КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Кваліфікаційна робота бакалавра

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

Здобувач: **Афонін Микола Валерійович**
Спеціальність: **Кібербезпека**
Група: **БІКС-23с**
Керівник: **к.т.н., доцент Котенко А. М.**

• Київ 2026 •

ЗАГАЛЬНІ ВІДОМОСТІ

Об'єкт, предмет, мета та завдання

Об'єкт дослідження

Процес захисту інформації з обмеженим доступом

Предмет дослідження

Захист інформації з обмеженим доступом в АС-2

МЕТА: Проєктування та практична реалізація КСЗІ з обмеженим доступом в автоматизованій системі класу 2 з урахуванням нормативних вимог, актуальних загроз і моделі порушника.

ЗАВДАННЯ

1. Дослідити теоретичні та нормативно-правові основи захисту ІзОД.
2. Виконати категоріювання ОІД та обстеження середовища АС.
3. Побудувати модель загроз та модель порушника.
4. Розробити політику безпеки та обрати профіль захищеності.
5. Сформувати структуру КСЗІ та розробити технічне завдання.
6. Оцінити ефективності застосованих засобів захисту інформаційної безпеки.

РОЗДІЛ 1 · ТЕОРЕТИЧНІ ОСНОВИ

Класифікація автоматизованих систем

за НД ТЗІ 2.5-005-99

Клас 1

Одномашинний однокористувацький комплекс

Клас 2

Локалізований багатомашинний багатокористувацький комплекс

◆ ОБ'ЄКТ РОБОТИ

Клас 3

Розподілений комплекс із передаванням через незахищене середовище

Безпека інформації визначається трьома властивостями: **конфіденційність** · **цілісність** · **доступність**. Обробка інформації відбувається у контрольованому середовищі без передавання через глобальну мережу.

РОЗДІЛ 1 · ТЕОРЕТИЧНІ ОСНОВИ

Загрози та канали витоку інформації

ТРИ ГРУПИ ЗАГРОЗ

- Несанкціонований доступ до інформаційних ресурсів
- Витік інформації технічними каналами
- Порушення працездатності системи

ТЕХНІЧНІ КАНАЛИ ВИТОКУ (АКТУАЛЬНІ ДЛЯ ОІД)

Мережа електроживлення
наведення у колах живлення 220 В

Контур заземлення
наведення на коло заземлення

ПЕМВН провідними комунікаціями
наведення на лінії, що виходять за КЗ

Побічні випромінювання у простір
сигнали моніторів і ПЕОМ

РОЗДІЛ 2 · ПРОЄКТУВАННЯ

Об'єкт інформаційної діяльності ТОВ «Огун»

Характеристика ОІД

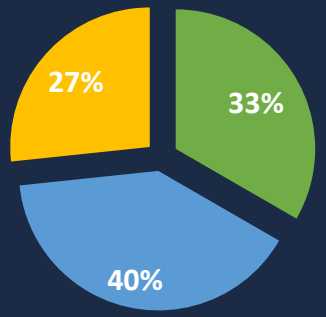
- Підприємство у сфері інформаційних технологій (м. Київ)
- З ресурсами АС працюють 15 співробітників
- В ОІД виконується обробка персональних даних, комерційної таємниці замовників, службової інформації
- Інформація яка церкулює в ОІД не належить до державної таємниці
- Під час проведення Категоріювання було присвоєно IV категорія за НД ТЗІ 1.6-005-2013

В ХОДІ ОБСТЕЖЕННЯ БУЛО ВИЯВЛЕНО ПЕРЕДУМОВИ ЗАГРОЗ

- Відсутній спеціалізований засіб захисту від НСД
- Відсутній захист мережі електроживлення та заземлення
- Відсутній захист від побічних електромагнітних випромінювань
- Неповна реєстрація подій безпеки
- Відсутня технічна система охорони

Модель загроз та модель порушника

ЗА РЕЗУЛЬТАТАМИ ОБСТЕЖЕНННЯ БУЛО ПОБУДОВАНО МОДЕЛЬ ЗАГРОЗ ЯКА МІСТИТЬ 15 АКТУАЛЬНИХ ЗАГРОЗ



- НСД до ресурсів – 6 (40%)
- Витік технічними каналами – 4 (27%)
- Порушення працездатності – 5 (33%)

Актуальних загроз

Класифікація за джерелом, характером впливу та способом реалізації (з урахуванням MITRE ATT&CK).

МОДЕЛЬ ПОРУШНИКА

Внутрішні порушники з розширеними правами: користувачі, системний адміністратор, адміністратор безпеки	ВИСОКИЙ
Зовнішні озброяні технічними засобами перехоплення	СЕРЕДНІЙ
Зовнішні з доступом на територію	ПРИПУСТИМИЙ

Функціональний профіль захищеності

Для нейтралізації загроз обрано функціональний профіль

Профіль 2.КЦ.1 Рівень гарантій **Г-3**

НД ТЗІ 2.5-004-99, 2.5-005-99, **2.5-008-2002**

КД-2
Довірча конфіденційність

ЦД-1
Довірча цілісність

НР-2
Реєстрація (захищений журнал)

НИ-2
Ідентифікація і автентифікація

НК-1
Достовірний канал

НО-1
Розподіл обов'язків

НЦ-1
Цілісність КЗЗ

Профіль обрано для службової та конфіденційної інформації без віднесення до державної таємниці.

РОЗДІЛ 2 · АРХІТЕКТУРА

Структура КСЗІ: що складається з п'яти підсистем

Захист від НСД
На базу комплексу

«Лоза-2»

Антивірусний захист

ESET Endpoint Security

Захист від витоку тех. каналами

ФЗП-103-2 · Базальт-5ГЕШ

Технічна система охорони

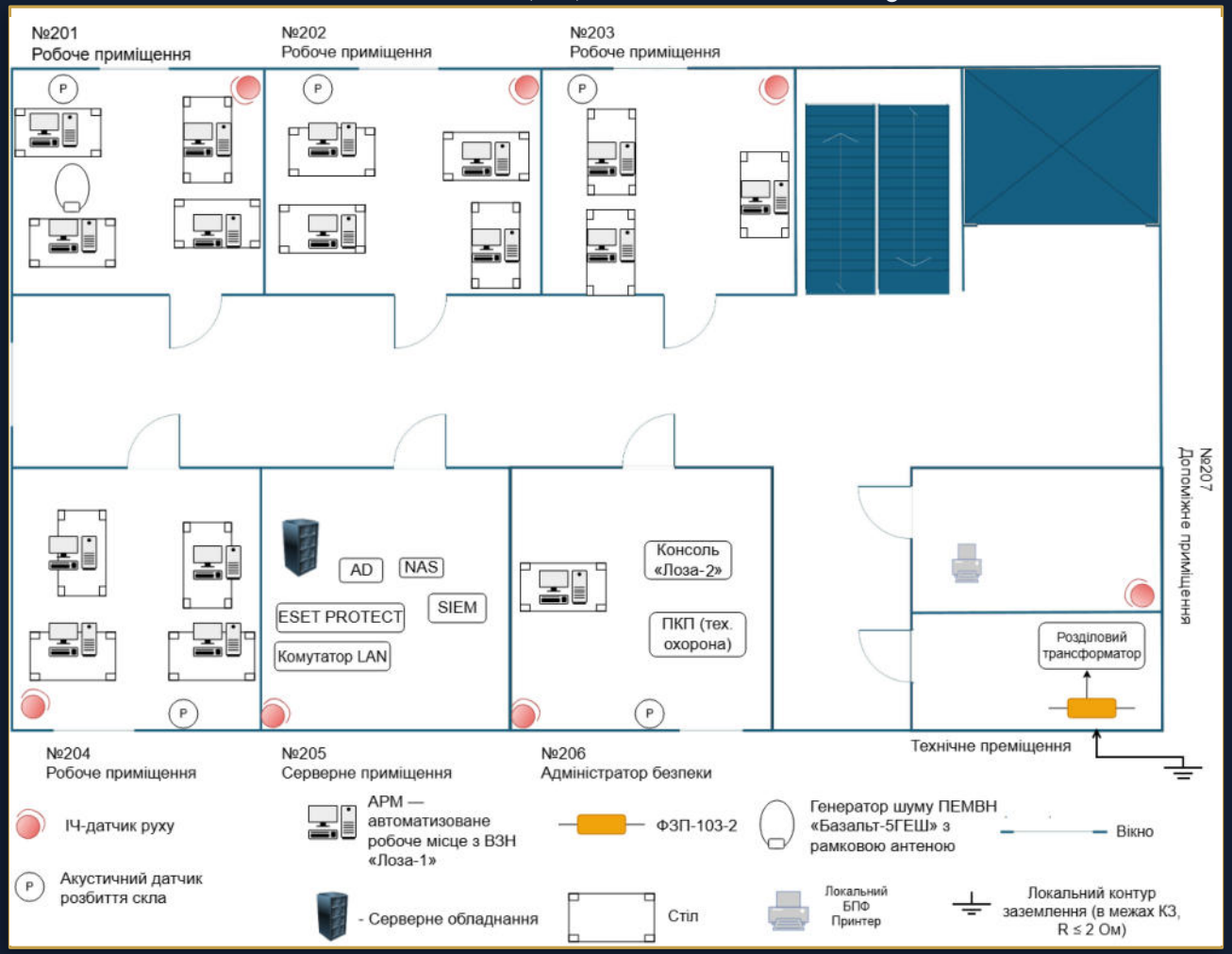
ІЧ + акустичні сповіщувачі

Організаційно-розпорядче забезпечення

Документування подій безпеки в ОІД

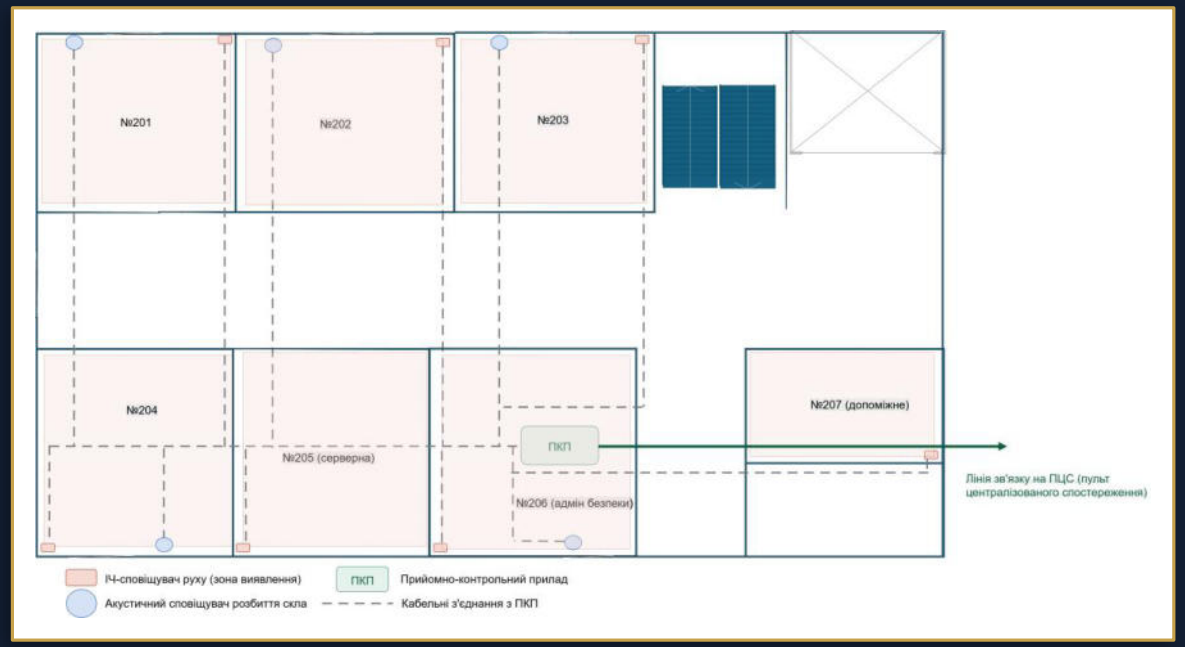
Реалізація профілю 2.КЦ.1 (Г-3) забезпечується спільною роботою всіх п'яти підсистем + розроблене технічне завдання на створення КСЗІ.

Розміщення засобів КСЗІ на ОІД ТОВ «Огун»

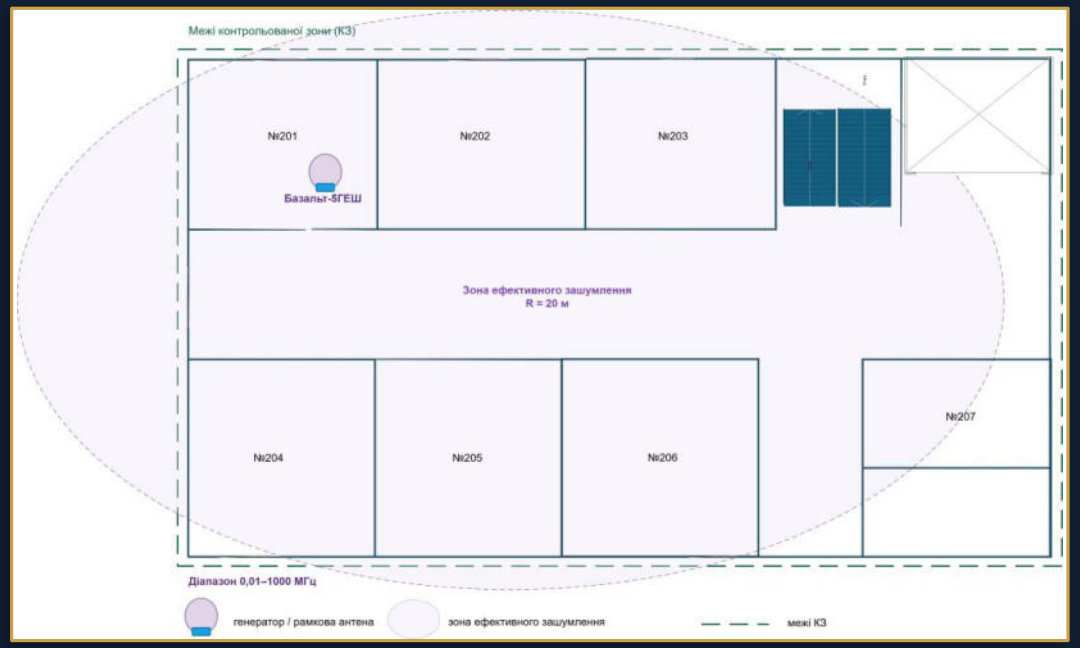


Приміщення №201–207 у межах контрольованої зони: робочі АРМ із «Лоза-2», серверне приміщення (ESET PROTECT, SIEM), адміністратор безпеки, фільтр «ФЗП-103-2» з розділовим трансформатором, генератор «Базальт-5ГЕШ», локальний контур заземлення, ІЧ- та акустичні сповіщувачі.

Технічна охорона та захист від ПЕМВН



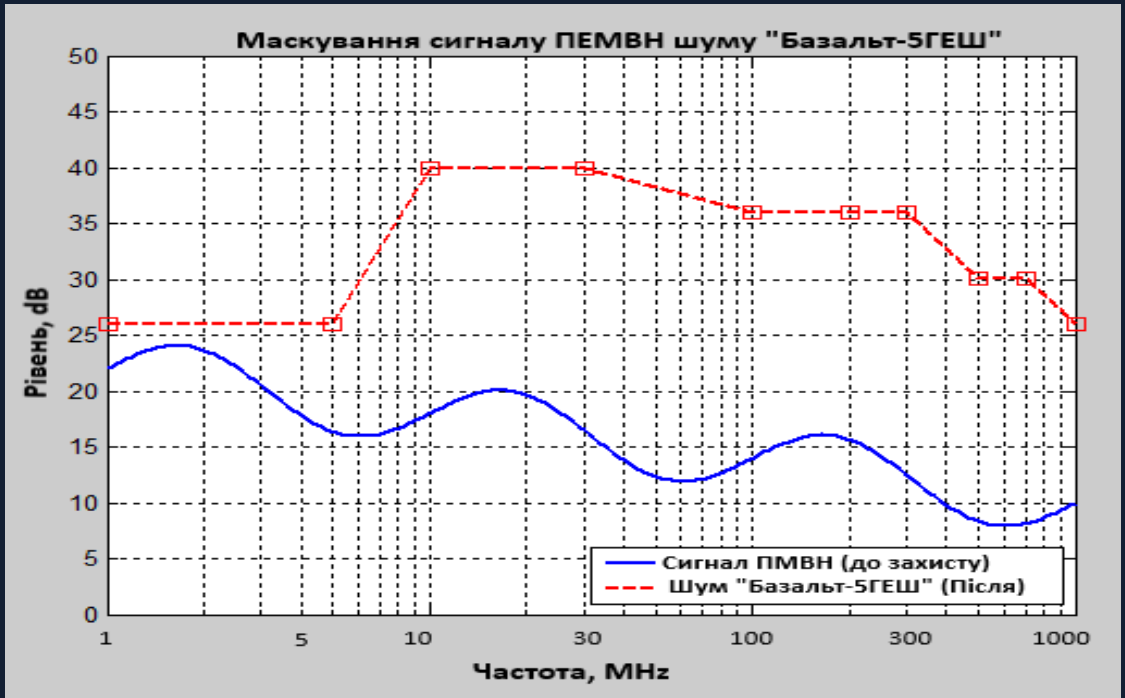
Технічна система охорони: ІЧ- та акустичні сповіщувачі → ПКП → ПЦС

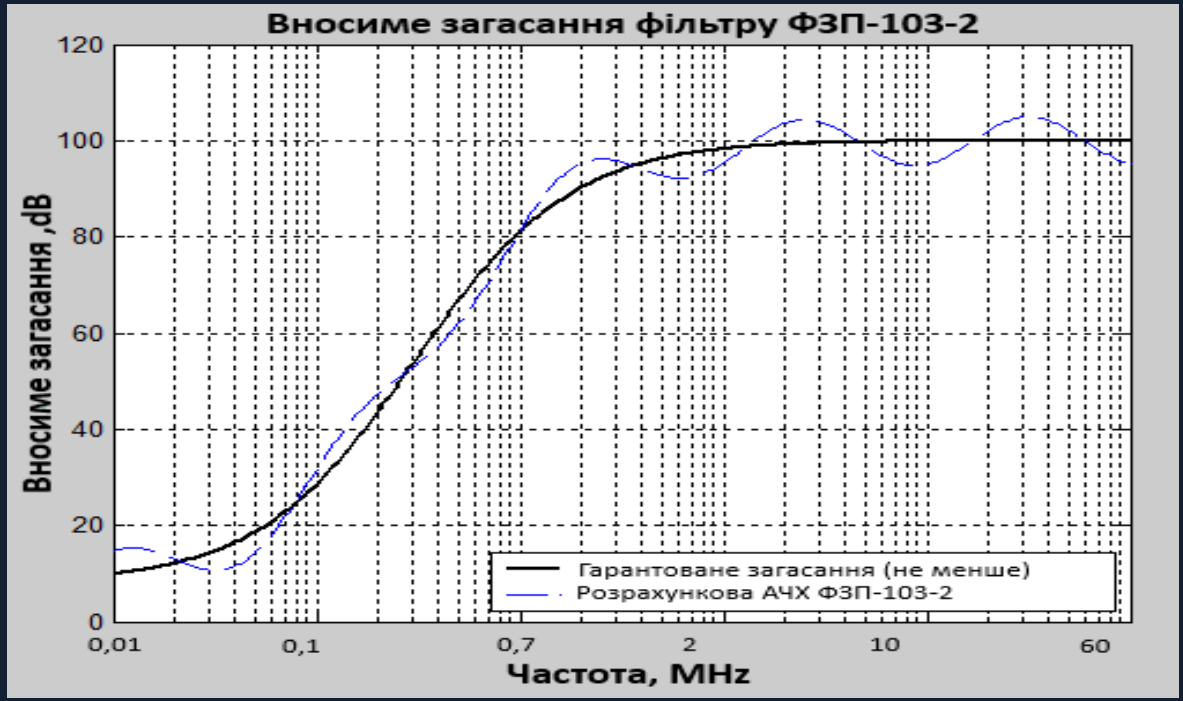


Зона ефективного зашумлення «Базальт-5ГЕШ» (R ≈ 20 м, 0,01–1000 МГц)

РОЗДІЛ 3 · РЕЗУЛЬТАТИ

Ефективність застосованих засобів ТЗІ





- Базальт-5ГЕШ: рівень шуму (45–80 дБ) перекриває сигнал ПЕМВН у всьому діапазоні 0,1–1000 МГц — сигнал замаскований.
- ФЗП-103-2: вносиме загасання зростає до ~100 дБ — завада в колах живлення придушена в діапазоні 10 кГц–1000 МГц.

Розрахункова оцінка за нормованими (паспортними) характеристиками засобів. Інструментальні вимірювання — напрям подальших досліджень.

ПІДСУМОК

Висновки

- Досліджено теоретичні та нормативно-правові основи захисту ІзОД в АС класу 2.
- Виконано категоріювання ОІД (IV категорія) та обстеження середовища функціонування АС.
- Побудовано модель загроз (15 загроз) і модель порушника; обрано профіль 2.КЦ.1 (Г-3).
- Спроєктовано та реалізовано КСЗІ у складі п'яти підсистем зі схваленими засобами захисту.
- Мету досягнуто, всі завдання виконано; рішення придатні для впровадження на підприємствах.

Дякую за увагу!

Доповідь закінчено

Афонін М. В. • група БІКСс-23 • Київ 2026