КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Кібербезпеки та комп'ютерної інженерії
(назва випускової кафедри)

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

на тему:

Комплексна система захисту інформації з обмеженим доступом в автоматизованій системі класу 2

Афонін Микола Валерійович
(прізвище, ім'я та по батькові здобувача повністю)

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)
Кібербезпеки та комп'ютерної інженерії
(назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
Делембовський М.М.
„___" _____2026 року

КВАЛІФІКАЦІЙНА РОБОТА ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

Комплексна система захисту інформації з обмеженим доступом в автоматизованій системі класу 2
(назва)

Я як здобувач вищої освіти КНУБА розумію і підтримую політику закладу з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших

Здобувач Афонін Микола Валерійович
(прізвище, ім'я та по батькові повністю)
125 «Кібербезпека»
(спеціальність)
Безпека інформаційних і комунікаційних систем
(освітня програма)
Група БІКСс-23
Керівник Котенко А. М.
(прізвище та ініціали)
Кандидат технічних наук, доцент
(вчене звання, науковий ступінь)
Рецензент Терентьєв О.О.
(прізвище та ініціали)
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.
„___" _____2026 року

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

Афонін Микола Валерійович
(прізвище, ім'я та по батькові здобувача)

1.Тема роботи «Комплексна система захисту інформації з обмеженим доступом в автоматизованій системі класу 2»
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
(прізвище, ім'я та по батькові, науковий ступінь, вчене звання)

3. Термін подання здобувачем роботи до захисту_____
4. Зміст пояснювальної записки за розділами:
Р. 1. Теоретичні основи захисту інформації в автоматизованих системах
Р. 2. Проєктування КСЗІ для АС класу 2
Р. 3. Практична реалізація КСЗІ в АС класу 2
Р. 4. _____
Р. 5. _____

5. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1. Теоретичні основи захисту інформації в автоматизованих системах	11.05.2026
Розділ 2. Проєктування КСЗІ для АС класу 2	22.05.2026
Розділ 3. Практична реалізація КСЗІ в АС класу 2	30.05.2026
Розділ 4.	
Розділ 5	
Остаточне оформлення роботи	05.06.2026
Направлення роботи для перевірки на плагіат	__.__.2026
Попередній захист роботи на випусковій кафедрі	__.__.2026
Направлення роботи на рецензування	

6. Дата видачі завдання _____

Керівник _____ _____
(підпис) (прізвище та ініціали)

Здобувач _____ _____
(підпис) (прізвище та ініціали)

РЕЗЮМЕ (SUMMARY) *до кваліфікаційної випускової роботи здобувача*	*Афонін Микола Валерійович* *Afonin Mykola Valeriiovych*		
ЗВО	Київський національний університет будівництва і архітектури		
Тема *(українською та англійською)*	Комплексна система захисту інформації з обмеженим доступом в автоматизованій системі класу 2 / Comprehensive Information Security System for Restricted-Access Information in a Class 2 Automated System.		
Освітній ступінь	бакалавр		
Факультет	Автоматизації і інформаційних технологій		
Випускова кафедра	Кібербезпеки та комп'ютерної інженерії		
Спеціальність	125 «Кібербезпека»		
Освітня програма	Безпека інформаційних і комунікаційних систем		
Керівник	к.т.н., доцент Котенко Андрій Миколайович		
Обсяг роботи:	*Пояснювальна записка, стор.*	*Розділів*	*Презентація, кількість слайдів*
	90	три	12
Розділ 1	Теоретичні основи захисту інформації в автоматизованих системах		
Розділ 2	Проєктування КСЗІ для АС класу 2		
Розділ 3	Практична реалізація КСЗІ в АС класу 2		
Висновки по роботі	Роботу присвячено проєктуванню та практичній реалізації комплексної системи захисту інформації з обмеженим доступом в АС класу 2. Запропоновані проєктні рішення та архітектура КСЗІ забезпечують протидію загрозам несанкціонованого доступу і витоку інформації технічними каналами та придатні для впровадження на підприємствах.		
Ключові слова: Keywords:	комплексна система захисту інформації, автоматизована система класу 2, інформація з обмеженим доступом, технічні канали витоку / comprehensive information security system, class 2 automated system, restricted-access information, technical leakage channels		

Здобувач _____/ _____

Керівник _____/ _____

АНОТАЦІЯ

Афонін М. В. «Комплексна система захисту інформації з обмеженим доступом в автоматизованій системі класу 2»

У роботі досліджено теоретичні та практичні основи захисту інформації з обмеженим доступом в автоматизованих системах класу 2 — локалізованих багатомашинних багатокористувацьких комплексах. Проаналізовано класифікацію автоматизованих систем, основні загрози й канали витоку інформації, а також нормативно-правове забезпечення створення КСЗІ.

У роботі запропоновано архітектуру комплексної системи захисту інформації, що поєднує підсистеми захисту від несанкціонованого доступу, антивірусного захисту, захисту від витоку інформації технічними каналами, технічної системи охорони та організаційно-розпорядчого забезпечення. Виконано категоріювання об'єкта інформаційної діяльності, побудовано моделі загроз і порушника, обрано функціональний профіль захищеності та розроблено технічне завдання на створення КСЗІ.

У практичній частині роботи реалізовано комплекс заходів захисту із застосуванням засобу від НСД «Лоза-2», антивірусного захисту ESET Endpoint Security, мережевого фільтра «ФЗП-103-2», генератора шуму «Базальт-5ГЕШ» та технічної системи охорони. Сформовано матрицю розмежування доступу і побудовано систему моніторингу та аудиту безпеки.

Отримані результати підтверджують, що комплексний підхід до захисту дозволяє забезпечити необхідний рівень захищеності інформації з обмеженим доступом в АС класу 2 відповідно до вимог нормативних документів системи технічного захисту інформації.

Ключові слова: комплексна система захисту інформації, автоматизована система класу 2, технічний захист інформації, модель загроз, ПЕМВН.

ABSTRACT

Afonin M. V. "Comprehensive Information Security System for Restricted Access Information in a Class 2 Automated System"

The thesis investigates the theoretical and practical foundations of restricted access information protection in Class 2 automated systems, which represent localized multi-machine multi-user complexes. The classification of automated systems, the main threats and information leakage channels, as well as the regulatory and legal framework for the development of a comprehensive information security system are analyzed.

The thesis proposes the architecture of a comprehensive information security system that combines subsystems for protection against unauthorized access, antivirus protection, protection against information leakage through technical channels, a technical security system, and organizational and administrative support. The categorization of the information activity facility is performed, threat and intruder models are developed, the functional security profile is selected, and the technical specification for the creation of the security system is prepared.

In the practical part of the thesis, a set of protection measures is implemented using the access control tool "Loza-2", the antivirus solution ESET Endpoint Security, the power line noise suppression filter "FZP-103-2", the electromagnetic noise generator "Bazalt-5HESH", and a technical security system. An access control matrix is established, and a security monitoring and audit system is developed.

The results obtained confirm that a comprehensive approach to information protection provides the required level of security for restricted access information in Class 2 automated systems in accordance with the requirements of the regulatory documents of the technical information protection system of Ukraine.

Keywords: comprehensive information security system, Class 2 automated system, technical information protection, threat model, electromagnetic emanations and interference.

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АРМ – автоматизоване робоче місце

АС – автоматизована система

АС класу 2 – локалізований багатомашинний багатокористувацький комплекс

БД – база даних

Держспецзв'язку – Державна служба спеціального зв'язку та захисту інформації України

ІБ – інформаційна безпека

ІКС – інформаційно-комунікаційна система

ІзОД – інформація з обмеженим доступом

КЗЗ – комплекс засобів захисту

КЗІ – криптографічний захист інформації

КСЗІ – комплексна система захисту інформації

НД ТЗІ – нормативний документ системи технічного захисту інформації

НСД – несанкціонований доступ

ОІД – об'єкт інформаційної діяльності

ОС – операційна система

ПЕМВН – побічні електромагнітні випромінювання і наведення

ПЗ – програмне забезпечення

РНБО – Рада національної безпеки і оборони України

ТЗ – технічне завдання

ТЗІ – технічний захист інформації

USB – універсальна послідовна шина для підключення периферійних пристроїв і носіїв інформації

ISO/IEC – Міжнародна організація зі стандартизації та Міжнародна електротехнічна комісія

NIST – Національний інститут стандартів і технологій США

MITRE ATT&CK – база знань про тактики, техніки та процедури кіберзагроз

OWASP – відкритий проєкт із безпеки вебзастосунків

ВСТУП

Розвиток інформаційно-комунікаційних технологій супроводжується істотним зростанням обсягів інформації, що обробляється в автоматизованих системах підприємств і установ. Значна частина цих відомостей має обмежений режим доступу – персональні дані, службова інформація, комерційна таємниця, технічна документація, – неправомірне розголошення або модифікація яких може спричинити організаційні, правові, репутаційні та матеріальні наслідки.

Актуальність теми кваліфікаційної роботи обумовлена необхідністю створення комплексної системи захисту інформації для автоматизованих систем класу 2, що характеризуються локалізованою багатомашинною багатокористувацькою структурою, та узгоджується із засадами державної політики у сфері кібербезпеки, визначеними Законом України «Про основні засади забезпечення кібербезпеки України» [1] та Стратегією кібербезпеки України [2]. Подібні системи потребують одночасного застосування програмно-технічних, інженерно-технічних та організаційних заходів захисту з протидією як загрозам несанкціонованого доступу, так і загрозам витоку інформації технічними каналами.

Метою кваліфікаційної роботи є проєктування та практична реалізація комплексної системи захисту інформації з обмеженим доступом в автоматизованій системі класу 2 з урахуванням нормативних вимог, особливостей об’єкта інформаційної діяльності, актуальних загроз та моделі порушника.

Для досягнення поставленої мети сформовано такі завдання:

1. Дослідити теоретичні та нормативно-правові основи захисту інформації з обмеженим доступом в автоматизованих системах класу 2.
2. Виконати категоріювання об’єкта інформаційної діяльності та обстеження середовища функціонування АС.
3. Побудувати модель загроз інформаційній безпеці та модель потенційного порушника.
4. Розробити політику безпеки інформації та обрати функціональний профіль захищеності АС.

5. Сформувати структуру та архітектуру КСЗІ, розробити технічне завдання на її створення.
6. Реалізувати організаційні, програмно-технічні та інженерно-технічні заходи захисту інформації, побудувати систему моніторингу та аудиту безпеки.

Об’єктом дослідження є процес захисту інформації з обмеженим доступом. Предметом дослідження є захист інформації з обмеженим доступом в автоматизованій системі класу 2 засобами комплексної системи захисту інформації.

Методи дослідження – аналіз нормативно-правових документів системи технічного захисту інформації, системний аналіз об’єкта інформаційної діяльності, моделювання загроз і порушника, структурне проєктування КСЗІ, узагальнення результатів обстеження середовища функціонування АС.

Практичне значення роботи полягає у розробці проєктних рішень та комплекту документації, що можуть бути використані для створення або вдосконалення КСЗІ в локалізованих багатомашинних багатокористувацьких автоматизованих системах класу 2 на підприємствах, що обробляють інформацію з обмеженим доступом без віднесення до державної таємниці.

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. У першому розділі розкрито теоретичні та нормативні основи захисту інформації в АС класу 2. У другому розділі виконано проєктування КСЗІ для ТОВ «Огун» з категоріюванням, обстеженням, побудовою моделей загроз і порушника, формуванням політики безпеки, архітектури КСЗІ та технічного завдання. У третьому розділі подано практичну реалізацію організаційних, інженерно-технічних та програмно-технічних заходів захисту інформації.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

1.1 Поняття інформації з обмеженим доступом та особливості її захисту

Розвиток інформаційних технологій супроводжується постійним збільшенням обсягів даних, що обробляються в автоматизованих системах, серед яких значну частку становлять відомості, доступ до яких регламентується на законодавчому або організаційному рівні. Обмеження доступу до інформації обумовлюється необхідністю запобігання її неправомірному використанню, витоку або модифікації, що може призвести до негативних наслідків як для окремих організацій, так і для держави загалом. В умовах функціонування автоматизованих систем, інформація виступає ключовим ресурсом, від якого залежить ефективність управління, прийняття рішень та забезпечення стабільності діяльності [3].

Інформація з обмеженим доступом, являє собою сукупність відомостей, щодо яких встановлено спеціальний режим доступу відповідно до вимог законодавства або внутрішніх нормативних документів організації. Спеціальний режим визначає порядок отримання, обробки, зберігання та передачі інформації, перелік осіб, які мають право працювати з нею [3]. Регламентація доступу до інформаційних ресурсів є одним з ключових інструментів забезпечення інформаційної безпеки, оскільки дозволяє мінімізувати ризики несанкціонованого впливу [4].

Важливе значення має систематизація інформації за категоріями доступу, оскільки вона дозволяє визначити необхідний рівень захищеності та обрати відповідні засоби протидії загрозам. Класифікація інформації з обмеженим доступом базується на характері відомостей, рівні їх важливості та можливих наслідках у разі порушення встановленого режиму захисту. Узагальнення основних категорій наведено в таблиці 1.1 (складено автором на основі [3], [5–7]).

.

Таблиця 1.1 – Основні категорії інформації з обмеженим доступом

Категорія інформації	Характеристика	Особливості захисту
Конфіденційна інформація	Відомості, доступ до яких обмежується фізичною або юридичною особою	Регламентація доступу, ідентифікація та автентифікація користувачів
Таємна інформація	Відомості, що становлять державну таємницю	Жорсткий контроль доступу, використання сертифікованих засобів захисту
Службова інформація	Дані, що використовуються в межах організації	Встановлення внутрішніх політик безпеки, контроль дій користувачів

Конфіденційні відомості, які належать суб’єктам господарювання, здебільшого потребують впровадження механізмів ідентифікації користувачів, контролю доступу та журналювання подій [5]. У випадку таємної інформації, яка охоплює державну таємницю, вимоги до захисту суттєво посилюються та включають застосування сертифікованих засобів криптографічного та технічного захисту, а також, проведення державної експертизи [6]. Службова інформація, що використовується у внутрішніх процесах організації, вимагає впровадження локальних регламентів безпеки, які визначають порядок роботи з нею та відповідальність персоналу [7].

Зазначена класифікація має прикладне значення під час створення комплексної системи захисту інформації, оскільки саме від категорії інформації залежить структура майбутньої системи, перелік захисних механізмів та рівень їх

складності. Вибір засобів захисту без врахування категорії інформації може призвести до недостатнього рівня безпеки або, навпаки, до надмірного ускладнення системи, що негативно вплине на ефективність її функціонування.

Особливості захисту інформації з обмеженим доступом визначаються не лише її категорією, але й умовами обробки в автоматизованих системах. Дані системи, це складні технічні комплекси, що об’єднують апаратні, програмні та комунікаційні компоненти. В процесі функціонування зазначених компонентів, виникають різноманітні канали витоку інформації, пов’язані з фізичними процесами, програмними вразливостями або діями користувачів. Наявність великої кількості потенційних джерел загроз ускладнює процес забезпечення захисту та потребує застосування комплексного підходу [8].

Забезпечення інформаційної безпеки в автоматизованих системах ґрунтується на необхідності збереження ключових властивостей інформації. До основних характеристик, які підлягають захисту, належать конфіденційність, цілісність та доступність. Узагальнення зазначених властивостей наведено в таблиці 1.2 (складено автором на основі [1], [8–10]).

Таблиця 1.2 – Основні властивості інформації, що підлягають захисту

Властивість	Опис	Можливі загрози
Конфіденційність	Обмеження доступу до інформації	Несанкціонований доступ, витік даних
Цілісність	Збереження точності та повноти інформації	Модифікація, підміна даних
Доступність	Забезпечення доступу уповноваженим користувачам	Відмова в обслуговуванні, блокування ресурсів

Порушення конфіденційності може призвести до розголошення чутливої інформації, що завдає шкоди репутації організації або створює загрозу національній безпеці. Втрата цілісності даних, впливає на достовірність інформації, що використовується під час прийняття управлінських рішень, а порушення доступності, унеможливлює своєчасне отримання необхідних відомостей [8].

Надмірна концентрація на одному аспекті без врахування інших, може призвести до зниження загальної ефективності системи безпеки. Наприклад, посилення механізмів контролю доступу без урахування потреб користувачів здатне ускладнити роботу системи, тоді як недостатній рівень захисту створює передумови для реалізації загроз.

Процес забезпечення захисту інформації з обмеженим доступом передбачає комплексне врахування нормативних вимог, характеристик інформаційних ресурсів та особливостей функціонування автоматизованої системи. На практиці це реалізується шляхом впровадження сукупності організаційних та технічних заходів, спрямованих на запобігання витоку інформації, несанкціонованому доступу та іншим видам загроз. Важливу роль відіграє підготовка персоналу, який безпосередньо взаємодіє з інформаційними ресурсами, оскільки людський фактор часто виступає одним з ключових джерел ризику [11].

Системний характер забезпечення захисту інформації передбачає взаємодію всіх складових безпеки в межах єдиної структури, що дозволяє підвищити рівень захищеності інформаційних ресурсів, забезпечити стійкість автоматизованої системи до зовнішніх та внутрішніх впливів, створити передумови для ефективного функціонування комплексної системи захисту інформації в умовах реальної експлуатації.

1.2 Класифікація автоматизованих систем та вимоги до АС класу 2

Автоматизована система є організаційно-технічним комплексом, призначеним для автоматизованого виконання інформаційних процесів, пов’язаних зі збиранням, накопиченням, зберіганням, обробкам, передаванням і

використанням даних. Її функціонування забезпечується сукупністю технічних засобів, програмного забезпечення, інформаційних ресурсів, користувачів, адміністраторів, експлуатаційних процедур та правил доступу. Для сфери захисту інформації принципове значення має не лише наявність програмно-апаратних компонентів, а характер взаємодії між користувачами, обчислювальними ресурсами, носіями інформації та середовищем передавання даних.

Автоматизована система не зводиться лише до комп'ютерної техніки або програмного забезпечення. Її склад охоплює обчислювальну систему, фізичне середовище розміщення обладнання, технологію обробка інформації, сукупність користувачів, правила адміністрування, порядок доступу до ресурсів та процедури контролю дій персоналу. Через це захист інформації в автоматизованій системі повинен враховувати технічні, програмні, організаційні та експлуатаційні чинники, оскільки порушення безпеки може виникнути не лише через технічну вразливість, а й через помилки користувача, недоліки в регламентах або неправильне налаштування засобів доступу [9].

Відповідно до НД ТЗІ 2.5-005-99 класифікація автоматизованих систем здійснюється не за загальними ознаками призначення, архітектури або масштабу, а за сукупністю характеристик, які мають безпосереднє значення для захисту інформації від несанкціонованого доступу. До таких характеристик належать кількість користувачів, кількість обчислювальних засобів, характер локалізації системи, спосіб передавання інформації, наявність або відсутність взаємодії через незахищене середовище, а також особливості оброблюваної інформації. Саме за цими ознаками виділяються автоматизовані системи класу 1, класу 2 та класу 3. НД ТЗІ 2.5-005-99 встановлює принципи класифікації автоматизованих систем і формування стандартних функціональних профілів захищеності інформації від несанкціонованого доступу.

Для наочного подання класифікації за НД ТЗІ 2.5-005-99 доцільно використати (рис. 1.1).

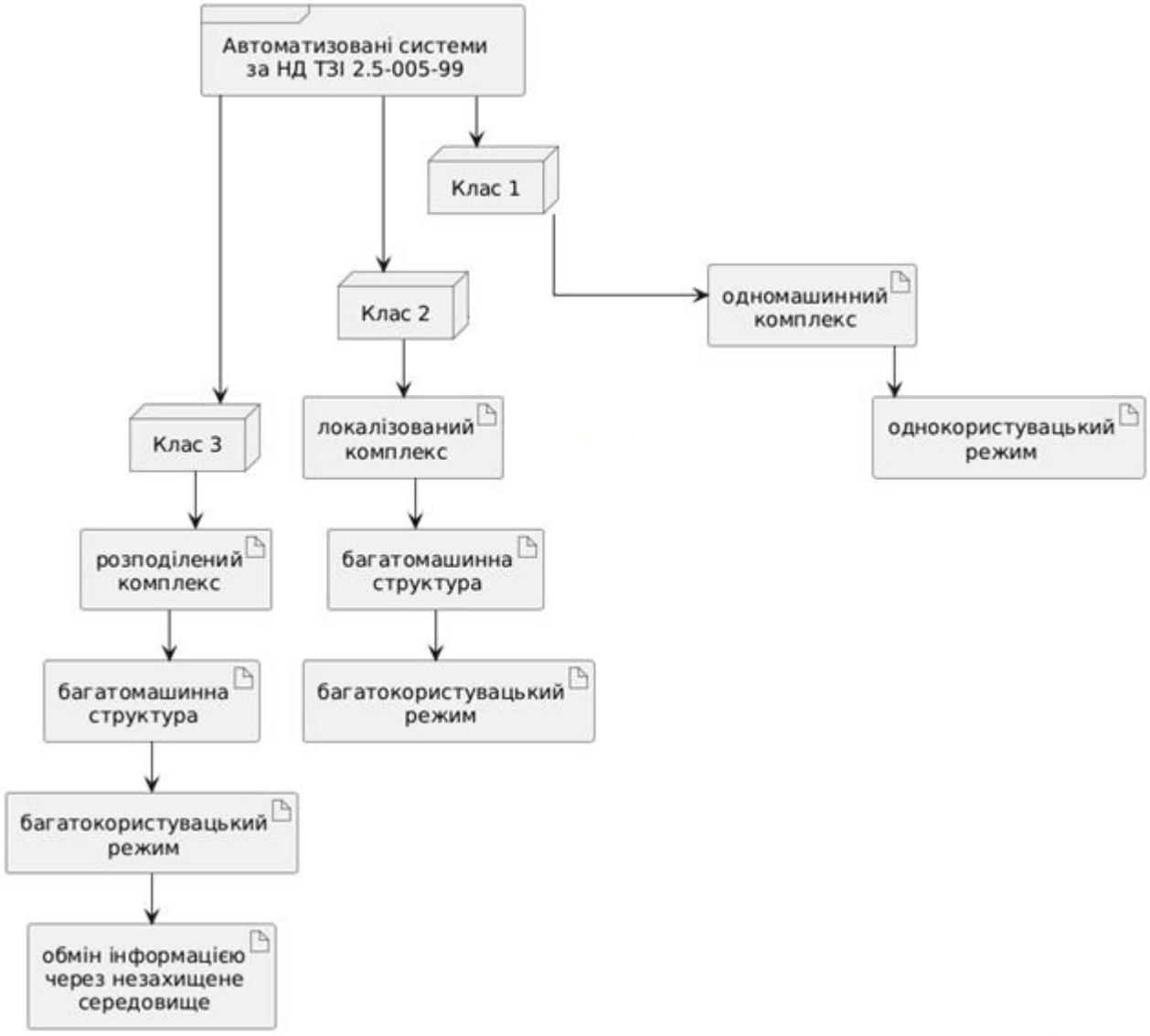

Рисунок 1.1 – Класифікація автоматизованих систем за НД ТЗІ 2.5-005-99 (розроблено автором)

Автоматизована система класу 1 є одномашинним однокористувацьким комплексом. Для неї характерна робота одного користувача з одним обчислювальним засобом у певний момент часу. Подібна система може обробляти інформацію, що потребує захисту, але її структура залишається найменш складною порівняно з іншими класами. Основна особливість полягає у відсутності багатокористувацького режиму та локальної мережевої взаємодії між декількома машинами. Через це основна увага під час захисту спрямовується на контроль фізичного доступу до робочої станції, автентифікацію користувача, захист носіїв

інформації, контроль запуску програм і недопущення несанкціонованого копіювання даних [12].

Автоматизована система класу 2 є локалізованим багатомашинним багатокористувацьким комплексом. Саме до такого класу належить об’єкт, що розглядається в дипломній роботі, оскільки він передбачає функціонування кількох робочих станцій, серверного або іншого спільного інформаційного ресурсу, а також роботу декількох користувачів з різними повноваженнями. За НД ТЗІ 2.5-005-99 АС класу 2 визначається як локалізований багатомашинний багатокористувачевий комплекс; офіційні матеріали на базі нормативного документа фіксують поділ АС на клас 1, клас 2 і клас 3, де клас 2 описується саме через локалізовану багатомашинну багатокористувацьку структуру [12].

Локалізований характер АС класу 2 означає, що обробка інформації здійснюється в контрольованому середовищі без передавання захищуваної інформації через глобальну мережу або інше незахищене середовище. Зв’язок між компонентами організовується через локальну мережу, внутрішню комунікаційну інфраструктуру або спільний обчислювальний комплекс. На практиці до АС класу 2 можуть належати локальні мережі організації, сервери з робочими станціями, автоматизовані робочі місця підрозділів, бази даних із розмежованим доступом, системи внутрішнього документообігу або облікові системи, де обробляється інформація з обмеженим доступом.

Багатомашинність АС класу 2 створює додаткові вимоги до захисту, оскільки інформація обробляється не на одному комп’ютері, а в сукупності технічних засобів. Це означає наявність кількох точок входу до системи, різних каналів передавання інформації, спільних ресурсів, локальних серверів, мережевого обладнання та адміністраторських інтерфейсів. Порушення безпеки може виникнути не лише на рівні окремої робочої станції, а й через неправильне налаштування мережевого доступу, неконтрольований обмін файлами, помилки в політиках користувачів або недостатній контроль адміністративних повноважень.

Багатокористувацький характер АС класу 2 означає, що в системі працюють користувачі з різними функціями, правами і рівнями доступу. Одні користувачі можуть лише переглядати інформацію, інші мають право вносити зміни, адміністратори керують обліковими записами та налаштуваннями системи, відповідальні особи контролюють дотримання правил безпеки. Через це в АС класу 2 обов'язковим елементом захисту є розмежування доступу. Кожен користувач повинен отримувати лише необхідний обсяг прав для виконання службових обов'язків, а доступ до критичних ресурсів має надаватися на підставі встановлених повноважень [12].

АС класу 2 зазвичай обробляє інформацію з обмеженим доступом, яка не належить до державної таємниці, але потребує захисту через можливість завдання матеріальної, репутаційної або організаційної шкоди в разі розголошення, модифікації чи втрати. До складу таких даних можуть входити службова інформація, персональні дані працівників або клієнтів, фінансові відомості, внутрішня документація, матеріали управлінського обліку, інформація про договірні відносини, технічні параметри системи та інші ресурси, доступ до яких обмежується власником або нормативними вимогами.

Автоматизована система класу 3 має складнішу структуру, оскільки є розподіленим багатомашинним багатокористувацький комплексом, де передавання інформації здійснюється через незахищене середовище, зокрема глобальну мережу. Наявність взаємодії через незахищене середовище суттєво змінює характер загроз, оскільки зростає ймовірність перехоплення, підміни, блокування або спотворення інформації під час передавання. Саме відсутність обробка захищуваної інформації через глобальну мережу є однією з ознак, яка дозволяє віднести об'єкт дипломної роботи не до класу 3, а до класу 2.

Отже, об'єкт дипломної роботи обґрунтовано належить до АС класу 2, оскільки передбачає локалізовану багатомашинну багатокористувацьку структуру, обробка інформації з обмеженим доступом, наявність різних категорій користувачів, потребу розмежування повноважень і відсутність передавання

захищуваної інформації через глобальну мережу як основного технологічного середовища. Така класифікація має принципове значення для подальшого проєктування КСЗІ, оскільки саме клас автоматизованої системи визначає склад функціональних послуг безпеки, вимоги до комплексу засобів захисту та зміст організаційних процедур [10, 12].

Вимоги до АС класу 2 формуються з урахуванням положень НД ТЗІ 2.5-005-99, НД ТЗІ 2.5-004-99 та загальних принципів захисту інформації від несанкціонованого доступу. НД ТЗІ 2.5-004-99 встановлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу, а тому застосовується для визначення необхідних послуг безпеки, рівнів гарантій, механізмів контролю доступу, реєстрації подій, забезпечення цілісності й доступності ресурсів.

Однією з базових вимог до АС класу 2 є ідентифікація та автентифікація користувачів. Система повинна забезпечувати встановлення особи користувача до надання доступу до інформаційних ресурсів. Ідентифікація дозволяє пов'язати дії в системі з конкретним обліковим записом, а автентифікація підтверджує правомірність використання облікових даних. Для АС класу 2 така вимога має особливе значення через багатокористувацький режим роботи та наявність різних категорій доступу.

Не менш важливою вимогою є розмежування доступу до інформаційних ресурсів. Доступ користувачів має визначатися на підставі їх функціональних обов'язків і ролей. У системі необхідно відокремлювати права перегляду, створення, редагування, видалення, адміністрування та експортування інформації. Розмежування доступу запобігає ситуаціям, коли користувач отримує можливість працювати з інформацією, яка не потрібна для виконання його службових завдань [10].

АС класу 2 повинна забезпечувати реєстрацію та облік подій безпеки. Журнали подій необхідні для фіксації входу користувачів, завершення сеансів, спроб доступу до ресурсів, зміни прав, модифікації даних, дій адміністраторів і

помилок системи. Наявність реєстраційної інформації дозволяє виявляти порушення, аналізувати інциденти, встановлювати причини відхилень і підтверджувати відповідальність користувачів за виконані операції.

Захист цілісності інформації має забезпечувати виявлення несанкціонованої модифікації даних і програмного середовища. Для АС класу 2 це означає необхідність контролю змін у базах даних, службових файлах, конфігураціях, програмних модулях і параметрах доступу. Втрата цілісності може призвести до викривлення результатів обробка інформації, неправильних управлінських рішень або порушення роботи всієї системи.

Окрема вимога стосується забезпечення доступності інформаційних ресурсів. АС класу 2 повинна підтримувати працездатність основних компонентів, а у разі збоїв забезпечувати можливість відновлення інформації та функцій системи. Для цього передбачаються резервне копіювання, контроль стану обладнання, обмеження дій, здатних порушити працездатність, і регламент відновлення після аварійних ситуацій.

Для АС класу 2 необхідним є захист від витоку інформації технічними каналами. Багатомашинне локальне середовище передбачає наявність робочих станцій, мережевих пристроїв, ліній зв’язку, периферійного обладнання та приміщень, де можуть виникати побічні електромагнітні випромінювання, наведення, акустичні та віброакустичні прояви. Захист не обмежується програмними механізмами, а повинен охоплювати фізичне середовище, контроль доступу до приміщень, розміщення обладнання, використання засобів зниження рівня побічних сигналів і перевірку достатності реалізованих заходів.

Організаційні вимоги до АС класу 2 охоплюють розроблення політики безпеки, призначення відповідальних осіб, регламентацію прав користувачів, порядок адміністрування, правила роботи з носіями інформації, процедури реагування на інциденти та контроль виконання вимог. Для локалізованої багатокористувацької системи організаційні процедури мають важливе значення,

як і технічні засоби, оскільки значна частина порушень пов’язана з неправильними діями персоналу або відсутністю чітких правил [7].

1.3 Характеристика загроз та каналів витоку інформації

Функціонування автоматизованих систем супроводжується впливом значної кількості факторів, які можуть порушити нормальний перебіг інформаційних процесів. Обробка, передавання та зберігання даних відбуваються в складному технічному середовищі, де взаємодіють апаратні засоби, програмні компоненти та користувачі. Дана взаємодія формує передумови для виникнення загроз, що можуть призвести до втрати інформації, її спотворення або несанкціонованого розголошення. Розуміння природи загроз та механізмів їх реалізації, має ключове значення для побудови ефективної системи захисту.

Загроза інформаційній безпеці розглядається як потенційна можливість реалізації впливу на інформаційні ресурси або інфраструктуру їх обробки, що призводить до порушення конфіденційності, цілісності або доступності. Джерелом загрози може бути як людина, так і технічний засіб, програмний компонент або зовнішній фактор природного характеру. В сучасних умовах, особливо складними є комбіновані загрози, реалізація яких відбувається за участю декількох факторів одночасно.

Систематизація загроз здійснюється за рядом ознак, що дозволяє оцінити їх характер та визначити способи протидії. Однією з базових ознак є джерело виникнення. Зовнішні впливи пов’язані з діяльністю осіб або технічних засобів, які не мають законного доступу до системи. Реалізація представлених впливів відбувається через мережеві інтерфейси, канали зв’язку або фізичний доступ до обладнання. Внутрішні загрози формуються внаслідок дій персоналу, який має доступ до інформаційних ресурсів. Причиною може бути як навмисне порушення правил, так і помилки, обумовлені недостатнім рівнем підготовки або неуважністю [9].

Характер впливу дозволяє виділити два принципово різні типи загроз. Пасивні дії спрямовані на отримання інформації без зміни її стану. В такому випадку, користувач або технічний засіб здійснює спостереження або перехоплення даних. Активні дії супроводжуються зміною інформації або порушенням функціонування системи. Прикладом може бути модифікація даних, блокування доступу або впровадження шкідливого програмного забезпечення. Різниця між пасивними та активними діями визначає підхід до організації захисту, оскільки пасивні загрози складніше виявити, а активні можуть мати швидкий та руйнівний ефект.

Технічні загрози пов’язані з використанням фізичних властивостей обладнання та середовища функціонування. Програмні загрози виникають через наявність вразливостей в програмному забезпеченні або помилки в алгоритмах обробки даних. Організаційні загрози обумовлені недоліками в управлінні доступом, відсутністю чітких процедур або порушенням встановлених правил. Природні фактори включають вплив зовнішніх умов, таких як пожежі, затоплення або перебої в електропостачанні. Узагальнення класифікації загроз інформаційній безпеці наведено на рисунку 1.2.

Рисунок 1.2 – Класифікація загроз інформаційній безпеці
(розроблено автором)

Реальні інциденти, як правило, виникають в результаті поєднання декількох факторів, що ускладнює їх виявлення та нейтралізацію [9].

Окрім загроз, важливе значення має аналіз каналів витоку інформації, які визначають можливі шляхи її несанкціонованого отримання. Канал витоку являє собою сукупність умов, за яких інформація може бути передана від джерела до стороннього спостерігача без контролю з боку власника. Формування таких каналів пов’язане як з фізичними процесами, що супроводжують роботу обладнання, так і з особливостями організації інформаційних процесів.

Електромагнітні канали виникають під час роботи електронних пристроїв, які генерують побічні випромінювання. Інформаційні сигнали можуть бути зафіксовані на відстані за допомогою спеціалізованих технічних засобів, що створює загрозу перехоплення даних без безпосереднього доступу до системи. Акустичні канали формуються внаслідок звукових коливань, які виникають під час роботи обладнання або мовлення користувачів. В умовах відсутності належної ізоляції, дані сигнали можуть бути використані для відновлення інформації [13].

Вібраційні канали пов’язані з передачею механічних коливань через тверді середовища, включаючи конструкції будівель. Коливання можуть містити інформацію про процеси, що відбуваються в технічних засобах. Оптичні канали формуються за рахунок випромінювання світла або відображення зображень від поверхонь, що дозволяє отримувати інформацію шляхом візуального спостереження або використання оптичних пристроїв. Основні канали витоку інформації узагальнено в таблиці 1.3(складено автором на основі [9], [13], [14]).

Таблиця 1.3 – Основні канали витоку інформації

Тип каналу	Джерело виникнення	Характеристика передачі інформації
Електромагнітний	Робота електронних компонентів	Передавання сигналів через випромінювання
Акустичний	Звукові коливання	Поширення інформації через повітря

Продовження таблиці 1.3

Тип каналу	Джерело виникнення	Характеристика передачі інформації
Вібраційний	Механічні процеси	Передача через тверді середовища
Оптичний	Світлові явища	Візуальне спостереження або зчитування

Забезпечення захисту від витоку інформації передбачає врахування всіх можливих каналів та впровадження відповідних заходів. До заходів безпеки належать обмеження доступу до приміщень, контроль використання технічних засобів, застосування екранізації та створення умов, що унеможливлюють несанкціоноване спостереження.

1.4 Нормативно-правове забезпечення створення КСЗІ

Створення комплексної системи захисту інформації в автоматизованій системі класу 2 потребує чіткого нормативно-правового обґрунтування, оскільки захист інформації з обмеженим доступом не може будуватися лише на загальних технічних міркуваннях або внутрішніх рішеннях організації. Проєктування КСЗІ має спиратися на чинні законодавчі акти України, постанови Кабінету Міністрів України та нормативні документи системи технічного захисту інформації, які визначають правовий режим інформації, порядок її обробки, класифікацію автоматизованих систем, критерії оцінювання захищеності, вимоги до технічного завдання та послідовність виконання робіт зі створення системи захисту [15].

Нормативно-правове забезпечення КСЗІ виконує декілька взаємопов’язаних функцій. Воно встановлює підстави для захисту інформації з обмеженим доступом, визначає обов’язковість впровадження захисних заходів, регламентує порядок створення системи захисту, задає критерії оцінювання її достатності та формує вимоги до документального супроводу. Без врахування нормативної бази

неможливо коректно визначити клас автоматизованої системи, обрати потрібний функціональний профіль захищеності, сформувати модель загроз, розробити технічне завдання та підтвердити відповідність створеної КСЗІ встановленим вимогам [16].

Правову основу захисту інформації під час її обробки в інформаційно-комунікаційних системах формує Закон України «Про захист інформації в інформаційно-комунікаційних системах». У ньому визначено правові засади захисту інформації в системах, об’єкти захисту та загальні вимоги до забезпечення безпеки інформації, яка обробляється з застосуванням технічних та програмних засобів. Законодавче значення акту полягає в закріпленні вимоги щодо захисту інформації, яка обробляється в системі, а також, програмного забезпечення, призначеного для її обробки. Для автоматизованої системи класу 2, норми закону створюють базову правову підставу для впровадження КСЗІ, оскільки в даній системі обробляється інформація з обмеженим доступом, розголошення або модифікація якої може спричинити негативні наслідки для власника інформації чи користувачів системи.

Загальний правовий режим інформації, порядок доступу до неї та принципи інформаційних відносин регламентуються Законом України «Про інформацію». Значення цього закону полягає в тому, що він дозволяє визначити категорію відомостей, з якими працює автоматизована система, та встановити, чи належать вони до відкритої інформації або інформації з обмеженим доступом. Для побудови КСЗІ, класифікація інформації має принципове значення, оскільки саме правовий режим відомостей впливає на подальше визначення вимог до доступу, обробки, зберігання, передавання та знищення інформації. В практичній площині, закон створює основу для розмежування прав користувачів, визначення відповідальності за неправомірне використання відомостей та формування внутрішніх регламентів роботи з інформаційними ресурсами [3].

Підзаконний рівень регулювання конкретизує вимоги до захисту систем, де обробляються державні інформаційні ресурси або інформація з обмеженим

доступом. Одним з головних документів такого рівня є Постанова Кабінету Міністрів України № 373 від 29.03.2006 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем». З урахуванням змін, внесених постановою Кабінету Міністрів України № 1171 від 14.10.2022, документ визначає сукупність організаційних та технічних вимог до заходів захисту інформації та кіберзахисту. В Мінімальних вимогах прямо зазначено, що вони застосовуються до систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Зміст постанови № 373 має безпосереднє значення для автоматизованої системи класу 2, оскільки вона визначає загальну рамку організаційних та технічних заходів безпеки. До таких заходів належать управління доступом, захист інформації від несанкціонованих дій, забезпечення цілісності та доступності інформаційних ресурсів, впровадження процедур реагування на інциденти, контроль функціонування системи захисту та підтримання належного стану документації. В контексті створення КСЗІ, постанова № 373 задає обов’язковий мінімум, нижче якого рівень захисту системи не може вважатися достатнім [11].

Методичну основу організації робіт зі створення КСЗІ визначає НД ТЗІ 3.7-003-2023 «Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі». Документ регламентує порядок прийняття рішень щодо складу КСЗІ залежно від умов функціонування системи та видів оброблюваної інформації, визначає обсяг та зміст робіт, етапність, основні завдання кожного етапу та порядок їх виконання. В галузі використання документу зазначено, що він поширюється на інформаційно-комунікаційні системи, де інформація обробляється автоматизованим способом, а положення документу систематизують чинні вимоги, норми та правила щодо створення захищених систем [15].

Застосування порядку, встановленого НД ТЗІ 3.7-003-2023, дає змогу побудувати процес створення КСЗІ як послідовність взаємопов’язаних робіт. На

початковому етапі, аналізуються умови функціонування автоматизованої системи, склад інформації, порядок доступу до ресурсів, технічне середовище, програмні компоненти та організаційні процедури. Далі визначаються загрози, формуються вимоги до захисту, обираються технічні та організаційні заходи, готується необхідна документація, впроваджуються захисні механізми та забезпечується супровід системи. Для АС класу 2, дана послідовність важлива через наявність кількох користувачів, кількох технічних засобів, локалізованого середовища обробки інформації та потреби в розмежуванні доступу.

Класифікація автоматизованої системи здійснюється з урахуванням НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». Документ встановлює поділ автоматизованих систем на класи залежно від характеристик обробки інформації, кількості користувачів, кількості обчислювальних засобів, локалізації системи та наявності або відсутності передавання інформації через незахищене середовище. Саме за наведеними ознаками, автоматизована система класу 2 визначається як локалізований багатомашинний багатокористувацький комплекс, який обробляє інформацію з обмеженим доступом без використання незахищеного середовища як основного каналу передавання інформації, яка потребує захисту.

Нормативна класифікація за НД ТЗІ 2.5-005-99 має практичне значення, оскільки вона впливає на вибір стандартного функціонального профілю захищеності. Клас автоматизованої системи не є формальною характеристикою, а визначає сукупність вимог до комплексу засобів захисту, функцій безпеки, механізмів розмежування доступу та контролю дій користувачів. Для АС класу 2, особливо важливими є ідентифікація та автентифікація користувачів, керування правами доступу, реєстрація подій, контроль цілісності інформації, захист від несанкціонованого копіювання, обмеження адміністративних повноважень та підтримка працездатності системи в разі відмов окремих компонентів [12].

Критерії оцінювання захищеності інформації від несанкціонованого доступу встановлюються НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». За своїм призначенням, документ визначає методологічну базу для формування вимог до захисту інформації, створення захищених комп'ютерних систем та засобів захисту, а також, оцінювання рівня реалізації захисних функцій. Положення критеріального документу застосовуються під час визначення функціональних послуг безпеки, пов'язаних з конфіденційністю, цілісністю, доступністю, спостережуваністю, керуванням доступом та реєстрацією дій користувачів.

Для автоматизованої системи класу 2, критерії оцінки захищеності мають особливе значення, оскільки багатокористувацький режим роботи підвищує ризик неправомірного доступу, помилкових дій персоналу та неконтрольованої модифікації інформації. Наявність декількох користувачів з різними повноваженнями, потребує не лише технічного обмеження доступу, але й перевірки достатності реалізованих механізмів. Якщо система формально має паролі або ролі, але не забезпечує реєстрацію подій, контроль адміністративних дій, розмежування доступу до об'єктів та захист службових параметрів, рівень її захищеності не може вважатися належним.

Загальні методологічні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу визначаються НД ТЗІ 1.1-002-99. Норми цього документу формують понятійну основу захисту інформації, пояснюють логіку визначення вимог до захисту, підходи до створення захищених комп'ютерних систем та принципи оцінювання придатності засобів безпеки для вирішення конкретних завдань[9].

Організаційна частина захисту інформації регламентується документами, які визначають відповідальність персоналу та порядок управління системою безпеки. Діяльність служби захисту інформації в автоматизованій системі описується в НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі». Документ встановлює вимоги до структури та змісту

нормативного документу, що регламентує діяльність служби захисту інформації, та призначений для суб'єктів, діяльність яких пов'язана з обробкою інформації в автоматизованих системах.

Для АС класу 2, організаційна складова має не менше значення, ніж технічна. Локалізований багатомашинний багатокористувацький комплекс потребує чіткого розподілу відповідальності між адміністратором, користувачами, власником інформації та особами, відповідальними за захист. Служба захисту інформації або призначена відповідальна особа, повинна контролювати виконання політики безпеки, вести облік користувачів, брати участь в розгляді інцидентів, організовувати контроль за налаштуваннями системи, перевіряти актуальність документації та забезпечувати взаємодію між технічними та адміністративними компонентами КСЗІ [17].

Підготовка технічного завдання на створення КСЗІ виконується з урахуванням НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі». Значення технічного завдання полягає у фіксації вихідних даних, призначення системи захисту, складу об'єкту, вимог до функцій безпеки, складу захисних засобів, порядку контролю, вимог до документації та умов введення системи в експлуатацію. Технічне завдання перетворює загальні нормативні положення на конкретні вимоги до системи, яка розробляється для конкретного об'єкту.

Особливість технічного завдання полягає в тому, що воно поєднує результати обстеження автоматизованої системи, дані про категорію інформації, модель загроз, модель порушника та вимоги до комплексу засобів захисту. Для АС класу 2, в технічному завданні необхідно відобразити локалізований характер системи, багатомашинну структуру, кількість та ролі користувачів, склад інформаційних ресурсів, порядок доступу, вимоги до реєстрації подій, захисту цілісності, резервування, адміністрування та контролю технічних каналів витоку [16].

Захист інформації від витоку технічними каналами має окреме нормативне підґрунтя, оскільки загрози такого типу пов’язані не лише з доступом користувачів до програмного середовища, але й з фізичними процесами роботи обладнання. Під час оцінювання повноти реалізованих заходів застосовуються положення НД ТЗІ 2.1-002-07, який визначає основи випробування комплексу технічного захисту інформації. Зазначений документ пов’язаний з перевіркою повноти та достатності реалізованих заходів захисту на об’єктах інформаційної діяльності, атестацією комплексу ТЗІ та підготовкою висновків за результатами випробувань[14].

Для автоматизованої системи класу 2, контроль технічних каналів витоку повинен охоплювати приміщення, робочі комп’ютери, серверне обладнання, мережеві лінії, периферійні пристрої та допоміжні технічні засоби. Під час обробки інформації з обмеженим доступом можуть виникати побічні електромагнітні випромінювання і наведення, акустичні та віброакустичні прояви, оптичні канали спостереження, ризики неконтрольованого доступу до носіїв інформації. Через це організація КСЗІ повинна передбачати не лише програмний контроль доступу, але й технічні та режимні заходи, спрямовані на недопущення витоку інформації за межі контрольованої зони[13].

За потреби захисту інформації криптографічними методами, застосовуються нормативні вимоги до засобів криптографічного захисту інформації. Вимоги, затверджені наказом Адміністрації Держспецзв’язку від 07.05.2021, поширюються на засоби КЗІ, призначені для захисту таємної інформації, що не становить державної таємниці, та конфіденційної інформації під час її використання в інформаційно-телекомунікаційних системах. Застосування криптографічних засобів в АС класу 2 доцільне для захисту інформації під час зберігання, передавання локальними каналами, резервного копіювання, адміністрування та обміну службовими даними [18].

Підтвердження відповідності створеної системи захисту встановленим вимогам пов’язане з процедурою державної експертизи. Нормативне регулювання експертизи КСЗІ передбачає перевірку, аналіз та оцінювання об’єктів експертизи

щодо відповідності вимогам нормативних документів системи технічного захисту інформації [19]. На прикладі чинного порядку, затвердженого наказом Міністерства оборони України № 630 від 13.09.2024 для систем Міністерства оборони, видно загальну логіку організації експертизи: подання документації, проведення експертних випробувань, аналіз декларацій, підготовка експертного висновку або атестату відповідності [20].

Оцінювання КСЗІ має не формальний, а практичний зміст та дозволяє перевірити, чи відповідають реалізовані організаційні, технічні та програмні заходи заявленим вимогам, чи забезпечується розмежування доступу, чи фіксуються події безпеки, чи захищені критичні параметри системи, чи забезпечено відновлення після збоїв, чи достатньо враховані канали витоку інформації. Для АС класу 2 експертиза або внутрішня перевірка відповідності є завершальним етапом, який підтверджує готовність системи до безпечної експлуатації.

Нормативно-правове забезпечення створення КСЗІ має багаторівневий характер. Законодавчі акти визначають правову природу інформації та обов’язок її захисту. Постанова Кабінету Міністрів України № 373 конкретизує мінімальні організаційні та технічні вимоги до систем, де обробляється інформація з обмеженим доступом. Нормативні документи системи ТЗІ визначають порядок створення КСЗІ, класифікацію автоматизованих систем, критерії оцінювання захищеності, методологічні положення захисту від несанкціонованого доступу, вимоги до служби захисту інформації, технічного завдання, випробувань і застосування спеціалізованих засобів захисту. Актуальний перелік чинних нормативних документів системи технічного захисту інформації підтримується Державною службою спеціального зв'язку та захисту інформації України [21].

Комплексне застосування зазначених нормативних актів дозволяє обґрунтувати належність об’єкта до автоматизованої системи класу 2, визначити перелік вимог до захисту інформації з обмеженим доступом, сформувати структуру КСЗІ, підготувати необхідну документацію та забезпечити відповідність проєктних рішень вимогам системи технічного захисту інформації.

Висновки до розділу 1

У першому розділі досліджено теоретичні та нормативні основи захисту інформації з обмеженим доступом в автоматизованих системах.

Розглянуто поняття інформації з обмеженим доступом та особливості її захисту, встановлено, що такий захист потребує врахування як технічних, так і організаційних факторів, а збереження конфіденційності, цілісності та доступності неможливе без комплексного підходу.

Проаналізовано класифікацію автоматизованих систем за НД ТЗІ 2.5-005-99 та визначено, що АС класу 2 як локалізований багатомашинний багатокористувацький комплекс потребує впровадження механізмів ідентифікації, розмежування доступу, контролю дій користувачів та захисту від технічних впливів.

Охарактеризовано основні загрози інформаційній безпеці та канали витоку інформації, при цьому встановлено, що канали витоку через фізичні процеси роботи технічних засобів вимагають окремих заходів захисту, не пов’язаних безпосередньо з логічною обробкою даних.

Розглянуто нормативно-правове забезпечення створення КСЗІ – законодавчі акти, постанови Кабінету Міністрів України та нормативні документи системи ТЗІ, що формують єдину основу для побудови систем захисту інформації.

Узагальнення результатів першого розділу обґрунтовує необхідність застосування комплексного підходу до захисту інформації в АС класу 2 та створює теоретичну основу для подальшого проєктування КСЗІ у Розділі 2.

РОЗДІЛ 2 ПРОЄКТУВАННЯ КСЗІ ДЛЯ АС КЛАСУ 2

2.1 Загальна характеристика об’єкта інформаційної діяльності (ОІД)

Об’єктом інформаційної діяльності, для якого виконується проєктування комплексної системи захисту інформації, обрано приміщення ТОВ «Огун» – підприємства, що здійснює діяльність у сфері інформаційних технологій на території м. Києва. Підприємство надає послуги, пов’язані з адмініструванням, технічним супроводом та моніторингом інформаційно-комунікаційної інфраструктури підприємств-замовників, що зумовлює постійну роботу персоналу з відомостями обмеженого доступу як власного, так і клієнтського походження.

Загальна чисельність працівників ТОВ «Огун» становить 24 особи. Безпосередню роботу з ресурсами автоматизованої системи, для якої проєктується КСЗІ, здійснюють 15 співробітників, які виконують функції адміністраторів, інженерів технічної підтримки, керівників проєктів та осіб, відповідальних за документальний супровід виконуваних робіт. Решта персоналу до інформаційних ресурсів автоматизованої системи доступу не має та виконує адміністративні функції, не пов’язані з обробкою інформації з обмеженим доступом.

ОІД розміщений на одному поверсі офісної будівлі, що відповідає ознакам локалізованого розташування технічних засобів обробки інформації. Всі автоматизовані робочі місця, серверне обладнання, мережеве обладнання локальної мережі та допоміжні технічні засоби знаходяться в межах єдиної контрольованої зони, доступ до якої обмежений організаційними та інженерно-технічними заходами. Передавання інформації з обмеженим доступом за межі контрольованої зони через незахищене середовище в межах основної технологічної діяльності не передбачено, що дозволяє віднести систему до АС класу 2 згідно з НД ТЗІ 2.5-005-99.

Підставою для прийняття рішення про створення КСЗІ слугували результати попереднього аналізу інформаційних ресурсів, які відносяться до ОІД, та нормативно-правових вимог щодо їх захисту. Встановлено, що в процесі діяльності підприємства обробляються відомості, доступ до яких обмежено законодавством

України, зокрема персональні дані працівників та представників замовників, відомості, що становлять комерційну таємницю замовників та передані ТОВ «Огун» на підставі угод про нерозголошення, а також службова інформація самого підприємства. Захист зазначених відомостей є обов’язковим відповідно до Закону України «Про захист інформації в інформаційно-комунікаційних системах», Закону України «Про захист персональних даних» та Постанови Кабінету Міністрів України № 373 від 29.03.2006 (у редакції постанови № 1171 від 14.10.2022) [5, 8, 11].

За результатами проведеного аналізу прийнято рішення про необхідність створення комплексної системи захисту інформації, оформлене відповідним наказом керівника ТОВ «Огун». Створення КСЗІ передбачає реалізацію сукупності взаємопов’язаних організаційних, інженерно-технічних та програмно-апаратних заходів, спрямованих на запобігання несанкціонованому доступу до інформації, її модифікації, знищенню та витоку технічними каналами в межах ОІД.

Призначенням створюваної КСЗІ є забезпечення конфіденційності, цілісності та доступності інформації з обмеженим доступом, що обробляється засобами АС класу 2 ТОВ «Огун», протягом всього технологічного циклу її обробки та зберігання. КСЗІ повинна функціонувати в межах режимів роботи автоматизованої системи, не порушуючи виконання основних виробничих завдань підприємства, та забезпечувати можливість контролю стану захищеності інформаційних ресурсів з боку відповідальних посадових осіб.

Архітектурно-планувальні особливості ОІД враховують вимоги до розміщення технічних засобів обробки інформації з обмеженим доступом. Приміщення мають капітальні стіни, металопластикові двері та віконні отвори, що виходять на внутрішню територію будівлі. Контрольована зона ОІД охоплює робочі приміщення основного персоналу, серверне приміщення, кімнату адміністратора безпеки та допоміжні приміщення, безпосередньо пов’язані з функціонуванням автоматизованої системи. Доступ сторонніх осіб до

контрольованої зони обмежений організаційними заходами та засобами фізичного контролю.

До складу замовників послуг ТОВ «Огун» належать суб'єкти господарювання різних форм власності, з якими укладено угоди про конфіденційність, що накладають додаткові зобов'язання щодо захисту переданої інформації. Невиконання зазначених зобов'язань тягне за собою як договірну відповідальність перед замовниками, так і відповідальність відповідно до законодавства України, що додатково підтверджує доречність створення КСЗІ.

Передумовами проєктування КСЗІ є наявність затвердженого керівництвом переліку відомостей, що становлять інформацію з обмеженим доступом, призначення посадової особи, відповідальної за захист інформації, та виділення матеріально-технічних ресурсів для впровадження захисних заходів. На підставі зазначених передумов сформовано вихідні дані для виконання подальших етапів проєктування, що передбачають категоріювання ОІД, обстеження середовища функціонування автоматизованої системи, побудову моделей загроз та порушника, розробки політики безпеки та формування технічного завдання на створення КСЗІ.

2.2 Визначення видів інформації та рівнів обмеження доступу

З метою формування обґрунтованих вихідних даних для проєктування комплексної системи захисту інформації, на ОІД ТОВ «Огун» проведено категоріювання об'єкту інформаційної діяльності та аналіз видів інформації, які знаходяться в складі автоматизованої системи. Зазначені роботи виконані відповідно до вимог нормативних документів системи технічного захисту інформації, з урахуванням характеру діяльності підприємства, кола замовників та номенклатури оброблюваних відомостей.

Категоріюванню підлягають приміщення ОІД, технічні засоби обробки інформації, а також, автоматизована система в цілому, оскільки на об'єкті циркулює інформація з обмеженим доступом. Підставою для віднесення відомостей до відповідної категорії слугували положення чинного законодавства

України, внутрішні нормативні документи ТОВ «Огун», а також, зобов’язання, які випливають з договорів з замовниками послуг.

За результатами аналізу інформаційних потоків встановлено, що в межах автоматизованої системи містяться відомості, які за правовим режимом доступу поділяються на відкриту інформацію та інформацію з обмеженим доступом. Відкрита інформація включає загальнодоступні дані, що використовуються в процесі господарської діяльності та не підлягають захисту в межах КСЗІ; правовий режим такої інформації та порядок доступу до неї регламентується Законом України «Про доступ до публічної інформації» [4]. Інформація з обмеженим доступом охоплює відомості, доступ до яких регламентується законодавством України або внутрішніми документами підприємства, та підлягає захисту засобами створюваної системи.

У складі інформації з обмеженим доступом, які відноситься до ОІД, виділено наступні види:

– персональні дані працівників ТОВ «Огун» та представників підприємств-замовників, захист яких регламентується Законом України «Про захист персональних даних»;

– інформація, що становить комерційну таємницю замовників та передана ТОВ «Огун» на підставі укладених угод про нерозголошення, зокрема відомості про структуру інформаційно-комунікаційних систем замовників, конфігурації обладнання, параметри доступу до серверних та мережевих ресурсів, дані технічної документації;

– службова інформація ТОВ «Огун», що використовується для забезпечення внутрішньої діяльності підприємства та включає внутрішні регламенти, накази, посадові інструкції, фінансово-господарські відомості, договірну документацію;

– облікові дані користувачів автоматизованої системи, журнали реєстрації подій безпеки, конфігураційні параметри засобів захисту, що мають службовий характер та визначають правомірність використання інформаційних ресурсів.

За результатами проведеного аналізу встановлено, що інформація з обмеженим доступом, яка обробляється в АС класу 2 ТОВ «Огун», не належить до державної таємниці. Зазначене дозволяє сформувати вимоги до КСЗІ з урахуванням положень НД ТЗІ 2.5-008-2002, який регламентує захист службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2, без застосування додаткових вимог режиму секретності [7].

Категоріювання ОІД виконано відповідно до НД ТЗІ 1.6-005-2013, який встановлює порядок категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці [22]. З урахуванням визначеного складу інформації, особливостей її обробки та зобов'язань підприємства перед замовниками, ОІД ТОВ «Огун» віднесено до четвертої (IV) категорії, яка встановлюється для об'єктів обробки інформації з обмеженим доступом без віднесення до державної таємниці. Акт категоріювання є чинним протягом п'яти років за умови незмінності умов функціонування об'єкта. Прийняте рішення оформлено Актом категоріювання (Додаток А), який слугує підставою для виконання подальших етапів робіт зі створення КСЗІ.

Затвердження Акту категоріювання слугує підставою для переходу до наступного етапу робіт зі створення КСЗІ – обстеження середовища функціонування автоматизованої системи, результати якого використовуються для побудови моделей загроз і порушника та формування вимог до комплексу засобів захисту.

2.3 Обстеження середовища функціонування автоматизованої системи

Обстеження середовища функціонування автоматизованої системи проведено з метою отримання достовірних вихідних даних про склад технічних засобів, особливості розміщення обладнання, характеристики приміщень, склад персоналу та порядок взаємодії користувачів з інформаційними ресурсами. Результати обстеження є основою для побудови моделі загроз і моделі порушника,

формування вимог до комплексу засобів захисту та розроблення технічного завдання на створення КСЗІ.

Роботи з обстеження виконані комісією, призначеною наказом керівника ТОВ «Огун» № 19 від 12.03.2026, у складі відповідального за захист інформації, системного адміністратора та представника керівництва. Обстеження охопило три взаємопов’язані середовища функціонування АС класу 2 – обчислювальне, фізичне та середовище користувачів, що дозволило сформувати цілісне уявлення про поточний стан об’єкту інформаційної діяльності та виявити передумови для реалізації загроз інформаційній безпеці.

Характеристика обчислювального середовища. До складу обчислювальної системи АС класу 2 ТОВ «Огун» входить дві групи технічних засобів – основні засоби обробки інформації та допоміжні технічні засоби, що забезпечують функціонування системи.

До основних засобів обробки інформації належать:

– 15 автоматизованих робочих місць користувачів на базі персональних електронно-обчислювальних машин в комплекті з рідкокристалічними моніторами, клавіатурою, маніпулятором типу «миша» та з’єднувальними шнурами;

– 1 сервер локальних служб (контролер домену, файловий сервер) у виконанні rack-mount;

– 1 сервер моніторингу та реєстрації подій;

– 1 мережевий пристрій зберігання даних (NAS) для зберігання резервних копій;

– багатофункціональний пристрій друку, що підключений до локальної мережі.

Об’єднання технічних засобів в локальну мережу здійснюється через керовані комутатори рівня доступу та центральний комутатор серверного приміщення. Передавання інформації між робочими комп’ютерами та серверним обладнанням відбувається виключно в межах локальної мережі ТОВ «Огун», без

використання загальнодоступних мереж як основного технологічного каналу для обробки інформації з обмеженим доступом.

Базове програмне забезпечення автоматизованих робочих місць включає операційну систему Microsoft Windows 11 Pro, офісний пакет, спеціалізовані засоби адміністрування інфраструктури замовників, антивірусний захист та клієнтське програмне забезпечення для роботи з ресурсами серверного обладнання. На серверному обладнанні застосовуються мережеві операційні системи, системи керування базами даних та засоби моніторингу подій інформаційної безпеки.

На момент обстеження засоби захисту від несанкціонованого доступу, що мають експертний висновок Держспецзв'язку, у складі автоматизованої системи відсутні. Розмежування доступу здійснюється виключно штатними засобами операційних систем без додаткового контролю з боку спеціалізованого комплексу засобів захисту, що створює передумови для реалізації загроз інформаційній безпеці.

Характеристика фізичного середовища. Об'єкт інформаційної діяльності розташований за адресою: м. Київ, вул. Героїв Оборони, 15, та охоплює приміщення №№ 201–207 розміщений у межах одного поверху офісної будівлі. Контрольована зона ОІД визначена планом контрольованої зони, затвердженим керівником ТОВ «Огун», та збігається з межами орендованих приміщень.

Огороджувальні конструкції приміщень виконані з цегли, товщина зовнішніх стін становить 380 мм, внутрішніх – 250 мм. Вхідні двері до приміщень ОІД металеві з замикальним пристроєм, внутрішні двері між приміщеннями металопластикові. Віконні отвори обладнані металопластиковими склопакетами та виходять на внутрішній двір будівлі, не межуючи з вулично-дорожньою мережею. В суміжних з ОІД приміщеннях інформація з обмеженим доступом не обробляється, неконтрольоване перебування сторонніх осіб в межах ОІД неможлива завдяки організаційними заходами.

Серверне обладнання розміщене в окремому приміщенні № 205, доступ до якого обмежений колом адміністраторів. Автоматизовані робочі місця

користувачів розташовані в робочих приміщеннях №№ 201-204, при цьому розташування моніторів забезпечує можливість обмеження видимості екранів з боку віконних отворів та входів до приміщень.

Електроживлення ОІД здійснюється від трансформаторної підстанції, що розташована за межами контрольованої зони. Підведення мережі електроживлення до приміщень виконане через окремий ввідний щит, від якого здійснюється розподіл живлення на робочі та допоміжні споживачі. Система заземлення підключена до загальнобудинкового контуру заземлення, який також виходить за межі контрольованої зони. На момент обстеження засобів захисту мережі електроживлення та заземлення від витоку інформації каналами наводок не встановлено.

Засоби захисту від витоку інформації за рахунок побічних електромагнітних випромінювань на момент обстеження також відсутні, що створює передумови для перехоплення інформативних сигналів від моніторів автоматизованих робочих місць та інших технічних засобів обробки інформації спеціальними приймальними засобами поза межами контрольованої зони.

В приміщеннях ОІД присутні допоміжні технічні засоби та системи, що не беруть участі в обробці інформації з обмеженим доступом, але можуть виступати середовищем поширення інформативних сигналів за межі контрольованої зони. До таких засобів належать системи опалення, водопостачання, вентиляції, а також лінії пожежної сигналізації, що мають вихід за межі ОІД. Зазначені фактори враховуються під час формування моделі загроз.

Характеристика середовища користувачів**.** Безпосередню роботу з ресурсами автоматизованої системи здійснюють 15 співробітників ТОВ «Огун», що мають різні функціональні обов’язки та різний обсяг повноважень щодо інформаційних ресурсів. За рівнем повноважень суб’єкти доступу до АС поділяються на категорії, наведені в таблиці 2.1 (складено автором на основі [7], [10], [17]).

Таблиця 2.1 – Категорії суб’єктів доступу до АС класу 2 ТОВ «Огун»

Категорія	Кількість	Функціональні обов’язки
Керівник підприємства	1	Загальне керівництво, прийняття управлінських рішень, доступ до повного обсягу інформаційних ресурсів
Адміністратор безпеки	1	Контроль виконання політики безпеки, керування правами доступу, аналіз журналів подій
Системний адміністратор	1	Адміністрування технічних засобів і програмного забезпечення, супровід серверного обладнання
Інженери технічної підтримки	8	Надання послуг адмініструванню інфраструктури замовників, робота з технічною документацією
Керівники проєктів	2	Координація робіт за договорами, ведення документації з замовниками
Особа з документального супроводу	2	Опрацювання договірної документації, ведення внутрішніх регламентів

Доступ до інформаційних ресурсів АС надається на підставі функціональних обов’язків кожної категорії суб’єктів. На момент обстеження розмежування доступу здійснюється засобами операційних систем без застосування додаткового спеціалізованого комплексу засобів захисту, реєстрація подій безпеки виконується частково, контроль адміністративних дій не реалізований в повному обсязі. Зазначені обставини є передумовами для реалізації загроз внутрішнього походження та потребують протидії в процесі впровадження КСЗІ.

Автоматизована система функціонує в трьох основних режимах: основному режимі обробки інформації, режимі технічного обслуговування під час виконання робіт з адміністрування та аварійному режимі у разі виникнення відмов окремих компонентів. Регламентація режимів роботи та порядок переходу між ними на момент обстеження не оформлені окремим внутрішнім документом, що також враховується при формуванні вимог до КСЗІ.

Результати обстеження. За результатами обстеження середовища функціонування АС встановлено наявність комплексу передумов, що знижують рівень захищеності інформації з обмеженим доступом. До основних встановлених фактів належать відсутність спеціалізованого комплексу засобів захисту від несанкціонованого доступу, відсутність засобів захисту мережі електроживлення та заземлення від витоку інформації, відсутність засобів захисту від витоку інформації за рахунок побічних електромагнітних випромінювань технічних засобів обробки інформації, неповна реєстрація подій безпеки, відсутність регламентованих процедур розмежування доступу та керування повноваженнями, відсутність технічної системи охорони, що забезпечує своєчасне виявлення спроб несанкціонованого проникнення в межі контрольованої зони.

Виявлені обставини зафіксовано в Акті обстеження ОІД (Додаток Б), який слугує вихідним документом для побудови моделі загроз, моделі порушника та формування комплексу захисних заходів у складі створюваної КСЗІ.

2.4 Побудова моделі загроз інформаційній безпеці

Модель загроз інформаційній безпеці розроблено на підставі результатів обстеження середовища функціонування АС класу 2 ТОВ «Огун», з урахуванням складу інформаційних ресурсів, виявлених передумов реалізації загроз та особливостей розміщення технічних засобів на об’єкті інформаційної діяльності. Метою побудови моделі є систематизація актуальних загроз, визначення джерел їх виникнення, можливих способів реалізації та наслідків впливу на властивості інформації, що підлягає захисту. Для класифікації можливих способів реалізації загроз додатково враховано підходи бази знань MITRE ATT&CK, що систематизує тактики та техніки дій порушників в інформаційних системах [23]. Результати моделювання є вихідними даними для розробки моделі порушника, формування політики безпеки та визначення складу комплексу засобів захисту інформації.

За результатами аналізу виявлених передумов на ОІД ТОВ «Огун» виділено три групи актуальних загроз, загрози несанкціонованого доступу до інформаційних

ресурсів АС, загрози витоку інформації технічними каналами та загрози порушення працездатності системи. Дана класифікація відповідає підходу, закладеному в нормативних документах системи ТЗІ, та дозволяє узгодити склад загроз з функціональними послугами безпеки, що визначатимуться у складі КСЗІ.

Загрози несанкціонованого доступу. Локалізований багатомашинний багатокористувацький характер АС класу 2 та відсутність на момент обстеження спеціалізованого комплексу засобів захисту створюють передумови для реалізації загроз з боку як зовнішніх, так і внутрішніх джерел. До найбільш суттєвих загроз цієї групи належать несанкціонований доступ до інформаційних ресурсів з використанням облікових даних інших користувачів, перевищення наданих повноважень, несанкціоноване копіювання інформації на знімні носії, неконтрольоване виведення інформації на друк, обхід штатних механізмів розмежування доступу через адміністративні інтерфейси.

Окрему категорію складають загрози впровадження шкідливого програмного забезпечення через зовнішні носії інформації, електронну пошту або веб-ресурси, що використовуються в процесі виконання службових завдань. Реалізація таких загроз може призвести як до порушення конфіденційності інформації, так і до її модифікації або знищення.

Загрози витоку інформації технічними каналами. З урахуванням особливостей розміщення ОІД та виходу інженерних комунікацій за межі контрольованої зони, актуальними є загрози витоку інформації через електромагнітні та електричні канали. На момент обстеження засоби захисту мережі електроживлення та заземлення від витоку інформації відсутні, що створює передумови для перехоплення інформативних сигналів за допомогою спеціальних технічних засобів.

Окрему групу загроз становить витік інформації за рахунок побічних електромагнітних випромінювань технічних засобів обробки інформації безпосередньо в простір. В процесі функціонування моніторів, системних блоків та інших засобів обробки інформації генеруються електромагнітні сигнали, що

містять компоненти, корельовані з оброблюваною інформацією. За відсутності засобів активного захисту, сигнали поширюються в навколишньому просторі та можуть бути зафіксовані спеціальними приймальними засобами, розміщеними поза межами контрольованої зони, з подальшим відновленням оброблюваної інформації.

Витік інформації каналами побічних електромагнітних випромінювань і наводок (ПЕМВН) можливий внаслідок наведення інформативних сигналів від технічних засобів обробки інформації на провідні комунікації, що виходять за межі контрольованої зони. До подібних комунікацій належать мережа електроживлення, контур заземлення, лінії пожежної сигналізації та інші провідні системи. Підключення спеціальних засобів реєстрації до зазначених комунікацій поза межами контрольованої зони дозволяє виокремити інформативні сигнали з рівня шумів та відновити інформацію, що оброблялась технічними засобами.

Окрему загрозу становить можливість витоку інформації через систему електроживлення внаслідок наведення сигналів від ПЕОМ на провідники мережі 220 В. За відсутності завадозаглушувальних фільтрів та розділового трансформатора інформативні сигнали поширюються мережею електроживлення за межі контрольованої зони, де можуть бути зафіксовані спеціальними приймальними засобами.

Загрози порушення працездатності системи. До цієї групи належать загрози, реалізація яких призводить до порушення доступності інформаційних ресурсів та неможливості виконання основних виробничих завдань. Зокрема, актуальними є загрози фізичного пошкодження технічних засобів внаслідок несанкціонованого проникнення в межі контрольованої зони, відмови обладнання через відсутність регламентного обслуговування, втрати інформації внаслідок відсутності резервного копіювання, порушення працездатності системи через дії шкідливого програмного забезпечення.

Окремо враховуються загрози, пов’язані з відсутністю на момент обстеження технічної системи охорони. За відсутності сповіщувачів несанкціонованого

проникнення можливе тривале знаходження сторонніх осіб в межах контрольованої зони без своєчасного виявлення, що створює умови для реалізації як загроз НСД, так і загроз фізичного впливу на технічні засоби.

Систематизований перелік актуальних загроз для АС класу 2 ТОВ «Огун» з визначенням джерел виникнення, способів реалізації та властивостей інформації, що порушуються внаслідок реалізації загроз, наведено у таблиці 2.2 (складено автором на основі [7], [9], [13], [14]).

Таблиця 2.2 – Зведена модель загроз інформаційній безпеці АС класу 2 ТОВ «Огун»

№	Найменування загрози	Джерело виникнення	Спосіб реалізації	К	Ц	Д
1	Несанкціонований доступ до інформаційних ресурсів АС	Сторонні особи, персонал	Використання чужих облікових даних, обхід механізмів автентифікації	+	+	+
2	Перевищення наданих повноважень користувачами	Персонал АС	Виконання дій, що виходять за межі функціональних обов’язків	+	+	–
3	Несанкціоноване копіювання інформації на знімні носії	Персонал АС, сторонні особи	Підключення USB-носіїв, копіювання файлів	+	–	–
4	Неконтрольоване виведення інформації на друк	Персонал АС	Друк документів з інформацією з обмеженим доступом без обліку	+	–	–
5	Маскування під зареєстрованого користувача	Сторонні особи, персонал	Перехоплення облікових даних, підглядання процесу входу в систему	+	+	+
6	Впровадження шкідливого програмного забезпечення	Сторонні особи, персонал	Зовнішні носії, електронна пошта, веб-ресурси	+	+	+

Продовження таблиці 2.2

№	Найменування загрози	Джерело виникнення	Спосіб реалізації	К	Ц	Д
7	Витік інформації через мережу електроживлення	Сторонні особи	Підключення засобів реєстрації до мережі 220 В поза межами КЗ	+	–	–
8	Витік інформації через коло заземлення	Сторонні особи	Підключення засобів реєстрації до контуру заземлення поза межами КЗ	+	–	–
9	Витік інформації каналами ПЕМВН через провідні комунікації	Сторонні особи	Перехоплення наведень на лінії пожежної сигналізації, інженерні комунікації	+	–	–
10	Витік інформації через побічні електромагнітні випромінювання технічних засобів у простір	Сторонні особи	Перехоплення електромагнітних сигналів моніторів і ПЕОМ спеціальними приймальними засобами поза межами КЗ	+	–	–
11	Несанкціоноване проникнення в межі контрольованої зони	Сторонні особи	Подолання вхідних дверей, проникнення через віконні отвори	+	+	+
12	Фізичне пошкодження технічних засобів	Сторонні особи, персонал	Цілеспрямовані дії, необережне поводження	–	+	+
13	Втрата інформації внаслідок відмови обладнання	Технічні засоби	Відмова накопичувачів, збої електроживлення, програмні помилки	–	+	+
14	Модифікація службових файлів та конфігурацій	Персонал АС, шкідливе ПЗ	Несанкціонована зміна параметрів системи захисту	–	+	+
15	Блокування доступу до інформаційних ресурсів	Шкідливе ПЗ, сторонні особи	Шифрування файлів, перевантаження ресурсів	–	–	+

Примітка: К – конфіденційність, Ц – цілісність, Д – доступність.

Класифікація загроз за джерелом виникнення дозволяє виділити внутрішні загрози, пов’язані з діями персоналу АС, та зовнішні загрози, що реалізуються сторонніми особами або технічними засобами поза межами контрольованої зони. За характером впливу загрози поділяються на пасивні, спрямовані на отримання інформації без зміни її стану, та активні, що супроводжуються модифікацією інформації або порушенням працездатності системи. За способом реалізації виділяються технічні, програмні, організаційні та комбіновані загрози. Узагальнена класифікація загроз для АС класу 2 ТОВ «Огун» наведена на (рис. 2.1).

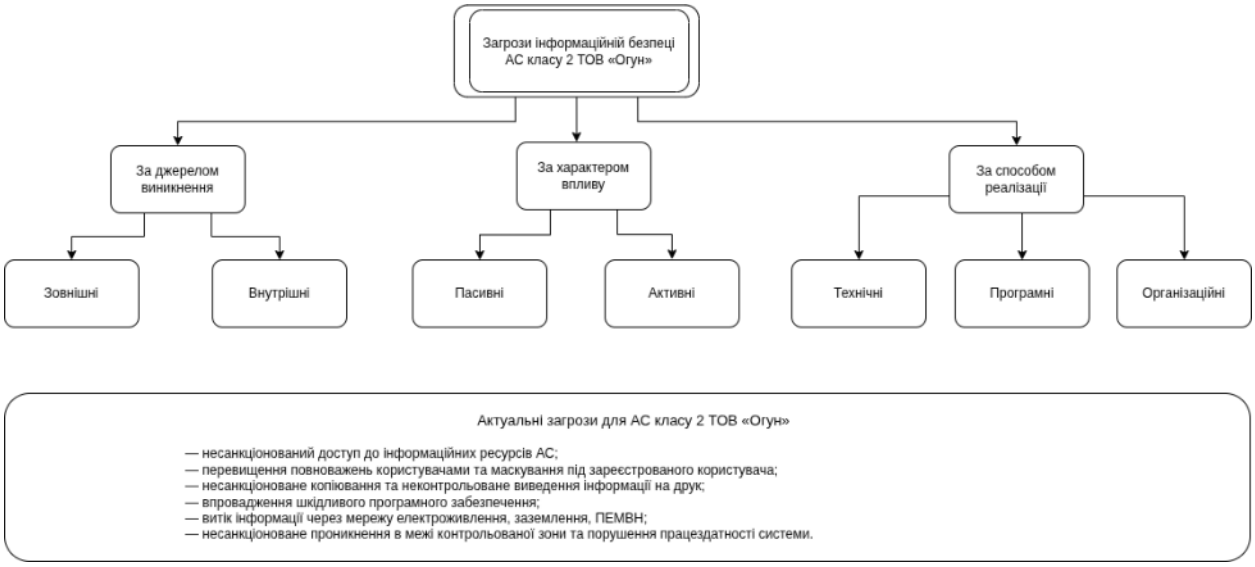

Рисунок 2.1 – Класифікація загроз інформаційній безпеці АС класу 2 ТОВ «Огун» (розроблено автором)

Згідно зі статистичними даними міжнародних звітів про інциденти інформаційної безпеки, значна частка реалізованих порушень пов’язана саме з діями внутрішніх користувачів або компрометацією їхніх облікових записів [24].

З урахуванням специфіки локалізованого багатомашинного багатокористувацького комплексу та виявлених передумов, найбільшу актуальність становлять загрози несанкціонованого доступу з боку персоналу АС, загрози витоку інформації через систему електроживлення і заземлення, а також, загрози витоку через побічні електромагнітні випромінювання технічних засобів обробки інформації безпосередньо в простір. Менш вірогідними, але такими, що

потребують врахування, є загрози витоку через провідні комунікації, що виходять за межі контрольованої зони.

2.5 Побудова моделі порушника

Модель порушника побудована з метою визначення кола осіб, які за наявних умов функціонування АС класу 2 ТОВ «Огун» можуть здійснити спробу реалізації виявлених в моделі загроз дій, спрямованих на порушення конфіденційності, цілісності або доступності інформації з обмеженим доступом. Модель відображає категорії потенційних порушників, рівень їх кваліфікації, можливості використання технічних засобів, мотиви здійснення порушень, а також, просторово-часові характеристики потенційних дій. Результати моделювання є вихідними даними для формування політики безпеки та визначення вимог до функціональних послуг безпеки в складі комплексу засобів захисту.

Під порушником в межах цієї моделі розуміється особа, яка внаслідок навмисних дій, помилкових дій унаслідок недостатньої обізнаності або з інших мотивів здійснює спробу виконати в межах АС операції, що призводять або можуть призвести до порушення властивостей інформації, визначених політикою безпеки. Поняття порушника охоплює як осіб, що мають правомірний доступ до АС у межах виконання службових обов’язків, так і осіб, доступ яких до системи не передбачено.

Категорії порушників**.** За результатами аналізу складу персоналу ТОВ «Огун», особливостей розміщення ОІД та виявлених передумов реалізації загроз, виділено дві основні категорії порушників – внутрішні та зовнішні. Розподіл порушників за категоріями з визначенням їх характеристик наведено в таблиці 2.3 (складено автором на основі [7], [10], [13], [17]).

Таблиця 2.3 – Категорії потенційних порушників АС класу 2 ТОВ «Огун»

Категорія	Склад	Характеристика
Внутрішні порушники		
– користувачі АС	Інженери технічної підтримки, керівники проєктів, особи з документального супроводу	Мають правомірний доступ до інформаційних ресурсів у межах функціональних обов'язків, обізнані щодо порядку роботи АС, можуть діяти з мотивів корисливості, помилки або недостатньої обізнаності
– обслуговуючий персонал	Системний адміністратор	Має розширені повноваження щодо адміністрування технічних засобів і програмного забезпечення, обізнаний щодо архітектури та налаштувань системи
– адміністратори безпеки	Особа, відповідальна за захист інформації	Має повний доступ до засобів керування КСЗІ, журналів подій, налаштувань комплексу засобів захисту
Зовнішні порушники		
– сторонні особи з доступом на територію	Відвідувачі підприємства, представники замовників, працівники служб обслуговування будівлі	Можуть короткостроково перебувати в межах контрольованої зони у супроводі відповідальних осіб або без супроводу за відсутності контролю
– особи без доступу на територію	Сторонні особи, що знаходяться поза межами контрольованої зони	Можуть здійснювати дії з використанням технічних засобів перехоплення інформації, не отримуючи фізичного доступу до приміщень ОІД

Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо АС. За показниками кваліфікації та обізнаності щодо архітектури і функціонування автоматизованої системи виділено чотири рівні підготовки потенційного порушника. Перший рівень охоплює осіб, які володіють загальною інформацією про функціональні особливості засобів обчислювальної техніки та вміють

користуватися штатними засобами операційних систем і прикладного програмного забезпечення. Другий рівень характеризує осіб з досвідом роботи з технічними засобами автоматизованих систем та обслуговування обчислювальної техніки. Третій рівень включає осіб, які володіють поглибленими знаннями у галузі обчислювальної техніки, програмування та експлуатації автоматизованих систем. Наступний рівень відповідає особам, обізнаним щодо принципів роботи та механізмів реалізації засобів захисту в автоматизованих системах.

Специфікація моделі порушника за можливостями використання засобів і методів подолання системи захисту. За показниками доступних засобів реалізації несанкціонованого доступу до інформації виділяються чотири рівні. Перший рівень передбачає використання виключно агентурних методів отримання відомостей без застосування технічних засобів. Другий рівень охоплює застосування пасивних технічних засобів перехоплення інформативних сигналів, зокрема приймальної апаратури для реєстрації побічних електромагнітних випромінювань і наводок. Третій рівень включає використання штатних засобів автоматизованих систем або експлуатацію недоліків в реалізації системи захисту інформації. Наступний рівень відповідає застосуванню активних засобів впливу на АС, що передбачає підключення додаткового обладнання, модифікацію штатних технічних засобів або впровадження спеціального програмного забезпечення.

Специфікація моделі порушника за місцем дії. За показниками просторового розташування під час реалізації загроз виділяються п’ять рівнів. Перший рівень характеризує дії порушника без отримання фізичного доступу на територію підприємства. Другий рівень передбачає отримання доступу на територію в межах контрольованої зони без доступу до робочих місць АС. Третій рівень включає отримання доступу до робочого місця користувача АС. Наступний рівень передбачає доступ до масивів інформації, що накопичується та зберігається в АС, зокрема до серверного обладнання та засобів резервного копіювання. Останній рівень відповідає отриманню доступу до засобів адміністрування АС та керування комплексом засобів захисту інформації.

Специфікація моделі порушника за часом дії. За показниками часу здійснення несанкціонованих дій виділяються три рівні. Перший рівень охоплює дії, що здійснюються лише в робочий час підприємства за умови присутності персоналу. Другий рівень передбачає дії в позаробочий час за наявності фізичного доступу до приміщень ОІД. Третій рівень характеризує можливість дій в будь-який час доби, зокрема з використанням віддалених засобів реалізації загроз.

Специфікація за мотивами здійснення порушень. Мотивація потенційних порушників визначається їх категорією та особистими обставинами. Для внутрішніх порушників характерними є мотиви корисливості, особистої образи, помилкові дії внаслідок недостатньої обізнаності або необережності, дії під впливом сторонніх осіб шляхом шантажу або підкупу. Для зовнішніх порушників домінуючими є мотиви корисливості, виконання замовлення третіх осіб, а також, ідеологічні мотиви, спрямовані на завдання шкоди діяльності підприємства.

Зведена характеристика моделі порушника. Сукупна оцінка потенційних порушників АС класу 2 ТОВ «Огун» за всіма наведеними показниками подана в таблиці 2.4 (складено автором на основі [7], [10], [13], [17]). Рівень загрози від кожної категорії порушників визначений за чотирибальною шкалою, де 1 – незначний рівень, 2 – припустимий рівень, 3 – середній рівень, 4 – високий рівень.

Таблиця 2.4 – Зведена характеристика моделі порушника АС класу 2 ТОВ «Огун»

Категорія порушника	Кваліфікація	Засоби	Місце	Час	Сумарний рівень
Користувачі АС	1–2	3	3	1	3
Системний адміністратор	3	3–4	4	2	4
Адміністратор безпеки	4	4	5	2	4
Сторонні особи з доступом на територію	1–2	1–2	2	1	2
Сторонні особи без доступу на територію	2–4	2	1	3	3

Найбільший рівень потенційної загрози становлять внутрішні порушники з числа обслуговуючого персоналу та адміністраторів безпеки, оскільки вони володіють поглибленими знаннями щодо архітектури АС і мають розширені повноваження. Зовнішні порушники без доступу на територію також становлять суттєву загрозу через можливість використання пасивних технічних засобів перехоплення інформативних сигналів за межами контрольованої зони, що особливо актуально з огляду на виявлені передумови витоку інформації через мережу електроживлення та контур заземлення.

Побудована модель порушника використовується для формування політики безпеки інформації в АС, визначення вимог до функціональних послуг безпеки та обґрунтування вибору комплексу засобів захисту. Даний підхід узгоджується з міжнародною практикою управління ризиками інформаційної безпеки, закріпленою в NIST SP 800-37 «Risk Management Framework» [25]. Зокрема, врахування високого рівня загрози від внутрішніх порушників з розширеними повноваженнями зумовлює необхідність реалізації механізмів реєстрації дій адміністраторів та контролю цілісності засобів захисту, а врахування загрози від зовнішніх порушників, які використовують технічні засоби перехоплення, – необхідність впровадження засобів захисту мережі електроживлення та заземлення.

2.6 Розробка політики безпеки інформації в АС

Політика безпеки інформації в автоматизованій системі ТОВ «Огун» розроблена на підставі результатів категоріювання ОІД, обстеження середовища функціонування АС, побудованих моделі загроз і моделі порушника, з урахуванням вимог нормативних документів системи технічного захисту інформації. Документ визначає принципи, правила та обмеження, які мають впроваджуватися в межах створюваної КСЗІ для забезпечення захисту інформації з обмеженим доступом протягом усього технологічного циклу її обробки.

Положення політики безпеки є обов’язковими для всіх категорій користувачів АС, а їх виконання забезпечується сукупністю організаційних, програмно-технічних та інженерно-технічних заходів. Загальну відповідальність за стан інформаційної безпеки несе керівник ТОВ «Огун», безпосередня організація робіт та контроль виконання покладаються на відповідального за захист інформації.

Розмежування доступу та автентифікація. Доступ користувачів до інформаційних ресурсів АС надається за принципом мінімально необхідних повноважень на підставі функціональних обов’язків. Принцип мінімально необхідних повноважень є базовим у сучасних моделях керування доступом, в тому числі в моделі атрибутного контролю доступу ABAC, що систематизована у NIST SP 800-162 [26]. Кожен користувач отримує індивідуальний обліковий запис, використання якого іншими особами заборонено. Автентифікація здійснюється з використанням паролів, що відповідають вимогам складності та підлягають періодичній зміні. Вимоги до автентифікаторів та керування ними деталізовано у NIST SP 800-63B «Digital Identity Guidelines: Authentication and Authenticator Management» [27]. Обліковий запис автоматично блокується після визначеної кількості невдалих спроб входу. Надання, зміна та анулювання прав доступу оформлюються заявками, погодженими з відповідальним за захист інформації, з періодичним переглядом не рідше одного разу на півріччя.

Реєстрація подій безпеки. В межах АС забезпечується реєстрація входу та завершення сеансів користувачів, спроб доступу до ресурсів, виконання адміністративних дій, зміни прав доступу, операцій з носіями інформації. Журнали зберігаються протягом не менше шести місяців, періодичний аналіз виконує адміністратор безпеки з метою виявлення відхилень від штатного режиму роботи.

Робота з носіями та антивірусний захист. Використання знімних носіїв обмежується переліком зареєстрованих та закріплених за користувачами носіїв. Підключення сторонніх носіїв заборонене. На всіх АРМ та серверному обладнанні функціонують засоби антивірусного захисту з регулярним оновленням баз

сигнатур. Знищення інформації з носіїв виконується гарантованими методами з документальним оформленням.

Технічний захист та фізична безпека. Для запобігання витоку інформації застосовуються мережеві завадозаглушувальні фільтри та засоби локального захищеного заземлення в межах контрольованої зони. Винесення технічних засобів з обробки ІзОД за межі КЗ дозволяється виключно після гарантованого видалення інформації. Доступ до приміщень ОІД в позаробочий час контролюється технічними засобами охорони, допуск сторонніх осіб здійснюється у супроводі співробітників з фіксацією в журналі обліку відвідувачів.

Реагування на інциденти. При виявленні подій з ознаками інциденту інформаційної безпеки забезпечується ізоляція джерела, збереження доказових записів, з’ясування обставин та документальне оформлення, що відповідає загальноприйнятому міжнародному підходу до управління інцидентами інформаційної безпеки [28]. За результатами розгляду вносяться відповідні корективи до налаштувань засобів захисту або положень політики.

Функціональний профіль захищеності АС. Сукупність функціональних послуг безпеки, що реалізуються у складі КСЗІ для виконання положень політики безпеки, оформлюється у вигляді функціонального профілю захищеності оброблюваної інформації від несанкціонованого доступу. Профіль формується відповідно до НД ТЗІ 2.5-004-99, який встановлює критерії оцінки захищеності інформації в комп’ютерних системах, та НД ТЗІ 2.5-005-99, який визначає стандартні функціональні профілі захищеності для автоматизованих систем різних класів. Для АС класу 2, в якій обробляється службова та конфіденційна інформація без віднесення до державної таємниці, додатково враховуються вимоги НД ТЗІ 2.5-008-2002 щодо мінімально необхідного переліку функціональних послуг безпеки.

З урахуванням визначеного складу інформації з обмеженим доступом, побудованої моделі загроз та моделі порушника, для АС класу 2 ТОВ «Огун» обрано функціональний профіль захищеності, склад якого наведено в таблиці 2.5 (складено автором на основі [7], [9], [10], [12]).

Таблиця 2.5 – Функціональний профіль захищеності АС класу 2 ТОВ «Огун»

Послуга	Найменування	Рівень	Обґрунтування
КД	Довірча конфіденційність	КД-2	Розмежування доступу до інформаційних ресурсів на підставі прав доступу, встановлених власником інформації, з керуванням потоками
ЦД	Довірча цілісність	ЦД-1	Захист цілісності інформації від несанкціонованої модифікації на підставі прав доступу, визначених власником
НР	Реєстрація	НР-2	Реєстрація подій безпеки із захистом журналу від несанкціонованого доступу та модифікації
НИ	Ідентифікація і автентифікація	НИ-2	Ідентифікація користувача за обліковим записом з підтвердженням паролем до надання доступу
НК	Достовірний канал	НК-1	Достовірний канал введення облікових даних під час автентифікації
НО	Розподіл обов’язків	НО-1	Розмежування повноважень між адміністратором і звичайним користувачем системи
НЦ	Цілісність КЗЗ	НЦ-1	Контроль цілісності компонентів комплексу засобів захисту

Сукупний функціональний профіль захищеності АС класу 2 ТОВ «Огун» має такий вигляд:

2.КЦ.1 = { КД-2, ЦД-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1 }

Профіль належить до групи функціональних профілів захищеності для АС класу 2, призначених для обробки інформації, що потребує забезпечення конфіденційності та цілісності за умов підвищених вимог до спостережності системи. Обраний склад функціональних послуг забезпечує мінімально необхідний рівень захищеності для службової та конфіденційної інформації відповідно до НД ТЗІ 2.5-008-2002 та враховує специфіку локалізованого багатомашинного багатокористувацького комплексу.

Рівень гарантій реалізації функціонального профілю**.** Відповідно до НД ТЗІ 2.5-004-99, для АС класу 2, в якій обробляється службова та конфіденційна інформація без віднесення до державної таємниці, встановлюється рівень гарантій

Г-3. Даний рівень гарантій передбачає, що розробник комплексу засобів захисту забезпечує документоване підтвердження реалізації заявлених функціональних послуг, проведення випробувань КЗЗ за програмою та методикою, узгодженою з замовником, а також документоване підтвердження керованості процесу розробки та супроводу засобів захисту.

Реалізація обраного функціонального профілю 2.КЦ.1 з рівнем гарантій Г-3 забезпечується сукупним застосуванням програмно-апаратного комплексу засобів захисту від несанкціонованого доступу, технічних засобів захисту від витоку інформативних сигналів каналами наводок, інженерно-технічних засобів обмеження фізичного доступу та організаційних заходів, що визначаються в структурі та архітектурі КСЗІ.

Контроль виконання положень політики. Контроль за дотриманням положень політики безпеки здійснює адміністратор безпеки шляхом аналізу журналів реєстрації подій, проведення планових перевірок стану засобів захисту, контролю фактичних повноважень користувачів. Періодичність планових перевірок становить не рідше одного разу на квартал. Внесення змін до політики безпеки здійснюється у разі зміни нормативної бази, складу інформаційних ресурсів АС, виявлення нових загроз або за результатами розгляду інцидентів інформаційної безпеки.

Розроблена політика безпеки інформації, сформалізована у вигляді функціонального профілю захищеності 2.КЦ.1 з рівнем гарантій Г-3, використовується як основа для формування технічного завдання на створення КСЗІ та визначення складу комплексу засобів захисту, що проєктується у наступних підрозділах.

2.7 Формування структури та архітектури КСЗІ

Структура комплексної системи захисту інформації для АС класу 2 ТОВ «Огун» формується з урахуванням обраного функціонального профілю захищеності 2.КЦ.1 з рівнем гарантій Г-3, виявлених в процесі обстеження

передумов реалізації загроз, побудованої моделі загроз та моделі порушника. Архітектура КСЗІ є сукупністю взаємопов’язаних підсистем, кожна з яких реалізує визначений набір захисних функцій та забезпечує протидію відповідних груп загроз.

Склад підсистем КСЗІ. За результатами аналізу вимог до захисту та виявлених передумов до складу КСЗІ ТОВ «Огун» включено п’ять взаємопов’язаних підсистем:

– підсистема захисту від несанкціонованого доступу, що забезпечує реалізацію функціональних послуг безпеки, визначених у функціональному профілі;

– підсистема антивірусного захисту, що забезпечує виявлення та блокування шкідливого програмного забезпечення на технічних засобах АС;

– підсистема захисту від витоку інформації технічними каналами, що забезпечує запобігання витоку інформативних сигналів через мережу електроживлення, контур заземлення та провідні комунікації, що виходять за межі контрольованої зони;

– технічна система охорони, що забезпечує виявлення спроб несанкціонованого проникнення в межі контрольованої зони у позаробочий час;

– підсистема організаційно-розпорядчого забезпечення, що включає документальне забезпечення функціонування КСЗІ та регламентацію дій персоналу.

Основу підсистеми складає засіб захисту інформації від несанкціонованого доступу «Лоза-2», що має чинний експертний висновок Держспецзв'язку та відповідає вимогам функціонального профілю 2.КЦ.1. Засіб спеціально призначений для застосування у складі КСЗІ автоматизованих систем класу 2 (локальних обчислювальних мереж) та забезпечує реалізацію функціональних послуг безпеки, передбачених НД ТЗІ 2.5-004-99 і НД ТЗІ 2.5-008-2002.

Функціональні можливості «Лоза-2» включають ідентифікацію та автентифікацію користувачів з використанням облікових даних, розмежування

доступу до інформаційних ресурсів на підставі повноважень користувачів, реєстрацію подій безпеки в захищеному журналі, контроль цілісності компонентів засобу захисту, розмежування повноважень адміністраторів та користувачів, контроль виведення інформації на знімні носії, гарантоване видалення інформації з пам’яті носіїв.

Засіб «Лоза-2» встановлюється на всіх 15 автоматизованих робочих місцях користувачів та на серверному обладнанні АС. Керування засобом захисту здійснюється з робочого місця адміністратора безпеки, що розташоване в окремому приміщенні № 206 відповідно до результатів обстеження ОІД.

Підсистема антивірусного захисту. Підсистема антивірусного захисту реалізована з використанням продукту ESET Endpoint Security, що має чинний експертний висновок Державної служби спеціального зв’язку та захисту інформації України. Експертний висновок підтверджує відповідність продукту нормативним документам, що регламентують вимоги до засобів технічного захисту інформації, та дозволяє використання рішення у складі КСЗІ автоматизованих систем, в яких обробляється інформація з обмеженим доступом

Функціональні можливості ESET Endpoint Security включають проактивне виявлення шкідливого програмного забезпечення з використанням сигнатурного та поведінкового аналізу, контроль виконуваних процесів і автозавантаження, контроль підключення знімних носіїв інформації, контроль мережевого трафіку на рівні робочих комп’ютерів, ведення журналів виявлених загроз. Продукт встановлюється на всіх 15 автоматизованих робочих місцях та серверному обладнанні АС.

Централізоване керування підсистемою антивірусного захисту здійснюється через консоль ESET PROTECT, що розгортається на сервері локальних служб. Консоль забезпечує централізоване розповсюдження оновлень антивірусних баз, керування політиками антивірусного захисту, моніторинг стану захисту на кінцевих пристроях та формування звітів про виявлені загрози. Адміністрування підсистеми здійснюється з робочого місця адміністратора безпеки.

Підсистема захисту від витоку інформації технічними каналами. З урахуванням виявлених у підрозділі 2.3 передумов витоку інформації через мережу електроживлення та контур заземлення, до складу підсистеми включено сукупність активних та пасивних засобів захисту:

– мережевий завадозаглушувальний фільтр «ФЗП-103-2» виробництва ТОВ «ЕМСБІ», що забезпечує захист інформації в широкому діапазоні частот від 10 кГц до 1000 МГц від витоку колами електроживлення основних і допоміжних технічних засобів цифрової та аналогової обробки інформації;

– розділовий трансформатор, що забезпечує гальванічну розв’язку мережі електроживлення ОІД від загальнобудинкової мережі та запобігає поширенню інформативних сигналів за межі контрольованої зони;

– локальний контур заземлення в межах контрольованої зони з опором, що не перевищує 2 Ом, який забезпечує відведення інформативних сигналів без виходу за межі ОІД.

– генератор шуму електромагнітних випромінювань «Базальт-5ГЕШ» виробництва ПрАТ «Холдингова компанія "Укрспецтехніка"», що забезпечує активний захист технічних засобів обробки інформації від витоку каналами побічних електромагнітних випромінювань шляхом створення в навколишньому просторі електромагнітного поля шуму.

Фільтр «ФЗП-103-2» встановлюється на вході мережі електроживлення в приміщення ОІД та забезпечує фільтрацію всіх ліній живлення, що проходять у бік технічних засобів обробки інформації. Розділовий трансформатор розміщується послідовно з фільтром та формує закінчену пасивно-активну систему захисту мережі електроживлення. Локальний контур заземлення прокладається в межах контрольованої зони з обладнанням окремого заглибленого заземлювача.

Генератор шуму «Базальт-5ГЕШ» розміщується в робочому приміщенні № 201 та забезпечує формування електромагнітного поля шуму за допомогою рамкової антени. Дальність ефективної дії генератора охоплює всі робочі приміщення з розміщеними автоматизованими робочими місцями.

Електромагнітне поле шуму, що формується генератором, маскує інформативні сигнали побічних випромінювань технічних засобів обробки інформації та унеможливлює їх виокремлення приймальними засобами поза межами контрольованої зони. Електроживлення генератора здійснюється від мережі електроживлення ОІД через фільтр «ФЗП-103-2», що забезпечує одночасне використання двох рівнів захисту – пасивного фільтра у колах живлення та активного зашумлення у просторі.

Технічна система охорони. З метою виявлення спроб несанкціонованого проникнення в межі контрольованої зони у позаробочий час до складу КСЗІ включено технічну систему охорони, що складається з прийомно-контрольного приладу, сповіщувачів виявлення проникнення та засобів сповіщення відповідальних осіб. До складу системи входять:

- інфрачервоні сповіщувачі руху, що встановлюються в робочих приміщеннях, серверному приміщенні та приміщенні адміністратора безпеки для виявлення переміщення осіб в позаробочий час;

- акустичні сповіщувачі розбиття скла, що встановлюються поблизу віконних отворів для виявлення спроб несанкціонованого проникнення через вікна;

- прийомно-контрольний прилад, що приймає сигнали від сповіщувачів, забезпечує їх обробку, ведення журналу подій та формування сигналів тривоги.

Технічна система охорони функціонує в автономному режимі у позаробочий час, її стан контролюється відповідальною особою з фіксацією факту постановки та зняття з охорони в журналі. При спрацьовуванні сповіщувачів формується сигнал тривоги, який передається на пульт централізованого спостереження.

Системи відеоспостереження у складі технічної системи охорони не передбачаються з огляду на обмеження щодо застосування засобів візуальної реєстрації на об’єктах, де обробляється інформація з обмеженим доступом.

Підсистема організаційно-розпорядчого забезпечення. Підсистема включає сукупність внутрішніх документів ТОВ «Огун», що забезпечують функціонування КСЗІ та регламентують дії персоналу. До складу документів входять наказ

керівника про створення КСЗІ, положення про службу захисту інформації, посадова інструкція відповідального за захист інформації, інструкція з реагування на інциденти, журнал обліку відвідувачів, журнал обліку знімних носіїв інформації, журнал реєстрації змін у налаштуваннях засобів захисту.

Розміщення засобів КСЗІ на ОІД. Розташування технічних засобів обробки інформації та засобів захисту в межах контрольованої зони наведено на (рис. 2.2). Схема відображає взаємне розміщення автоматизованих робочих місць користувачів, серверного обладнання з консоллю ESET PROTECT, засобу захисту мережі електроживлення «ФЗП-103-2», розділового трансформатора, контуру локального заземлення та сповіщувачів технічної системи охорони.

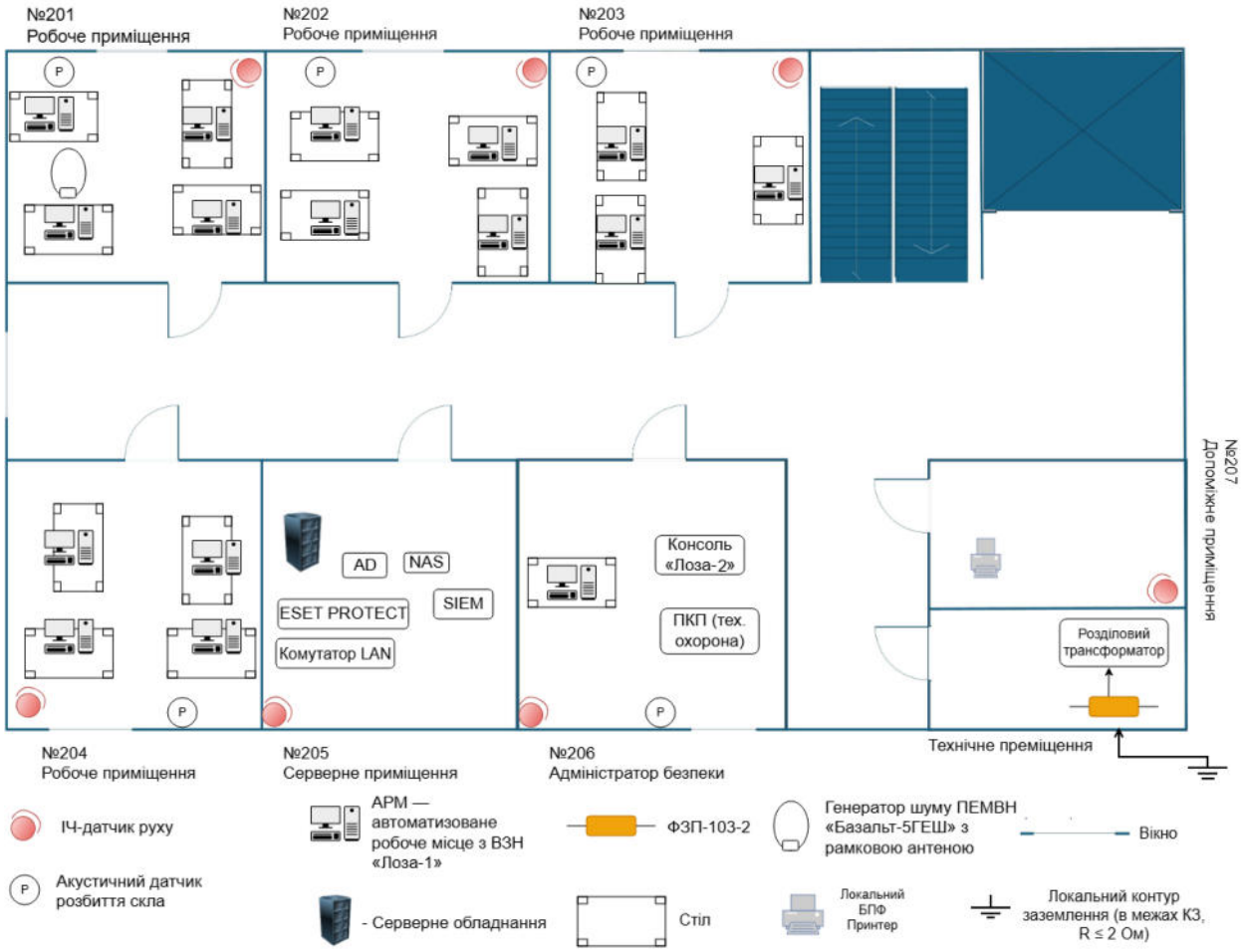

Рисунок 2.2 – Схема приміщення ТОВ «Огун» з розміщенням засобів КСЗІ (розроблено автором)

Розміщення засобів КСЗІ виконано з урахуванням наступних принципів: основні засоби обробки інформації розташовуються максимально віддалено від

огороджувальних конструкцій, що межують з неконтрольованою зоною; засіб захисту мережі електроживлення встановлюється на вводі живлення у приміщення для забезпечення фільтрації всього обсягу електричних кіл; серверне обладнання та робоче місце адміністратора безпеки розміщуються в окремих приміщеннях з обмеженим доступом; сповіщувачі технічної системи охорони встановлюються таким чином, щоб забезпечити повне покриття приміщень ОІД зонами виявлення.

Узагальнена структура КСЗІ. Взаємодія підсистем КСЗІ та виконуваних ними функцій забезпечує реалізацію функціонального профілю 2.КЦ.1 на рівні гарантій Г-3. Підсистема захисту від несанкціонованого доступу реалізує функціональні послуги КД-2, ЦД-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1 програмно-апаратними засобами. Підсистема антивірусного захисту забезпечує протидію загроз впровадження шкідливого програмного забезпечення через зовнішні носії, електронну пошту та веб-ресурси. Підсистема захисту від витоку інформації технічними каналами доповнює захист від НСД з боку технічних каналів, які не можуть бути парирувані програмними засобами. Технічна система охорони забезпечує своєчасне виявлення спроб фізичного проникнення в межі контрольованої зони. Підсистема організаційно-розпорядчого забезпечення регламентує дії персоналу та забезпечує документальне супроводження функціонування КСЗІ.

2.8 Розробка технічного завдання на створення КСЗІ

Технічне завдання на створення комплексної системи захисту інформації в АС класу 2 ТОВ «Огун» розроблено на підставі результатів усіх попередніх етапів проєктування – категоріювання ОІД, обстеження середовища функціонування АС, побудованих моделі загроз і моделі порушника, розробленої політики безпеки та сформованої структури і архітектури КСЗІ. Документ виконано з урахуванням вимог НД ТЗІ 3.7-001-99 щодо розробки технічного завдання на створення КСЗІ та НД ТЗІ 3.7-003-2023 щодо порядку проведення робіт зі створення КСЗІ в інформаційно-комунікаційній системі.

Технічне завдання визначає вимоги до сукупності організаційних та технічних заходів забезпечення захисту інформації в АС класу 2 ТОВ «Огун», порядок виконання робіт, склад документації та умови приймання системи в експлуатацію. Положення ТЗ є обов'язковими для виконання на всіх етапах життєвого циклу КСЗІ та слугують підставою для контролю відповідності реалізованих рішень заявленим вимогам.

Повний текст розробленого технічного завдання наведено у Додатку Г та використовується як основа для виконання подальших етапів робіт зі створення КСЗІ, що детально розглядаються у Розділі 3 кваліфікаційної роботи.

Висновки до розділу 2

В другому розділі виконано проєктування комплексної системи захисту інформації для автоматизованої системи класу 2 ТОВ «Огун».

Надано характеристику ОІД та обґрунтовано необхідність створення КСЗІ для захисту персональних даних, службової інформації та комерційної таємниці замовників.

Проведено категоріювання ОІД, за результатами якого об'єкту присвоєно IV категорію та оформлено відповідний Акт категоріювання.

Виконано обстеження середовища функціонування АС, за результатами якого встановлено передумови реалізації загроз і оформлено Акт обстеження ОІД.

Побудовано модель загроз з 15 актуальних загроз, об'єднаних в три групи – НСД, витік технічними каналами та порушення працездатності, з акцентом на витік через мережу електроживлення.

Розроблено модель порушника з визначенням внутрішніх та зовнішніх категорій, при цьому встановлено найвищий рівень загрози від внутрішніх порушників з розширеними повноваженнями та зовнішніх порушників з технічними засобами перехоплення.

Сформовано політику безпеки інформації в АС та обрано функціональний профіль захищеності 2.КЦ.1 з рівнем гарантій Г-3.

Спроєктовано структуру КСЗІ у складі п'яти підсистем на базі засобів «Лоза-2», ESET Endpoint Security, генератора шуму «Базальт-5ГЕШ» та «ФЗП-103-2» з розділовим трансформатором.

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ КСЗІ В АС КЛАСУ 2

3.1 Організаційні заходи захисту інформації в АС 2

На виконання вимог технічного завдання та політики безпеки інформації, розроблених у попередньому розділі, на підприємстві ТОВ «Огун» впроваджено сукупність організаційних заходів, що забезпечують функціонування комплексної системи захисту інформації. Організаційні заходи становлять фундамент КСЗІ, оскільки саме вони визначають порядок взаємодії персоналу з інформаційними ресурсами, регламентують повноваження та відповідальність, а також забезпечують підтримку в належному стані технічних компонентів системи захисту протягом всього життєвого циклу.

Призначення відповідальних осіб. Наказом керівника ТОВ «Огун» № 18 від 10.03.2026 створено комплексну систему захисту інформації в АС класу 2 та призначено відповідального за захист інформації – Бондаренка О. В. На відповідального покладено функції організації робіт зі створення та супроводу КСЗІ, контролю виконання положень політики безпеки, керування налаштуваннями засобів захисту, аналізу журналів подій безпеки та подання керівнику пропозицій щодо удосконалення системи захисту. Окремим наказом № 19 від 12.03.2026 утворено комісію з категоріювання та обстеження ОІД, до складу якої увійшли відповідальний за захист інформації, системний адміністратор та представник керівництва.

Впроваджено комплект організаційно-розпорядчих документів. Документальна основа функціонування КСЗІ сформована з урахуванням вимог НД ТЗІ 1.4-001-2000 щодо типового положення про службу захисту інформації в автоматизованій системі, НД ТЗІ 3.7-003-2023 щодо порядку проведення робіт зі створення КСЗІ, а також, з урахуванням загальноприйнятих міжнародних практик організаційного забезпечення інформаційної безпеки, систематизованих у CIS Critical Security Controls [29]. Перелік впроваджених документів наведено у таблиці 3.1 (складено автором на основі [7], [15], [17], [22]).

Таблиця 3.1 – Перелік організаційно-розпорядчих документів КСЗІ ТОВ «Огун»

№	Найменування документа	Призначення
1	Наказ про створення КСЗІ № 18 від 10.03.2026	Підстава для виконання робіт зі створення КСЗІ
2	Наказ про утворення комісії з категоріювання та обстеження ОІД № 19 від 12.03.2026	Підстава для проведення категоріювання та обстеження
3	Акт категоріювання ОІД від 15.03.2026	Документальне закріплення IV категорії об’єкта
4	Акт обстеження ОІД від 16.03.2026	Фіксація стану ОІД та виявлених передумов реалізації загроз
5	Положення про відповідального за захист інформації	Регламентація повноважень і відповідальності особи, що відповідає за захист
6	Посадова інструкція відповідального за захист інформації	Деталізація службових обов’язків відповідального
7	Інструкція користувача АС	Правила роботи з інформаційними ресурсами для рядових користувачів
8	Інструкція системного адміністратора АС	Регламент адміністрування технічних засобів і програмного забезпечення
9	Інструкція з реагування на інциденти інформаційної безпеки	Порядок дій персоналу у разі виявлення інцидентів
10	Інструкція з експлуатації засобу захисту «Лоза-2»	Порядок використання та адміністрування КЗЗ від НСД

Продовження таблиці 3.1

№	Найменування документа	Призначення
11	Інструкція з експлуатації засобу антивірусного захисту ESET Endpoint Security	Порядок використання консолі ESET PROTECT та політик захисту
12	Інструкція з експлуатації мережевого фільтра «ФЗП-103-2»	Регламент обслуговування засобу захисту мережі електроживлення
13	Журнал обліку відвідувачів	Реєстрація факту перебування сторонніх осіб у межах ОІД
14	Журнал обліку знімних носіїв інформації	Облік закріплених за користувачами носіїв
15	Журнал реєстрації змін у налаштуваннях засобів захисту	Документальна фіксація адміністративних дій

Реалізація рольової моделі. На підставі результатів категоріювання та структури автоматизованої системи, для 15 співробітників, що працюють з ресурсами АС, встановлено такі ролі: керівник підприємства, адміністратор безпеки, системний адміністратор, інженер технічної підтримки, керівник проєкту, особа з документального супроводу. Кожна роль має визначений у відповідній інструкції набір функціональних обов’язків та обсяг повноважень щодо інформаційних ресурсів АС. Функціональна послуга НО-1 обраного профілю реалізується через виділення адміністратора та відокремлення його повноважень від повноважень звичайних користувачів системи. Додатково на організаційному рівні повноваження з адміністрування технічних засобів (системний адміністратор) відокремлено від повноважень з керування засобами захисту та контролю подій безпеки (адміністратор безпеки).

Навчання персоналу. Перед початком експлуатації КСЗІ для всіх 15 співробітників, що працюють з ресурсами АС, проведено інструктивне навчання з питань інформаційної безпеки. Програма навчання охоплювала ознайомлення з положеннями політики безпеки, правилами роботи з обліковими записами та паролями, порядком використання знімних носіїв інформації, процедурами реагування на інциденти, обмеженнями щодо роботи з ІзОД в межах контрольованої зони. Факт проходження навчання зафіксовано в журналі обліку інструктажів, кожен співробітник підписав зобов’язання про нерозголошення інформації з обмеженим доступом.

Введення режиму контрольованої зони. Встановлено пропускний режим в рамках ОІД, що передбачає допуск сторонніх осіб (представники замовників, працівники служб обслуговування будівлі) виключно у супроводі співробітника ТОВ «Огун» з реєстрацією факту перебування в журналі обліку відвідувачів. Доступ до серверного приміщення № 205 та приміщення адміністратора безпеки № 206 обмежено колом відповідальних осіб. Внесення стороннього обладнання та особистих електронних пристроїв в рамках ОІД заборонене, винесення технічних засобів за межі КЗ здійснюється виключно з дозволу відповідального за захист інформації після виконання процедур гарантованого видалення інформації відповідно до загальноприйнятих методичних рекомендацій з очищення носіїв інформації [30].

Регламентація процедур контролю. На відповідального за захист інформації покладено проведення планових перевірок стану КСЗІ з періодичністю не рідше одного разу на квартал. При перевірках виконується аналіз журналів реєстрації подій безпеки, контроль фактичних повноважень користувачів, перевірка стану засобів захисту, контроль виконання положень політики безпеки. Результати перевірок оформлюються відповідними актами, що зберігаються в комплекті документації КСЗІ. Виявлені відхилення усуваються за окремими планами, з документальним підтвердженням виконання коригувальних заходів.

3.2 Інженерно-технічні засоби захисту інформації в АС 2

На виконання вимог технічного завдання та сформованої архітектури КСЗІ, на ОІД ТОВ «Огун» впроваджено сукупність інженерно-технічних засобів захисту інформації, спрямованих на протидії загроз витоку інформативних сигналів технічними каналами та виявлення спроб несанкціонованого проникнення в межі контрольованої зони. Реалізована підсистема охоплює засоби захисту мережі електроживлення, локальний контур заземлення та технічну систему охорони, об’єднані в єдиний комплекс інженерно-технічного забезпечення безпеки інформації.

3.2.1 Захист мережі електроживлення

Захист мережі електроживлення впроваджено для протидії виявлених передумов витоку інформації через провідні комунікації, що виходять за межі контрольованої зони. На момент обстеження мережа електроживлення ОІД підключалась безпосередньо до загальнобудинкової мережі, що створювало можливість поширення інформативних сигналів, наведених від технічних засобів обробки інформації, за межі КЗ та їх перехоплення спеціальними технічними засобами.

Для усунення виявлених передумов реалізовано двоступеневу систему захисту мережі електроживлення, що включає активний фільтр високочастотних завад та розділовий трансформатор. Схема підключення засобів захисту наведена на (рис.3.1).

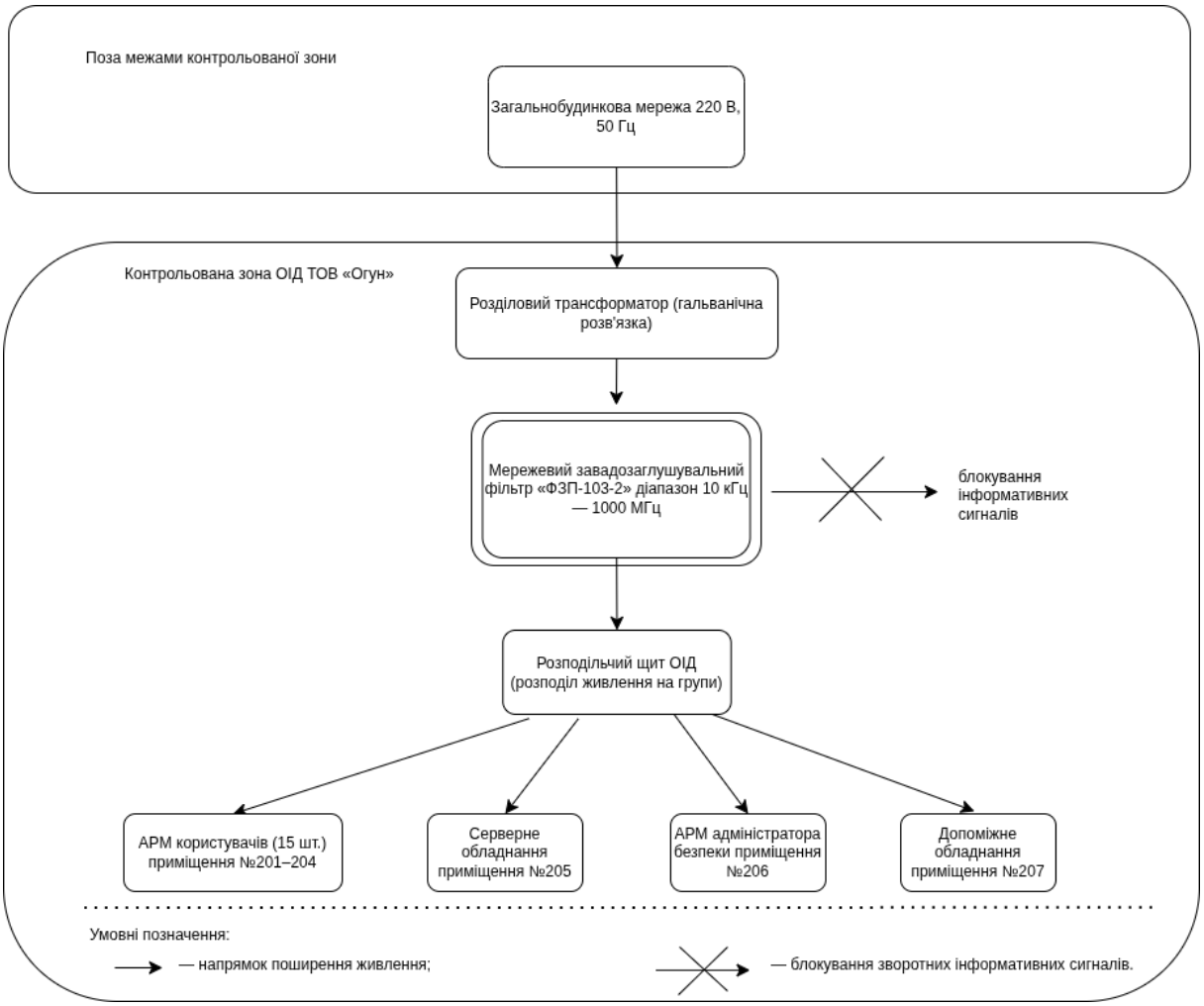

Рисунок 3.1 – Блок-схема підключення засобів захисту мережі електроживлення (розроблено автором)

Розділовий трансформатор встановлено на вводі мережі електроживлення в межі контрольованої зони. Призначення трансформатора полягає у забезпеченні гальванічної розв’язки мережі електроживлення ОІД від загальнобудинкової мережі. Завдяки відсутності прямого електричного зв’язку між первинною та вторинною обмотками, інформативні сигнали, наведені на провідники мережі живлення з боку технічних засобів обробки інформації, не передаються у загальнобудинкову мережу та не можуть бути зафіксовані поза межами КЗ.

Послідовно з розділовим трансформатором встановлено мережевий завадозаглушувальний фільтр «ФЗП-103-2» виробництва ТОВ «ЕМСБІ». Фільтр забезпечує придушення інформативних сигналів у широкому діапазоні частот від 10 кГц до 1000 МГц, що відповідає діапазону можливих наводок від технічних

засобів обробки інформації. Зовнішній вигляд мережевого завадозаглушувального фільтра «ФЗП-103-2» наведено на (рис. 3.2). Технічні характеристики реалізованого засобу захисту мережі електроживлення наведено в таблиці 3.2 (складено автором на основі джерела [31]).

Рисунок 3.2 – Зовнішній вигляд мережевого завадозаглушувального фільтра «ФЗП-103-2»

Технічні характеристики мережевого завадозаглушувального фільтра «ФЗП-103-2» наведено в таблиці 3.2 (складено автором на основі джерела [31]).

Таблиця 3.2 – Технічні характеристики мережевого завадозаглушувального фільтра «ФЗП-103-2»

Параметр	Значення
Діапазон робочих частот	10 кГц – 1000 МГц
Робоча напруга мережі	220 В, 50 Гц
Максимальний робочий струм	16 А на лінію
Кількість фільтрованих ліній	2 (фаза, нейтраль)
Загасання сигналу в робочому діапазоні	не менше 80 дБ
Тип монтажу	стаціонарне настінне розміщення на вводі живлення
Відповідність нормативним вимогам	експертний висновок Держспецзв’язку, ТУ У 31.1-31731859-001-2003

Фільтр «ФЗП-103-2» встановлено в спеціально обладнаній шафі розподільчого щита, що розміщена при вході до приміщення № 207. Підключення засобу виконано штатним монтажним персоналом з дотриманням вимог виробника щодо порядку приєднання живлячих і фільтрованих ліній. Після підключення проведено перевірку працездатності фільтра шляхом контрольного вимірювання загасання сигналу в робочому діапазоні частот.

Реалізована двоступенева система захисту мережі електроживлення забезпечує протидію загроз № 7 «Витік інформації через мережу електроживлення» і № 9 «Витік інформації каналами ПЕМВН через провідні комунікації», визначених у моделі загроз (таблиця 2.2).

3.2.2 Захист від витоку інформації каналами побічних електромагнітних випромінювань

Захист від витоку інформації за рахунок побічних електромагнітних випромінювань технічних засобів обробки інформації реалізовано на виконання вимог технічного завдання для протидії загрозі № 10 «Витік інформації через побічні електромагнітні випромінювання технічних засобів у простір» з моделі загроз. На момент обстеження ОІД активні засоби захисту від витоку каналами ПЕМВН відсутні, що створювало можливість перехоплення інформативних сигналів моніторів та системних блоків автоматизованих робочих місць спеціальними приймальними засобами поза межами контрольованої зони.

Для усунення виявленої передумови у складі КСЗІ впроваджено генератор шуму електромагнітних випромінювань «Базальт-5ГЕШ» виробництва ПрАТ «Холдингова компанія "Укрспецтехніка"», що має чинний експертний висновок Держспецзв’язку. Принцип дії генератора полягає у формуванні в навколишньому просторі електромагнітного поля шуму, спектр якого перекриває діапазон можливих побічних випромінювань технічних засобів обробки інформації. Інтенсивність поля шуму, що створюється генератором, перевищує рівень інформативних сигналів технічних засобів, унаслідок чого виокремлення

корисного сигналу спеціальними приймальними засобами стає неможливим. Зовнішній вигляд генератора шуму «Базальт-5ГЕШ» наведено на рис. 3.3 (складено автором на основі джерела [32]).

Рисунок 3.3 – Зовнішній вигляд генератора шуму «Базальт-5ГЕШ»

Технічні характеристики реалізованого засобу захисту наведено в таблиці 3.3 (складено автором на основі джерела [32]).

Таблиця 3.3 – Технічні характеристики генератора шуму «Базальт-5ГЕШ»

Параметр	Значення
Тип випромінювача	Рамкова антена
Діапазон робочих частот	0,01 – 1000 МГц
Спектральна щільність шуму	не менше 60 дБ відносно фонового рівня
Дальність ефективної дії	до 20 м
Електроживлення	220 В, 50 Гц
Споживана потужність	не більше 6 Вт
Габаритні розміри блока керування	700 × 70 × 130 мм
Маса	1,1 кг
Тип монтажу	стаціонарне розміщення з винесеною рамковою антеною
Відповідність нормативним вимогам	експертний висновок Держспецзв’язку

Блок керування генератора «Базальт-5ГЕШ» розміщено в робочому приміщенні № 201 в центральній частині ОІД. Рамкова антена винесена та закріплена на стіні приміщення на висоті 2,1 м від підлоги, що забезпечує оптимальну діаграму спрямованості створюваного поля. Розташування генератора в центральній частині ОІД зумовлене необхідністю забезпечення ефективного покриття полем шуму всіх приміщень, в яких розміщені автоматизовані робочі місця та серверне обладнання. Схема розміщення засобу захисту з зоною ефективної дії наведена на (рис. 3.4).

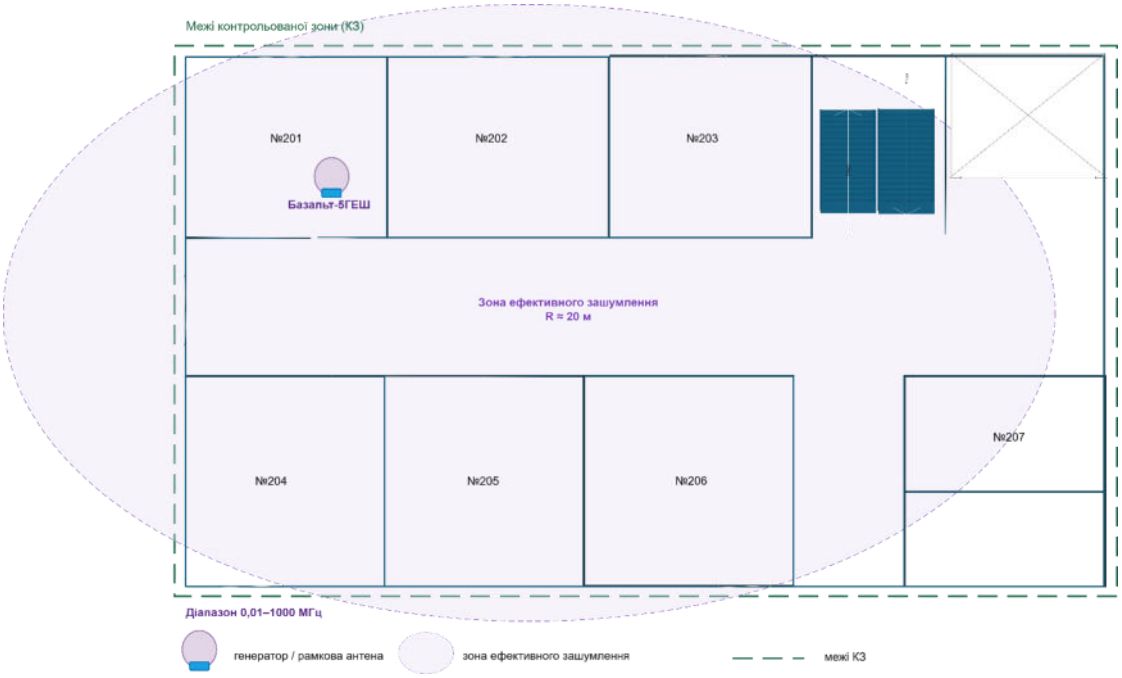

Рисунок 3.4 – Схема розміщення генератора шуму «Базальт-5ГЕШ» на ОІД ТОВ «Огун» (розроблено автором)

Електроживлення генератора здійснюється від мережі ОІД через мережевий завадозаглушувальний фільтр «ФЗП-103-2», що забезпечує одночасне функціонування двох взаємодоповнюючих рівнів захисту – активного зашумлення електромагнітних випромінювань в простір та пасивної фільтрації наводок у колах живлення. Дана конфігурація робить неможливим як перехоплення інформативних сигналів безпосередньо в просторі за межами ОІД, так і поширення інформативних сигналів через мережу електроживлення поза межі контрольованої зони.

Налаштування генератора виконано з урахуванням розмірів контрольованої зони та розміщення джерел інформативних випромінювань. Режим роботи

передбачає постійне ввімкнення генератора протягом усього часу обробки інформації з обмеженим доступом в АС. Контроль працездатності засобу забезпечується індикацією на блоці керування та періодичним вимірюванням параметрів створюваного поля шуму в межах планових перевірок стану КСЗІ.

Реалізований активний захист від витоку каналами ПЕМВН разом з пасивними засобами захисту мережі електроживлення формує комплексну систему протидії загрозам витоку через електромагнітні канали, що забезпечує відповідність вимогам нормативних документів системи технічного захисту інформації для АС класу 2.

3.2.3 Захист системи заземлення

На момент обстеження система заземлення ОІД підключалась до загальнобудинкового контуру заземлення, що виходить за межі контрольованої зони. Спільне використання контуру заземлення створювало передумови для перехоплення інформативних сигналів, наведених на коло заземлення з боку технічних засобів обробки інформації.

Для усунення виявленої передумови в рамках контрольованої зони обладнано локальний контур заземлення, не пов’язаний електрично з загальнобудинковим контуром. Схема організації локального заземлення наведена на (рис.3.5).

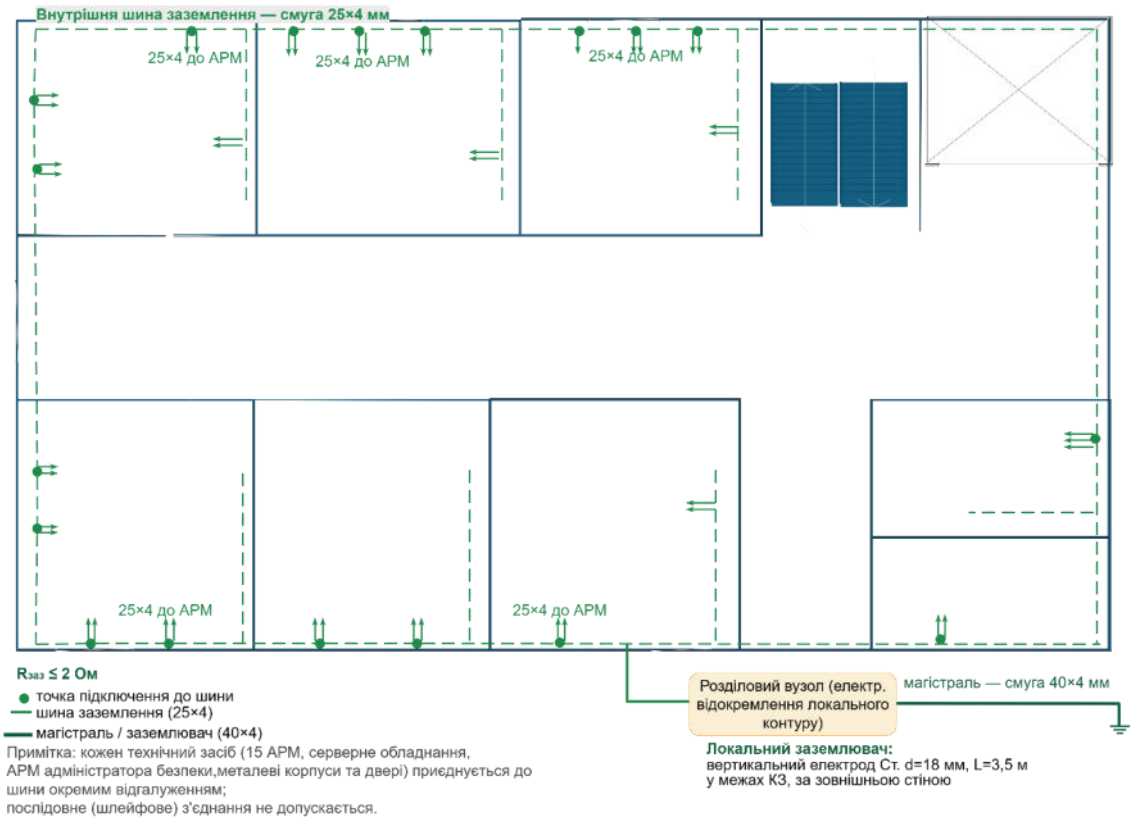

Рисунок 3.5 – Схема локального контуру заземлення ОІД ТОВ «Огун» (розроблено автором)

Локальний заземлювач виконано у вигляді заглибленого вертикального електрода із сталевого прокату довжиною 3 м, розміщеного на території, що належить до контрольованої зони. Підключення електрода до шини заземлення в межах приміщень ОІД виконано мідним провідником поперечного перерізу не менше 16 мм². Шина заземлення прокладена по периметру приміщень ОІД та забезпечує підключення корпусів технічних засобів обробки інформації, металевих корпусів обладнання, металевих дверей, корпуса розподільчого щита електроживлення.

Виміряний опір локального контуру заземлення становить 1,8 Ом, що задовольняє нормативну вимогу не більше 2 Ом. Результати вимірювань оформлено протоколом, що включено до комплекту документації КСЗІ. Електричне відокремлення локального контуру від загальнобудинкового контуру заземлення забезпечує неможливість поширення інформативних сигналів за межі

контрольованої зони, що забезпечує протидію загрозі № 8 «Витік інформації через коло заземлення» з моделі загроз.

3.2.4 Технічна система охорони

Для протидії загрозі № 11 «Несанкціоноване проникнення в межі контрольованої зони» з моделі загроз впроваджено технічну систему охорони, що забезпечує виявлення спроб несанкціонованого проникнення в межі ОІД в позаробочий час. Реалізована система складається з прийомно-контрольного приладу, сповіщувачів виявлення проникнення двох типів та засобів сповіщення відповідальних осіб. План розміщення засобів технічної системи охорони наведено на (рис. 3.6).

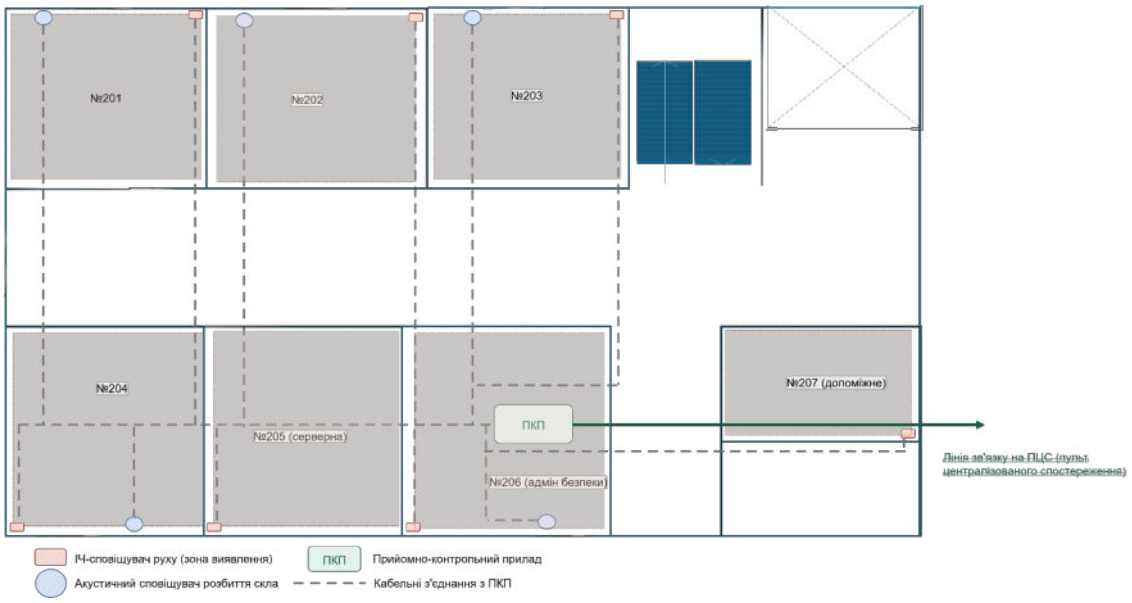

Рисунок 3.6 – План розміщення сповіщувачів технічної системи охорони на ОІД ТОВ «Огун» (розроблено автором)

ІЧ-сповіщувачі руху встановлено в кожному з 7 приміщень ОІД на висоті 2,4 м у куті, що забезпечує максимальне покриття площі приміщення зоною виявлення. Технічні параметри сповіщувачів передбачають кут огляду 90°, дальність виявлення до 12 м, що повністю покриває розміри робочих приміщень. Зона виявлення налаштована на реєстрацію руху об’єктів в горизонтальній площині на висоті 0,3–2,1 м від підлоги, що відповідає габаритам людини.

Акустичні сповіщувачі розбиття скла встановлено на стінах робочих та серверного приміщень поблизу віконних отворів. Сповіщувачі реагують на характерний акустичний спектр розбиття віконного скла з робочою дальністю до 6 м, що забезпечує виявлення спроб проникнення через будь-який з віконних отворів ОІД.

Прийомно-контрольний прилад розміщено в приміщенні адміністратора безпеки № 206. ПКП забезпечує прийом сигналів від всіх сповіщувачів, їх первинну обробку, ведення журналу подій з фіксацією часу спрацювання та номера зони, формування сигналів тривоги та передачу повідомлень про спрацювання на пульт централізованого спостереження. Всі сповіщувачі підключено до ПКП окремими шлейфами, що забезпечує можливість точної локалізації спрацювання за номером зони.

Постановка ОІД на охорону здійснюється відповідальною особою наприкінці робочого дня з фіксацією факту постановки в журналі. Зняття з охорони виконується на початку робочого дня, що також фіксується в журналі. У разі спрацювання сповіщувачів в час, коли об’єкт знаходиться під охороною, формується сигнал тривоги, який передається на пульт централізованого спостереження для організації реагування.

Реалізована підсистема інженерно-технічних засобів захисту забезпечує протидію виявленим у моделі загроз ризикам витоку інформації через провідні комунікації, електромагнітні випромінювання у простір та несанкціонованого фізичного проникнення в межі ОІД. Двоступенева система захисту мережі електроживлення на базі розділового трансформатора та фільтра «ФЗП-103-2» унеможливлює поширення інформативних сигналів за межі контрольованої зони через канали наводок в мережі живлення. Генератор шуму «Базальт-5ГЕШ» забезпечує активний захист від витоку каналами побічних електромагнітних випромінювань технічних засобів обробки інформації в простір. Локальний контур заземлення усуває можливість перехоплення сигналів через коло заземлення. Технічна система охорони з ІЧ-сповіщувачами руху та акустичними

сповіщувачами розбиття скла забезпечує своєчасне виявлення спроб несанкціонованого проникнення в межі ОІД у позаробочий час.

3.3 Захист від несанкціонованих дій з інформацією в АС 2

Захист від несанкціонованих дій з інформацією в АС 2 ТОВ «Огун» реалізовано на виконання вимог обраного функціонального профілю захищеності 2.КЦ.1 та з урахуванням загроз несанкціонованого доступу, перевищення повноважень, несанкціонованого копіювання інформації та впровадження шкідливого програмного забезпечення, визначених в моделі загроз. Реалізована підсистема ґрунтується на двох взаємодоповнюючих засобах: комплексі засобів захисту від несанкціонованого доступу «Лоза-2» та засобі антивірусного захисту ESET Endpoint Security з централізованою консоллю керування ESET PROTECT.

3.3.1 Налаштування комплексу засобів захисту «Лоза-2»

Засіб захисту «Лоза-2» встановлено на всіх 15 автоматизованих робочих місцях користувачів та на серверному обладнанні АС, що забезпечує єдиний рівень захисту інформаційних ресурсів незалежно від точки доступу. Інсталяція засобу виконана в режимі, який передбачає його участь в процесі завантаження операційної системи, що робить неможливим доступ до інформаційних ресурсів в обхід механізмів захисту.

В рамках налаштування «Лоза-2» створено 15 індивідуальних облікових записів користувачів – за кількістю співробітників, що працюють з АС. Кожному обліковому запису присвоєно унікальний ідентифікатор, що відповідає прізвищу та ініціалам співробітника. Колективні облікові записи не створювалися, за винятком технологічних службових облікових записів для сервісів операційних систем, доступ під якими користувачам не надається.

Розмежування доступу реалізовано через систему ролей, що відповідає категоріям персоналу, визначеним у підрозділі 2.3. Кожній ролі надано набір

повноважень щодо інформаційних ресурсів, обраний за принципом мінімально необхідних прав. Схема ролей у «Лоза-2» наведена на (рис. 3.7).

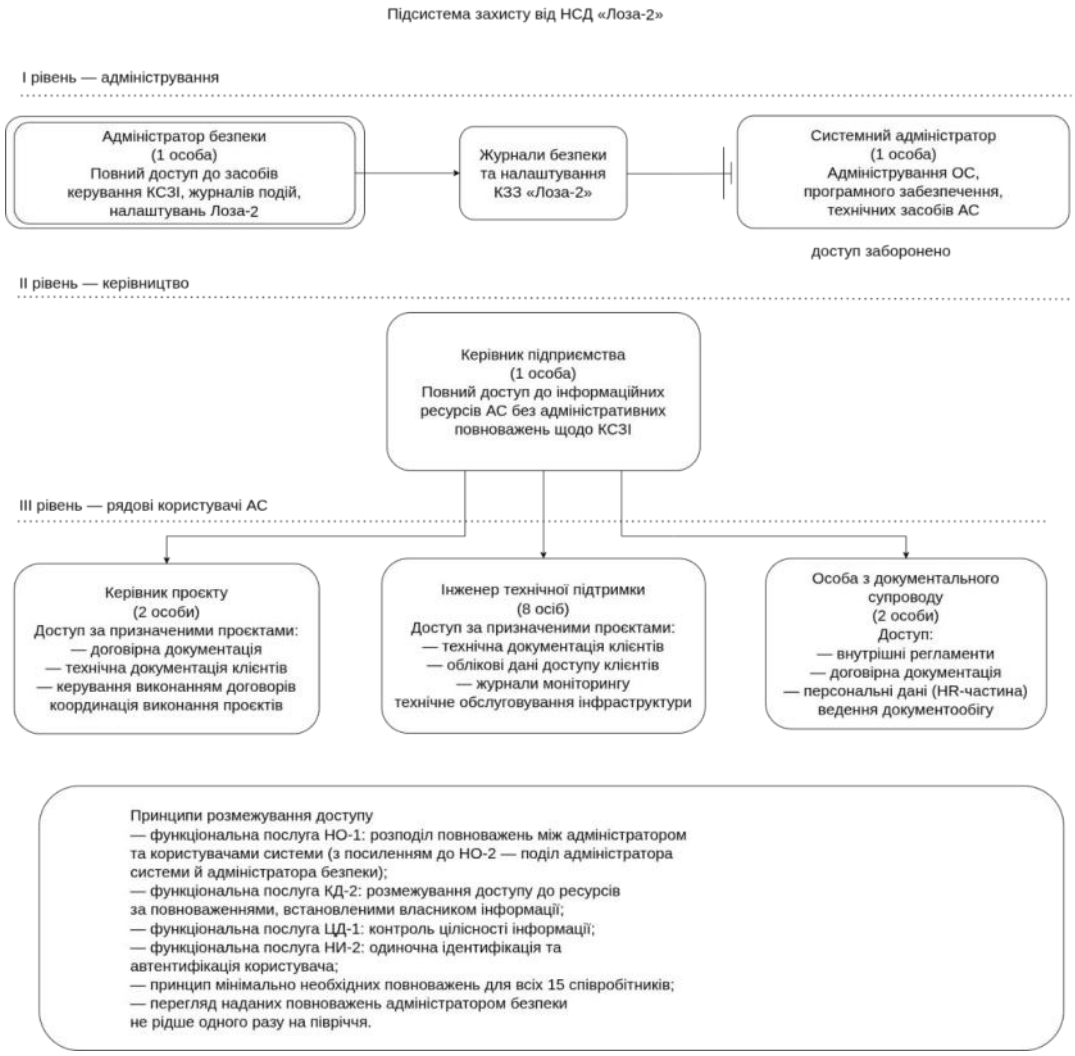

Рисунок 3.7 – Блок-схема ролей у «Лоза-2» для АС 2 ТОВ «Огун» (розроблено автором)

Налаштування функціональних послуг безпеки виконано відповідно до обраного функціонального профілю. Реалізацію кожної послуги представлено у таблиці 3.4 (складено автором на основі [7], [9], [10], [12]).

Таблиця 3.4 – Реалізація функціональних послуг безпеки засобами «Лоза-2»

Послуга	Найменування	Реалізація в «Лоза-2»
КД-2	Довірча конфіденційність	Розмежування доступу до файлів і каталогів на підставі прав доступу, встановлених власником ресурсу, з керуванням потоками інформації між об'єктами
ЦД-1	Довірча цілісність	Контроль модифікації захищених файлів і каталогів на підставі прав доступу, визначених власником інформації
НР-2	Реєстрація	Реєстрація подій безпеки в журналі із захистом записів від модифікації, неможливість зміни журналу адміністратором системи
НИ-2	Ідентифікація і автентифікація	Ідентифікація користувача за обліковим записом, автентифікація паролем з вимогами складності
НК-1	Достовірний канал	Захищений діалог введення облікових даних, що унеможливлює перехоплення сторонніми процесами
НО-1	Розподіл обов'язків	Розмежування повноважень між адміністратором та звичайними користувачами системи
НЦ-1	Цілісність КЗЗ	Контроль цілісності модулів засобу захисту при завантаженні, блокування роботи у разі порушення цілісності

Налаштування політик паролів виконано згідно з вимогами політики безпеки: мінімальна довжина – 10 символів, обов'язкове використання літер різних регістрів, цифрових символів і спеціальних знаків, термін дії паролю – 90 днів, заборона повторного використання останніх 5 паролів. Автоматичне блокування облікового запису налаштовано після 5 послідовних невдалих спроб входу.

Реєстрація подій безпеки активована в обсязі, що передбачає фіксацію входу та завершення сеансів користувачів, спроб доступу до захищених ресурсів (в тому числі неуспішних), модифікації прав доступу, виконання адміністративних дій,

операцій з знімними носіями, спроб обходу механізмів захисту. Журнал подій зберігається в захищеному вигляді з контролем цілісності записів. Доступ до журналу має виключно адміністратор безпеки, термін зберігання записів – не менше 6 місяців.

3.3.2 Налаштування антивірусного захисту ESET Endpoint Security

Підсистема антивірусного захисту реалізована з використанням продукту ESET Endpoint Security, що має чинний експертний висновок Держспецзв'язку. Архітектура підсистеми передбачає централізоване керування захистом всіх кінцевих точок з єдиної консолі ESET PROTECT, розгорнутої на сервері локальних служб в приміщенні № 205. Схема архітектури підсистеми антивірусного захисту наведена на (рис. 3.8).

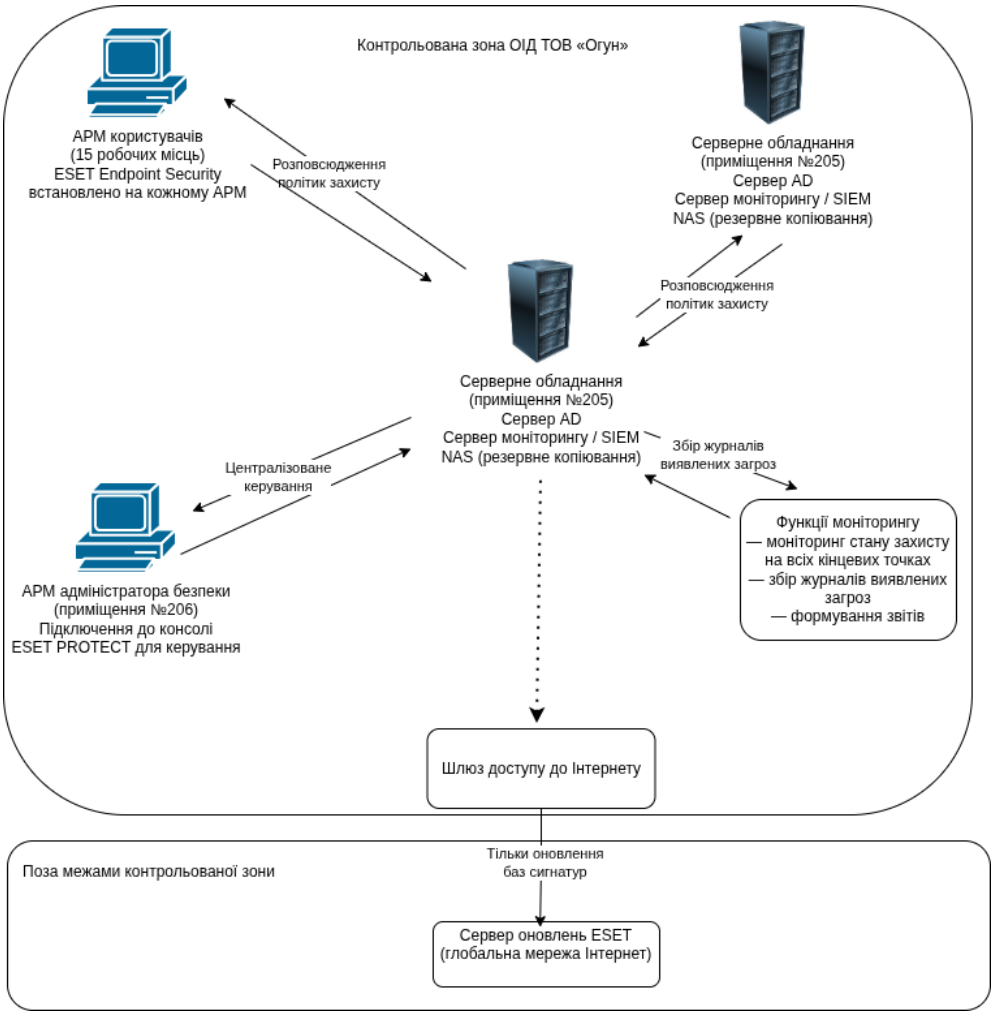

Рисунок 3.8 – Блок-схема архітектури підсистеми антивірусного захисту ESET Endpoint Security (розроблено автором)

На всіх 15 АРМ користувачів і серверному обладнанні встановлено клієнтський модуль ESET Endpoint Security, який включає такі компоненти захисту як модуль сигнатурного виявлення шкідливого ПЗ, модуль поведінкового аналізу процесів, модуль контролю автозавантаження, модуль контролю знімних носіїв, модуль захисту мережевого трафіку на рівні робочої станції, модуль сканування електронної пошти.

В консолі ESET PROTECT створено окремі групи політик захисту для різних категорій робочих станцій. Для АРМ користувачів застосовано політику, що передбачає блокування підключення знімних носіїв, не зареєстрованих у системі обліку, заборону виконання файлів з певних каталогів, увімкнення поведінкового аналізу для виявлення невідомих загроз. Для серверного обладнання застосовано окрему політику з оптимізацією сканування, що враховує специфіку серверного навантаження.

Оновлення антивірусних баз сигнатур налаштовано в автоматичному режимі з періодичністю не рідше одного разу на годину. Оновлення завантажуються з зовнішніх серверів ESET виключно сервером з консоллю ESET PROTECT, після чого розповсюджуються на клієнтські модулі в межах локальної мережі ОІД.

У разі виявлення шкідливого ПЗ клієнтський модуль виконує його ізоляцію (карантин), а на консоль ESET PROTECT відправляється повідомлення про подію. Адміністратор безпеки отримує сповіщення на власне робоче місце в режимі реального часу та виконує процедури реагування відповідно до інструкції з реагування на інциденти.

Реалізована підсистема захисту від несанкціонованих дій з інформацією забезпечує виконання всіх семи функціональних послуг безпеки, передбачених функціональним профілем 2.КЦ.1, на встановленому рівні гарантій Г-3. Засіб «Лоза-2» реалізує контроль доступу, реєстрацію подій, ідентифікацію та автентифікацію, розподіл повноважень адміністраторів і контроль цілісності КЗЗ. Засіб ESET Endpoint Security з консоллю ESET PROTECT забезпечує захист від

шкідливого програмного забезпечення та контроль знімних носіїв. Спільне застосування цих засобів унеможливлює реалізацію загроз № 1-6 з моделі загроз, які стосуються несанкціонованого доступу, перевищення повноважень, копіювання інформації, маскування під зареєстрованого користувача та впровадження шкідливого ПЗ.

3.4 Організація контролю доступу до інформаційних ресурсів АС

Контроль доступу до інформаційних ресурсів АС 2 ТОВ «Огун» реалізовано як одну з ключових функцій захисту інформації, що забезпечує виконання положень політики безпеки та функціональних послуг КД-2, ЦД-1, НИ-2 і НО-1 з обраного функціонального профілю. Принципом реалізації контролю доступу є надання користувачам мінімально необхідних повноважень для виконання посадових обов’язків з документальним оформленням всіх процедур надання, зміни та анулювання прав.

Класифікація інформаційних ресурсів АС

Для формування матриці доступу всі інформаційні ресурси, що циркулюють в АС, об’єднано у шість категорій за функціональним призначенням та видом інформації. До категорій інформаційних ресурсів належать: персональні дані співробітників і клієнтів, договірна документація з замовниками, технічна документація клієнтських інфраструктур (схеми мереж, конфігурації обладнання), облікові дані доступу до клієнтських систем, фінансово-господарська документація підприємства, журнали моніторингу та реєстрації подій безпеки.

Матриця розмежування доступу

На підставі функціональних обов’язків та категорій персоналу, сформовано матрицю розмежування доступу, що визначає для кожної категорії користувачів дозволені операції з кожною категорією інформаційних ресурсів. Матриця доступу наведена в таблиці 3.5 (складено автором на основі [5], [7], [10], [26]).

Таблиця 3.5 – Матриця розмежування доступу до інформаційних ресурсів АС 2 ТОВ «Огун»

Категорія користувачів (осіб)	Персональні дані	Договірна документація	Технічна документація клієнтів	Облікові дані доступу	Фінансово-госп. документація	Журнали безпеки
Керівник підприємства (1)	П, М	П, М	П	П	П, М	П
Адміністратор безпеки (1)	П	П	П	–	–	П, М, А
Системний адміністратор (1)	–	–	П, М	П, М	–	П
Керівник проєкту (2)	–	П, М (за проєктом)	П, М (за проєктом)	–	–	–
Інженер техн. підтримки (8)	–	П (за проєктом)	П, М (за проєктом)	П, М (за проєктом)	–	–
Особа з докум. супроводу (2)	П, М (HR-частина)	П, М	–	–	П, М	–

Умовні позначення: П – перегляд; М – модифікація; А – адміністрування (видалення, налаштування); «–» – доступ заборонено; «(за проєктом)» – доступ виключно до ресурсів призначених замовників.

Матриця доступу реалізована технічними засобами через систему ролей у «Лоза-2» (рис.3.7) та через стандартні механізми розмежування доступу операційних систем і файлових серверів. Кожен користувач отримує доступ виключно до тих ресурсів, які передбачені його роллю, без можливості розширення

повноважень самостійно. Спроби доступу до ресурсів поза наданими повноваженнями фіксуються в журналі безпеки та аналізуються адміністратором безпеки під час планових перевірок.

Управління правами доступу здійснюється протягом усього періоду трудових відносин кожного співробітника та охоплює чотири послідовні етапи. На етапі надання доступу за фактом прийняття співробітника на посаду відповідальний за захист інформації отримує заявку від керівника підрозділу з визначенням ролі та переліку необхідних інформаційних ресурсів. Після погодження заявки відповідальний за захист створює обліковий запис у «Лоза-2», призначає відповідну роль та налаштовує доступ до конкретних ресурсів за матрицею. Факт створення облікового запису фіксується в журналі реєстрації змін у налаштуваннях засобів захисту.

На етапі поточного функціонування обліковий запис використовується виключно його власником без передачі облікових даних іншим особам. Періодична зміна паролю виконується самим користувачем в термін до 90 днів, контроль виконання забезпечується механізмами «Лоза-2».

На етапі зміни повноважень при переведенні співробітника на іншу посаду виконується перегляд призначеної йому ролі та переліку доступних ресурсів. Зайві повноваження анулюються, нові – додаються згідно з вимогами нової посади. Зміни оформлюються заявкою керівника відповідного підрозділу та реєструються у журналі.

На етапі завершення трудових відносин обліковий запис звільненого співробітника блокується в день припинення трудового договору. Дані облікового запису зберігаються в заблокованому стані протягом терміну, визначеного внутрішніми документами підприємства, для забезпечення можливості розслідування інцидентів, які можуть бути виявлені після звільнення.

Періодичний перегляд призначених повноважень виконує відповідальний за захист інформації не рідше одного разу на півріччя. В рамках перегляду здійснюється звірка фактично наданих прав доступу з матрицею розмежування,

аналіз журналів використання облікових записів, виявлення невикористовуваних або надлишкових повноважень. За результатами перегляду формується звіт з переліком виявлених відхилень та пропозицій щодо коригування. Звіт затверджується керівником підприємства, після чого реалізуються відповідні зміни в налаштуваннях засобів захисту.

Окремий позачерговий перегляд повноважень виконується у разі виявлення інцидентів інформаційної безпеки, зміни функціональних обов'язків окремих категорій персоналу, появи нових інформаційних ресурсів або зміни вимог нормативної бази системи технічного захисту інформації.

Реалізована система контролю доступу до інформаційних ресурсів АС забезпечує дотримання принципу мінімально необхідних повноважень для всіх 15 співробітників ТОВ «Огун», що працюють з АС. Матриця розмежування доступу (таблиця 3.5) формалізує дозволені операції за категоріями користувачів та інформаційних ресурсів. Регламент управління життєвим циклом доступу та процедури періодичного перегляду забезпечують підтримку актуальності повноважень впродовж всього періоду експлуатації КСЗІ. Спільне застосування технічних механізмів розмежування доступу та організаційних процедур забезпечує протидію загрозам № 1 «Несанкціонований доступ до інформаційних ресурсів АС» і № 2 «Перевищення наданих повноважень користувачами» з моделі загроз.

3.5 Побудова системи моніторингу та аудиту безпеки

Завершальним компонентом реалізації КСЗІ є побудова системи моніторингу та аудиту безпеки, що забезпечує постійний контроль стану захищеності інформаційних ресурсів АС, своєчасне виявлення інцидентів інформаційної безпеки та документальне підтвердження ефективності функціонування комплексної системи захисту. Реалізована система базується на сукупності журналів реєстрації подій безпеки, що формуються засобами «Лоза-2», ESET Endpoint Security, прийомно-контрольним приладом технічної системи охорони та

операційними системами, з централізованим аналізом отриманих даних адміністратором безпеки.

Перелік подій безпеки, що реєструються

На виконання вимог функціональної послуги НР-2 «Захищений журнал» з обраного функціонального профілю в АС реалізовано реєстрацію подій безпеки в обсязі, що забезпечує можливість аналізу всіх категорій загроз, визначених у моделі загроз. Перелік подій, що підлягають обов'язковій реєстрації, наведено у таблиці 3.6 (складено автором на основі [7], [10], [28], [29]).

Таблиця 3.6 – Перелік подій безпеки, що реєструються в АС 2 ТОВ «Огун»

Категорія	Події, що реєструються	Джерело реєстрації
Автентифікація користувачів	Успішний вхід, невдалі спроби входу, завершення сеансу, блокування облікового запису	«Лоза-2»
Доступ до ресурсів	Звернення до захищених файлів і каталогів, спроби доступу поза наданими повноваженнями	«Лоза-2»
Адміністративні дії	Створення, зміна, видалення облікових записів, зміна налаштувань КЗЗ, керування політиками	«Лоза-2»
Робота зі знімними носіями	Підключення та відключення носіїв, операції копіювання файлів на носії	«Лоза-2», ESET
Антивірусні події	Виявлення шкідливого ПЗ, ізоляція об'єктів у карантин, оновлення баз сигнатур	ESET PROTECT
Цілісність системи захисту	Порушення цілісності модулів КЗЗ, спроби обходу механізмів захисту	«Лоза-2»
Технічна охорона	Спрацювання сповіщувачів руху, спрацювання сповіщувачів розбиття скла, постановка та зняття з охорони	ПКП

Доступ до журналів має виключно адміністратор безпеки, що відповідає вимогам функціональної послуги НР-2 щодо захисту журналу реєстрації від несанкціонованого доступу та модифікації, у тому числі з боку адміністратора системи.

Процедури моніторингу подій безпеки виконує адміністратор безпеки на постійній основі протягом робочого часу. Загальна логіка взаємодії учасників процесу моніторингу та аудиту наведена на (рис. 3.9), що відображає процес опрацювання подій від моменту їх виникнення в АС до прийняття коригувальних заходів.

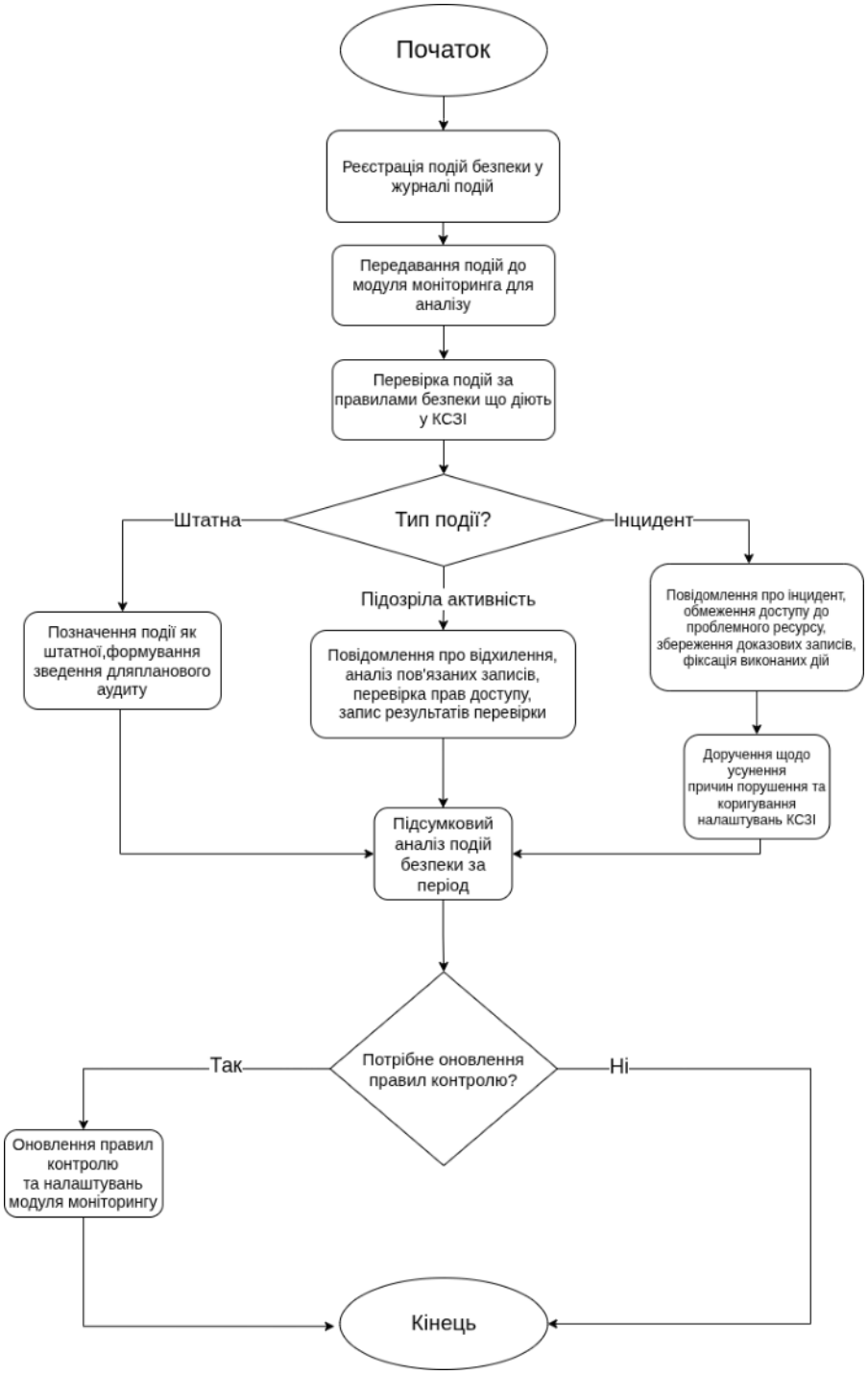

Рисунок 3.9 – Блок-схема процесу моніторингу та аудиту безпеки в АС класу 2 (розроблено автором)

Аналіз подій безпеки виконується в двох режимах. Оперативний моніторинг передбачає реагування на події в режимі реального часу шляхом відстеження повідомлень, що автоматично формуються модулем моніторингу при спрацюванні правил виявлення підозрілої активності. Плановий аудит виконується періодично з метою комплексного аналізу журналів за визначений період часу для виявлення тенденцій, повторюваних відхилень та оцінки загального стану захищеності.

У разі виявлення події, що відповідає правилам безпеки, подія позначається у журналі як штатна та включається до зведення для планового аудиту. При виявлені підозрілої активності адміністратор безпеки виконує аналіз пов'язаних записів, перевірку прав доступу залученого облікового запису та налаштувань системи, після чого результати перевірки фіксуються в журналі. Якщо за результатами перевірки встановлено ознаки інциденту інформаційної безпеки, ініціюється процедура реагування на інциденти, що передбачає обмеження доступу до проблемного ресурсу, збереження доказових записів, інформування керівника підприємства та виконання коригувальних заходів.

Плановий аудит стану інформаційної безпеки в АС виконується відповідальним за захист інформації не рідше одного разу на квартал. В рамках аудиту здійснюється комплексний аналіз журналів реєстрації подій за період, що минув від попереднього аудиту, перевірка фактичних повноважень користувачів на відповідність матриці доступу (таблиця 3.5), контроль стану засобів захисту, перевірка актуальності експлуатаційної документації.

За результатами кожного аудиту формується звіт, що містить узагальнену статистику подій безпеки, перелік виявлених відхилень, оцінку ефективності реалізованих захисних заходів та пропозиції щодо удосконалення КСЗІ. Звіт затверджується керівником підприємства, після чого затверджені пропозиції реалізуються у визначені терміни з документальним підтвердженням виконання.

Реалізована система моніторингу та аудиту безпеки забезпечує постійний контроль стану КСЗІ протягом усього періоду її експлуатації. Реєстрація подій безпеки в обсязі семи категорій з різних джерел – «Лоза-2», ESET PROTECT, ПКП

технічної системи охорони – створює достатню інформаційну базу для виявлення інцидентів інформаційної безпеки та аналізу їх обставин. Оперативний моніторинг і плановий аудит, виконувані адміністратором безпеки, забезпечують своєчасне реагування на загрози та підтримку КСЗІ в належному стані відповідно до сформованих в Розділі 2 проєктних рішень.

Висновки до розділу 3

В третьому розділі виконано практичну реалізацію КСЗІ для АС класу 2 ТОВ «Огун» на підставі проєктних рішень Розділу 2.

Впроваджено комплект організаційно-розпорядчих документів, призначено відповідальних осіб та проведено інструктивне навчання персоналу.

Реалізовано підсистему інженерно-технічних засобів захисту з фільтром ФЗП-103-2, розділовим трансформатором, генератором шуму «Базальт-5ГЕШ», локальним контуром заземлення та технічною системою охорони.

Налаштовано засіб «Лоза-2» та антивірусний захист ESET Endpoint Security, що забезпечує виконання функціонального профілю 2.КЦ.1 на рівні гарантій Г-3.

Сформовано матрицю розмежування доступу та регламентовано процедури управління життєвим циклом повноважень користувачів.

Реалізовано систему моніторингу та аудиту безпеки з реєстрацією подій зі всіх джерел захисту та квартальним плановим аудитом.

Впроваджені заходи забезпечують протидію всім актуальним загрозам, виявленим в моделі загроз, та реалізують вимоги розробленого технічного завдання.

ВИСНОВКИ

В кваліфікаційній роботі виконано проєктування та практичну реалізацію комплексної системи захисту інформації з обмеженим доступом в автоматизованій системі класу 2 на прикладі ТОВ «Огун». Поставлену мету досягнуто шляхом послідовного виконання теоретичного дослідження, проєктних робіт та практичної реалізації захисних заходів.

В ході дослідження теоретичних основ захисту інформації встановлено, що локалізований багатомашинний багатокористувацький характер АС класу 2 формує специфічні вимоги до системи захисту, які охоплюють як програмно-технічні, так і інженерно-технічні та організаційні складові. Проаналізовано класифікацію автоматизованих систем за НД ТЗІ 2.5-005-99, охарактеризовано основні загрози інформаційній безпеці та канали витоку інформації, а також досліджено нормативно-правову базу створення КСЗІ.

На етапі проєктування виконано категоріювання об’єкта інформаційної діяльності з присвоєнням четвертої категорії та проведено обстеження середовища функціонування АС, що дозволило виявити передумови реалізації загроз. На підставі результатів обстеження побудовано модель загроз з визначенням 15 актуальних загроз та модель потенційного порушника з виділенням внутрішніх і зовнішніх категорій. Сформовано політику безпеки інформації та обрано функціональний профіль захищеності 2.КЦ.1 з рівнем гарантій Г-3 відповідно до вимог НД ТЗІ 2.5-008-2002 для АС класу 2 з обробкою службової та конфіденційної інформації. Спроєктовано архітектуру КСЗІ в складі п’яти взаємопов’язаних підсистем та розроблено технічне завдання, що деталізує всі вимоги до створюваної системи захисту.

В рамках практичної реалізації КСЗІ впроваджено комплект організаційно-розпорядчих документів, налаштовано засіб захисту від несанкціонованого доступу «Лоза-2» та антивірусний захист ESET Endpoint Security з централізованою консоллю ESET PROTECT, що забезпечує виконання всіх семи функціональних послуг безпеки обраного профілю. Реалізовано інженерно-технічний захист на базі мережевого завадозаглушувального фільтра «ФЗП-103-2», розділового

трансформатора, генератора шуму електромагнітних випромінювань «Базальт-5ГЕШ» та локального контуру заземлення, що забезпечує протидію загрозам витоку інформації через мережу електроживлення, коло заземлення та побічні електромагнітні випромінювання технічних засобів обробки інформації. Розгорнуто технічну систему охорони з ІЧ-сповіщувачами руху та акустичними сповіщувачами розбиття скла, сформовано матрицю розмежування доступу для шести категорій користувачів та побудовано систему моніторингу і аудиту безпеки з реєстрацією подій зі всіх джерел захисту.

Всі реалізовані технічні засоби захисту мають чинні експертні висновки Державної служби спеціального зв’язку та захисту інформації України та відповідають вимогам чинних нормативних документів системи технічного захисту інформації.

Практичне значення роботи полягає в тому, що розроблені проєктні рішення, документація та запропонована архітектура КСЗІ можуть бути використані для створення або вдосконалення комплексних систем захисту інформації в локалізованих багатомашинних багатокористувацьких автоматизованих системах класу 2 на підприємствах, що обробляють інформацію з обмеженим доступом без віднесення до державної таємниці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 02.05.2026).
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021 [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 02.05.2026).
3. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 20 січ. 2026 р. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 03.05.2026).
4. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI : станом на 8 серп. 2025 р. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 03.05.2026).
5. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 14 черв. 2025 р. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 05.05.2026).
6. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII : станом на 27 серп. 2025 р. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 05.05.2026).
7. НД ТЗІ 2.5-008-2002. Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Чинний від 2002-12-20. Вид. офіц. Київ, 2002. 35 с. [Електронний

ресурс]. URL: https://tzi.com.ua/downloads/2.5-008-2002.pdf (дата звернення: 07.05.2026).

8. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : станом на 20 квіт. 2025 р. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 07.05.2026).
9. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
Чинний від 1999-04-28. Вид. офіц. Київ, 1999. 21 с. [Електронний ресурс]. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf (дата звернення: 08.05.2026).
10. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Чинний від 1999-04-28. Вид. офіц. Київ, 1999. 67 с. [Електронний ресурс]. URL: https://tzi.ua/assets/files/НД-ТЗІ-2.5-004-99.pdf (дата звернення: 08.05.2026).
11. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах :
Постанова Каб. Міністрів України від 29.03.2006 № 373 : станом на 2 груд. 2025 р. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text (дата звернення: 10.05.2026).
12. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Чинний від 1999-04-28. Вид. офіц. Київ, 1999. 18 с. [Електронний ресурс]. URL: https://tzi.com.ua/downloads/2.5-005%20-99.pdf (дата звернення: 13.05.2026).
13. ТР ТЗІ-ПЕМВН-95. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. Чинний від 1995-06-09. Вид. офіц. Київ, 1995. 20 с. [Електронний ресурс]. URL: https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-tr-pemvn-95.pdf (дата звернення: 14.05.2026).

14. НД ТЗІ 2.1-002-07. Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення. Чинний від 2007-12-12. Вид. офіц. Київ, 2007. 20 с. [Електронний ресурс]. URL: https://tzi.com.ua/downloads/2.1-002-07.pdf (дата звернення: 15.05.2026).
15. НД ТЗІ 3.7-003-2023. Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі. На заміну НД ТЗІ 3.7-003-2005 ; чинний від 2023-01-01. Вид. офіц. Київ, 2023. 23 с. [Електронний ресурс]. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66099 (дата звернення: 16.05.2026).
16. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Чинний від 1999-04-28. Вид. офіц. Київ, 1999. 35 с. [Електронний ресурс]. URL: https://tzi.com.ua/downloads/3.7-001-99.pdf (дата звернення: 17.05.2026).
17. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Чинний від 2000-12-04. Вид. офіц. Київ, 2000. 37 с. [Електронний ресурс]. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf (дата звернення: 19.05.2026).
18. Про затвердження Вимог до засобів криптографічного захисту інформації, призначених для захисту таємної інформації, яка не становить державної таємниці, та конфіденційної інформації в державних органах, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, військових формуваннях, які створені відповідно до закону : Наказ Адмін. Держ. служби спец. зв'язку та зах. інформації України від 07.05.2021 № 278. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/z0696-21#Text (дата звернення: 19.05.2026).

19. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. Чинний від 2011-03-25. Вид. офіц. Київ : Держспецзв'язку, 2011. 130 с. [Електронний ресурс]. URL: https://tzi.com.ua/downloads/2.6-001-11.pdf (дата звернення: 20.05.2026).
20. Про затвердження Порядку проведення державної експертизи комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах Міністерства оборони України : Наказ М-ва оборони України від 13.09.2024 № 630 : станом на 8 серп. 2025 р. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/z1500-24#Text (дата звернення: 21.05.2026).
21. Держспецзв'язку. Нормативні документи системи технічного захисту інформації. Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс]. URL: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024 (дата звернення: 21.05.2026).
22. Про затвердження нормативного документа системи технічного захисту інформації 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» : Наказ Адмін. Держспецзв'язку від 15.04.2013 № 215 [Електронний ресурс]. URL: https://zakon.rada.gov.ua/rada/show/v0215519-13#Text (дата звернення: 22.05.2026).
23. MITRE. MITRE ATT&CK enterprise matrix. MITRE ATT&CK. [Електронний ресурс]. URL: https://attack.mitre.org/matrices/enterprise/ (дата звернення: 24.05.2026).
24. Verizon. 2025 data breach investigations report. Verizon Business, 2025. 117 p. [Електронний ресурс].

URL: https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf (дата звернення: 25.05.2026).

25. Joint Task Force. Risk management framework for information systems and organizations: a system life cycle approach for security and privacy. Gaithersburg, MD : National Institute of Standards and Technology, 2018 [Електронний ресурс]. URL: https://csrc.nist.gov/pubs/sp/800/37/r2/final (дата звернення: 25.05.2026).
26. Guide to attribute based access control (ABAC) definition and considerations / Hu V. C et al. Gaithersburg, MD : National Institute of Standards and Technology, 2014 [Електронний ресурс].
URL: https://csrc.nist.gov/pubs/sp/800/162/final (дата звернення: 26.05.2026).
27. Digital identity guidelines: authentication and authenticator management / D. Temoshok et al. Gaithersburg, MD : National Institute of Standards and Technology, 2025 [Електронний ресурс].
URL: https://doi.org/10.6028/NIST.SP.800-63b-4 (дата звернення: 27.05.2026).
28. ISO/IEC 27035-1:2023. Information technology – Information security incident management – Part 1: principles and process. Replaces ISO/IEC 27035-1:2016 ; effective from 2023-02-01. Official edition. Geneva : ISO, 2023 [Електронний ресурс]. URL: https://www.iso.org/standard/78973.html (дата звернення: 28.05.2026).
29. Center for Internet Security. CIS critical security controls. version 8.1. East Greenbush, NY : Center for Internet Security, 2024.
[Електронний ресурс]. URL: https://www.cisecurity.org/controls/v8-1 (дата звернення: 29.05.2026).
30. Chandramouli R., Hibbard E. Guidelines for media sanitization. Gaithersburg, MD : National Institute of Standards and Technology, 2025 [Електронний ресурс]. URL: https://doi.org/10.6028/NIST.SP.800-88r2 (дата звернення: 30.05.2026).

31. Фільтри ЕМСБІ типу ФЗП-103-2 - ТЗІ - інформаційна безпека та захист інформації - Інформаційна безпека та захист інформації [Електронний ресурс]. URL: https://tzi.ua/ua/fltri_emsb_tipu_fzp-103-2.html (дата звернення: 03.06.2026).
32. Генератор шуму «БАЗАЛЬТ - 5ГЕШ» - ТЗІ - інформаційна безпека та захист інформації - Інформаційна безпека та захист інформації [Електронний ресурс]. URL: https://tzi.ua/ua/generator_shumu_bazalt_-_5gesh.html (дата звернення: 03.06.2026).

Додатки

Додаток А

Акт категоріювання

«ЗАТВЕРДЖУЮ»
Керівник ТОВ «Огун»
_____ Коваленко І. С.
«15» березня 2026 р.
М. П.

АКТ

категоріювання автоматизованої системи класу 2 інв. № 002145 приміщень № 201–207

(найменування/реквізити об'єкта категоріювання)

1. Підстава для категоріювання — наказ №18 від 10.03.2026 про створення КСЗІ, наказ №19 від 12.03.2026 про утворення комісії з категоріювання та обстеження об'єктів інформаційної діяльності

(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання, зміна ознак, за якою була встановлена категорія об'єкта, тощо; посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

2. Вид категоріювання — первинне

(первинне, чергове, позачергове)

(у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання; посилання/реквізити на акт, яким було встановлено цю категорію)

3. На ОІД здійснюється — обробка інформації технічними засобами

(обробка інформації технічними засобами та/або озвучування інформації)

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об'єкті — службова та конфіденційна інформація (персональні дані)

(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України «Про доступ до

Рисунок А.1 – Акт категоріювання (перша сторінка)

публічної інформації»; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

5. Встановлена категорія — IV (четверта)

Голова комісії: _____ І. С. Коваленко

(підпис)

Члени комісії: _____ О. В. Бондаренко

_____ Д. М. Шевченко

(підпис)

Рисунок А.2 – Акт категоріювання (друга сторінка)

Додаток Б

Акт обстеження

«ЗАТВЕРДЖУЮ»
Керівник ТОВ «Огун»
_____ Коваленко І. С.
«16» березня 2026 р.
М. П.

АКТ

обстеження об'єкта інформаційної діяльності ТОВ «Огун»

(найменування об'єкта інформаційної діяльності)

1. Підстава для проведення обстеження — наказ №19 від 12.03.2026 про утворення комісії з категоріювання та обстеження об'єктів інформаційної діяльності ТОВ «Огун»

(посилання/реквізити на розпорядчий документ)

2. Склад комісії з обстеження — голова комісії Бондаренко О. В., відповідальний за захист інформації; члени комісії: Шевченко Д. М., системний адміністратор; Мельник Т. І., інженер з технічного захисту інформації
3. Адреса розташування ОІД — м. Київ, вул. Героїв Оборони, 15, приміщення №№ 201–207, другий поверх
4. Характеристика приміщень ОІД:

– загальна площа: 142 кв. м;

– склад приміщень: робочі приміщення №№ 201–204, серверне приміщення №205, приміщення адміністратора безпеки №206, допоміжне приміщення №207;

– огороджувальні конструкції: цегляні стіни товщиною 380 мм (зовнішні) та 250 мм (внутрішні), металеві вхідні та металопластикові внутрішні двері, металопластикові віконні отвори;

– виходи комунікацій за межі КЗ: система електроживлення, контур заземлення, лінії пожежної сигналізації, інженерні комунікації (опалення, водопостачання, вентиляція)

5. Характеристика складу технічних засобів:

– 15 автоматизованих робочих місць користувачів;

– 1 сервер локальних служб;

Рисунок Б.1 – Акт обстеження (перша сторінка)

– 1 сервер моніторингу та реєстрації подій;

– 1 мережевий пристрій зберігання даних;

– 1 багатофункціональний пристрій друку;

– комутаційне обладнання локальної мережі

6. Характеристика системи електроживлення:

– джерело електроживлення розташоване за межами контрольованої зони;

– засоби захисту мережі електроживлення від витоку інформації відсутні

7. Характеристика системи заземлення:

– контур заземлення спільний з будівлею, виходить за межі контрольованої зони;

– засоби локального захищеного заземлення відсутні

8. Наявні засоби захисту інформації на момент обстеження — штатні засоби розмежування доступу операційних систем, антивірусний захист загального призначення; спеціалізований комплекс засобів захисту з експертним висновком Держспецзв'язку відсутній, засоби активного захисту від витоку інформації каналами ПЕМВН відсутні

9. Виявлені передумови реалізації загроз інформаційній безпеці — відсутність спеціалізованого КЗЗ від НСД, відсутність захисту мережі електроживлення від витоку інформативних сигналів, відсутність засобів захисту від витоку через побічні електромагнітні випромінювання технічних засобів обробки інформації, відсутність технічної системи охорони, неповна реєстрація подій безпеки, відсутність регламентованих процедур розмежування доступу

10. Дані щодо термінів проведення категоріювання та оформлення документації — Акт категоріювання ОІД ТОВ «Огун» від 15.03.2026

Голова комісії: _____ О. В. Бондаренко

(підпис)

Члени комісії: _____ Д. М. Шевченко

_____ Т. І. Мельник

(підпис)

Рисунок Б.2 – Акт обстеження (друга сторінка)

Додаток В

Технічне завдання

УЗГОДЖЕНО
Відповідальний за захист
інформації ТОВ «Огун»
_____ О. В. Бондаренко
«____» _____ 2026 р.
М. П.

ЗАТВЕРДЖУЮ
Керівник ТОВ «Огун»
_____ І. С. Коваленко
«____» _____ 2026 р.
М. П.

АВТОМАТИЗОВАНА СИСТЕМА
КЛАСУ 2 ТОВ «ОГУН»
КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ
Технічне завдання
Київ — 2026 р.

ЗМІСТ

1. Перелік скорочень

АРМ — автоматизоване робоче місце

Рисунок В.1 – Технічне завдання (перша сторінка)

АС — автоматизована система

ІзОД — інформація з обмеженим доступом

КЗ — контрольована зона

КЗЗ — комплекс засобів захисту

КСЗІ — комплексна система захисту інформації

НД ТЗІ — нормативний документ системи технічного захисту інформації

НСД — несанкціонований доступ

ОІД — об'єкт інформаційної діяльності

ОС — операційна система

ПЕМВН — побічні електромагнітні випромінювання і наводки

ТЗ — технічне завдання

ТЗІ — технічний захист інформації

2. Загальні відомості

Це технічне завдання визначає вимоги до комплексної системи захисту інформації в автоматизованій системі класу 2 ТОВ «Огун».

Умовне позначення АС — АС-2 ТОВ «Огун».

Замовник робіт — ТОВ «Огун», м. Київ.

Виконавець робіт — визначається на конкурсних засадах з числа суб'єктів господарювання, що мають дозвіл на провадження діяльності з технічного захисту інформації відповідно до законодавства України.

Підставою для виконання робіт є наказ керівника ТОВ «Огун» №18 від 10.03.2026 про створення комплексної системи захисту інформації.

Технічне завдання оформлено відповідно до вимог НД ТЗІ 3.7-001-99 та НД ТЗІ 3.7-003-2023.

3. Мета та призначення комплексної системи захисту інформації

Метою створення КСЗІ є забезпечення захисту інформації з обмеженим доступом, що обробляється засобами АС класу 2 ТОВ «Огун», від несанкціонованого доступу, модифікації, знищення та витоку технічними каналами протягом усього технологічного циклу обробки інформації.

КСЗІ призначена для:

Рисунок В.2 – Технічне завдання (друга сторінка)

– реалізації функціональних послуг безпеки відповідно до обраного функціонального профілю захищеності 2.КЦ.1 з рівнем гарантій Г-3;

– ідентифікації та автентифікації користувачів АС;

– розмежування доступу до інформаційних ресурсів за принципом мінімально необхідних повноважень;

– реєстрації та обліку подій безпеки в захищеному журналі;

– контролю цілісності інформаційних ресурсів та компонентів засобів захисту;

– захисту від впровадження шкідливого програмного забезпечення;

– запобігання витоку інформації через мережу електроживлення, контур заземлення та інші провідні комунікації, що виходять за межі контрольованої зони;

– виявлення спроб несанкціонованого проникнення в межі контрольованої зони у позаробочий час;

– забезпечення документального супроводу функціонування КСЗІ та регламентації дій персоналу.

4. Загальна характеристика АС та умов її функціонування

АС класу 2 ТОВ «Огун» є локалізованим багатомашинним багатокористувацьким комплексом, призначеним для автоматизованої обробки інформації в процесі надання послуг адміністрування та технічного супроводу інформаційно-комунікаційної інфраструктури підприємств-замовників.

До складу АС входять 15 автоматизованих робочих місць користувачів, сервер локальних служб, сервер моніторингу подій, мережевий пристрій зберігання даних, мережеве комутаційне обладнання та допоміжна периферія. Технічні засоби розміщені на одному поверсі офісної будівлі в межах єдиної контрольованої зони, локалізована мережа об'єднує АРМ та серверне обладнання без використання загальнодоступних мереж як основного технологічного каналу для обробки ІзОД.

Найвищий ступінь обмеження доступу інформації, що обробляється засобами АС, — службова та конфіденційна інформація (персональні дані). Обробка інформації, що становить державну таємницю, у складі АС не передбачена.

Рисунок В.3 – Технічне завдання (третя сторінка)

Режим обробки інформації — реального часу, у штатний робочий час підприємства.

Безпосередню роботу з ресурсами АС здійснюють 15 співробітників ТОВ «Огун» різних категорій повноважень, у тому числі керівник, адміністратор безпеки, системний адміністратор, інженери технічної підтримки, керівники проєктів, особи з документального супроводу.

Базове програмне забезпечення АРМ включає операційну систему Microsoft Windows 11 Pro, офісний пакет, спеціалізоване ПЗ для адміністрування інфраструктури замовників та клієнтське ПЗ для роботи з ресурсами серверного обладнання. На серверному обладнанні застосовуються мережева операційна система, система керування базами даних та засоби моніторингу подій інформаційної безпеки.

5. Вимоги до комплексної системи захисту інформації

5.1. Загальні вимоги до КСЗІ

КСЗІ повинна реалізовуватися як сукупність узгоджених за часом та місцем застосування організаційних, інженерно-технічних та програмно-технічних заходів захисту інформації. Робота АС у штатних режимах повинна бути можлива виключно за умови функціонування системи захисту інформації.

Архітектура КСЗІ повинна забезпечувати реалізацію функціонального профілю захищеності 2.КЦ.1 з рівнем гарантій Г-3 та включати п'ять взаємопов'язаних підсистем: підсистему захисту від НСД, підсистему антивірусного захисту, підсистему захисту від витоку інформації технічними каналами, технічну систему охорони та підсистему організаційно-розпорядчого забезпечення.

Розташування, монтаж та прокладка інженерно-технічних комунікацій АС, у тому числі систем заземлення та електроживлення, повинні виконуватися з дотриманням вимог чинних нормативних документів системи ТЗІ.

5.2. Вимоги до функціональних послуг безпеки

Комплекс засобів захисту КСЗІ повинен реалізовувати функціональний профіль захищеності інформації від несанкціонованого доступу 2.КЦ.1 = {КД-2, ЦД-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1} відповідно до НД ТЗІ 2.5-005-99.

Рисунок В.4 – Технічне завдання (четверта сторінка)

Для реалізації функціональних послуг застосовується засіб захисту інформації від несанкціонованого доступу «Лоза-2» версії 3 з чинним експертним висновком Держспецзв'язку. Засіб встановлюється на всіх 15 автоматизованих робочих місцях та серверному обладнанні АС.

Для протидії загроз впровадження шкідливого програмного забезпечення застосовується продукт ESET Endpoint Security з чинним експертним висновком Держспецзв'язку. Централізоване керування підсистемою антивірусного захисту здійснюється через консоль ESET PROTECT, що розгортається на сервері локальних служб.

5.3. Вимоги до гарантій реалізації

Рівень гарантій реалізації функціонального профілю захищеності — Г-3 відповідно до НД ТЗІ 2.5-004-99. Реалізація вимог рівня Г-3 передбачає документоване підтвердження виконання заявлених функціональних послуг, проведення випробувань КЗЗ за погодженою програмою та методикою, документоване підтвердження керованості процесу розроблення та супроводу засобів захисту.

Архітектура КЗЗ повинна базуватися на принципі мінімуму повноважень, забезпечувати можливість керування налаштуваннями та контролю стану засобів захисту, передбачати розмежування повноважень адміністратора та звичайних користувачів системи.

Розробник повинен забезпечити документовані методики керування конфігурацією КЗЗ на всіх стадіях життєвого циклу АС. Внесення змін у конфігурацію засобів захисту здійснюється на основі формальних процедур з документальним оформленням.

5.4. Вимоги до захисту від витоку інформації технічними каналами

Захист від витоку інформації технічними каналами повинен забезпечувати протидію загроз витоку через мережу електроживлення, контур заземлення та провідні комунікації, що виходять за межі контрольованої зони.

Для захисту мережі електроживлення застосовується мережевий завадозаглушувальний фільтр «ФЗП-103-2» виробництва ТОВ «ЕМСБІ», що

Рисунок В.5 – Технічне завдання (п’ята сторінка)

встановлюється на вводі мережі живлення в межі контрольованої зони. Робочий діапазон фільтра — від 10 кГц до 1000 МГц.

Для забезпечення гальванічної розв'язки мережі електроживлення ОІД від загальнобудинкової мережі встановлюється розділовий трансформатор, що включається послідовно з фільтром ФЗП-103-2.

У межах контрольованої зони обладнується локальний контур заземлення з опором не більше 2 Ом, що забезпечує відведення інформативних сигналів без виходу за межі ОІД.

Контроль ефективності реалізованих заходів захисту від витоку інформації технічними каналами виконується за вимогами НД ТЗІ 2.1-002-07.

Для захисту від витоку інформації за рахунок побічних електромагнітних випромінювань технічних засобів обробки інформації у простір застосовується генератор шуму електромагнітних випромінювань «Базальт-5ГЕШ» виробництва ПрАТ «Холдингова компанія "Укрспецтехніка"», що має чинний експертний висновок Держспецзв'язку. Генератор забезпечує створення в навколишньому просторі електромагнітного поля шуму з робочим діапазоном частот, що перекриває спектр можливих побічних випромінювань технічних засобів обробки інформації.

6. Вимоги до складу проектної та експлуатаційної документації

До складу проектної документації КСЗІ входять: технічне завдання на створення КСЗІ, акт категоріювання ОІД, акт обстеження ОІД, модель загроз інформаційній безпеці, модель порушника, політика безпеки інформації в АС, проект розміщення засобів КСЗІ, схеми підключення засобів захисту.

До складу експлуатаційної документації входять: положення про службу захисту інформації, посадова інструкція відповідального за захист інформації, інструкції користувачів АС, інструкція з реагування на інциденти, інструкції з експлуатації засобів захисту «Лоза-2», ESET Endpoint Security та «ФЗП-103-2», журнал обліку відвідувачів, журнал обліку знімних носіїв, журнал реєстрації змін у налаштуваннях засобів захисту.

7. Етапи виконання робіт

Рисунок В.6 – Технічне завдання (шоста сторінка)

Етапи створення КСЗІ та результати, що отримуються на кожному етапі, наведено у таблиці 1.

Таблиця 1 — Етапи виконання робіт зі створення КСЗІ

№	Найменування етапу	Результат етапу
1	Попередній етап	
1.1	Обстеження ОІД	Акт обстеження ОІД
1.2	Визначення переліку загроз та можливих каналів витоку	Модель загроз, модель порушника
1.3	Визначення вимог до КЗЗ у частині захисту від НСД та витоку технічними каналами	Відповідні розділи ТЗ
2	Етап проектування та розробки КСЗІ	
2.1	Проектування підсистем КСЗІ	Проектні рішення
2.2	Розробка робочої та експлуатаційної документації	Проектна та експлуатаційна документація
2.3	Виконання робіт із захисту інформації від витоку технічними каналами	Протоколи спецдосліджень, приписи на експлуатацію
2.4	Налаштування засобів захисту «Лоза-2» та ESET Endpoint Security	Виконані налаштування, протокол приймання
2.5	Розробка організаційної документації та впровадження організаційних заходів	Затверджена організаційна документація
2.6	Розробка програми та методики випробувань КСЗІ	Програма та методики випробувань
3	Етап випробувань та передачі КСЗІ в експлуатацію	
3.1	Проведення попередніх випробувань КСЗІ	Протоколи попередніх випробувань, акт приймання в дослідну експлуатацію

Рисунок В.7 – Технічне завдання (сьома сторінка)

3.2	Навчання користувачів та адміністраторів	Програма навчання, акт завершення навчання
3.3	Проведення дослідної експлуатації КСЗІ	Журнали дослідної експлуатації, акт завершення дослідної експлуатації
3.4	Підготовка документації для проведення державної експертизи	Комплект документації для державної експертизи
4	Державна експертиза КСЗІ	Атестат відповідності

8. Порядок проведення випробувань комплексної системи захисту інформації

Випробування КСЗІ проводяться згідно з програмою та методикою випробувань, що розробляються на етапі проектування та повинні містити процедури перевірки реалізації всіх заявлених функціональних послуг безпеки. Випробування проводяться у два етапи: попередні випробування для оцінки відповідності реалізованої КСЗІ вимогам технічного завдання, та дослідна експлуатація для перевірки функціонування системи в умовах штатного використання.

Перевірка реалізації функціональних послуг безпеки виконується з використанням контрольних прикладів, що моделюють спроби реалізації виявлених у моделі загроз дій. Перевірка ефективності захисту від витоку інформації технічними каналами виконується шляхом проведення спецдосліджень відповідно до НД ТЗІ 2.1-002-07. За результатами випробувань оформлюються протоколи, що додаються до комплекту документації КСЗІ.

9. Порядок внесення змін і доповнень до ТЗ

Внесення змін і доповнень до технічного завдання здійснюється у разі зміни нормативної бази системи ТЗІ, складу інформаційних ресурсів АС, появи нових загроз інформаційній безпеці або за результатами випробувань КСЗІ. Зміни оформлюються додатками до ТЗ, що погоджуються та затверджуються в порядку, аналогічному порядку погодження та затвердження самого ТЗ.

Рисунок В.8 – Технічне завдання (восьма сторінка)