КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
ФАКУЛЬТЕТ РАДІОФІЗИКИ, ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ
Кафедра радіотехніки та радіоелектронних систем

«На правах рукопису»

Робота допущена до захисту в ЕК
рішенням кафедри радіотехніки та радіоелектронних систем
від __ червня 2024 року, протокол №___.
Завідувач кафедри доктор фіз.-мат. наук, професор
Ігор АНІСІМОВ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА
на тему:

«Захист інформації від витоку технічними каналами та спеціального впливу командно-штабної машини К-1450-05»

Виконав:
студент 4-го курсу
денної форми навчання
спеціальності 172 - Телекомунікації та радіотехніка
ОНП «Інформаційна безпека телекомунікаційних систем і мереж»
Картель Ігор Юрійович

Науковий керівник:
кандидат військових наук, доцент
Довбня Сергій Якович
Рецензенти:
Доктор технічних наук, професор
Іванченко Сергій Олександрович
Заступник головного конструктора ТОВ «ТЕЛЕКАРТ-ПРИЛАД»
Баранов Сергій Володимирович

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів без
відповідних посилань
Студент **Ігор Картель**

Київ 2024

РЕФЕРАТ

Кваліфікаційна робота: 37с., 6 табл., 7 рис., 22 джерела.

Захист інформації від витоку технічними каналами та спеціального впливу командно-штабної машини К-1450-05

Мета роботи: аналіз потенційних вразливостей командно-штабної машини К-1450-05 та розробка рекомендацій, що покликані підвищити інформаційну безпеку та запобігти витоку інформації технічними каналами.

Кваліфікаційна робота спрямована на ідентифікацію та нейтралізацію потенційних технічних каналів витоків інформації та зниження ризиків від спеціального впливу.

У рамках дослідження було проведено аналіз існуючих захисних механізмів машини, оцінено потенційні загрози і вразливості обладнання, а також розроблено додаткові технічні та програмні заходи для підвищення рівня безпеки. Дослідження охоплювало фізичні, технічні та оперативні аспекти безпеки, інтеграцію сучасних технологій захисту даних та систем моніторингу.

Основні досягнення:

- Розробка рекомедацій захисту: Створена система включає рішення для блокування технічних каналів витоку інформації (далі – ТКВІ), захисту від спеціального впливу (далі СВ, для електромагнітних сигналів – ЕМІ) та радіочастотних перешкод.
- Виявлення та усунення вразливостей: Ідентифіковано критичні слабкі місця в системах комунікації та обробки даних, а також розроблено методи їх нейтралізації.

Зміст

ВСТУП

У сучасному світі, де інформація стає все більш цінним ресурсом, її захист від небажаного доступу та розповсюдження набуває особливої актуальності. Це особливо важливо в контексті військових та оборонних технологій, де витік інформації може призвести до непоправних наслідків. Командно-штабна машина К-1450-05, яка є важливим компонентом управління і контролю на тактичному рівні, вимагає особливої уваги щодо забезпечення інформаційної безпеки.

Враховуючи, що технічні канали витоку інформації та спеціальний вплив можуть бути різноманітними і непередбачуваними, розробка комплексних методів захисту є не тільки актуальною, але й критично необхідною задачею. Такі методи повинні включати не тільки фізичні заходи захисту, але й програмні технології, а також процедури реагування на інциденти, що включають розробку сценаріїв потенційних атак та витоків інформації.

Ця робота має на меті проаналізувати існуючі та потенційні канали витоку інформації, а також розробити методологію захисту інформації в командно-штабній машині К-1450-05.

Будуть розглянуті технічні, організаційні та правові аспекти захисту інформації, з метою створення комплексної системи, що забезпечує максимальний захист від витоків та несанкціонованого доступу.

Проблематика інформаційної безпеки в межах військових командно-штабних машин є виключно важливою в контексті сучасних військових конфліктів і зміцнення обороноздатності держави. У зв'язку з цим, дана робота має практичне спрямування на безпеку функціонування командно-штабної машини К-1450-05.

Розділ 1. Оцінка ризиків витоку інформації технічними каналами та спеціального впливу для К-1450-05

1.1 Аналіз конструкції та основних елементів КШМ

Проведений аналіз конструкції та основних елементів КШМ К-1450 на підставі документів [1-3] дає можливість зробити висновки, які наведено в таблиці 1.

Таблиця 1

Зовнішні вводи	Зовнішні лінії	Можливість витоку інформації за рахунок ПЕМВН	Захист від спеціального впливу
Кабельний ввід для ліній відкритого зв'язку	- двопроводова телефонна лінія за допомогою польового кабелю П-274М через затискачі військового виконання; - чотирьох двопроводових телефонних ліній на захищений роз'єм RJ-45 за допомогою кабелю типу S(F)TP Cat 5 через виносний щиток типу ВЩ-45/2 з роз'ємом RJ-45; – двох каналів Ethernet 10/100 Мбіт/с через захищені роз'єми RJ-45 станції широкосмугового доступу Р-402 через захищений роз'єм типу RJ-45 до PoE-адаптеру; – однієї двопроводової (чотирипроводової) ліній зв'язку з забезпеченням пакетної передачі інформації Ethernet із застосуванням технології за стандартом ITU-T G.921.2 SHDSL через затискачі військового виконання; – фідера станцій стандарту DMR «Либідь К-2РБ» (Motorola DM 4600); – фідера ретранслятора «Либідь К-2РТД» (SlR 5500);	Не потребує захисту від витоку каналами ПЕМВН	Комутаційні панелі ліній відкритого зв'язку повинні забезпечувати захист телекомунікаційного обладнання від перенапруги зовнішніх телефонних, Ethernet та фідерних ліній. Усі високочастотні кабелі повинні підключатись через грозозахист.

	– фідерів радіостанцій виробництва корпорацій Harris (Aselsan); – двох двопроводових ліній зв'язку з використанням кабелю П-274М для підключення виносних телефонних апаратів типу ТА-01.01 до АВЗК; – однієї двопроводової лінії зв'язку з використанням кабелю П-274М для підключення виносного дистанційного модуля управління до аналогічного модуля з комплекту пристрою дистанційного управління Harris RF-7800R-RC110, що змонтований у КШМ.		
Кабельний ввід ліній захищеного зв’язку	– одного каналу Ethernet 10/100 Мбіт/с через захищений роз’єм типу RJ-45; - однієї двопроводової телефонної лінії за допомогою польового кабелю П-274М через затискачі військового виконання; - чотирьох двопроводових телефонних ліній на захищений роз'єм RJ-45 за допомогою кабелю типу S(F)TP Cat 5 через виносний щиток типу ВЩ-45/2 з роз'ємом RJ-45;	Потребує захисту від ПЕМ наведень на з’єднувальні лінії	Комутаційні панелі ліній захищеного зв'язку повинні забезпечувати захист телекомунікаційного обладнання від перенапруги зовнішніх телефонних, Ethernet ліній.
Кабельний ввід електроживлення	– кабелю електроживлення 220 В; – кабелю електроживлення 220 В для транзитного підключення; кабелів заземлення.	Потребує захист від ПЕМ наведень на лінії електроживлення та заземлення	Потребує захисту від спеціального впливу по лініях електроживлення

Детальна інформація щодо конструкційних особливостей КШМ наведена у Додатку А.

Оцінка захисту інформації в КШМ показала, що використання дозволених електронних засобів, будова системи з використанням проводових ліній, без застосування методів та засобів технічного захисту інформації від витоку

технічними каналами та спеціального впливу не забезпечує захист інформації, що для спеціальних умов експлуатації КШМ не відповідає вимогам.

1.2 Інженерний аналіз основних та допоміжних систем та засобів КШМ

Проведений на підставі [2-4] інженерний аналіз структурної схеми КШМ К-1450-05 (рисунок 1 Додатку А) дав змогу визначити основні характеристики технічних каналів витоку інформації (далі – ТКВІ) та спеціального впливу (далі – СВ).

Перелік та характеристики основних ТКВІ та СВ наведено в таблиці 2.

Таблиця 2

ТА Славутич- П-274, КВ2-ТЛФ, КП Тлф, -VoIP шлюз						
Частота (КГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційного сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціального впливу Рсп	Необхідність в блокуванні технічного каналу
0,1-15	12-24 В	500	Аналоговий сигнал 5-7 хв.	1	1	+
VoIP шлюз – Кабель_ ПК ПД, Ethernet 100/1000 Mbit(RJ45). В-271Р						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційного сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціального впливу Рсп	Необхідність в блокуванні технічного каналу
17,5-500/1000	2.8 3.3 В	500-1000	5-7 хв.	1	1	+
Захищена ПЕОМ кабель Ethernet 100,1000 Mbit(RJ45), КВ 2, ПК ПД, В-271Р						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційного сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціального впливу Рсп	Необхідність в блокуванні технічного каналу
17.5-500/1000	2.8 - 3.3 В	500-1000	0,5 – 2 с	1	1	+
ПЕОМ – 120 GB SSD інтерфейс SAS						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційного сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціального впливу Рсп	Необхідність в блокуванні технічного каналу
1500	-0.5 0.5 В	3000	300 мкс	1	1	+
ПЕОМ DVI 1080x1094 60 Гц						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційного сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціального впливу Рсп	Необхідність в блокуванні технічного каналу
1500	0 0.7 В	3000	Від 0.1 с до 2 хвл.	1	1	+
ПЕОМ – Принтер						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі	Ймовріність витоку інформації	Ймовірність спеціального впливу	Необхідність в блокуванні

			інформаційного сигналу	Ртк	Рсп	технічного каналу
20 -1000	-0.5 0.5 В	120	300 мкс	1	1	+

Таким чином в КШМ наявно 6 основних технічних каналів витоку інформації за рахунок побічних електромагнітних випромінювань та наведень та більш 20 (антенні вводи, кабелі електроживлення, КВ1 – кабелі телефонних ліній та Ethernet 100/1000 Mbit (RJ45) по яких також може бути здійснено електромагнітне нав’язування хибної інформації, або блокування передачі інформації.

Загальна характеристика небезпечного електромагнітного поля та сигналів КШМ:

- смуга випромінювання небезпечних сигналів - 20 – 3000 МГц;
- можливість створення електромагнітних наводив в лініях електроживлення та заземлення – токи до 500 МГц та напруга до 1200 МГц;
- при використанні кручених пар крім електричної складової (20 – 517 МГц) буде магнітна складова електромагнітного поля – до 30 МГц.

Висновок – КШМ без застосування методів та засобів технічного захисту інформації є незахищеним від витоку технічними каналами та спеціального впливу.

Найбільш небезпечним для КШМ є вплив ЕМІ на такі пристрої, як ПЕОМ, засіб КЗІ, шлюзи, маршрутизатори, проводові, радіо, радіорелейні, супутникові пристрої, від яких залежить стійке функціонування КШМ у цілому. Виведення їх з ладу може призвести до блокування (відключення) спеціалізованих мереж зв’язку від КШМ, істотній затримці передачі пакетів інформації.

Командно-штабна машина не відповідає усім критеріям для запобігання неконтрольованому доступу до інформації через технічні та спеціалізовані канали.

Детальний опис наведено у Додатку Б.

Висновок.

Потрібно розробити комплекс організаційно-технічних заходів щодо забезпечення захисту КШМ та максимізації блокування всіх технічних каналів витоку інформації та спеціального впливу, шляхом створення комплексу технічного захисту інформації КШМ отриманні Акту атестації та введенні в експлуатацію.

Розділ 2. Розробка рекомендацій щодо захисту КШМ від витоку інформації

2.1 Рекомендації щодо блокування ТКВІ та каналів СВ

На підставі наведеного аналізу структури та конструкції КШМ К-1450-05 запропоновано наступні рекомендації:

1. Панелі комутації ліній для відкритого та захищеного зв'язку мають забезпечувати захист телекомунікаційних систем від перепадів напруги, що виникають у зовнішніх телефонних, Ethernet та фідерних лініях.
2. Всі високочастотні кабелі, що підключені до кабельних вводів, мають бути оснащені пристроями захисту від блискавок.
3. Зовнішні частини всіх кабельних вводів повинні мати заземлюючий контакт (гвинт).
4. Кабельні вводи мають бути оснащені спеціальними кріпленнями для надійного утримання силових, абонентських та радіочастотних кабелів.

5. До всіх кабельних вводів повинні входити сучасні засоби фільтрації імпульсних завад та захисту від ЕМІ та високої напруги:

- ввід для відкритого зв'язку;
- ввід для захищеного зв'язку;
- ввід для електроживлення і заземлення.

В разі неможливості розгортання КШМ подалі від потенційних джерел високих завад, таких як високовольтні лінії, потужні радіостанції, зварювальне обладнання тощо, на відстань від 500 до 1000 метрів, до складу маскувальних засобів повинні входити радіонепрозорі матеріали (радіотехнічна ткань тощо) для додаткового екранування кунгу.

6. КШМ має забезпечувати рівень електромагнітного екранування не менше 30 дБ для частот від 150 до 1000 кГц і не менше 60 дБ для частот

від 1 МГц до 1 ГГц. Це вимагає використання екранованих конструкцій для КУНГу і всіх засобів за стандартами 3-ої категорії захисту інформації. Для одного відсіку можна використовувати шафу з аналогічним рівнем екранування, що може змінити формулювання цієї вимоги.

КШМ також має забезпечувати екранування на рівні не гірше 20 дБ для частот від 150 до 1000 кГц і не гірше 30 дБ для частот від 1 МГц до 1 ГГц, але лише для перших двох відсіків.

7. Спеціальні вимоги до захищеного автоматизованого робочого місця на базі ПЕОМ (ЗАРМ) включають обробку інформації з обмеженим доступом (ІзОД) з рівнем захисту “3”. Процеси, що включають обробку ІзОД, охоплюють введення через клавіатуру, виведення на монітор, запис та читання з жорсткого диска, обмін через локальні мережі та використання оптичних носіїв.

ЗАРМ має бути підключений до системи заземлення КШМ через заземлюючий контакт вилки електроживлення і повинен підключатися до засобу КЗІ виключно через оптичний кабель.

ПЕОМ та мережеве обладнання, що підключаються до локальних мереж КЗІ, не повинні містити бездротові інтерфейси або веб-камери і повинні бути перевірені на відсутність прихованих пристроїв. Вони також повинні мати документацію на проведення спеціальних досліджень або відповідний висновок від Державної служби спеціального зв’язку та захисту інформації України.

ПЕОМ повинні оснащуватися оптичним LAN Ethernet портом.

Отже, в КШМ існує шість основних технічних шляхів витоку інформації через побічні електромагнітні випромінювання і наведення, а також понад 20 потенційних джерел (антенні входи, кабелі електроживлення, КВ1 – телефонні лінії та Ethernet 100/1000 Mbit(RJ45)), через які можливе нав’язування хибної інформації або блокування передачі даних.

Характеристики небезпечного електромагнітного поля та сигналів КШМ включають:

Спектр випромінювання небезпечних сигналів від 20 до 3000 МГц;

Можливість виникнення електромагнітних наведень на лініях електроживлення та заземлення з токами до 500 МГц та напругою до 1200 МГц;

Наявність електричної (20 – 517 МГц) та магнітної (до 30 МГц) складових у кручених парах.

Висновок полягає у тому, що КШМ без використання методів і засобів технічного захисту інформації залишається вразливою до технічних витоків та спеціальних впливів.

Аналіз захисту інформації в КШМ показав, що просте використання дозволених електронних засобів та будівництво системи з проводовими лініями без застосування спеціалізованих методів та засобів технічного захисту інформації не забезпечує адекватний захист від витоків через технічні канали та зовнішні впливи, що є неприйнятним для спеціальних умов експлуатації КШМ.

Необхідно розробити комплекс організаційно-технічних заходів для забезпечення захисту КШМ, що включає створення системи технічного захисту інформації, отримання акту атестації та подальше введення в експлуатацію для ефективного блокування всіх технічних шляхів витоку інформації та зовнішніх впливів.

2.2 Список додаткового обладнання, необхідного для забезпечення захисту інформації від витоку технічними каналами та спеціального впливу

Для забезпечення захисту інформації від витоку ТКВІ та СВ до складу командно-штабної машини К-1450-05 необхідно ввести наступні компоненти:

- Генератор акустичного шуму стаціонарний «РІАС–2ГС» (модифікація 2);
- Система активного захисту інформації від витоку каналами ПЕМВН DELTA-7;
- Випромінювач акустичний РІАС–2ВА (4 шт.);
- Вібровипромінювач п’єзоелектричний РІАС–2ВП (4шт.);
- Розділовий трансформатор з екранованою обмоткою РІАС–4ТР/2.

Крім того перевірити всі кабельні вводи та вводи антен на захист від спеціального впливу (при необхідності засоби «грозо захисту» замінити на сучасні.)

Детальний опис засобів технічного захисту інформації наведено у додатку В.

Введення до складу засобів ТЗІ дозволить забезпечити блокування технічних каналів витоку інформації (акустичних та віброакустичних, акустоелектричних та за рахунок побічних електромагнитних випромінювань та наведень) також спеціального впливу по лініях електроживлення.

Для блокування каналів спеціального впливу (електромагнитні поля та сигнали) потрібно провести модернізацію кунгу КШМ (радіоелектронний захист - екранування), кабельних та антенних вводів (захист від наведення ЕМІ)

Також потрібно створити комплекс технічного захисту інформації КШМ (від витоку ТКВІ та спеціального впливу), провести його атестацію на відповідність нормативно-правовим актам та вимогам з технічного захисту інформації з обмеженим доступом.

Висновок

Робота була присвячена аналізу потенційних вразливостей командно-штабної машини К-1450-05 та розробці рекомендацій, що покликані підвищити інформаційну безпеку та запобігти витоку інформації технічними каналами.

У роботі був проведений аналіз конструкції командно-штабної машини (комплектація К-1450-05) та її окремих елементів з метою отримання даних про потенційні вразливості. Були розроблені спеціальні рекомендації для покращення конструкції окремих елементів машини та її комплектації засобами технічного захисту інформації з метою запобігання витоку інформації технічними каналами та спеціального впливу на неї.

У ході аналізу захисту інформації в КШМ було виявлено, що нинішня комплектація засобами електронних комунікацій, ПЕОМ, яка базується на використанні закордонних електронних засобів (базового рівня захисту) та проводових ліній без застосування спеціалізованих методів технічного захисту, не забезпечує адекватний захист від витоку інформації технічними каналами та спеціального впливу.

Розроблені рекомендації та вжиті заходи можуть забезпечити захист командно-штабної машини К-1450-05 від можливих технічних витоків та спеціальних впливів. Проте, у зв’язку зі зростанням технологічних можливостей та зміною характеру загроз, необхідно постійно оновлювати і адаптувати заходи безпеки, щоб вони відповідали сучасним вимогам і технологіям.

Таким чином, дана кваліфікаційна робота вносить значний внесок у підвищення безпеки командно-штабних машин та може бути використана як основа для подальших досліджень і розробок у цій галузі.

Список використаних джерел

1. Закон України «Про інформацію».
2. Закон України «Про захист інформації в інформаційно-комунікаційних системах».
3. Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.99 № 1229.
4. Постанова Кабінету Міністрів України від 29 березня 2006 року №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах».
5. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
6. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
7. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
8. НД ТЗІ 1.6-005-2013.Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. Затверджено наказом ДСТСЗІ СБ України від 15.04.2013 року № 215.
9. МАШИНА КОМАНДНО-ШТАБНА К-1450-05. Технічні умови ТУ У 30.4–24982189-233:2020 ААНЗ.461262.002-05 ТУ. ТОВ «Телекарт-Прилад», м. Одеса – 135 с.
10. Технічний захист інформації від несанкціонованого доступу машини командно-штабної К-1450-05 ААНЗ.461262.002-05. Технічні вимоги. Дослідний зразок. ФОП «Довбня С.Я.», м. Київ – 45 с.
11. ТР ЕОТ-95. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, АС і мережах від витоку каналами побічних електромагнітних випромінювань та наведень.
12. Безпека електрозв’язку та інформаційних технологій. Огляд, зміст та застосування діючих Рекомендацій МСЕ-Т для забезпечення захищеного електрозв'язку. МСЕ-Т – Бюро стандартизації електрозв'язку (БСЕ). Place des Nations – CH-1211 Geneva 20-Switzerland, 2009. – 162 с. Веб сайт: www.itu.int/ITU-T, ел. Пошта: tsbmail@itu.int.
13. Г.Ф. Конахович та інші. Захист інформації в телекомунікаційних системах: Навчальний посібник. – К.: НАУ, 2009.-380 с.
14. Основи інформаційної безпеки. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 268 с.

15. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем.-К.: Видавнича група BHV, 2009 – 608с.:іл.
16. Педагогічний програмний засіб (ППЗ) «Телекомунікаційні системи та мережі. Структура й основні функції. Том 1». Автори: Поповський В.В, Лемешко О.В.; Ковальчук В.К.; Плотніков М.Д.; Картушин Ю.П.; Попонін О.М.; Агєєв Д.В.; Сабурова С.О., Олійник В.Ф., Персиков А.В.; Лошаков В.А. Селіванов К.О. Друге видання. Виправлено та доповнено. 2018.
17. Голев Д.В. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. / Голев Д.В., Кононович В.Г., Хомич С.В.; за ред. чл.-кор. МАЗ В.Г. Кононовича. - Одеса: ОНАЗ ім. О.С. Попова, 2013. - 218 с.
18. С.Я. Довбня. Методи (моделі) розробки комплексів технічного захисту інформації на об’єктах інформаційної діяльності та радіоелектронної техніки: Навчальний посібник. – К.: ДП «Український центр «Безпека», 2019. – 95 с.
19. С.Я. Довбня, П.П. Наталенко. Основи використання, адміністрування та забезпечення захисту інформації в автоматизованих системах: Навчальний посібник. – К.: ТОВ «Софтлайн ІТ», 2017. – 164 с.
20. Акт обстеження ОІД/ фізичного середовища ІТС дослідного зразка машини командно-штабної К-1450-05, ТОВ «ТЕЛЕКАРТ-ПРИЛАД», м. Одеса, ФОП «Довбня С.Я.», м. Київ – 20 с.
21. Герасимов Б.М., Домарев В.В. Вибір оптимального варіанту системи захисту інформації на основі застосування методів нечіткої багатокритеріальної оптимізації// Захист інформації. №3.
22. Василевич Л.Ф., Проскурин В.М. Вибір способів та пристроїв захисту інформації на основі теорії ігор// Праці КВІУЗ. Випуск 2. 1998. С.95-100.

Додаток А

Основні технічні елементи КШМ К-1450-05 та їх характеристики

Командно-штабна машина К-1450-05 побудована на базі шасі Renault D15 High P4x4 300E3 і має жорстку каркасну конструкцію з металевими трубами, обшиту сталлю. Вона розрахована на транспортування спеціального радіообладнання і особового складу, здатна працювати в екстремальних умовах завдяки герметичності кузова, що захищає від біологічних і хімічних загроз. Внутрішній простір поділений на три основні відділення: технологічне, відділення зв'язку та управління, кожне з яких має спеціалізоване обладнання для виконання своїх функцій.

У відділенні управління командно-штабної машини К-1450-05 знаходиться автоматизоване робоче місце, оснащене персональним електронно-обчислювальним комплексом (ПЕОМ) типу Notebook. Тут зосереджені важливі засоби для управління, планування та комунікації, які є критично важливими для функціонування машини в оперативних умовах.

Таблиця А.1 - Загальні технічні характеристики ПЕОМ Dell Latitude 7424 Rugged

Назва	Характеристика
Екран	Діагональ 14", роздільна здатність: 1920x1080
Процесор	8th Gen Intel Core i5-8350U Processor (Quad Core, 6M Cache, 1.7GHz,15W, vPro)
Операційна система	Windows 10 Pro (64Bit) Ukranian
Оперативна пам’ять	8GB, 1x8GB, DDR4 Non-ECC
Жорсткий диск	M.2 128GB PCIe NVMe Class 35 Solid State Drive
Відеокарта	Intel Core i5-8350U Processor Base with Integrated Intel UHD 620 Graphics
Інтерфейси	Ethernet 10/100/1000 Мбіт/с RJ-45 x 1 RS-232 x 1 HDMI x 1 USB 2.0 x 3 аудіороз’єм 3,5 мм для підключення навушників та мікрофону
Живлення	літій-іонний акумулятор, адаптер живлення від мережі 110 – 240 В, 50/60 Гц

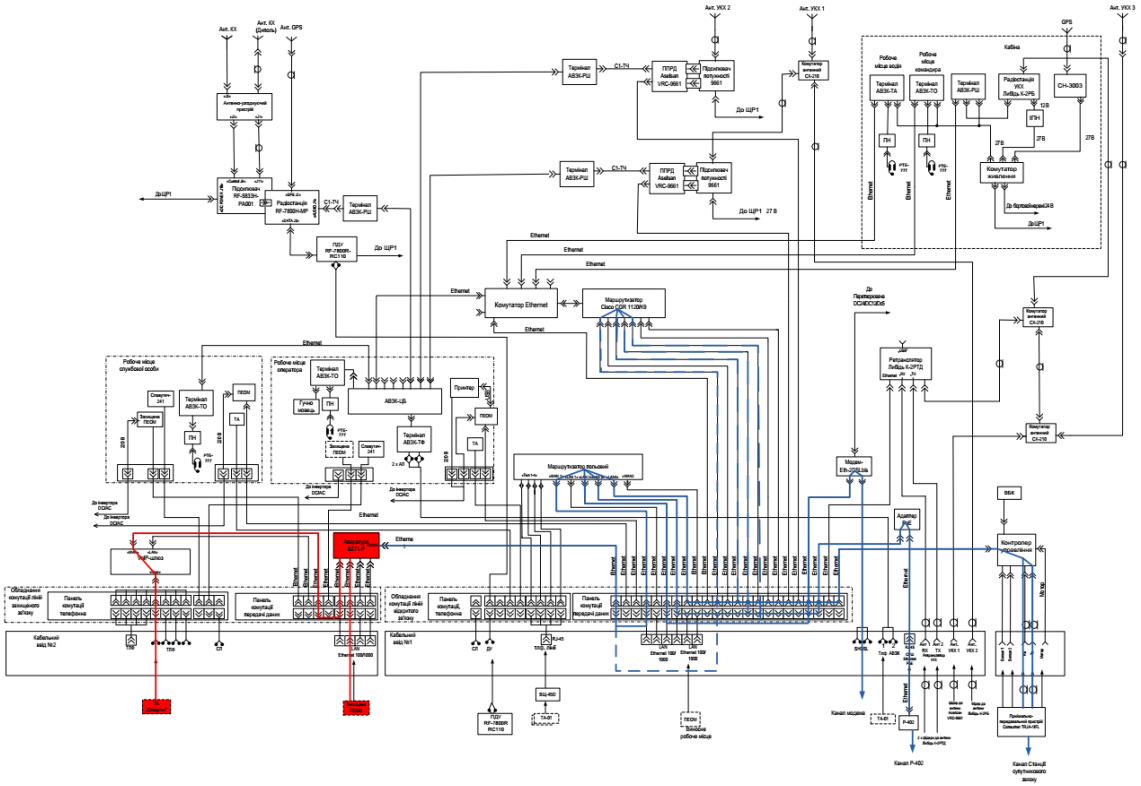

Рисунок А.1 Структурна схема командно-штабної машини К-1450-05

Основні елементи системи:

- Мережеві інтерфейси: В схемі зазвичай використовуються різні мережеві інтерфейси для забезпечення з'єднань між компонентами. Це можуть бути Ethernet-порти, VoIP шлюзи, та інші мережеві пристрої, які забезпечують комунікацію внутрішніх та зовнішніх мереж.
- Пристрої криптографічного захисту: Ключовим елементом є пристрої для криптографічного захисту інформації, які забезпечують шифрування даних перед їх передачею через мережу, забезпечуючи безпеку конфіденційної інформації.
- Комутатори та маршрутизатори: Комутатори та маршрутизатори використовуються для керування потоками даних в мережі, забезпечуючи маршрутизацію та розподіл трафіку згідно з встановленими правилами та політиками.
- Антивірусне програмне забезпечення: Забезпечує захист від зовнішніх загроз та вірусів, що можуть спробувати проникнути в систему через мережеві з'єднання.

Принцип роботи:

- Потік даних: Інформація перетікає через різні елементи мережі, починаючи від введення (через інтерфейси користувача) до виходу (наприклад, до інших вузлів мережі або до зовнішніх систем).
- Захист інформації: На кожному етапі передачі даних використовуються механізми захисту, включаючи шифрування та аутентифікацію, щоб забезпечити конфіденційність та цілісність переданих даних.
- Детекція та реагування на інциденти: Системи моніторингу та антивірусне програмне забезпечення постійно аналізують мережевий трафік на предмет виявлення потенційних загроз та вживають відповідних заходів для їх нейтралізації.

Захист командно-штабної машини К-1450-05 здійснюється через інтеграцію комплексу обладнання для контролю і захисту інформації. Це включає:

Засоби ліній обміну матеріалами (ЛОМ): до складу яких входить польовий маршрутизатор К-1211 (ААНЗ.468371.027 ТУ), VoIP-шлюз (ААНЗ.465265.013ТУ), та автоматизовані робочі місця (АВЗК, ААНЗ.465211.012ТУ).

Системи управління: Спеціалізовані автоматизовані робочі місця, що функціонують на базі ОС Windows 10 або іншої оперативної системи, яка відповідає вимогам технічного захисту інформації згідно з експертними висновками.

Для захисту зовнішніх ліній зв'язку, які виходять за межі контрольованої зони, використовуються сертифіковані засоби криптографічного захисту інформації (КЗІ), які також мають необхідні експертні висновки. Ці засоби повинні бути схвалені для використання відповідно до установлених процедур.

Додаток Б

Аналіз основних небезпечних сигналів

Засоби електронно-обчислювальної техніки (елементи КШМ) потенційно вразливі до впливу ЕМІ, оскільки побудовані на МОП-приладах високої щільності, що дуже чуттєві до впливу високовольтних перехідних процесів. Для МОП-приладів є характерним те, що потрібно дуже небагато енергії для того, щоб зашкодити або знищити їх. Будь-яка напруга на рівні десяти вольт може викликати ефект, який знищує пристрій. Навіть, якщо імпульс не має енергії, достатньої для термічного ураження, джерело струму пристрою самостійно додасть енергії, щоб завершити процес знищення. Пошкодженні пристрої можуть ще функціонувати, проте їх надійність буде значно нижчою. В табл. 7.2, 7.3 наведено дані, що відображають характеристики ефектів та пошкоджень, що виникають у засобах ЕОТ за умов впливу ЕМІ.

Характер пошкоджень засобів ЕОТ під час впливу ЕМІ

Таблиця Б.1

Клас виробу	Характер пошкоджень
Інтегральні мікросхеми	Деградація параметрів діодів та транзисторів у складі ІМС, пробої, плавлення та вигорання металізації, руйнування контактних доріжок, обрив з'єднувальних проводів, руйнування резисторів
Напівпровідникові елементи: чутливі елементи ЕОМ; малопотужні транзистори; малопотужні перемикаючі діоди	Різні види пробою та структурних пошкоджень р–п-переходів
Конденсатори	Пошкодження діелектриків, повітряних та вакуумних проміжків
Композиційні та проводові резистори	Іскріння (внутрішнє пошкодження), тепловий перегрів, розрив між виводами високоомних резисторів

Методи силового деструктивного впливу

Силовий деструктивний вплив (СДВ) - це різкий виплеск напруги у мережах живлення, комунікацій або сигналізації комп'ютерних систем (КС) з

амплітудою, тривалістю та енергією, що здатні спричинити пошкодження - від збоїв у роботі обладнання КС до повного її знищення.

Технічні засоби силового деструктивного впливу (ТЗ СДВ) є різновидом технічних засобів електромагнітного впливу.

За умов забезпечення відповідної потужності електромагнітного імпульсу ТЗ СДВ здатні дистанційно уразити практично будь-яку комп'ютерну систему. Враховуючи те, що причина пошкодження обладнання може бути як навмисна (напад), так і ненавмисна (наприклад індукція від блискавки), то аналіз знищеного обладнання не дозволяє однозначно ідентифікувати причину її виникнення.

Електронні засоби можуть зазнавати силового деструктивного впливу по трьох основних каналах (КСДВ), рис. Б.1:

- по мережах електроживлення (КСДВ-1);
- по провідних лініях (КСДВ-2);
- по ефіру з використанням потужних коротких електромагнітних імпульсів (КСДВ-3).

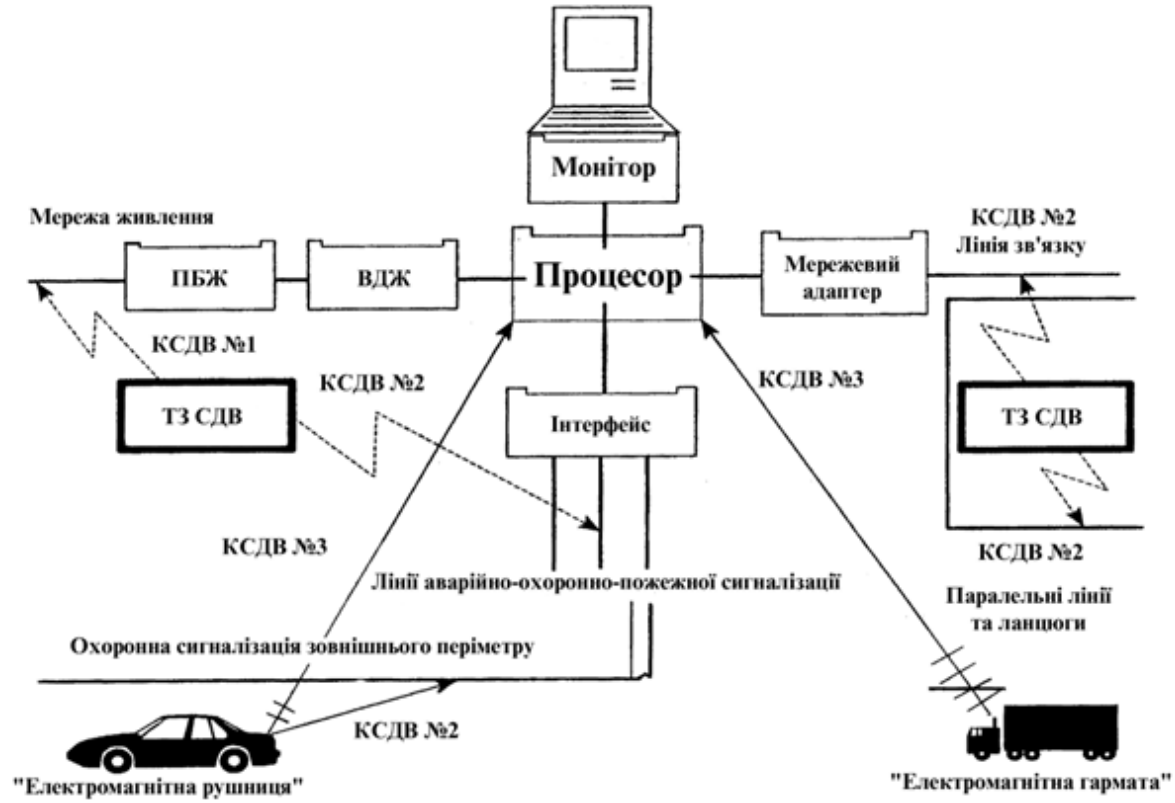

Рисунок Б.1. Основні канали силового деструктивного впливу

СДВ по мережах електроживлення

Проникнення енергії СДВ мережею електроживлення можливе по двох основних каналах:

- кондуктивний шлях через вторинні джерела живлення (ВДЖ);
- наводки через паразитні ємнісні та індуктивні зв’язки, як внутрішні, так і зовнішні (наприклад через сигнальні ланцюги й лінії зв’язку).

Для прикладу наведено стійкість компонентів основного елемента живлення КС вторинного джерела живлення. Типова принципова схема його наведено на рис. Б.2.

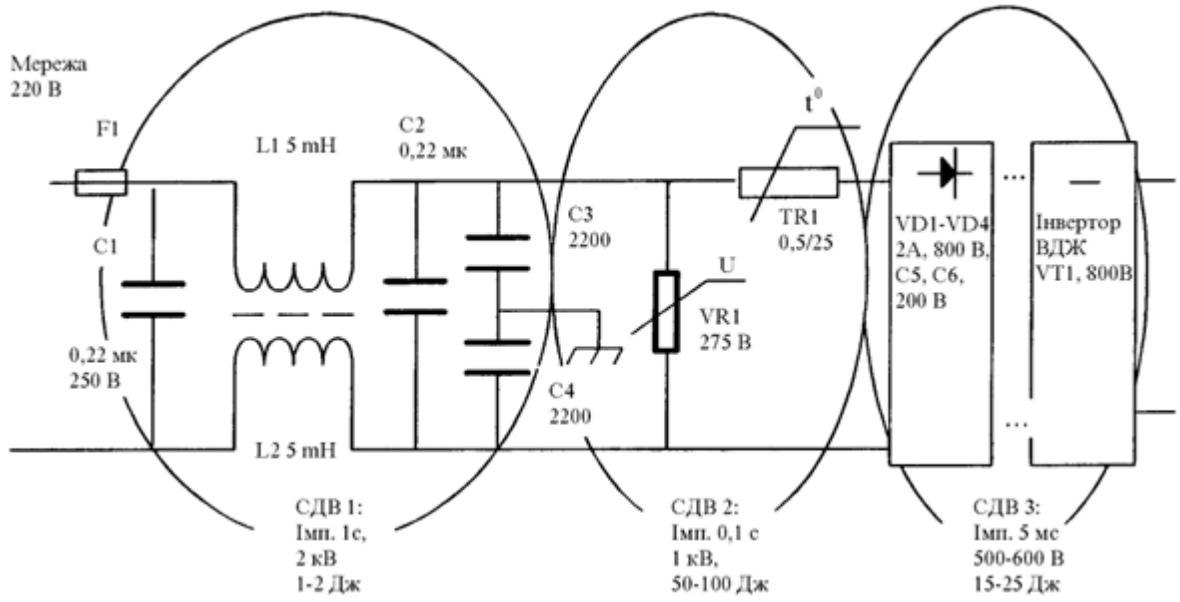

Рисунок Б.2. Принципова схема типового блоку вторинного джерела живлення

Передача даних у мережевому обладнанні відбувається через багатомодове оптичне волокно, використовуючи інтерфейс 100BaseFX, який є частиною специфікації Fast Ethernet. Цей інтерфейс дозволяє здійснювати передачу та прийом інформації по окремих волокнах, забезпечуючи високу швидкість та надійність з'єднання.

100BaseFX використовує багатомодове оптоволокно для створення високошвидкісних мережевих з'єднань зі швидкістю до 100 мегабіт на секунду. Особливість цього інтерфейсу полягає у використанні двох окремих оптичних волокон для передачі та прийому даних, що дозволяє максимізувати ефективність передачі інформації і знижує ризик перешкод.

100BaseFX широко використовується для підключення серверів, хабів, комутаторів та іншого мережевого обладнання у великих мережах. Його здатність передавати дані на великі відстані без втрат робить його ідеальним рішенням для кампусних мереж або мереж між будівлями, де потрібна висока пропускна спроможність та надійність з'єднання. На відміну від мідних рішень, 100BaseFX використовує багатомодове оптоволокно, що дозволяє уникнути електромагнітних перешкод та забезпечити більшу відстань передачі. Це робить його підходящим для використання в середовищах з високим рівнем шуму або там, де необхідні великі відстані між обладнанням. 00BaseFX може працювати в полудуплексному режимі, де дані передаються і приймаються по одному волокну, а також у повнодуплексному режимі, де використовуються два волокна для одночасної передачі та прийому даних.

Знизу на рис. Б3 представлена схема, згідно якої відбувається процес передачі інформації у даному інтерфейсі

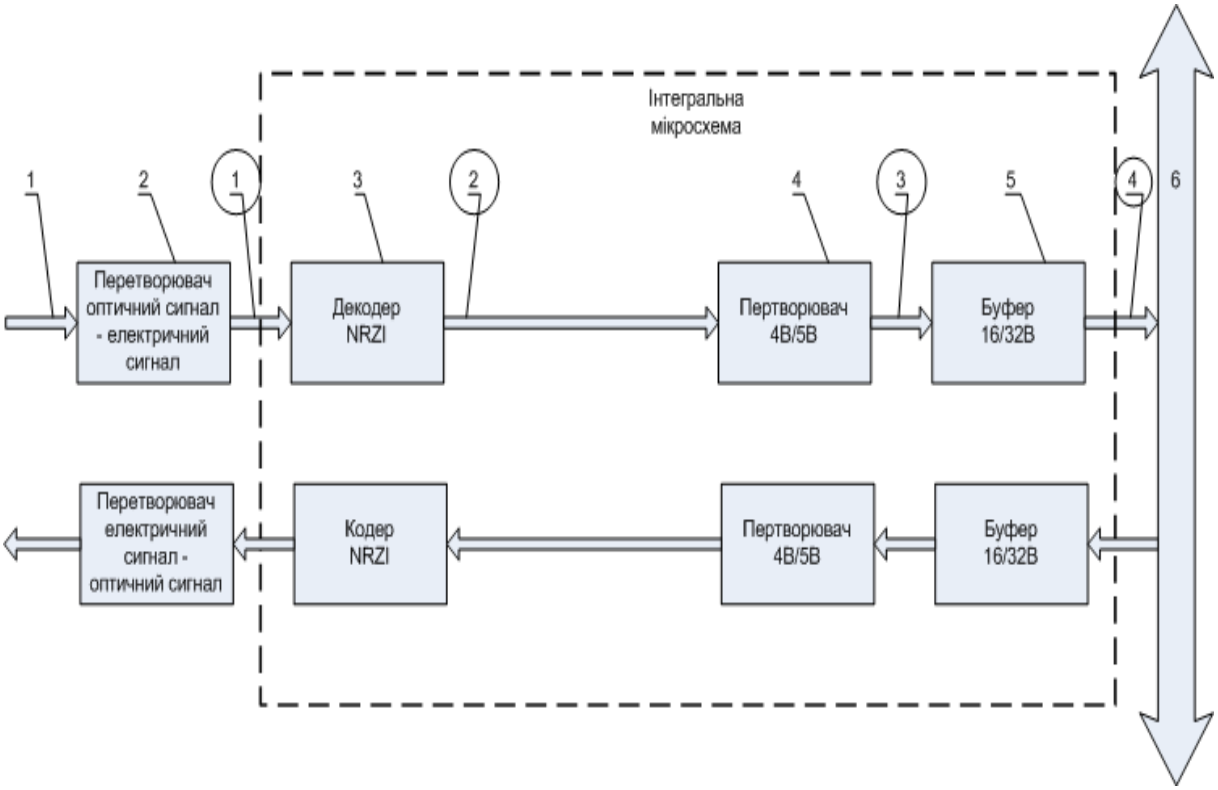

Рисунок Б.3 Структурна схема побудови вихідного каскаду інтегральних мікросхем інтерфейсу специфікації 100BaseFX

1 - вхід перетворювача оптичного випромінювання в електричний сигнал та електричного сигналу в оптичне випромінювання, до якого безпосередньо здійснюється підключення оптичного кабелю;

2 - перетворювач оптичного випромінювання в електричний сигнал та електричного сигналу в оптичне випромінювання;

3 - кодер/декодер канального коду NRZI

4 - перетворювач 4 інформаційних біт у 5 біт канального сигналу

5 - буфер-накопичувач – 4 послідовних біти на вході у 16(або 32) біти паралельного коду на виході

6 - внутрішня шина передачі даних між інтерфейсної мікросхемою та процесором (процесор на рисунку не зображено).

7 Потенційний код NRZI (без повернення до нуля із інверсією одиниці – *Non-Return to Zero, Invert to one*) передбачає , що рівень сигналу змінюється на протилежний на початку одиночного бітового інтервалу та не змінюється при передаванні нульового бітового інтервалу.

Принцип перетворення сигналу кодером NRZI описується на рис. Б.4

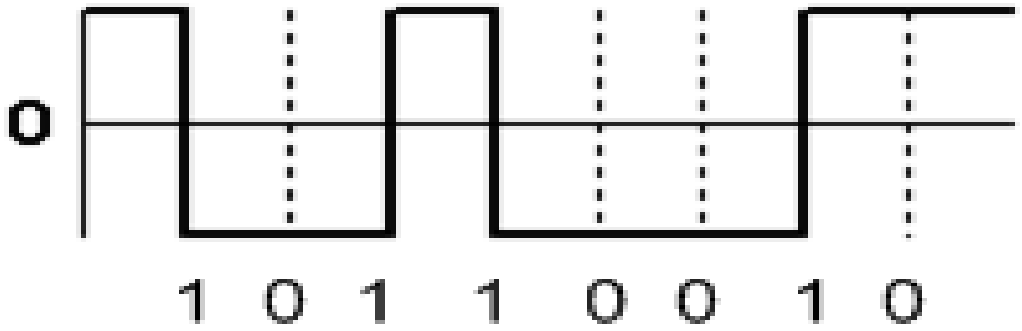

Рисунок Б.4

Принцип побудови канального коду NRZI

Перетворення 4B/5B здійснюється згідно таблиці Б.2

4B код 3 2 1 0	Шістнадцяткове число	5B код 4 3 2 1 0
0 0 0 0	0	1 1 1 1 0
0 0 0 1	1	0 1 0 0 1
0 0 1 0	2	1 0 1 0 0

0 0 1 1	3	1 0 1 0 1
0 1 0 0	4	0 1 0 1 0
0 1 0 1	5	0 1 0 1 1
0 1 1 0	6	0 1 1 1 0
0 1 1 1	7	0 1 1 1 1
1 0 0 0	8	1 0 0 1 0
1 0 0 1	9	1 0 0 1 1
1 0 1 0	A	1 0 1 1 0
1 0 1 1	B	1 0 1 1 1
1 1 0 0	C	1 1 0 1 0
1 1 0 1	D	1 1 0 1 1
1 1 1 0	E	1 1 1 0 0
1 1 1 1	F	1 1 1 0 1

Буфер 16B/32B використовується для накопичення даних з метою подальшої передачі на обробку до процесору.

Класифікація небезпечних сигналів, що можуть виникати в технічних засобах командно-штабної машини К-1450-05, є критично важливою для забезпечення її безпечної та ефективної експлуатації. Небезпечні сигнали можуть викликати різноманітні загрози, як-от несанкціонований витік інформації, збій у роботі системи чи зовнішнє втручання. Нижче наведено детальний опис основних категорій небезпечних сигналів, що можуть виникати у цій машині.

Електромагнітні випромінювання можуть випромінюватися від різних електронних компонентів та систем всередині машини, таких як процесори, монітори та інші пристрої обробки даних. Ці випромінювання можуть бути випадково перехоплені через:

- Випромінювання з проводів та кабелів, які переносять дані.
- Електромагнітне випромінювання з електронних плат і мікросхем, особливо якщо не забезпечено належне екранування.

Акустичні сигнали можуть генеруватися в результаті механічної роботи обладнання, такого як жорсткі диски, вентилятори охолодження та інші

пересувні компоненти. Ці сигнали можуть містити інформацію про стан або діяльність системи, що потенційно може бути перехоплена:

- Вібрація обладнання, що може створювати звукові хвилі, котрі відображають робочі цикли та процеси.
- Звуки клавіатури або інших устроїв введення, які можуть бути аналізовані для відновлення введеної інформації.

Сигнали, що проникають через системи електроживлення, можуть включати шуми або спотворення, які вносяться компонентами машини під час їх роботи. Ці сигнали можуть нести інформацію про діяльність або стан системи:

- Перепади напруги і шуми у мережі живлення, що можуть відбивати поточне навантаження та використання ресурсів.
- Гармонічні спотворення, які можуть виникати внаслідок специфічних робочих режимів обладнання.

Світлове випромінювання від індикаторів стану, екранів чи через неналежне ущільнення може становити ризик оптичного витоку:

- Візуальне спостереження за індикаторами стану або відображеннями на моніторах.
- Світлове випромінювання через щілини в корпусі або нещільно закриті доступи.

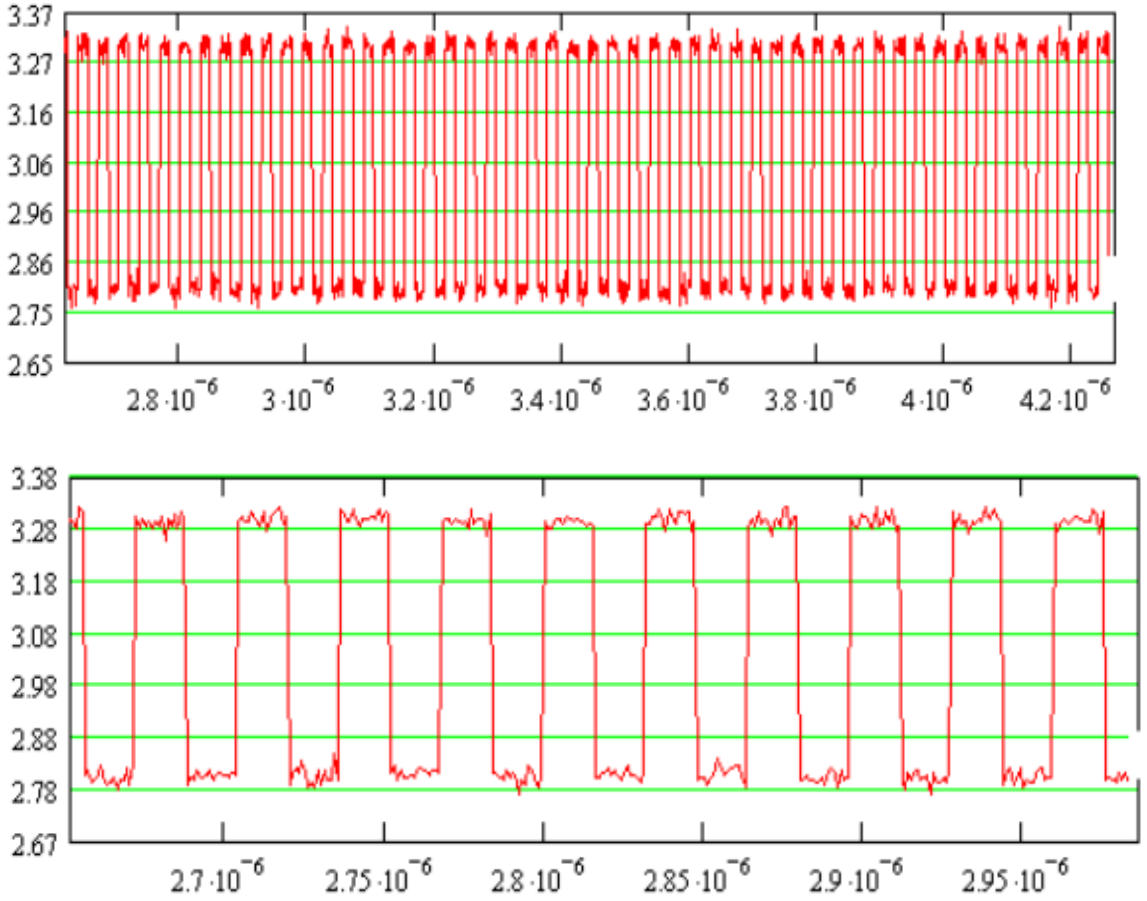

Рисунок Б.5

Епюри електричних сигналів на вході оптичного перетворювача інтерфейсу специфікації 100BaseFX

Основні параметри небезпечного сигналу:

- тип сигналу – імпульсний послідовний код;
- значення рівнів сигналу – +3.3, +2.8 В
- амплітуда сигналу - 0.5 В;
- тривалість передачі одного біту інформації – 8 нсек;
- повна кількість біт для передачі одного символу – 10 біт;
- кількість інформаційних біт у одному символі – 8 біт;
- смуга частот достатня для перехоплення сигналу – 125 МГц.

Виходячи з графіка, що показує вимірювання параметрів функціональних сигналів у колах передачі даних інтерфейсів 100BaseFX, можна зробити кілька ключових висновків щодо характеристик та стабільності сигналу:

На графіку видно, що сигнал демонструє високу періодичність із чітко вираженими піками та мінімумами, що вказує на стабільну роботу передавача. Частота сигналу, заснована на відстані між піками, вказує на відповідність заявленим характеристикам для 100BaseFX, який працює на частоті 125 МГц (мегагерц), оскільки базова модуляція передбачає передачу на кожному піднесенні або спаді сигналу.

Амплітуда сигналу стабільна та однорідна по всьому графіку, що свідчить про відсутність значних перешкод чи затухань у мережі. Значення амплітуди перебуває в межах від 2.65 до 3.37 вольт, що є типовим для оптоволоконних систем, де використовуються низькі напруги для передачі сигналів.

Сигнал показує гарну стабільність без видимих спотворень або шумів, що можуть вказувати на низький рівень помилок при передачі. Це свідчить про належну якість мережевих компонентів та ефективність застосованих технологій забезпечення цілісності даних.

Сигнал має виразну симетричну форму, що є показником правильної настройки системи та збалансованого передавання. Відсутність асиметрії або неоднорідності в амплітудах сигналів між різними циклами дозволяє забезпечити мінімальну кількість помилок та втрат при передачі даних.

Додаток В

Таблиця додаткового обладнання та його детальний опис

Генератор акустичного шуму стаціонарний «РІАС–2ГС» (модифікація 2) Призначений для захисту інформації з обмеженим доступом на об’єктах інформаційної діяльності від її витоку акустичними і віброакустичними каналами шляхом генерації шумового сигналу (шумової завади). Тип шумового сигналу, що генерується – аналоговий. Принцип формування шумового сигналу генератора – шумовий сигнал лавинного пробою p-n переходу малопотужного транзистора зі зворотнім включенням. Генератор має розширені функціональні можливості що включають - тимчасове відключення аналогових (АТЛ) і цифрових ліній (ЦТЛ) зв’язку та локальних мереж зв’язку LAN (Ethernet), на період циркулювання інформації з обмеженим доступом; - регульоване зашумлення АТЛ та ЦТЛ; - регульоване зашумлення мережі живлення; - адаптер шумового сигналу для підключення до зовнішніх приладів. Генератор забезпечує пригнічення акустичних сигналів в смузі частот від 180 Гц до 5,6 кГц. Вихідна середньоквадратична напруга акустичного (електромагнітного) каналу генератору при мінімальному опорі навантаження 4 Ом – не менше 5 В. Вихідна середньоквадратична напруга п’єзоелектричного каналу при сумарній ємності навантаження 0,15 мкФ – не менше 20 В. Діапазон регулювання : - низько- та високочастотних складових шумового сигналу у робочому діапазоні частот – не менше 20 дБ; - сигналів октавних частот - не менше 12дБ.	1 шт Для захисту ліній від Кабельний ввід ліній захищеного зв’язку Та створення КТЗІ від витоку акустичними та віброакустичними каналами в місці встановлення виносних засобів зв’язку	

Адаптер забезпечує : - рівень шумового сигналу до при навантаженні 120 Ом не менше 1В; - напругу живлення 12В при струмі до 0.5А.		
Випромінювач акустичний PIAC–2BA Призначений для захисту об'єктів від витоку конфіденційної інформації віброакустичними каналами шляхом перетворення електричних сигналів в акустичні коливання в звуковому діапазоні частот від 180 Гц до 5,6 кГц. Вихідна середньоквадратична напруга акустичного каналу при опорі навантаження 6 Ом - не менше 5 В. Усереднений максимальний рівень вихідного акустичного сигналу в діапазоні робочих частот з похибкою встановлення не більше 6 дБ на відстані 1 м від випромінювача для випромінювача не менше 70 дБ відносно нульового значення 2х10-5 Па (для звукового тиску).	4 шт створення КТЗІ від витоку акустичними та віброакустичними каналами в місці встановлення виносних засобів зв'язку	
Вібровипромінювач п'єзоелектричний PIAC–2BП Призначений для захисту об'єктів від витоку конфіденційної інформації віброакустичними каналами шляхом перетворення електричних сигналів в механічні коливання в звуковому діапазоні частот від 180 Гц до 5,6 кГц. Вихідна середньоквадратична напруга п'єзоелектричного каналу при максимальній ємності навантаження 0,5 мкФ - не менше 20 В. Усереднений максимальний рівень вихідного віброакустичного сигналу в діапазоні робочих частот з похибкою встановлення не більше 6 дБ на віброізольованій приєднаній сталевій масі 10 кГ циліндричної форми для вібровипромінювача не менше 70 дБ відносно нульового значення 3х10-4 м4с2 (для віброприскорення).	4 шт створення КТЗІ від витоку акустичними та віброакустичними каналами в місці встановлення виносних засобів зв'язку	

Розділовий трансформатор з екранованою обмоткою PIAC–4TP/2 Призначений для гальванічного розв'язування та технічного захисту інформації в однофазних двохпровідних ланках мережі електроживлення напругою до 250 В, частотою 50 Гц від її витоку через канал, який створюється за рахунок акустоелектричних перетворень та паразитної модуляції мовним сигналом високочастотного сигналу „накачування", утвореного засобами технічної розвідки. Забезпечує закриття каналу витоку мовної інформації в смузі частот пригнічення від 180 Гц до 30 МГц на величину не менше 30 дБ. Номінальна первинна та вторинна напруги - не більше 250 В. Номінальна потужність - 2 кВА. Забезпечує автоматичну систему захисту від перевищення струму.	1 шт. Кабельний ввід електроживлення Для захисту від витоку каналом ПЕМН та спеціального впливу по лініям електроживлення	
DELTA 7 Засіб активного захисту автоматизованих систем «DELTA-7» призначений для використання на об'єктах електронно-обчислювальної техніки, об'єктах спеціального зв'язку, а також інших об'єктах інформаційної діяльності, з метою забезпечення гарантованого перекриття спеціально організованими перешкодами інформативних сигналів побічних електромагнітних випромінювань і наведень, створюваних комп'ютерною та копіювальною технікою, мережевим обладнанням, засобами та комплексами спеціального зв'язку, їх комунікаціями, а також іншим обладнанням і елементами допоміжних технічних засобів і систем. Засіб забезпечує випромінювання захисних електромагнітних перешкод, фільтрацію паразитних високочастотних сигналів, що протікають по ланцюгах трактів, розрив яких воно може включатися, а також введення некорельованих струмових захисних перешкод в ланцюзі мереж електроживлення та систем заземлення (чи занулення).	**1 шт.** **Для ноутбука** **Захист від ПЕМВН**	

Виріб може бути застосовано як засіб цільової та/або груповий захисту при безпосередньому підключенні та/або розташуванні в безпосередній близькості до нього обладнання, що обробляє інформацію з обмеженим доступом. У процесі роботи, забезпечується безперервний автоматичний контроль параметрів захисних перешкод. У разі неприпустимого відхилення контрольованих параметрів, формується сигнал звукової сигналізації і світлової індикації порушення працездатності виробу. Спектральні характеристики формуються захисних перешкод в діапазоні частот від 9 кГц до 3,3ГГц, адаптовані до частотного розподілу компонент інформативних сигналів побічних електромагнітних випромінювань і наведень, створюваних сучасними телекомунікаційними засобами. При цьому забезпечуються: - коефіцієнт якості шуму, не менш 0,97; - коефіцієнт асиметрії, не гірше 0,98; - ексцес розподілу амплітуд, не більше 0,003; - значення межинтервальной кореляції, не вище 0,05; - значення межполосной кореляції, не вище 0,08. По своєму виконанню, засіб «DELTA-7» є захищеним від паразитних акустоэлектрических перетворень і може застосовуватися на об'єктах, на яких здійснюється озвучування мовної інформації Засіб призначений для підключення до однофазних електромереж змінного струму з напругою 85 ÷ 265 В, частотою 48 ÷ 63 Гц, із застосуванням з'єднувачів, у відповідності зі специфікацією IEC 60320 (IEC 320). При цьому, забезпечується навантажувальна здатність до 1,2 кВт або 600 Вт, при транзитному підключенні зовнішнього навантаження до електромережі з номінальною напругою 220В або 110В, відповідно. Засіб забезпечує можливість цілодобової експлуатації і явля-ється стійким до змін заявлених характеристик: - при експлуатації в робочому діапазоні температур від +10 до +35 ºС; - після транспортування при температурі навколишнього середовища від -35 до		

+65 ºС і подальшій витримці не менше 1 години до включення в робочому діапазоні температур. Масогабаритні характеристики Розмір виробу: 220×60×40 (довжина × ширина × висота). Вага виробу: 800 грам. Показники надійності та якості Серійне виробництво здійснюється спеціалізованим высокотех-нологическим підприємством з впровадженою Системою Управління Якістю, сертифікована на відповідність стандарту ДСТУ ISO 9001:2009 (між-народний стандарт ISO 9001:2008). Експертний висновок за результатами державної експертизи в сфері технічного захисту інформації від 21.09.2012 №374.		

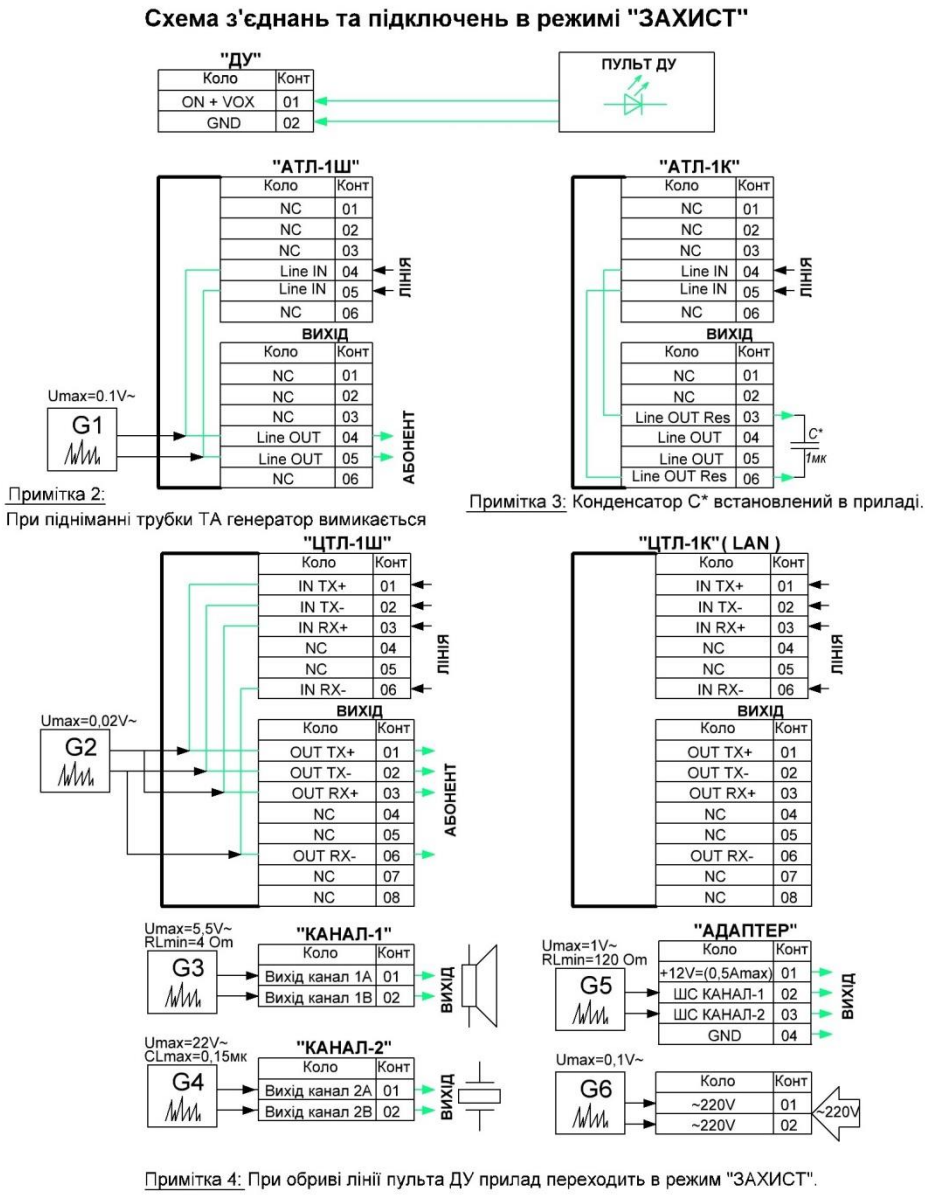

Рисунок В.1 Схема з’єднань та підключень у режимі “Захист”