

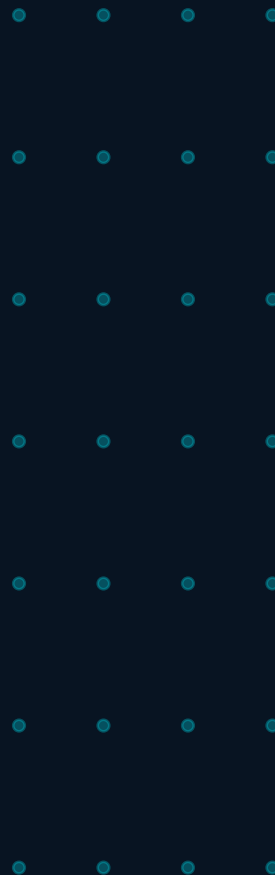
ЗАХИСТ ІНФОРМАЦІЇ

В АВТОМАТИЗОВАНІЙ СИСТЕМІ КЛАСУ 1

ВІД ВИТОКУ ЕЛЕКТРИЧНИМ КАНАЛОМ

Виконав: Гелету́ха Артем Васильович, гр. БІКСс-23

Керівник: к.т.н., доцент Котенко А.М.



ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ ТА АБРЕВІАТУР

Абрев.	Розшифрування
АС	Автоматизована система
ВКЗЗ	Виділений контур захисного заземлення
ВЧ	Висока частота
ДТЗС	Допоміжні технічні засоби та системи
ЕКВІ	Електричний канал витоку інформації
ЕРС	Електрорушійна сила
ЕРТ	Екранований розділовий трансформатор
ЗУ	Закон України
ІБ	Інформаційна безпека
ІзОД	Інформація з обмеженим доступом
ІТС	Інформаційно-телекомунікаційна система
КЗ	Контрольована зона

Абрев.	Розшифрування
КТ	Контрольна точка вимірювань
НД	Нормативний документ
НСД	Несанкціонований доступ
НЧ	Низька частота
ОІД	Об'єкт інформаційної діяльності
ПЕМВН	Побічні електромагнітні випромінювання та наводки
ПЕОМ	Персональна електронна обчислювальна машина
РТ	Розділовий трансформатор
СШ	Співвідношення сигнал/шум
ТЗІ	Технічний захист інформації
ТПКО	Технічні рекомендації щодо категоріювання об'єктів
ТР	Технічні рекомендації (нормативний документ)

* Латинські скорочення: FP1/FP2/FP3 — Filter Protection (клас мережевого фільтра) · DELTA-7, БАЗАЛЬТ-5ГЕШ — торгові назви засобів зашумлення

ОБ'ЄКТ, ПРЕДМЕТ, МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

ОБ'ЄКТ

Процес технічного захисту інформації з обмеженим доступом в умовах функціонування автоматизованої системи класу 1

ПРЕДМЕТ

Електричний канал витоку інформації в АС класу 1: фізична природа, механізми формування та засоби нейтралізації

МЕТА

Розробити комплекс організаційних та технічних рішень для захисту від витоку електричним каналом і обґрунтувати їх ефективність

МЕТОДИ

Аналіз НД ТЗІ · системний аналіз ОІД · розрахункові методи оцінки СШ · порівняльний аналіз технічних засобів захисту

ЗАВДАННЯ:

- 1. Вивчити нормативно-правові засади ТЗІ
- 2. Дослідити фізичну природу ЕКВІ
- 3. Побудувати модель загроз і модель порушника
- 4. Обґрунтувати підбір технічних засобів захисту
- 5. Виконати розрахункову оцінку ефективності

>65%

збитків ІБ пов'язані з
технічними каналами витоку
та людським фактором

Спеціальний
канал без НСД

ЕКВІ непомітний для засобів аудиту



Системна загроза

ЕКВІ формується через штатну інфраструктуру — лінії живлення, заземлення, телефонні та сигнальні кабелі. Об'єкт можна не відвідувати.



АС класу 1 — максимальний ризик

Весь інформативний трафік сконцентрований в одному місці → рівень ПЕМВН максимальний серед усіх класів АС.



Нормативна вимога

ТР ПЕМВН-95, НД ТЗІ 3.7-003-23 та ЗУ «Про захист інформації в ІТС» зобов'язують створювати КСЗІ та проводити спецдослідження.



Комплексний підхід обов'язковий

Окремі фільтри чи екрани не дають результату — потрібна інтеграція пасивних, активних і організаційних засобів.

НОРМАТИВНО-ПРАВОВА БАЗА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

ТР ПЕМВН-95

Нормативні значення СШ; методика вимірювань у КТ; класифікація засобів захисту FP1–FP3

НД ТЗІ 3.7-003-23

Послідовність етапів створення КСЗІ; склад обов'язкової документації; вимоги до спецдосліджень

НД ТЗІ 1.1-002-99

НД ТЗІ 2.5-004-99

Термінологія у сфері захисту від НСД; критерії оцінки захищеності; модель CIA

ЗУ «Про інформацію»

ЗУ «Про захист інформації в ІТС»

Класифікація ІзОД (відкрита, конфіденційна, держтаємниця). Вимоги до захисту при обробці в АС

ТПКО-95 / ТР ЕОТ-95

Категоріювання об'єктів інформатизації; порядок монтажу ЕОТ; вимоги до кабельних конструкцій

НД ТЗІ 1.6-005-2013

ДСТУ 3396.1-96

Положення про категоріювання ОІД; порядок проведення робіт з ТЗІ; атестаційні вимоги

ЕЛЕКТРИЧНИЙ КАНАЛ ВИТОКУ ІНФОРМАЦІЇ: ПРИРОДА ТА МЕХАНІЗМИ

ЕКВІ — канал несанкціонованої передачі захищеної інформації через електропровідні елементи (лінії живлення, заземлення, сигнальні та комунікаційні дроти) внаслідок виникнення паразитних електричних зв'язків або наведень.

ЄМНІСНЕ НАВЕДЕННЯ

- Між паралельними провідниками через паразитну ємність C_p
- $X_c = 1/\omega C \rightarrow$ рівень зростає зі збільшенням частоти (до 100+ МГц)
- Нейтралізація: розведення кабелів, металеві коробки, Y-конденсатори у фільтрі

ІНДУКТИВНЕ НАВЕДЕННЯ

- Змінний струм $\rightarrow$ змінне магнітне поле $\rightarrow$ ЕРС у суміжних провідниках
- Рівень залежить від геометрії контурів і взаємного розташування
- Нейтралізація: перехрещення кабелів під 90° , металеві екрани

ГАЛЬВАНІЧНЕ НАВЕДЕННЯ

- Через спільний активний опір шини живлення або заземлення
- $\beta = U_n/U_i$ — НЕ залежить від частоти; діє від DC до ВЧ
- Нейтралізація: виділений контур, розділовий трансформатор

⚡ Умова: вихід провідників за КЗ + фізична доступність лінії + засоби перехоплення злоумисника

АС КЛАСУ 1: ХАРАКТЕРИСТИКИ ТА ДЖЕРЕЛА ПЕМВН

АС КЛАСУ 1 — КЛЮЧОВІ ОСОБЛИВОСТІ

НД ТЗІ 2.5-005-99:

Один або чітко визначений склад користувачів з однаковим рівнем доступу

КЗ:

Будь-який вихід провідника за межі — потенційна точка витоку

Склад:

ПЕОМ, принтери, сканери, мережеве та телефонне обладнання

Ризик:

Максимальна концентрація інформативного трафіку в одному місці

Документація:

Акт обстеження, акт категоріювання, ТЗ, протоколи — обов'язкові

ДЖЕРЕЛА ТА ШЛЯХИ ПЕМВН В АС-1

Лінія живлення

Струм споживання синхронізований з оброблюваними даними → інформативні мікроімпульси напруги

Система заземлення

Шина з'єднана з металоконструкціями → паразитні струми доступні в будь-якій точці будівлі

Телефонні/сигнальні лінії

Наведений сигнал від активних кабелів; контактне підключення за межами КЗ

Кабельні траси

Безконтактне індукційне перехоплення без порушення ізоляції — немає слідів

ДТЗС (охор. сигнал., кондиц.)

Ненавмисний перенос інформативних наведень за межі КЗ

ОБСТЕЖЕННЯ ОБ'ЄКТА ТА КОНТРОЛЬНІ ТОЧКИ ВИМІРЮВАНЬ

СКЛАДОВІ ОБСТЕЖЕННЯ ОІД
Система живлення Схема щитів, виділеність мережі, доступність щита для сторонніх
Система заземлення Тип (виділений/природний), зв'язки з металоконструкціями будівлі
Кабельні траси Маршрути всіх кабелів, точки виходу з КЗ, паралельне прокладання
ДТЗС Охоронна/пожежна сигнал., кондиціонери — потенційні випадкові антени
Допуск персоналу Сервісний персонал, суміжні технічні приміщення, режим доступу

КТ	Місце вимірювання	Канал загрози
КТ-1	Ввід силової мережі до КЗ	Канал по живленню
КТ-2	Вузол шини заземлення	Канал по заземленню
КТ-3	Вихід телефонної лінії	Телефонний канал
КТ-4	Вихід кабелю LAN	Мережевий канал
КТ-5	Суміжні кабельні траси	Безконтактне перехоплення

Методика (ТР ПЕМВН-95):

СШ = $U_c - U_n$ (дБмкВ)
 $KA = CШ_{вим} - CШ_{норм} + \Delta K \quad | \quad \Delta K = 6-10 \text{ дБ}$
 $CШ_{норм} = 30 \text{ дБмкВ (категорія 1)}$

МОДЕЛЬ ЗАГРОЗ: МАТРИЦЯ РИЗИКІВ (НД ТЗІ 1.6-005-2013)

Загроза	Ймов. (1–3)	Збиток (1–3)	Пріоритет	Засіб нейтралізації
Витік по мережі електроживлення	3	3	 Критичний	Мережевий фільтр FP3, виділена мережа живлення
Витік по системі заземлення	2	3	 Високий	Виділений контур (топология «зірка»), ізоляція від природних заземлювачів
Контактне підключення до тел./сигн. лінії	2	2	 Середній	Пристрій гальванічної розв'язки (оптрон / трансф.)
Безконтактне індукційне перехоплення	1	2	 Низький	Металеві коробки з суцільним заземленням
НСД під час сервісних робіт	2	3	 Середній	Регламент сервісу, пломбування, присутність адм. безп.
Закладний пристрій	1	3	 Середній	Спецобстеження, контроль ланцюга постачань, заборона несертиф. обл.

Пасивне перехоплення

Без активних впливів — штатний аудит не виявить

Оцінка ризику

Ймовір.×Збиток → 1–9; Критичний ≥ 7

Динамічна модель

Переглядається при зміні конфігурації або меж КЗ

Документ-основа

НД ТЗІ 1.6-005-2013 — склад та порядок моделі загроз

МОДЕЛЬ ПОРУШНИКА: КАТЕГОРІЇ, МОТИВАЦІЯ ТА СЦЕНАРІЇ

1

КАТЕГОРІЯ 1 — Непідготовлений сторонній

- Перебуває поза КЗ, без спеціального обладнання
- Використовує загальнодоступні методи (відкрита розетка в коридорі)

- Нейтрал.: замкнений щит, пломби, обмеження доступу

Загрожує: КТ-1 (живлення), КТ-3 (телефон) — якщо доступні

2

КАТЕГОРІЯ 2 — Кваліфікований фахівець без доступу до КЗ

- Знання у галузі технічної розвідки; аналізатор спектра, індукційні датчики
- Здатний до пасивного перехоплення за межами КЗ без фізичного порушення

- Мотивація: конкурент або спецслужба; тривала спланована операція

Загрожує: КТ-1, КТ-2, КТ-4, КТ-5 — дистанційно

3

КАТЕГОРІЯ 3 — Інсайдер або особа під виглядом техперсоналу ⚠

- Легальний тимчасовий доступ до КЗ та технічних вузлів
- Може встановити закладний пристрій або змінити конфігурацію

- Нейтрал.: принцип двох осіб, журнал сервісу, відеофіксація, пломби

Загрожує: Усі КТ + ризик закладних пристроїв

АРХІТЕКТУРА КСЗІ — ЧОТИРИ РІВНІ ЗАХИСТУ

4	КОНТРОЛЬНИЙ РІВЕНЬ Щорічні спецдослідження (вимірювання у всіх КТ) · щомісячний огляд пломб і стану обладнання · позапланові дослідження після будь-яких змін · аналіз інцидентів і ведення журналів
3	АКТИВНИЙ ТЕХНІЧНИЙ РІВЕНЬ Генератор просторового зашумлення БАЗАЛЬТ-5ГЕШ (0,1–1000 МГц) · засіб лінійного зашумлення DELTA-7 (вводить шум у лінії живлення та заземлення) · живлення від тієї самої мережі, що і захищуване обладнання
2	ПАСИВНИЙ ТЕХНІЧНИЙ РІВЕНЬ Мережевий фільтр FP3 (≥60 дБ, 10 кГц–300 МГц) · розділовий трансформатор (гальванічна ізоляція) · виділений контур заземлення (зірка, ≤10 Ом) · гальванічна розв'язка зовн. ліній · екранування кабелів у металевих коробах
1	ОРГАНІЗАЦІЙНИЙ РІВЕНЬ Межі КЗ та документальна фіксація · регламент допуску персоналу та сервісних робіт · журнал контролю, журнал сервісу, журнал змін конфігурації · інструктаж персоналу · пломбування критичних вузлів

Багаторівневість: кожна загроза зустрічає наступний рівень	Адресність: кожен засіб → конкретна загроза з моделі	Верифікованість: кожен захід має вимірний критерій	Нормативна обґрунтованість: посилання на конкретний НД ТЗІ
--	--	--	--

ПАСИВНІ ЗАСОБИ: МЕРЕЖЕВІ ФІЛЬТРИ ТА РОЗДІЛОВІ ТРАНСФОРМАТОРИ

МЕРЕЖЕВІ ФІЛЬТРИ (ТР ПЕМВН-95)

Принцип: LC-чотириполюсник (синфазний дросель + Y/X-конденсатори + варистори)

Клас	Призначення	Ослаблення
FP1	Окремі робочі місця	≥ 20 дБ
FP2	Захищений сектор	≥ 40 дБ
FP3	Ввід до КЗ (обраний)	≥ 60 дБ

Розрахунок (КТ-1):

$US = 68$ дБмкВ; $U_{\text{норм}} = 30$ дБмкВ; $\Delta K = 10$ дБ
→ $KA = 68 - 30 + 10 = 48$ дБ
FP3 дає 60 дБ → запас = 22 дБ 

Монтаж: кабель від щита до фільтра — в металевому коробі; корпус фільтра — до виділеного заземлення

РОЗДІЛОВІ ТРАНСФОРМАТОРИ

Звичайний РТ

Повна гальванічна ізоляція первинного/вторинного кіл. Блокує DC і НЧ складові. Ємнісний зв'язок між обмотками обмежує ефект на ВЧ.

Екранований РТ (ЕРТ)

Між обмотками — заземлений металевий екран → паразитна ємність зменшується на порядок. Рекомендований для кат. 1.

«Електродвигун–Генератор»

Зв'язок тільки через вал (механічний) — жодного електричного провідника. Максимальна ізоляція для найвищих вимог.

 Встановлюється після загального фільтра FP3. Від виходу РТ до обладнання — мінімально коротка ділянка.

ЕКРАНУВАННЯ, ВИДІЛЕНИЙ КОНТУР ЗАЗЕМЛЕННЯ ТА ГАЛЬВАНІЧНА РОЗ'ЯЗКА

ЕКРАНУВАННЯ КАБЕЛЬНИХ ТРАС

- Металеві коробки (сталь 1,5–2 мм) на всіх ділянках виходу кабелів з КЗ
- Фланцеві з'єднання між секціями → надійний електричний контакт
- Функція 1: ослаблення ПЕМВН (ємнісне + індуктивне наведення)
- Функція 2: фізична неможливість безконтактного зняття без порушення короба
- Корпус кожного короба → до шини виділеного захисного заземлення

ВИДІЛЕНИЙ КОНТУР ЗАЗЕМЛЕННЯ

- Топологія «зірка»: всі провідники сходяться в одній шині — замкнені контури виключені
- Повна ізоляція від природних заземлювачів (арматура, трубопроводи будівлі)
- Окремий стрижень або сітка, без контакту з фундаментом
- Опір розтікання ≤ 10 Ом (кат. 1); вимір: метод амперметра-вольтметра
- Результат (КТ-2): з 42 → 18 дБмкВ; $\Delta K = 24$ дБ; $R_k = 4,2$ Ом ✓

ГАЛЬВАНІЧНА РОЗ'ЯЗКА ЗОВНІШНІХ ЛІНІЙ

- Оптрон: ел. → оптичний → ел.; нульовий гальванічний зв'язок між входом і виходом
- Трансформаторний розв'язувач: магнітний зв'язок; природний ЧФ-фільтр для аналогових ліній
- Рівень ослаблення ≥ 60 дБ у робочому діапазоні (вимога ТЗ)
- Застосування: телефонна лінія, охоронна/пожежна сигналізація, ДТЗС
- Результат (КТ-3): з 35 → 8 дБмкВ; якість зв'язку збережено ✓

АКТИВНІ ЗАСОБИ ЗАХИСТУ: БАЗАЛЬТ-5ГЕШ ТА DELTA-7

БАЗАЛЬТ-5ГЕШ — Просторове зашумлення

Діапазон:	0,1 – 1000 МГц
Потужність:	≤ 15 Вт
Живлення:	220 В / 50 Гц
Сертифікат:	Держспецзв'язку
Розміщення:	Центр приміщення КЗ

Засіб	Діапазон, МГц	Потуж., Вт	Вартість
БАЗАЛЬТ-5ГЕШ ✓	0,1–1000	15	Середня
ГШ-1000М	0,01–1000	20	Висока
ГРОМ-3І-4	0,1–2000	12	Висока

Обрано БАЗАЛЬТ-5ГЕШ: оптимальний ціна/характеристики для кат. 1

DELTA-7 — Лінійне зашумлення

Принцип дії:

Генератор шуму → узгоджувальний трансформатор → ввід безпосередньо в лінії живлення та заземлення (на відміну від БАЗАЛЬТ — діє в провіднику, не в просторі)

Точка підключення:

Найближча до виходу захищеного сегмента за межі КЗ — після загального фільтра FP3

Критична вимога ⚠:

Живлення DELTA-7 — від тієї самої мережі та групи, що і захищуване обладнання. Порушення цього → зниження ефективності

Якість шумового сигналу:

Рівномірний розподіл імовірності + плоский спектр = максимальна ентропія; злоумисник не може ідентифікувати і відфільтрувати

Застосування: коли пасивні засоби не забезпечують нормативного СШ за результатами вимірювань у КТ

КОМПЛЕКСНА СХЕМА ЗАХИСТУ АС-1 ТА ПОРЯДОК ПІДКЛЮЧЕННЯ



ШИНА ВИДІЛЕНОГО ЗАХИСНОГО ЗАЗЕМЛЕННЯ (топология «зірка» · ізольована від природних заземлювачів · $R \leq 10 \text{ Ом}$)

БАЗАЛЬТ-5ГЕШ — центр приміщення КЗ
Живлення: після фільтра FP3, від тієї самої групи, що і ПЕОМ

DELTA-7 — точка виходу захищеного сегмента
Вводить шум одночасно в лінії живлення ТА заземлення

Телефонні + сигнальні лінії ДТЗС: оптронні пристрої гальванічної розв'язки ($\geq 60 \text{ дБ}$) на виходах з КЗ

Кабельні траси: металеві короби зі суцільним заземленням | Усі корпуси засобів -> шина виділеного заземлення

Організаційний контроль: пломбування корпусів фільтрів і коробів · журнал сервісних робіт · щомісячний огляд plomb · заборона несертифікованого обладнання

Всі корпуси та короби заземлені на одну шину виділеного заземлення · Генератори живляться від тієї самої мережі, що і ПЕОМ · Пасивні засоби передують активним

РОЗРАХУНКОВА ОЦІНКА ЕФЕКТИВНОСТІ ТА ЗАЛИШКОВИЙ РИЗИК

Методика ТР ПЕМВН-95: $CШ = U_c - U_n$ (дБмкВ) | $КА = CШ_{вим} - CШ_{норм} + \Delta K$ | $\Delta K = 6-10$ дБ | $CШ_{норм} = 30$ дБмкВ (кат. 1)

Контрольна точка	До захисту (дБмкВ)	Після (дБмкВ)	Осл. (дБ)	Засіб захисту	Запас (дБ)	Ризик
КТ-1: Ввід живлення до КЗ	68	8	60	Фільтр FP3 + Розд. трансф.	22	
КТ-2: Вузол шини заземлення	42	18	24	Виділений контур (зірка); R=4,2 Ом	12	
КТ-3: Телефонна лінія	35	8	27	Оптронний пристрій галвн. розв'язки	22	
КТ-4: Мережевий кабель LAN	33	12	21	Металевий екранований короб (сталь 2 мм)	18	
КТ-5: Суміжні кабельні траси	31	15	16	DELTA-7 + металеві коробки з заземл.	15	

В усіх 5 КТ СШ після захисту < 30 дБмкВ (норма); запас ≥ 12 дБ > мін. необхідних 10 дБ → система відповідає ТР ПЕМВН-95

Щомісячно

Огляд пломб і стану кабельних коробів; запис у журнал контролю

Щоквартально

Перевірка мережевих фільтрів; вимірювання R виділеного контуру заземлення

Щорічно

Повні спецдослідження: вимірювання у всіх 5 КТ; складання протоколів

ВИСНОВКИ

1

Нормативна база систематизована

ТР ПЕМВН-95, НД ТЗІ 3.7-003-23, ЗУ «Про захист інформації в ІТС» — основа проектування КСЗІ

2

Природу ЕКВІ розкрито

Три механізми (ємнісний, індуктивний, гальванічний) — кожен потребує власного засобу нейтралізації

3

Моделі загроз і порушника побудовано

6 загроз з матрицею ризиків; 3 категорії порушників; сценарії актуальні для конкретного ОІД

4

Обґрунтовано комплекс засобів

FP3, розд. трансформатор, виділений контур ($R=4,2 \text{ Ом}$), гальванічна розв'язка, БАЗАЛЬТ-5ГЕШ, DELTA-7

5

Ефективність підтверджено розрахунком

СШ у всіх 5 КТ $< 30 \text{ дБмкВ}$; запас $12-22 \text{ дБ} > \text{мін. } 10 \text{ дБ}$ — відповідає ТР ПЕМВН-95

6

Практичне значення

Комплекс готовий до впровадження; адаптується до будь-якого ОІД; запропоновано план регламентного контролю

Дякую за увагу. Готовий відповісти на запитання.