначеним для формування широкосмугового електромагнітного шуму в захищених приміщеннях з метою маскування ПЕМВН від засобів обчислювальної техніки. Пристрій відповідає вимогам чинних нормативних документів у сфері технічного захисту інформації і може застосовуватися в системах захисту інформації, де обробляється конфіденційна інформація і державна таємниця, мають сертифікат відповідності Держспецзв'язку.

Рисунок 3.3 – Приклад генератора просторового зашумлення для маскування побічних електромагнітних випромінювань

Таблиця 3.1 – порівняльна таблиця засобів захисту

Критерій	**БАЗАЛЬТ-5ГЕШ**	**ГШ-1000М**	**ГРОМ-ЗІ-4**
Діапазон, МГц	0,1–1000	0,01–1000	0,1–2000
Потужність, Вт	15	20	12
Сертифікат ТЗІ	Так	Так	Так
Вартість	Середня	Висока	Висока

Обрано БАЗАЛЬТ-5ГЕШ як оптимальний за співвідношенням ціна/характеристики для об'єктів першої категорії.

Технічні характеристики БАЗАЛЬТ-5ГЕШ включають: робочий частотний діапазон від 0,1 МГц до 1000 МГц; рівень шумового поля в приміщенні не менше нормативно необхідного з урахуванням вимог ТР ПЕМВН-95; живлення від мережі 220 В / 50 Гц з потужністю споживання не більше 15 Вт; масогабаритні характеристики, що дозволяють настільне або стінове встановлення.

Монтаж БАЗАЛЬТ-5ГЕШ здійснюється уповноваженою організацією з ліцензією у сфері ТЗІ відповідно до керівництва з експлуатації. Генератор розміщується в центральній зоні захищеного приміщення, антенна система (рамкові антени або відрізки дроту) встановлюється на стінах або стелі. Після встановлення

проводиться контрольне вимірювання рівня шуму в характерних точках приміщення і на виході ліній, що виходять за межі КЗ.

Живлення БАЗАЛЬТ-5ГЕШ підключається від тієї самої мережі, що і захищуване обладнання, - після загального мережевого фільтра. Це забезпечує синхронізацію роботи генератора з обладнанням і виключає ситуацію, коли генератор вимкнений, а обладнання продовжує працювати без захисту. При використанні джерела безперебійного живлення (ДБЖ) для захищуваного обладнання БАЗАЛЬТ-5ГЕШ також підключається до ДБЖ.

3.3.2. Засіб лінійного зашумлення DELTA-7

Засіб лінійного зашумлення DELTA-7 призначений для введення широкосмугового шумового сигналу безпосередньо в лінії електроживлення і заземлення, забезпечуючи зниження рівня інформативного сигналу в них до нормативно допустимого значення. На відміну від генератора просторового зашумлення, що формує шум у вільному просторі, DELTA-7 діє безпосередньо в провідниковому середовищі.

Рисунок 3.4 – Приклад засобу лінійного зашумлення для введення шумового сигналу в провідникові лінії

Принцип роботи DELTA-7 полягає у такому: генератор шуму формує сигнал з рівномірним спектральним розподілом у визначеному частотному діапазоні, після чого через узгоджувальний трансформатор вводить його в лінію живлення і/або лінію заземлення. Введений шумовий сигнал накладається на інформативний, підвищуючи рівень шуму в лінії до значення, при якому виокремлення інформативної складової є неможливим.

Підключення DELTA-7 здійснюється в точці, найближчій до виходу захищеного сегмента мережі за межі КЗ. Для лінії живлення це може бути точка підключення загального мережевого фільтра з боку зовнішньої мережі; для лінії заземлення - точка підключення виділеного захисного заземлення до шини заземлення.

3.3.3. Розділовий трансформатор і фільтр низьких частот

Розділовий трансформатор у складі системи захисту АС-1 виконує подвійну функцію: забезпечує гальванічну ізоляцію захищеного сегмента мережі живлення від зовнішньої мережі і природно ослаблює передачу завад на підвищених частотах. Для максимальної ефективності трансформатор встановлюється якнайближче до захищуваного обладнання, мінімізуючи довжину ділянки від трансформатора до обладнання, що залишається не ізольованою.

Фільтр низьких частот встановлюється паралельно з розділовим трансформатором або між виходом трансформатора і навантаженням. Його функція - додатково пригнічувати складові завад, що проникають через ємнісний зв’язок між обмотками трансформатора, і забезпечувати нормоване ослаблення у всьому робочому частотному діапазоні.

Поєднання розділового трансформатора і фільтра низьких частот дає синергетичний ефект: трансформатор забезпечує гальванічну ізоляцію і пригнічує низькочастотні завади, фільтр - забезпечує нормоване ослаблення у широкому частотному діапазоні, включаючи ті частоти, де ємнісний зв’язок між обмотками трансформатора залишається значущим.

3.3.4. Комплексна схема захисту і порядок підключення

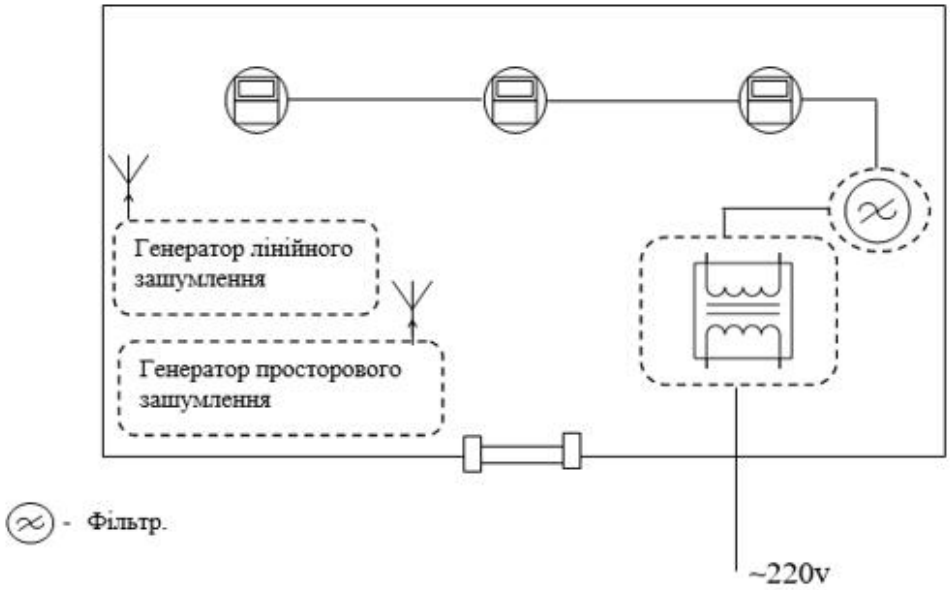

Рисунок 3.5 – Узагальнена схема підключення засобів зашумлення, фільтрації та живлення захищеної АС-1

Комплексна схема захисту АС-1 від витоку електричним каналом реалізується шляхом послідовного з’єднання технічних засобів таким чином, щоб кожен з них вирішував конкретну задачу захисту в своїй ланці.

На вводі живлення в КЗ встановлюється стаціонарний мережевий фільтр класу FP3, що ослаблює синфазні і диференційні завади між зовнішньою мережею і захищеним сегментом. Фільтр підключається до виділеного захисного заземлення. Від фільтра живлення підводиться до розділового трансформатора, що забезпечує додаткову гальванічну ізоляцію. Від виходу трансформатора через фільтр низьких частот живлення розводиться до робочих місць.

На кожному робочому місці встановлюється індивідуальний фільтр-подовжувач класу FP2, підключений до виділеного заземлення. Усі кабельні траси від обладнання до місць виходу за межі КЗ прокладені в металевих коробах з суцільним заземленням. На виходах телефонної і сигнальної ліній встановлено пристрої гальванічної розв’язки. У приміщенні КЗ встановлено генератор

просторового зашумлення БАЗАЛЬТ-5ГЕШ і засіб лінійного зашумлення DELTA-7. Усі металеві корпуси засобів захисту, короби і заземлювачі підключені до єдиної шини виділеного захисного заземлення. Шина виділеного захисного заземлення не має електричного зв'язку з шиною заземлення будівлі і природними заземлювачами. Живлення генераторів зашумлення підключене після загального мережевого фільтра, від тієї самої мережі, що і захищуване обладнання.

3.4. Контроль ефективності і підтримання захищеності

3.4.1. Планові спеціальні дослідження

Планові спеціальні дослідження є обов'язковою складовою системи підтримання захищеності і служать для документального підтвердження того, що досягнутий рівень захищеності зберігається протягом усього терміну експлуатації АС. Без регулярного підтвердження неможливо стверджувати, що стан системи захисту відповідає вимогам нормативних документів, оскільки з часом відбувається деградація компонентів, можуть виникати нові канали витоку внаслідок змін у конфігурації і появи нових загроз.

Періодичність планових спеціальних досліджень встановлюється в технічному завданні і, як правило, становить один раз на рік для систем зі стабільною конфігурацією. Якщо за рік відбулися суттєві зміни в складі обладнання або конфігурації інженерних систем, позапланові дослідження призначаються відразу після відповідних змін. У будь-якому разі, максимальний інтервал між дослідженнями не повинен перевищувати двох років, навіть якщо за цей час не відбулося жодних видимих змін.

Програма планових спеціальних досліджень охоплює всі контрольні точки, що були включені до первинного переліку при введенні системи в експлуатацію, а також будь-які нові точки, що виникли внаслідок зміни конфігурації. Для кожної точки виконуються вимірювання рівня інформативного сигналу і рівня шуму в режимі максимального навантаження обладнання, що дозволяє розрахувати фактичне значення СШ і порівняти його з нормативним.

3.4.2. Методика вимірювань у контрольних точках

Вимірювання рівня інформативного сигналу виконуються за методикою, що регламентована ТР ПЕМВН-95. Основним вимірювальним приладом є аналізатор спектра, що дозволяє визначити спектральний склад сигналу в точці вимірювання і виявити всі інформативні складові в широкому частотному діапазоні. Для підключення аналізатора до точки вимірювання застосовуються відповідні датчики: токові кліщі або узгоджувальний трансформатор для вимірювання в ланцюгах живлення і заземлення, антени відповідного типу - для вимірювання електромагнітного поля.

Вимірювання проводяться у двох режимах: в режимі максимального навантаження обладнання (для визначення рівня інформативного сигналу) і в режимі вимкненого обладнання (для визначення рівня власного шуму мережі). Різниця між виміряними значеннями дає рівень інформативного сигналу. Рівень власного шуму є важливим параметром, оскільки він визначає, наскільки легко зловмисник може виокремити інформативний сигнал на тлі завад у мережі.

Для забезпечення відтворюваності результатів вимірювань необхідно дотримуватися однакових умов: один і той самий вид навантаження обладнання (той самий набір запущених програм, той самий обсяг даних, що обробляються), та сама точка підключення вимірювального датчика, той самий тип датчика з відомими метрологічними характеристиками. Застосовуваний аналізатор спектра повинен мати метрологічну атестацію і перебувати в межах дійсного терміну перевірки.

Отримані результати заносяться в протокол спеціальних досліджень із зазначенням: дати і умов вимірювань, найменування і реєстраційних даних вимірювального обладнання, терміну дійсності метрологічної перевірки, схеми контрольних точок, виміряних значень у кожній точці, нормативно допустимих значень і висновку про відповідність.

3.4.3. Перевірка мережевих фільтрів і засобів гальванічної розв’язки

Стан мережевих фільтрів потребує регулярного контролю, оскільки їх компоненти - особливо конденсатори і варистори - мають обмежений ресурс і деградують з часом під дією напруги, температури і струмових навантажень. Ознаками деградації конденсаторів є зменшення їх ємності, зростання тангенса кута діелектричних втрат і зниження напруги пробою. Все це призводить до зменшення коефіцієнта ослаблення і погіршення характеристик фільтра.

Контроль стану мережевих фільтрів включає два аспекти: візуальний огляд і інструментальне вимірювання. Візуальний огляд проводиться при кожному плановому огляді КСЗІ і включає перевірку цілісності корпусу фільтра, наявності і цілісності пломб, надійності підключення провідників, відсутності слідів перегріву, опіків або механічних пошкоджень. Інструментальне вимірювання коефіцієнта ослаблення на контрольних частотах проводиться не рідше одного разу на рік і обов’язково після будь-яких підозрілих подій.

Методика вимірювання коефіцієнта ослаблення мережевого фільтра полягає в подачі на його вхід каліброваного сигналу від генератора і вимірюванні рівня сигналу на виході фільтра. Коефіцієнт ослаблення K дорівнює відношенню рівнів вхідного і вихідного сигналів, виражений у децибелах: $K = 20 \cdot \lg(U_{вх} / U_{вих})$. Вимірювання виконуються на всіх нормованих частотах у межах робочого діапазону фільтра. Якщо виміряний коефіцієнт ослаблення менший за нормативний хоча б на одній з частот -фільтр потребує заміни.

Пристрої гальванічної розв’язки контролюються вимірюванням рівня сигналу на виході лінії при наявності тестового сигналу на вході. Якість голосового зв’язку через телефонний розв’язувач перевіряється прослуховуванням. Для цифрових розв’язувачів контролюється цілісність передачі стандартних тестових послідовностей.

3.4.4. Аналіз інцидентів і коригувальні заходи

Кожна аномальна подія, виявлена в процесі планового або позапланового огляду, підлягає документуванню і аналізу. Аномальними подіями є: порушення цілісності пломби; виявлення нового або зміненого кабелю, що не відповідає затвердженій схемі; присутність стороннього обладнання або пристрою; результати вимірювань, що виходять за межі нормативних значень.

Процедура розслідування інциденту починається з фіксації всіх ознак у письмовому акті з приблизним зазначенням часу виникнення (на підставі дати останнього огляду, що не виявив аномалій) і опису виявлених порушень. Якщо виявлено сторонній пристрій - він фотографується, описується і вилучається з максимальним збереженням ознак. Обладнання АС відключається від мережі до завершення розслідування.

Після розслідування і усунення причини інциденту виконується позапланове спеціальне дослідження для підтвердження відновлення нормативного рівня захищеності. За результатами складається акт, що включає опис інциденту, встановлені причини, вжиті заходи і результати контрольних вимірювань.

Практика систематичного аналізу інцидентів дає цінну інформацію про ефективність системи захисту і дозволяє виявляти повторювані закономірності, що можуть вказувати на системні вразливості. Наприклад, якщо протягом року двічі виявлялося порушення пломби на одному і тому самому вузлі - це свідчить про недостатню ефективність режиму контролю доступу або про необхідність більш захищеного конструктивного рішення для цього вузла.

3.5. Розрахункова оцінка ефективності захисних рішень

3.5.1. Розрахунок необхідного ослаблення мережевого фільтра

Розрахунок необхідного коефіцієнта ослаблення мережевого фільтра є ключовим кількісним обґрунтуванням технічного рішення, що включається до технічного завдання. Він базується на результатах вимірювань рівня

інформативного сигналу в контрольній точці і нормативних значеннях допустимого рівня для відповідної категорії об’єкта.

Вихідні дані для розрахунку: - виміряний рівень інформативного сигналу у контрольній точці (ввід живлення) до встановлення засобів захисту: US = 68 дБмкВ; - нормативно допустимий рівень сигналу відповідно до ТР ПЕМВН-95 для об’єктів першої категорії: Uнорм = 30 дБмкВ; - заданий запас захищеності: ΔK = 10 дБ.

Необхідний коефіцієнт ослаблення фільтра: KA = US – Uнорм + ΔK = 68 – 30 + 10 = 48 дБ.

Для вибору фільтра обираємо стаціонарний мережевий фільтр класу FP3, що забезпечує коефіцієнт ослаблення не менше 60 дБ у діапазоні від 10 кГц до 300 МГц. Фактичний запас захищеності після встановлення фільтра: ΔKфакт = 60 – 48 = 12 дБ.

Ця величина перевищує мінімально необхідний запас 10 дБ, що підтверджує правильність вибору фільтра. Фактичний рівень сигналу після встановлення фільтра: Uфакт = US – K = 68 – 60 = 8 дБмкВ.

Це значення значно нижче нормативного рівня 30 дБмкВ, що забезпечує запас захищеності: ΔK = 30 – 8 = 22 дБ.

3.5.2. Оцінка ефективності виділеного контуру заземлення

Для оцінки ефективності заходів щодо вдосконалення системи заземлення виконуються вимірювання рівня інформативного сигналу в точці заземлення до і після встановлення виділеного контуру і відключення природних заземлювачів.

Вихідні дані: - рівень сигналу в точці заземлення до вдосконалення (при наявності зв’язку з природними заземлювачами): US_з = 42 дБмкВ; - нормативно допустимий рівень: Uнорм = 30 дБмкВ; - рівень сигналу після встановлення виділеного контуру: US_з_після = 18 дБмкВ.

Досягнуте ослаблення: ΔUS = 42 – 18 = 24 дБ. Запас захищеності: ΔK = 30 – 18 = 12 дБ.

Виміряний опір виділеного контуру заземлення: RK = 4,2 Ом, що відповідає нормативним вимогам. Нормативний опір для об’єктів першої категорії - не більше 10 Ом.

Результати підтверджують, що встановлення виділеного контуру заземлення є ефективним заходом, що забезпечує нормативний рівень захищеності із запасом 12 дБ.

3.5.3. Оцінка ефективності пристрою гальванічної розв’язки телефонної лінії

Вимірювання виконуються на виході телефонної лінії за межами КЗ до і після встановлення оптронного розв’язувача.

Вихідні дані: - рівень інформативного сигналу на виході телефонної лінії до встановлення розв’язувача: US_тел = 35 дБмкВ; - рівень сигналу після встановлення оптронного розв’язувача: US_тел_після = 8 дБмкВ; - нормативно допустимий рівень: Uнорм = 30 дБмкВ.

Досягнуте ослаблення: K = 35 – 8 = 27 дБ. Запас захищеності: ΔK = 30 – 8 = 22 дБ.

Після встановлення пристрою гальванічної розв’язки перевірена якість голосового зв’язку у телефонній лінії: якість відповідає нормам для телефонного зв’язку, що підтверджує сумісність засобу захисту з функціонуванням лінії зв’язку. функціональним призначенням лінії.

3.5.4. Зведена оцінка залишкового ризику

Зведена оцінка залишкового ризику виконується після впровадження всіх передбачених заходів захисту і показує, чи залишаються технічні канали витоку після фільтрації, гальванічної розв’язки, екранування, виділеного заземлення та зашумлення. На цьому етапі оцінюється не окремий засіб захисту, а сукупний результат роботи всієї системи.

Критеріями оцінювання є фактичний рівень інформативного сигналу після захисту, величина запасу відносно нормативного рівня та можливість погіршення

параметрів під час експлуатації. Якщо фактичний рівень сигналу нижчий за нормативний, а запас захищеності становить не менше 10 дБ, ризик вважається допустимим. Якщо запас мінімальний, контрольна точка потребує посиленого регламентного контролю.

Таблиця 3.2 – Зведена оцінка залишкового ризику витоку інформації електричним каналом

Контрольна точка	**До захисту, дБмкВ**	**Після захисту, дБмкВ**	**Ослаблення, дБ**	**Норма, дБмкВ**	**Запас, дБ**	**Оцінка ризику**
Ввід живлення	68	8	60	30	22	Низький
Вузол заземлення	42	18	24	30	12	Допустимий, потребує контролю
Телефонна лінія	35	8	27	30	22	Низький
Кабель LAN	33	12	21	30	18	Низький
Суміжна траса	31	15	16	30	15	Низький

З таблиці 3.2 видно, що в усіх п’яти контрольних точках фактичний рівень інформативного сигналу після впровадження засобів захисту є нижчим за нормативне значення 30 дБмкВ. Запас захищеності становить від 12 до 22 дБ, тобто перевищує мінімально необхідний запас 10 дБ. Це підтверджує достатність запропонованої системи захисту для зниження ризику витоку електричним каналом до допустимого рівня.

Найменший запас зафіксовано у вузлі заземлення - 12 дБ. Саме ця точка є найбільш чутливою до експлуатаційних змін, оскільки її параметри можуть погіршуватися через ослаблення контактів, корозію з’єднань, зміну опору ґрунту або несанкціоноване підключення до шини заземлення. Тому для вузла заземлення

залишковий ризик визначено як допустимий, але такий, що потребує посиленого контролю.

Для вводу живлення, телефонної лінії, кабелю LAN і суміжної траси залишковий ризик оцінюється як низький. У цих точках запас захищеності є достатнім, а використані засоби мають взаємодоповнювальний характер: мережеві фільтри знижують рівень сигналу в ланцюгах живлення, гальванічна розв'язка розриває провідниковий шлях поширення, екранування зменшує наведення на суміжні траси, а організаційні заходи обмежують доступ до критичних ділянок.

Отже, загальний залишковий ризик витоку інформації електричним каналом оцінюється як допустимий. Його підтримання на прийнятному рівні забезпечується щорічними спеціальними дослідженнями, періодичною перевіркою мережевих фільтрів і засобів гальванічної розв'язки, контролем опору виділеного контуру заземлення, оглядом пломб, веденням журналів сервісних робіт і проведенням позапланових вимірювань після будь-якої зміни конфігурації системи.

3.6. Порядок введення системи захисту в експлуатацію і подальший моніторинг

3.6.1. Підготовчий і монтажний етапи

Введення системи захисту в експлуатацію відбувається поетапно, відповідно до затвердженого плану впровадження. Підготовчий етап передбачає перевірку наявності та актуальності всієї вихідної документації: акта обстеження об'єкта, акта категоріювання, технічного завдання і схем електроживлення та заземлення. Уточнюється перелік необхідних засобів захисту, їх технічні характеристики і розміщення. Готується проектна документація на монтажні роботи, визначаються відповідальні виконавці і терміни.

Монтажно-інженерний етап включає виконання всіх будівельно-монтажних робіт: встановлення мережевих фільтрів, прокладання металевих кабельних коробів, монтаж виділеного контуру заземлення, встановлення пристроїв гальванічної розв'язки і генераторів зашумлення. Усі роботи виконуються

відповідно до проектної документації кваліфікованим персоналом уповноваженої організації в присутності відповідального представника замовника. Після завершення монтажу складаються виконавча документація і акт прихованих робіт.

Після монтажу технічних засобів актуалізуються організаційні документи: інструкції для персоналу, регламент контролю і журнали обліку. Персонал ознайомлюється з оновленими документами під підпис і проходить інструктаж щодо правил роботи з системою захисту та порядку дій при виявленні нештатних ситуацій.

3.6.2. Контрольний і приймальний етапи

Контрольний етап включає проведення вимірювань у всіх контрольних точках відповідно до програми спеціальних досліджень. Результати порівнюються з нормативними значеннями і фіксуються в протоколах. При виявленні точок, де нормативні значення не досягнуто, виконується аналіз причин, коригування технічних рішень і повторне вимірювання.

Приймальний етап - фінальна стадія введення системи в експлуатацію. Приймальна комісія перевіряє відповідність встановлених засобів захисту вимогам технічного завдання, стан документації, результати вимірювань і підтверджує відповідність всіх показників нормативним вимогам. За позитивними результатами комісія підписує акт введення системи в штатну експлуатацію. З моменту підписання акта система може використовуватися для обробки інформації обмеженого доступу.

3.6.3. Експлуатаційний моніторинг і регламентний контроль

Після введення системи в експлуатацію захищеність підтримується виконанням регламентного контролю. Щомісячно адміністратор безпеки здійснює візуальний огляд стану пломб, кабельних трас і корпусів обладнання, перевіряє журнали і фіксує результати в журналі контролю. Щоквартально проводиться поглиблена перевірка мережевих фільтрів (візуальний огляд і вибіркові вимірювання коефіцієнта ослаблення) і стану виділеного заземлення (вимірювання

опору розтікання). Щорічно виконуються спеціальні дослідження в повному обсязі з вимірюванням у всіх контрольних точках.

Будь-яка подія, що може вплинути на стан захисту, є підставою для позапланових заходів. До таких подій належать: сервісні роботи на обладнанні або інженерних системах, заміна або додавання обладнання, зміна конфігурації мережі, виявлені інциденти. Після кожної такої події адміністратор безпеки оцінює необхідність позапланового огляду або вимірювань.

Щорічний звіт про стан захищеності системи складається адміністратором безпеки і підписується власником системи. Звіт містить: результати планових спеціальних досліджень, дані про виявлені інциденти і вжиті заходи, оцінку залишкового ризику, рекомендації щодо вдосконалення системи захисту. Цей звіт є основою для прийняття рішень щодо модернізації або розширення КСЗІ у наступному році.

ВИСНОВКИ ДО РОЗДІЛУ ІІІ:

Третій розділ дипломної роботи присвячено розробленню і обґрунтуванню комплексної системи захисту інформації в автоматизованій системі класу 1 від витоку електричним каналом. На підставі теоретичного аналізу і практичних розрахунків зроблено такі висновки.

По-перше, ефективна система захисту від витоку електричним каналом будується за принципом багаторівневого захисту з поєднанням організаційних, технічних пасивних і технічних активних засобів. Жоден із цих рівнів окремо не може забезпечити нормативного рівня захищеності, однак їх взаємодоповнення дозволяє досягти необхідного результату навіть при використанні відносно простих і доступних засобів.

По-друге, організаційні заходи є критичною складовою КСЗІ, що забезпечує ефективність технічних засобів. Регламент сервісних робіт, контроль доступу, пломбування і регулярний огляд захищають технічні засоби від несанкціонованих змін і дозволяють своєчасно виявляти інциденти. Без організаційних заходів

технічні засоби захисту можуть бути нейтралізовані сервісним персоналом або внутрішнім порушником.

По-третє, вибір технічних засобів - мережевих фільтрів, засобів гальванічної розв'язки і генераторів зашумлення - здійснюється на основі результатів інструментальних вимірювань і розрахунку необхідного ослаблення для кожного каналу витоку окремо. Цей підхід виключає як надлишкові витрати на надмірно потужні засоби, так і ризик вибору недостатніх засобів через неправильну оцінку рівня загрози.

По-четверте, система контролю і підтримання захищеності - планові спеціальні дослідження, перевірка фільтрів, аналіз інцидентів - забезпечує довгострокову ефективність КСЗІ протягом усього терміну експлуатації. Деградація компонентів і зміни конфігурації можуть знижувати рівень захищеності з часом, тому регулярний контроль є не формальністю, а реальним інструментом підтримання безпеки.

По-п'яте, розрахункова оцінка ефективності підтверджує, що запропонований комплекс засобів - стаціонарний фільтр FP3 на вводі живлення, виділений контур заземлення, оптронна розв'язка телефонної лінії, екрановані короби для кабельних трас - забезпечує нормативний рівень захищеності в усіх п'яти контрольних точках із запасом від 12 до 22 дБ, що відповідає вимогам ТР ПЕМВН-95 для об'єктів першої категорії.

Отримані результати є підставою для формування практичного проєктного рішення та подальшого впровадження запропонованої системи захисту.

ВИСНОВКИ:

У кваліфікаційній роботі досліджено питання захисту інформації в автоматизованій системі класу 1 від витоку електричним каналом. Проаналізовано нормативно-правову базу технічного захисту інформації, визначено основні загрози, джерела небезпечних сигналів, фізичні механізми формування електричного каналу витоку та особливості його реалізації через лінії електроживлення, заземлення, сигнальні й комунікаційні провідники.

На основі проведеного аналізу розроблено модель загроз і модель порушника, визначено контрольні точки для оцінювання захищеності та обґрунтовано комплекс організаційних і технічних заходів захисту. Запропонована система передбачає використання мережевих фільтрів, розділового трансформатора, гальванічної розв’язки зовнішніх ліній, екранування кабельних трас, виділеного контуру заземлення, а також засобів просторового та лінійного зашумлення.

Розрахункова оцінка ефективності підтвердила доцільність запропонованих рішень, оскільки їх застосування забезпечує зменшення рівня інформативних сигналів до нормативно допустимих значень і знижує залишковий ризик витоку інформації. Отримані результати можуть бути використані під час проєктування, модернізації та експлуатаційного контролю КСЗІ на об’єктах, де обробляється інформація з обмеженим доступом.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України.

2. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України.

3. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України.

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України.

5. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX // База даних «Законодавство України» / Верховна Рада України.

6. Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем : Постанова Кабінету Міністрів України від 29.03.2006 № 373 // База даних «Законодавство України» / Верховна Рада України.

7. Про затвердження Положення про державну експертизу у сфері технічного захисту інформації : наказ Адміністрації Держспецзв'язку від 16.05.2007 № 93, зареєстрований у Міністерстві юстиції України 16.07.2007 за № 820/14087.

8. НД ТЗІ 3.7-003-23. Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі : затверджено наказом Адміністрації Держспецзв'язку від 28.10.2023 № 924.

9. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Київ : Держстандарт України, 1997.

10. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 № 1229/99 // База даних «Законодавство України» / Верховна Рада України.

11. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Київ : Держстандарт України, 1997.

12. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII // База даних «Законодавство України» / Верховна Рада України.

13. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу : затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

14. Про Положення про порядок здійснення криптографічного захисту інформації в Україні : Указ Президента України від 22.05.1998 № 505/98 // База даних «Законодавство України» / Верховна Рада України.

15. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

16. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу : затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

17. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу : затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

18. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі : затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 53.

19. НД ТЗІ 1.6-005-2013. Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці : затверджено наказом Адміністрації Держспецзв’язку від 15.04.2013 № 215.

20. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі : затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

21. ТР ПЕМВН-95. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок : затверджено наказом Державної служби України з питань технічного захисту інформації від 09.06.1995 № 25 ; із змінами згідно з наказом Адміністрації Держспецзв’язку від 03.11.2011 № 93/ДСК.

22. ТР ЕОТ-95. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок : затверджено наказом Державної служби України з питань технічного захисту інформації від 09.06.1995 № 25 ; із змінами згідно з наказом Адміністрації Держспецзв’язку від 03.11.2011 № 93/ДСК.

23. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). Київ : ДП «УкрНДНЦ», 2023.

24. ДСТУ ISO/IEC 27002:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки (ISO/IEC 27002:2022, IDT). Київ : ДП «УкрНДНЦ», 2023.

25. ДСТУ ISO/IEC 27005:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова щодо керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT). Київ : ДП «УкрНДНЦ», 2023.