

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
«ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ»**

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему: «Методи забезпечення безпеки передачі даних у
низькоорбітальних супутникових мережах»

здобувач: Леник Сергій Олександрович

(підпис)

Науковий керівник: Доцент. Пархоменко Іван Іванович

(підпис)

**Робота допущена до захисту перед екзаменаційною
комісією з атестації здобувачів вищої освіти (ЕК)**

Завідувач кафедри: д.ф.-м.н., проф. Джалладова І.А.

КИЇВ 2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

ПОГОДЖЕНО

Керівник проектної групи (гарант)
Освітньо-професійної програми

А.В. Бегун

(підпис) (ініціали, прізвище)
2026 р.

ЗАТВЕРДЖУЮ:

Завідувач кафедри

І.А. Джалладова

(підпис) (ініціали, прізвище)

2026 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувача вищої освіти Леник Сергій Олександрович
(прізвище, ім'я, по батькові)

очної (денної) **форми навчання**
очної (денної), заочної, дистанційної

на підготовку кваліфікаційної бакалаврської роботи
на тему « «Методи забезпечення безпеки передачі даних у низькоорбітальних супутникових мережах» »

Тему затверджено наказом ректора Університету від « » 2026 р. №

Кваліфікаційна бакалаврська робота виконується на матеріалах:
Департаменту кіберполіції Національної поліції України, зокрема на основі аналізу актуальних статистичних даних щодо кіберінцидентів у сфері соціальної інженерії та фішингових атак в українському сегменті мережі Інтернет

План кваліфікаційної бакалаврської роботи

Розділ 1 Теоретико-методичні основи забезпечення безпеки передачі даних у низькоорбітальних супутникових мережах

Розділ 2 Аналіз загроз, вразливостей та методів захисту даних у LEO-супутникових мережах

Розділ 3 Обґрунтування практичних рекомендацій щодо підвищення безпеки передачі даних у низькоорбітальних супутникових мережах

Об'єкт дослідження: процес передачі даних у низькоорбітальних супутникових мережах.

Предмет дослідження: методи та засоби забезпечення безпеки передачі даних у низькоорбітальних супутникових мережах.

Мета кваліфікаційної бакалаврської роботи: дослідження сучасних методів забезпечення безпеки передачі даних у низькоорбітальних супутникових мережах та розроблення рекомендацій щодо підвищення рівня їх захищеності від актуальних кіберзагроз.

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

1. Дослідити особливості побудови та функціонування низькоорбітальних супутникових мереж.
2. Визначити роль LEO-супутникових мереж у сучасних телекомунікаційних системах, критичній інфраструктурі та глобальному доступі до мережі Інтернет.
3. Проаналізувати основні загрози безпеці передачі даних у низькоорбітальних супутникових мережах, зокрема перехоплення, підміну, модифікацію трафіку, несанкціонований доступ та атаки на канали зв'язку.
4. Розглянути сучасні методи криптографічного захисту інформації, аутентифікації користувачів, контролю доступу та захисту мережевих протоколів.
5. Провести порівняльний аналіз методів захисту даних у супутникових мережах та визначити їх переваги й обмеження.

6. Сформувати практичні рекомендації щодо підвищення безпеки передачі даних у низькоорбітальних супутникових мережах.

Завдання підготував Пархоменко І.І.

науковий керівник (підпис)

Завдання одержав Леник С.О.

здобувач (підпис)

РЕФЕРАТ

Кваліфікаційна бакалаврська робота: 56 с., 11 рис., 11 табл., 4 додатки, 42 джерела.

Об'єкт дослідження: процес передачі даних у низькоорбітальних супутникових мережах.

Предмет дослідження: методи та засоби забезпечення безпеки передачі даних у низькоорбітальних супутникових мережах.

Мета кваліфікаційної бакалаврської роботи: дослідження сучасних методів забезпечення безпеки передачі даних у низькоорбітальних супутникових мережах та визначення шляхів підвищення рівня їх захищеності від актуальних кіберзагроз.

Методи дослідження: аналіз і узагальнення наукових джерел, системний аналіз архітектури низькоорбітальних супутникових мереж, класифікація загроз інформаційній безпеці, порівняльний аналіз методів криптографічного захисту, аутентифікації, контролю доступу та захищених протоколів передачі даних.

У роботі розглянуто особливості функціонування низькоорбітальних супутникових мереж, їх значення для забезпечення глобального доступу до мережі Інтернет, підтримки критичної інфраструктури, військового зв'язку та систем Інтернету речей. Визначено, що використання відкритого радіоканалу, велика кількість вузлів, динамічна топологія мережі та залежність від наземної інфраструктури створюють додаткові ризики для конфіденційності, цілісності та доступності даних.

Проаналізовано основні кіберзагрози для передачі даних у LEO-супутникових мережах, зокрема перехоплення трафіку, підміну даних, несанкціонований доступ, атаки типу «людина посередині», радіоелектронне придушення, спуфінг сигналів і порушення роботи наземних станцій. Окрему увагу приділено методам криптографічного захисту, механізмам аутентифікації, контролю доступу, захищеним мережевим протоколам та організаційно-технічним заходам безпеки.

У результаті дослідження узагальнено сучасні підходи до захисту передачі даних у низькоорбітальних супутникових мережах та визначено напрями підвищення їх кіберстійкості. Практичне значення отриманих результатів полягає у можливості використання запропонованих рекомендацій для підвищення рівня захищеності супутникових систем зв'язку, зменшення ризику перехоплення або модифікації інформації та забезпечення надійної роботи мереж у складних умовах експлуатації.

Напрями подальших досліджень: удосконалення криптографічних протоколів для супутникових мереж, впровадження постквантових алгоритмів захисту, розроблення адаптивних систем виявлення атак, підвищення стійкості каналів зв'язку до радіоелектронного впливу та інтеграція засобів моніторингу безпеки в архітектуру LEO-мереж.

Ключові слова: низькоорбітальні супутникові мережі, LEO, супутниковий зв'язок, кібербезпека, передача даних, криптографічний захист, аутентифікація, контроль доступу, захищені протоколи, кіберзагрози, конфіденційність, цілісність, доступність.

ВІДГУК
на кваліфікаційну бакалаврську роботу
студента **Леник Сергія Олександровича**
на тему «Методи забезпечення безпеки передачі даних у низькоорбітальних супутникових мережах»

Актуальність теми: обрана тема є актуальною з огляду на активний розвиток низькоорбітальних супутникових мереж і зростання їх ролі в сучасній телекомунікаційній інфраструктурі. LEO-мережі використовуються для забезпечення доступу до Інтернету, підтримки критичної інфраструктури, резервного зв'язку, військових і цивільних комунікацій. Водночас відкрите радіосередовище, динамічна топологія, велика кількість вузлів, залежність від наземного сегмента та необхідність безперервного керування каналами створюють додаткові ризики для конфіденційності, цілісності й доступності даних. За таких умов дослідження методів захисту передачі даних у LEO-супутникових мережах є своєчасним і має важливе практичне значення для сфери кібербезпеки.

Повнота розкриття теми: поставлене завдання опрацьоване послідовно й доведене до логічного завершення. Структура роботи відповідає темі та складається з трьох взаємопов'язаних розділів. У першому розділі розглянуто теоретико-методичні основи забезпечення безпеки передачі даних у низькоорбітальних супутникових мережах, зокрема архітектуру LEO-мереж, особливості радіоканалу, наземного сегмента, міжсупутникових каналів і службового керування. У другому розділі проаналізовано основні загрози, вразливості та методи захисту даних у LEO-супутникових мережах. У третьому розділі представлено практичну частину роботи, пов'язану з розробкою програмного засобу LEO Shield Analyzer для оцінювання рівня ризику та формування рекомендацій щодо підвищення захищеності каналу зв'язку. Усі поставлені завдання знайшли відображення у відповідних розділах роботи.

Теоретичний рівень: автор опрацював наукові, технічні та нормативні джерела, що стосуються кібербезпеки супутникових систем, ризик-орієнтованого підходу, захисту каналів зв'язку, автентифікації, керування ключами, моніторингу та безпечного оновлення програмного забезпечення. У роботі показано розуміння специфіки LEO-мереж, зокрема динамічної маршрутизації, процедур handover, ролі наземної інфраструктури, відкритості радіоканалу та залежності захисту від узгодженої роботи всіх сегментів системи. Варто відзначити, що автор не обмежився загальним описом засобів захисту, а сформував набір критеріїв оцінювання захищеності передачі даних, які надалі використано у практичній частині роботи.

Практична цінність: результатом роботи є власний програмний засіб LEO Shield Analyzer, призначений для навчально-аналітичного оцінювання ризику передачі даних у LEO-мережах. Програма передбачає вибір сценарію використання супутникового каналу, оцінювання груп контролів безпеки за шкалою від 0 до 3, урахування вагових коефіцієнтів, розрахунок інтегрального ризику, визначення рівня небезпеки та формування рекомендацій щодо посилення захисту. Практична цінність розробки полягає в тому, що вона наочно демонструє вплив окремих заходів безпеки на загальний рівень ризику та може використовуватися як допоміжний навчальний інструмент під час аналізу захищеності супутникових комунікацій.

Самостійність виконання: студент самостійно систематизував основні загрози для LEO-супутникових мереж, визначив критерії оцінювання захищеності, розробив логіку ризик-орієнтованого аналізу та реалізував програмний засіб для демонстрації запропонованого підходу. Вибір сценаріїв використання, груп контролів безпеки, вагових коефіцієнтів і рекомендацій свідчить про авторський підхід до виконання практичної частини роботи. Окремо слід відзначити, що програмна реалізація має завершену структуру, містить інтерфейс користувача, модуль розрахунку ризику, блок рекомендацій і можливість порівняння сценаріїв.

Якість оформлення, загальна та спеціальна грамотність: пояснювальна записка кваліфікаційної бакалаврської роботи оформлена відповідно до вимог, має логічну структуру та послідовний виклад матеріалу. Робота містить вступ, три основні розділи, висновки, список використаних джерел і додатки. Аналітичний матеріал систематизовано у таблицях, а основні положення роботи проілюстровано схемами, рисунками та скріншотами роботи програмного засобу. Додатки доповнюють основний текст і містять матеріали, що підтверджують практичну реалізацію роботи: фрагменти програмного коду, інструкцію користувача, контрольні тестові сценарії та скріншоти інтерфейсу LEO Shield Analyzer.

Переваги та недоліки роботи: до сильних сторін роботи слід віднести комплексний підхід до аналізу безпеки LEO-супутникових мереж, поєднання теоретичного дослідження з практичною програмною реалізацією, використання ризик-орієнтованої моделі оцінювання та наочне подання результатів у програмному засобі. Вдалим рішенням є застосування сценарного підходу, за якого рівень ризику залежить не лише від наявності окремих засобів захисту, а й від їхньої важливості для конкретного типу використання супутникового каналу. Позитивним також є те, що програма не просто визначає рівень ризику, а формує зрозумілі рекомендації щодо посилення окремих напрямів захисту.

До недоліків можна віднести те, що розроблений програмний засіб має навчально-аналітичний характер і не підключається до реальної телеметрії супутникової мережі. Оцінювання ризику базується на заданих користувачем параметрах і вагових коефіцієнтах, тому отримані результати слід розглядати як попередню експертну оцінку, а не як повноцінний інструмент моніторингу реальної LEO-інфраструктури. У подальшому програму доцільно доповнити можливістю імпорту реальних параметрів каналу, таких як рівень сигналу, втрати пакетів, події автентифікації, телеметрія шлюзової станції та журнали безпеки. Зазначене зауваження окреслює напрям подальшого розвитку й не знижує загальної цінності виконаної роботи.

Загальна оцінка роботи та висновок щодо рекомендації до захисту в ЕК: виконана робота показала, що Леник Сергій Олександрович здатний самостійно аналізувати складні завдання у сфері кібербезпеки, обґрунтовувати вибір методів захисту та реалізовувати практичні програмні рішення. У цілому кваліфікаційна бакалаврська робота є завершеним, актуальним і самостійним дослідженням, що відповідає вимогам до робіт за спеціальністю 125 «Кібербезпека», її автор — на присвоєння кваліфікації бакалавра за відповідною спеціальністю та освітньою програмою.

Керівник кваліфікаційної роботи
к.т.н., доцент кафедри системного
аналізу та кібербезпеки ННІ «Інститут
інформаційних технологій в економіці»
Київського національного економічного
університету імені Вадима Гетьмана

	Іван
	ПАРХОМЕНКО
	(ініціали,
(підпис)	прізвище)

«8» червня 2026 р.

РЕЦЕНЗІЯ

на кваліфікаційну бакалаврську роботу

студента Леника Сергія Олександровича гр. ІК-401

(прізвище, ініціали)

на тему: Методи забезпечення безпеки передачі даних у низькоорбітальних супутникових мережах.

Актуальність теми зумовлена стрімким розвитком низькоорбітальних супутникових мереж, які забезпечують глобальне покриття та доступ до високошвидкісного зв'язку. Зростання обсягів переданих даних і розширення сфер застосування таких систем підвищують ризики несанкціонованого доступу, перехоплення інформації та кібератак. Тому розробка й удосконалення методів захисту даних у низькоорбітальних супутникових мережах є важливим завданням для забезпечення конфіденційності, цілісності та доступності інформації, а також підвищення надійності сучасних телекомунікаційних систем.

Наукова новизна полягає у вдосконаленні методів забезпечення безпеки передачі даних у низькоорбітальних супутникових мережах шляхом адаптації криптографічних механізмів до динамічної топології мережі, що дозволяє підвищити рівень захисту інформації та стійкість системи до сучасних кіберзагроз при збереженні ефективності передачі даних.

Якість проведеного аналізу: проведений аналіз є якісним, комплексним та актуальним, оскільки враховує сучасний стан розвитку низькоорбітальних супутникових мереж, наявні кіберзагрози та перспективні напрями забезпечення безпеки передачі даних в умовах стрімкого розвитку супутникових телекомунікаційних технологій.

Уміння користуватися літературними джерелами оцінюються позитивно. Виявлено високий рівень навичок роботи з літературними джерелами, здатність критично аналізувати наукову інформацію та ефективно використовувати її для розкриття теми дослідження.

Практична цінність висновків і рекомендацій: дослідження має практичне значення для підвищення безпеки передачі даних у низькоорбітальних супутникових мережах та можуть бути використані під час проєктування захищених систем зв'язку, удосконалення механізмів кіберзахисту та в освітній і науковій діяльності.

Переваги та недоліки: перевагами роботи є актуальність теми, ґрунтовний аналіз сучасних методів забезпечення безпеки передачі даних та практична значущість отриманих результатів. До недоліків можна віднести обмежений обсяг практичної апробації запропонованих рекомендацій і недостатньо детальний розгляд окремих перспективних напрямів розвитку засобів захисту.

Загальний висновок і оцінка роботи: кваліфікаційна робота є завершеним самостійним дослідженням, виконаним на належному науково-теоретичному рівні. Продемонстровано ґрунтовні знання предметної області, уміння аналізувати наукові джерела та формулювати обґрунтовані висновки. Поставлені мета та завдання досягнуті в повному обсязі, а отримані результати мають теоретичне і практичне значення. Робота відповідає встановленим вимогам до кваліфікаційних робіт та заслуговує на високу оцінку.

Рецензент доктор фізико-математичних наук, професор кафедри комп'ютерних наук та кібербезпеки Волинського національного університету імені Лесі Українки.

Я. М. Пастернак

(підпис)

(ініціали, прізвище)

Печатка

“ ” 2026р.

ЗМІСТ

ВСТУП.....	4
РОЗДІЛ 1 АНАЛІТИЧНИЙ ОГЛЯД ЛІТЕРАТУРИ ТА МЕТОДИЧНИХ ПІДХОДІВ ДО БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ У LEO-МЕРЕЖАХ	6
1.1. Стан дослідження проблеми безпеки низькоорбітальних супутникових мереж	
1.2. Архітектура передачі даних і методичні підходи до її захисту	11
1.3. Критерії оцінювання захищеності передачі даних у LEO-мережах	19
Висновки до розділу 1.....	21
РОЗДІЛ 2 АНАЛІЗ ЗАГРОЗ, ВРАЗЛИВОСТЕЙ ТА МЕТОДІВ ЗАХИСТУ ДАНИХ У LEO-СУПУТНИКОВИХ МЕРЕЖАХ	23
2.1. Класифікація загроз безпеці передачі даних у LEO-супутникових мережах...	23
2.2. Аналіз вразливостей основних компонентів LEO-супутникової мережі	25
2.3. Методи захисту передачі даних у LEO-супутникових мережах.....	27
2.4. Порівняльна оцінка методів захисту даних у LEO-мережах	29
2.5. Оцінка ризиків реалізації загроз у LEO-супутникових мережах	30
Висновки до розділу 2.....	33
РОЗДІЛ 3 НАУКОВЕ ОБҐРУНТУВАННЯ ПРОПОЗИЦІЙ І РОЗРОБКА ПРОГРАМНОГО ЗАСОБУ	34
3.1. Постановка задачі та функціональні вимоги до LEO Shield Analyzer	34
3.2. Проєктування архітектури програмного засобу.....	36
3.3. Алгоритм оцінювання ризику передачі даних у LEO-мережі	39
3.4. Реалізація програмного засобу LEO Shield Analyzer	42
3.5. Тестування програмного засобу та аналіз результатів	47
Висновки за розділом 3.....	49
ВИСНОВКИ.....	51
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	53
ДОДАТОК А	
ДОДАТОК Б	

ДОДАТОК В

ДОДАТОК Д

ВСТУП

Сучасний розвиток телекомунікаційних технологій сприяє активному впровадженню низькоорбітальних супутникових мереж (LEO), які забезпечують глобальне покриття, високу швидкість передачі даних та низькі затримки сигналу. Такі мережі широко використовуються для надання доступу до мережі Інтернет, підтримки критичної інфраструктури, військового зв'язку та систем Інтернету речей. Водночас використання відкритих каналів зв'язку та складна архітектура супутникових систем створюють додаткові ризики для інформаційної безпеки.

Актуальність теми зумовлена необхідністю забезпечення надійного захисту даних, що передаються через низькоорбітальні супутникові мережі. Зростання кількості кіберзагроз, спроб несанкціонованого доступу, перехоплення та модифікації інформації вимагає вдосконалення існуючих методів захисту та розроблення нових підходів до забезпечення безпеки супутникових комунікацій.

Питання захисту супутникових мереж досліджуються багатьма вітчизняними та зарубіжними науковцями. Значний внесок у розвиток криптографічних методів захисту інформації та безпечних протоколів передачі даних зробили Вітфілд Діффі, Мартін Геллман, Брюс Шнайер, Росс Андерсон та інші фахівці у сфері кібербезпеки. Незважаючи на значну кількість досліджень, проблема забезпечення безпеки передачі даних у низькоорбітальних супутникових мережах залишається актуальною через постійний розвиток технологій та появу нових загроз.

Метою дипломної роботи є дослідження методів забезпечення безпеки передачі даних у низькоорбітальних супутникових мережах та визначення шляхів підвищення рівня їх захищеності.

Для досягнення поставленої мети необхідно виконати такі завдання: проаналізувати особливості функціонування низькоорбітальних супутникових мереж; дослідити основні загрози інформаційній безпеці; розглянути сучасні методи криптографічного захисту даних; проаналізувати механізми

аутентифікації та контролю доступу; оцінити ефективність існуючих засобів захисту та надати рекомендації щодо підвищення безпеки передачі даних.

Об'єктом дослідження є процес передачі даних у низькоорбітальних супутникових мережах.

Предметом дослідження є методи та засоби забезпечення безпеки передачі даних у низькоорбітальних супутникових мережах.

У роботі використано методи аналізу наукових джерел, системного та порівняльного аналізу, а також методи оцінювання ефективності засобів захисту інформації.

Наукова новизна роботи полягає в узагальненні сучасних підходів до захисту передачі даних у низькоорбітальних супутникових мережах та визначенні актуальних напрямів підвищення їх безпеки.

Практичне значення одержаних результатів полягає у можливості використання запропонованих рекомендацій для підвищення рівня захищеності супутникових систем зв'язку та зниження ризиків реалізації кіберзагроз.

РОЗДІЛ 1 АНАЛІТИЧНИЙ ОГЛЯД ЛІТЕРАТУРИ ТА МЕТОДИЧНИХ ПІДХОДІВ ДО БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ У LEO-МЕРЕЖАХ

1.1. Стан дослідження проблеми безпеки низькоорбітальних супутникових мереж

Супутникові мережі на низькій навколоземній орбіті (LEO) сьогодні фактично стали одним із робочих інструментів глобального зв'язку, а не лише перспективною космічною технологією. NASA визначає низьку навколоземну орбіту як область із висотою до 2000 км, що пояснює її придатність для зв'язку, спостереження та підтримки космічних апаратів [1]. Порівняно з геостаціонарними системами сигнал у LEO проходить меншу відстань, тому затримка може бути нижчою. Водночас за це доводиться платити складнішою архітектурою: потрібні численні супутники, часті перемикання з'єднання і постійне керування динамічною топологією.

Питання безпеки передачі даних у таких мережах не можна звести лише до шифрування радіоканалу. LEO-мережа є кіберфізичною системою, де разом працюють космічний сегмент, наземні шлюзові станції, центри керування, користувацькі термінали, канали зв'язку, програмне забезпечення і зовнішні IP-мережі. У документах NIST окремо наголошується, що безпека наземного сегмента прямо впливає на керування супутниковими платформами, корисним навантаженням і сервісами зв'язку [2].

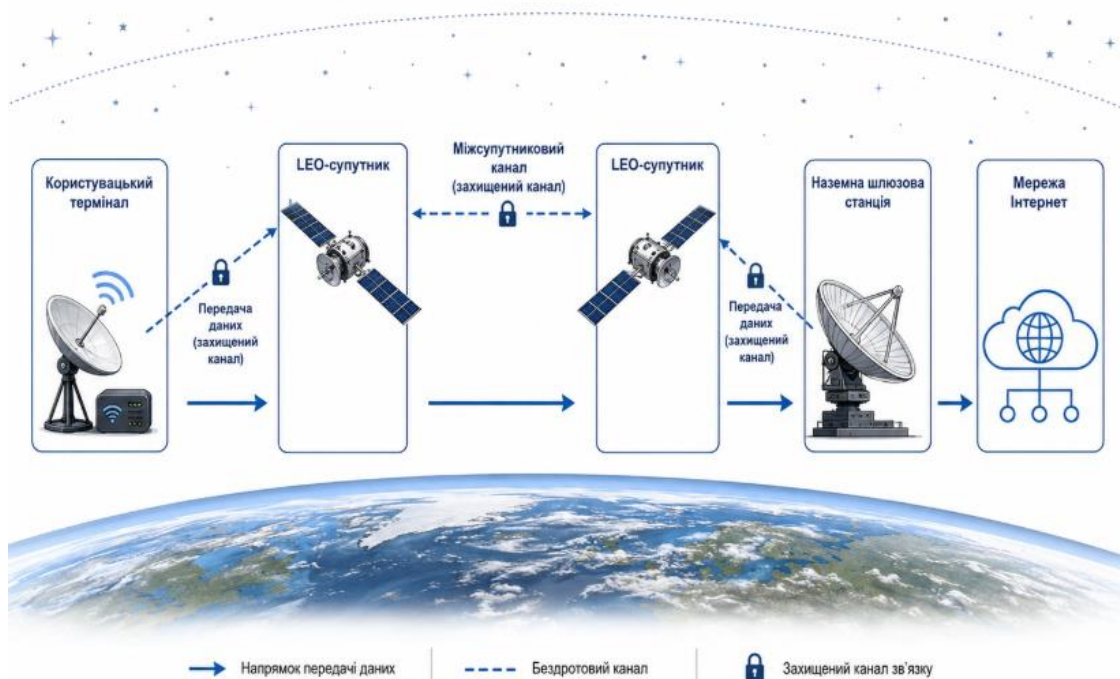


Рисунок 1.1 — Загальна структура передачі даних у LEO-супутниковій мережі

У наукових і прикладних роботах безпеку LEO-мереж зручно розглядати через класичну тріаду конфіденційності, цілісності та доступності. Конфіденційність потрібна, щоб користувачський і службовий трафік не розкривався стороннім особам. Цілісність дає змогу виявляти підміну повідомлень, маршрутної інформації або команд керування. Доступність показує, чи здатна мережа підтримувати зв'язок під час завад, атак на шлюзи, перевантаження або відмови окремих вузлів. Такий підхід узгоджується з логікою NIST Cybersecurity Framework та каталогом контролів NIST SP 800-53 [5].

LEO-мережі мають низку особливостей, які ускладнюють захист. Радіоканал залишається відкритим середовищем, тому існують ризики перехоплення, навмисних завад і спуфінгу. Топологія постійно змінюється через рух супутників, отже маршрути передавання даних не є сталими. Крім того, сучасне сузір'я може містити сотні або тисячі вузлів, а частина критичних функцій виконується на землі, де можливі звичні кібератаки на сервери, облікові записи, оновлення і канали керування [3; 10].

Практика вже показала, що такі ризики не є суто теоретичними. Атака на мережу KA-SAT 24 лютого 2022 року призвела до порушення супутникового

широкосмугового сервісу; за описом Viasat, проблема була пов'язана не з фізичним ураженням супутника, а з мережевою інфраструктурою та користувацькими модемами [7]. Для теми LEO це показовий приклад: слабкою ланкою може стати не орбітальний апарат, а наземний або абонентський сегмент.

У сучасних дослідженнях безпеки LEO-мереж простежується кілька основних напрямів: криптографічний захист даних, автентифікація користувачів і вузлів, керування ключами, захист фізичного радіоканалу, стійка маршрутизація, моніторинг аномалій, безпечне програмне забезпечення та захист наземної інфраструктури. CCSDS підкреслює, що безпека космічних систем має закладатися в архітектуру, а не додаватися після її розгортання [11].

Таблиця 1.1

Основні напрями дослідження безпеки LEO-супутникових мереж

Напрямок дослідження	Суть проблеми	Практичний фокус захисту
Криптографічний захист і керування ключами	Перехоплення радіосигналу або трафіку не повинно призводити до розкриття даних.	Шифрування, цифрові підписи, безпечний обмін і ротація ключів, підготовка до постквантової міграції.
Автентифікація та контроль доступу	Нелегітимний термінал, шлюз або службовий вузол може отримати доступ до мережі чи вплинути на маршрути.	Сертифікати, апаратні модулі безпеки, багатофакторна автентифікація адміністраторів, мінімальні привілеї.
Захист радіоканалу	Відкрите середовище передавання створює умови для завад, спуфінгу та аналізу сигналу.	Спрямовані антени, формування променя, завадостійке кодування, контроль аномалій фізичного рівня.
Безпечна маршрутизація	Динамічна топологія та міжсупутникові канали ускладнюють перевірку коректності маршрутів.	Автентифікація маршрутних повідомлень, перевірка цілісності таблиць, резервні маршрути, виявлення підозрілих змін.

Напрямок дослідження	Суть проблеми	Практичний фокус захисту
Моніторинг і реагування на інциденти	Масштаб мережі не дозволяє покладатися лише на ручний контроль.	IDS/IPS, журналювання, кореляція подій, поведінкова аналітика, автоматизоване блокування аномалій.
Захист наземного та користувацького сегментів	Шлюзи, центри керування й термінали часто доступніші для атак, ніж космічний сегмент.	Сегментація, захищені оновлення, контроль прошивки, резервування, аудит конфігурацій і доступу.

Криптографічний захист залишається базовим, але для LEO-мереж особливо складним є не сам вибір алгоритму, а весь життєвий цикл ключів. Велика кількість вузлів, часті handover-процедури, обмежені ресурси частини терміналів і вимога низької затримки ускладнюють централізоване керування ключами. Окремо слід враховувати постквантовий напрям: у 2024 році NIST затвердив стандарти FIPS 203, FIPS 204 і FIPS 205, а рекомендації з керування ключами визначають вимоги до їх генерації, зберігання, ротації та відкликання [8].

Автентифікація в LEO-мережі має охоплювати не тільки кінцевого користувача. Потрібно перевіряти термінал, шлюзову станцію, супутник, службові API, адміністратора і процеси керування. Якщо така перевірка слабка, з'являються ризики man-in-the-middle, підміни маршрутної інформації або підключення несанкціонованого обладнання. Тому в практиці доцільно поєднувати сертифікати, апаратні корені довіри, протоколи автентифікації та принципи Zero Trust [16].

Захист фізичного рівня варто розглядати окремо, бо навіть сильне шифрування не гарантує доступності сервісу. Навмисні завади, спуфінг, помилки наведення антени або деградація сигналу можуть зробити канал непридатним для роботи. Саме тому сучасні підходи враховують не лише криптографію, а й

радіотехнічні засоби: адаптивний вибір частот, формування вузьких променів, просторову фільтрацію, виявлення аномалій сигналу та резервування каналів [9].

Безпечна маршрутизація також стає складнішою через рух LEO-супутників. Міжсупутникові канали можуть змінюватися залежно від положення апаратів, завантаження та стану ліній зв'язку. У роботах щодо космічних інформаційних мереж підкреслюється зв'язок між маршрутними загрозами, сервісами і механізмами виявлення атак [9]. Отже, маршрутизацію слід розглядати як об'єкт захисту, а не лише як технічний спосіб доставки пакетів.

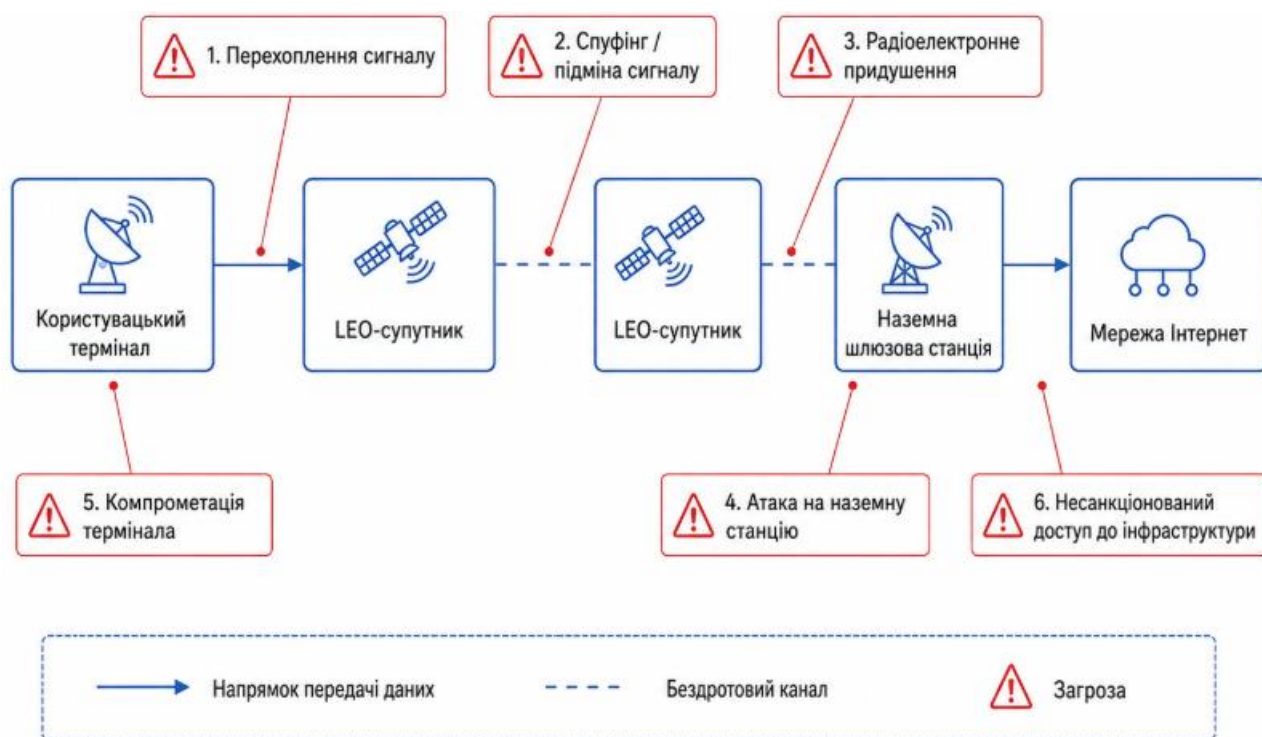


Рисунок 1.2 — Основні групи загроз для передачі даних у LEO-супутниковій мережі

Окремий блок досліджень присвячений наземному сегменту. NIST IR 8401 розглядає застосування Cybersecurity Framework до командування, керування, телеметрії та корисного навантаження [2]. NIST IR 8441 доповнює цей погляд для гібридних супутникових мереж, де взаємодіють компоненти з різними власниками і різними рівнями довіри [3]. Це добре відповідає реальності LEO-сервісів, де оператор супутників, наземні провайдери, хмарна інфраструктура та користувачі не завжди перебувають в одному контурі управління.

ENISA у звіті Space Threat Landscape 2025 звертає увагу, що кіберризиками для комерційних супутників охоплюють не лише експлуатацію, а й проектування, виробництво, ланцюг постачання, оновлення та виведення систем з роботи [6]. Схожу логіку містять рекомендації з кібербезпеки космічних систем і управління ризиками ланцюга постачання [24]. Тому безпеку LEO-мережі потрібно бачити як процес повного життєвого циклу, а не як набір разових технічних налаштувань.

Спільний висновок більшості джерел доволі практичний: ізольований засіб захисту не дає достатньої стійкості. Шифрування не усуває завад і DDoS-атак; автентифікація не виправляє помилки маршрутизації; моніторинг не компенсує слабкі оновлення прошивки; резервування не захищає облікові записи адміністраторів. Тому захист передачі даних має бути багаторівневим і поєднувати криптографічні, мережеві, радіотехнічні, програмні та організаційні заходи [15].

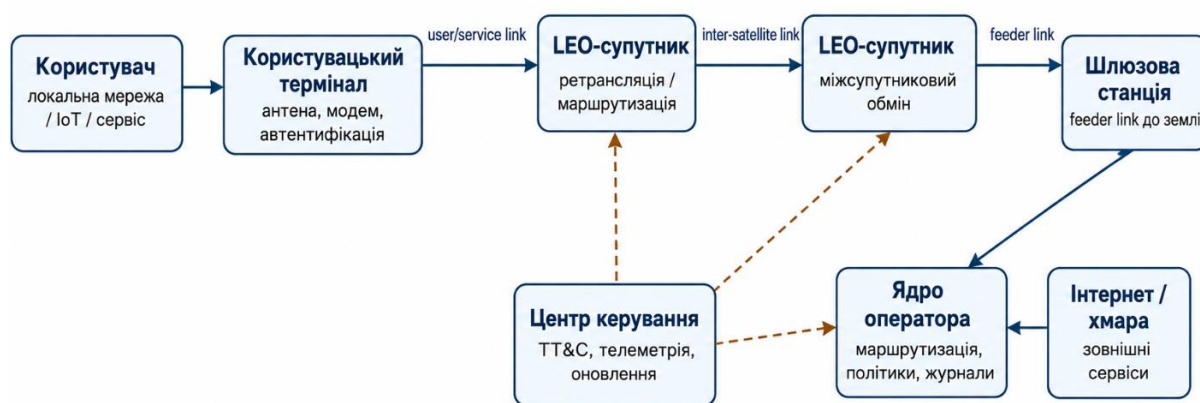
Отже, стан дослідження проблеми показує, що безпека низькоорбітальних супутникових мереж є міждисциплінарним завданням. Для цієї роботи ключовими напрямками є захист каналів передавання, автентифікація учасників обміну, керування ключами, протидія завадам і спуфінгу, безпечна маршрутизація, моніторинг аномалій та захист наземної інфраструктури. Саме ці напрями далі використовуються для аналізу загроз і оцінювання ризику [25].

1.2. Архітектура передачі даних і методичні підходи до її захисту

Архітектура передачі даних у LEO-мережі є розподіленою: трафік проходить через користувацький, космічний, наземний і зовнішній мережевий сегменти. Для безпеки важливо розрізняти не тільки фізичні компоненти, а й типи потоків: користувацькі дані, службову сигналізацію, телеметрію, команди керування, оновлення програмного забезпечення та адміністративний доступ. Коли ці потоки змішуються без сегментації, атака з одного сегмента може перейти в інший [10].

У типових NTN-архітектурах, які розглядає 3GPP, зв'язок між користувацьким обладнанням або VSAT-терміналом і платформою в космосі відбувається через user/service link, а взаємодія супутника з наземною інфраструктурою — через feeder link [22]. Для LEO-мереж додатково важливими є міжсупутникові канали. Вони підвищують гнучкість маршрутизації, але водночас вимагають автентифікації вузлів, контролю цілісності маршрутних повідомлень і захисту службового трафіку.

На практиці передача даних у LEO-мережі відбувається приблизно так: термінал встановлює з'єднання із супутником, мережа перевіряє право доступу, дані проходять через радіоканал до супутника, а далі передаються міжсупутниковим каналом або через шлюзову станцію до наземної IP-мережі, хмари чи іншого користувача. Паралельно працює контур керування: телеметрія, команди, оновлення, синхронізація часу та моніторинг стану вузлів [22].



суцільні лінії — користувацький трафік; пунктир — канали керування та телеметрії

Рисунок 1.3 — Архітектура передачі даних у LEO-супутниковій мережі

З позиції безпеки таку архітектуру варто ділити на площину даних, площину керування та площину адміністрування. Площина даних переносить користувацький трафік. Площина керування відповідає за встановлення з'єднань, маршрутизацію, перемикання між супутниками та службову сигналізацію. Площина адміністрування охоплює конфігурації, оновлення, журнали, ключі й

облікові записи. Компрометація будь-якої площини може вплинути на конфіденційність, цілісність або доступність [5].

Користувацький сегмент охоплює термінали, антени, модеми, локальні маршрутизатори та пристрої кінцевих користувачів. Його ризики зазвичай пов'язані з прошивкою, слабкою автентифікацією, помилковими налаштуваннями, підміною терміналу або використанням абонентського обладнання як точки входу до мережі. Захист має спиратися на унікальну ідентифікацію пристрою, контроль цілісності ПЗ, безпечне оновлення, мінімізацію відкритих сервісів і обмеження адміністративного доступу [12].

Космічний сегмент складається із супутників, які ретранслюють сигнали, маршрутизують трафік, обробляють службові повідомлення і підтримують зв'язок з іншими супутниками або шлюзами. Для LEO характерні часті handover-процедури, зміна видимості апаратів, обмежені енергетичні та обчислювальні ресурси. Тому механізми безпеки мають бути стійкими, але водночас не повинні створювати надмірної затримки чи перевантажувати бортове обладнання [22].

Наземний сегмент включає шлюзові станції, центри керування, мережеве ядро оператора, сервери автентифікації, системи моніторингу, канали підключення до Інтернету і хмарні сервіси. NIST IR 8401 розглядає його як ключову частину космічних операцій, оскільки саме тут виконуються командування, керування, оброблення телеметрії та взаємодія з корисним навантаженням [2]. Через це атака на шлюз або центр керування може порушити роботу мережі навіть без прямого доступу до супутника.

У гібридних супутникових мережах додаткову складність створює взаємодія різних організацій, провайдерів і технологічних доменів. NIST IR 8441 підкреслює, що компоненти таких мереж можуть мати різні рівні довіри, а безпеку потрібно оцінювати не лише для окремих вузлів, а й для інтерфейсів між ними [3]. Для LEO-сервісів це означає потребу чітко визначати межі відповідальності між оператором супутникового сегмента, наземним провайдером, хмарним провайдером і кінцевим користувачем.

Таблиця 1.2

Компоненти архітектури LEO-мережі та вимоги до їх захисту

Компонент	Функція у передачі даних	Ключові ризики	Базові заходи захисту
Користувачький термінал	Доступ користувача до супутникової мережі, формування та приймання трафіку.	Компрометація прошивки, підміна терміналу, несанкціоноване адміністрування.	Ідентифікація пристрою, захищене завантаження, цифровий підпис оновлень, обмеження локального доступу.
Радіоканал користувача	Передавання сигналу між терміналом і супутником.	Перехоплення, завади, спуфінг, деградація сигналу.	Шифрування, завадостійке кодування, спрямовані антени, моніторинг параметрів сигналу.
LEO-супутник	Ретрансляція, обробка службових повідомлень, маршрутизація трафіку.	Порушення цілісності ПЗ, підміна команд, перевантаження ресурсів.	Контроль цілісності, захищені команди, розмежування службового та користувацького трафіку.
Міжсупутниковий канал	Передавання даних між супутниками без негайного виходу на наземний шлюз.	Модифікація маршрутних повідомлень, перенаправлення трафіку, втрата синхронізації.	Автентифікація вузлів, контроль цілісності маршрутів, резервні маршрути, захищені службові протоколи.
Шлюзова станція	З'єднання супутникового сегмента із наземними IP-мережами.	DDoS, компрометація серверів, підміна конфігурацій, фізичний доступ.	Сегментація, IDS/IPS, фільтрація трафіку, резервування, журналювання, контроль доступу.
Центр керування	ТТ&С, телеметрія, оновлення, конфігурації, реагування на інциденти.	Підміна команд, компрометація адміністраторів, витік службових даних.	MFA, принцип мінімальних привілеїв, HSM, шифрування службових каналів, аудит дій.
Зовнішні мережі та хмара	Передавання трафіку до Інтернету, сервісів і корпоративних систем.	Атаки на маршрутизацію, витік даних, шкідливий трафік із зовнішніх мереж.	Захищені протоколи, політики доступу, моніторинг, міжмережеві екрани, перевірка ланцюга довіри.

Наведена структура показує кілька критичних точок контролю. Перша — вхід користувача в мережу, де перевіряються термінал, абонент і право доступу. Друга — радіоканал, де треба зменшити ризики перехоплення та втрати доступності. Третя — маршрутизація в космічному й наземному сегментах. Четверта — вихід до зовнішніх мереж, де супутниковий трафік стає частиною звичайної IP-інфраструктури та підпадає під типові мережеві загрози [5].

Методичний підхід до захисту цієї архітектури має спиратися на принцип *security by design*. Безпека повинна закладатися на етапі проєктування, а не додаватися після розгортання. Для LEO-мереж це особливо важливо: після запуску фізичний доступ до супутника практично неможливий, а помилки в архітектурі ключів, оновлень або командування складно виправляти під час експлуатації [24].

Базовим підходом є сегментація. Користувацький трафік, службова сигналізація, команди керування, телеметрія, оновлення та адміністративні сесії не мають проходити в одному неконтрольованому контурі. Сегментація обмежує наслідки компрометації: атака на термінал не повинна автоматично відкривати доступ до керування супутником або шлюзом. На практиці це реалізується через VLAN/VRF, окремі політики маршрутизації, фільтрацію, ізоляцію службових API та різні рівні довіри [16].

Другий підхід — наскрізний і каналний криптографічний захист. Наскрізне шифрування зберігає зміст користувацьких даних на проміжних ділянках маршруту. Канальний захист потрібен для службових повідомлень, телеметрії, команд і кадрів космічного зв'язку. CCSDS Space Data Link Security Protocol описує застосування служб безпеки до космічних протоколів передавання даних на каналному рівні [4].

Третій підхід стосується керування криптографічними ключами протягом усього життєвого циклу. Недостатньо вибрати стійкий алгоритм; потрібно забезпечити генерацію, розподіл, зберігання, ротацію, відкликання і знищення ключів. У LEO-мережі це ускладнюють велика кількість терміналів, супутників і шлюзів, часті handover-процедури та обмежені ресурси обладнання. Тому потрібні

апаратні модулі безпеки, короткоживучі сеансові ключі, автоматизоване відкликання облікових даних і план постквантової міграції [8; 20].

Четвертий підхід — сильна автентифікація та контроль доступу. Підтверджувати потрібно не лише користувача, а й термінал, супутник, шлюз, службовий процес і адміністратора. Контроль доступу має працювати за принципом мінімальних привілеїв: кожен компонент отримує тільки ті права, які потрібні для його функції. Для операторів центрів керування важливими є багатфакторна автентифікація, журналювання дій і розділення ролей [15; 16].



Рисунок 1.4 — Багаторівнева модель захисту передачі даних у LEO-мережі

П'ятий підхід — захист маршрутизації та процедур handover. Через рух супутників маршрут передачі даних у LEO-мережі змінюється частіше, ніж у наземній мережі. Якщо маршрутні повідомлення не автентифіковані, зловмисник може створити хибний маршрут, перенаправити трафік або перевантажити окремий вузол. Тому потрібні перевірка джерела маршрутної інформації, контроль цілісності таблиць маршрутизації, виявлення нетипових змін шляху, резервні маршрути та обмеження довіри до одного вузла [9].

Шостий підхід пов'язаний зі стійкістю фізичного каналу. Навіть за наявності шифрування передача даних може бути зірвана завадами або спуфінгом. Захист має включати адаптивний вибір частот, формування вузьких променів,

завадостійке кодування, контроль рівня сигналу, виявлення нетипових характеристик радіоефіру та резервування каналів. Для супутникового зв'язку доступність є такою ж критичною, як і конфіденційність [9].

Сьомий підхід — моніторинг, виявлення аномалій і реагування на інциденти. ENISA розглядає кіберзагрози для комерційних супутників протягом усього життєвого циклу, включно з експлуатацією, оновленнями та ланцюгом постачання [6]. Тому моніторинг LEO-мережі має охоплювати не лише IP-трафік, а й телеметрію, спроби автентифікації, зміни маршрутів, стан шлюзів, параметри сигналу, події оновлення та дії адміністраторів. Для реагування доцільно спиратися на підходи NIST SP 800-61 [19].

Восьмий підхід — захищене оновлення програмного забезпечення. Супутники, шлюзи й термінали працюють на складному ПЗ, у якому з часом можуть виявлятися вразливості. Оновлення мають надходити з довірених джерел, підписуватися цифровим підписом, перевірятися перед встановленням і мати механізм відкату. Для супутникових систем це критично, бо помилкове або підмінене оновлення може порушити роботу великої частини мережі [17].

Таблиця 1.3

Методичні підходи до захисту передачі даних у LEO-мережах

Підхід	Що захищає	Основні механізми	Обмеження
Сегментація та Zero Trust	Межі між користувачки м, службовим і адміністративним трафіком.	Мікросегментація, перевірка кожного запиту, мінімальні привілеї, окремі контури керування.	Потребує точного опису ролей, політик і міжсегментних взаємодій.
Криптографічний захист	Конфіденційність і цілісність даних та службових повідомлень.	TLS/IPsec, каналний захист, цифрові підписи, MAC, захищений обмін ключами.	Може збільшувати затримку та навантаження на термінали й бортові системи.
Керування ключами	Стійкість криптографії протягом	PKI, HSM, ротація ключів, відкликання сертифікатів,	Складність масштабування для великої кількості вузлів

Підхід	Що захищає	Основні механізми	Обмеження
	життєвого циклу мережі.	короткоживучі сеансові ключі.	і частих handover.
Захист маршрутизації	Коректність вибору маршруту й міжсупутникового обміну.	Автентифікація маршрутних повідомлень, контроль таблиць, резервні шляхи, аналіз аномалій.	Потрібно враховувати постійну зміну топології та завантаження каналів.
Стійкість радіоканалу	Доступність сервісу в умовах завад і спуфінгу.	Формування променя, адаптивні частоти, завадостійке кодування, контроль параметрів сигналу.	Не усуває потреби в криптографії та не гарантує повний захист від потужного РЕБ.
Моніторинг і реагування	Своєчасне виявлення атак, відмов і неправильних конфігурацій.	IDS/IPS, SIEM, телеметрія, кореляція подій, плани реагування, резервні сценарії.	Високий обсяг подій і потреба в автоматизації аналізу.
Захищене оновлення ПЗ	Цілісність супутників, терміналів, шлюзів і службових систем.	Підпис оновлень, secure boot, перевірка прошивки, контроль версій, відкат.	Помилка в оновленні може масштабно вплинути на працездатність мережі.

Для практичного проєктування безпеки LEO-мережі найбільш придатною є комбінована модель. На фізичному рівні пріоритетом є стійкість до завад і спуфінгу. На каналному рівні — захист кадрів і службових повідомлень. На мережевому рівні — безпечна маршрутизація, фільтрація і сегментація. На транспортному та прикладному рівнях — шифрування сеансів, автентифікація сервісів і контроль доступу. На рівні керування — захист ТТ&С, оновлень, журналів, ключів і адміністративних дій

Для LEO-мереж характерна сильна залежність між сегментами. Надійне шифрування користувацького трафіку не компенсує слабкий пароль адміністратора шлюзу. Захищений радіоканал не прибирає ризик підміни оновлення прошивки. Резервні маршрути не допоможуть, якщо маршрутна

інформація приймається без перевірки джерела. Тому кожен компонент архітектури повинен мати визначену роль, межу довіри, перелік ризиків і набір контролів [16].

Отже, архітектура передачі даних у LEO-супутниковій мережі охоплює термінали, радіоканали, супутники, міжсупутникові лінії, шлюзи, центри керування та зовнішні мережі. Її захист має поєднувати сегментацію, криптографію, сильну автентифікацію, керування ключами, безпечну маршрутизацію, стійкість фізичного каналу, моніторинг, реагування на інциденти й захищені оновлення. Така модель створює основу для аналізу конкретних загроз і вразливостей у другому розділі.

1.3. Критерії оцінювання захищеності передачі даних у LEO-мережах

Оцінювати захищеність передачі даних у LEO-мережах потрібно не лише за фактом наявності окремих засобів захисту. Важливіше зрозуміти, наскільки стійкою є вся архітектура на маршруті від терміналу до зовнішньої мережі. Такий підхід близький до методик оцінювання ризику, де враховуються активи, загрози, вразливості, наслідки та чинні контролі [13].

Перший критерій — конфіденційність. Перехоплення сигналу або мережевого трафіку не повинно відкривати зловмиснику зміст переданої інформації. Для цього використовують шифрування каналів зв'язку, захищений обмін ключами, ізоляцію службового трафіку і контроль доступу до критичних вузлів мережі [20].

Другий критерій — цілісність даних. У LEO-мережах потрібно гарантувати, що користувацькі повідомлення, службові команди, маршрутна інформація і параметри керування не були змінені під час передавання. Порушення цілісності може призвести до неправильного маршрутування, втрати з'єднання або виконання несанкціонованих команд. Для захисту застосовують цифрові підписи, контрольні коди, автентифікацію службових повідомлень і захищені протоколи

Третій критерій — доступність. Супутникова мережа повинна підтримувати зв'язок навіть за технічних збоїв, перевантаження, радіоелектронного придушення або атак на наземну інфраструктуру. Для цього потрібні резервування каналів, альтернативні маршрути, моніторинг стану вузлів, захист від DDoS-атак і механізми швидкого відновлення сервісу [5].

Окремо слід оцінювати автентичність учасників обміну. Система має перевіряти легітимність терміналів, супутників, шлюзових станцій, адміністраторів і службових сервісів. Недостатня автентифікація створює ризик підміни вузла, спуфінгу сигналу, несанкціонованого підключення або атаки типу «людина посередині»

Важливим критерієм є захищеність керування мережею. Канали телеметрії, команд, оновлення програмного забезпечення та адміністрування мають бути відокремлені від звичайного користувацького трафіку. Компрометація систем керування може вплинути не на один сеанс зв'язку, а на роботу всієї мережі [2].

Для LEO-мереж також потрібно враховувати стійкість до загроз фізичного рівня. Відкритий радіоканал створює ризики перехоплення, спуфінгу, завад і радіоелектронного придушення. Тому оцінювання захищеності має включати перевірку завадостійкості, спрямованості антен, резервування частот і здатності системи виявляти аномальні параметри сигналу [9].

Ще один критерій — масштабованість захисту. Сучасні LEO-сузір'я можуть містити багато супутників і обслуговувати значну кількість користувачів. Засоби безпеки не повинні створювати надмірну затримку, знижувати пропускну здатність або ускладнювати маршрутизацію. Отже, ефективний захист має поєднувати надійність, продуктивність і здатність працювати в умовах динамічної топології [22].

У підсумку захищеність передачі даних у LEO-мережах варто оцінювати за такими критеріями: конфіденційність, цілісність, доступність, автентичність, захищеність керування, стійкість до фізичних атак і масштабованість. Комплексне врахування цих критеріїв переводить аналіз від загального опису засобів захисту до практичного оцінювання ризиків і вразливостей [18].

Висновки до розділу 1

У першому розділі розглянуто теоретико-методичну основу безпеки передачі даних у низькоорбітальних супутникових мережах. Показано, що LEO-мережі є важливою частиною сучасної телекомунікаційної інфраструктури, оскільки можуть забезпечувати зв'язок із меншою затримкою, ніж геостаціонарні системи, і застосовуватися для доступу до Інтернету, критичної інфраструктури, військового зв'язку, транспорту та Інтернету речей.

Встановлено, що архітектура LEO-мережі складається з користувацького, космічного і наземного сегментів. Дані проходять через термінал, супутники, міжсупутникові канали, шлюзові станції, центр керування та зовнішню мережеву інфраструктуру. Кожен елемент має власні вразливості, тому захист не може обмежуватися лише шифруванням каналу.

Обґрунтовано, що основними напрямками безпеки є криптографічний захист, автентифікація користувачів і пристроїв, контроль доступу, захист маршрутизації, моніторинг трафіку, безпечне оновлення програмного забезпечення та захист наземної інфраструктури. Окремо потрібно враховувати загрози фізичного рівня: перехоплення сигналу, спуфінг і радіоелектронне придушення.

У розділі визначено критерії оцінювання захищеності передачі даних: конфіденційність, цілісність, доступність, автентичність, стійкість до атак, захищеність керування мережею та масштабованість. Вони дають змогу оцінити не лише наявність окремих засобів захисту, а й реальну здатність LEO-мережі протидіяти актуальним загрозам.

Безпека передачі даних у низькоорбітальних супутникових мережах має розглядатися як комплексне завдання. Ефективний результат можливий лише тоді, коли технічні, криптографічні, мережеві, радіотехнічні та організаційні заходи працюють разом. Це створює основу для подальшого аналізу загроз, вразливостей і методів захисту у другому розділі.

РОЗДІЛ 2 АНАЛІЗ ЗАГРОЗ, ВРАЗЛИВОСТЕЙ ТА МЕТОДІВ ЗАХИСТУ ДАНИХ У LEO-СУПУТНИКОВИХ МЕРЕЖАХ

2.1. Класифікація загроз безпеці передачі даних у LEO-супутникових мережах

Передача даних у LEO-супутникових мережах проходить через кілька пов'язаних сегментів: термінал користувача, радіоканал, супутниковий сегмент, міжсупутникові канали, наземні шлюзи, центр керування та зовнішню мережеву інфраструктуру. Через таку будову загрози не обмежуються перехопленням сигналу. Вони можуть виникати на фізичному, каналному, мережевому, прикладному та організаційному рівнях, що підтверджується сучасними оглядами загроз для космічних систем [6].

До першої групи належать загрози фізичного рівня: перехоплення радіосигналу, радіоелектронне придушення, навмисні завади, спуфінг і порушення стабільності каналу. Оскільки LEO-зв'язок використовує відкритий радіоканал, злоумисник може намагатися приймати сигнал, аналізувати його параметри або впливати на якість зв'язку. Навіть зашифровані дані вразливі до атак, які спрямовані не на зміст, а на доступність сервісу [9].

Друга група пов'язана з користувацькими терміналами. Кінцеве обладнання може бути скомпрометоване через слабку автентифікацію, вразливу прошивку, небезпечні налаштування, несанкціоноване оновлення або фізичний доступ до пристрою. Небезпека полягає в тому, що скомпрометований термінал може виглядати для мережі легітимним і використовуватися як точка входу [12].

Третя група охоплює загрози супутниковому та міжсупутниковому сегментам. Це порушення маршрутизації, підміна службових повідомлень, несанкціонований доступ до каналів керування, атаки на програмне забезпечення супутника і спроби впливу на міжсупутниковий обмін. Оскільки топологія LEO-

мережі постійно змінюється, незахищена маршрутизація може призвести до перенаправлення трафіку або втрати якості каналу [3].

Четверта група стосується наземної інфраструктури. Шлюзові станції, центри керування, сервери автентифікації, системи журналювання та адміністративні інтерфейси є критичними елементами мережі. Атаки на них можуть виконуватися через шкідливе ПЗ, DDoS, компрометацію облікових записів, помилки конфігурації або незахищений доступ. Практично наземний сегмент часто доступніший для зловмисника, ніж сам космічний апарат [2].

П'ята група охоплює загрози мережевого та прикладного рівнів: перехоплення IP-трафіку, атаки типу «людина посередині», підміну DNS-запитів, експлуатацію вразливостей сервісів, несанкціонований доступ до хмарної інфраструктури і порушення політик маршрутизації. Для користувача це може проявлятися як витік даних, підміна ресурсу, зниження швидкості або недоступність сервісу [5].

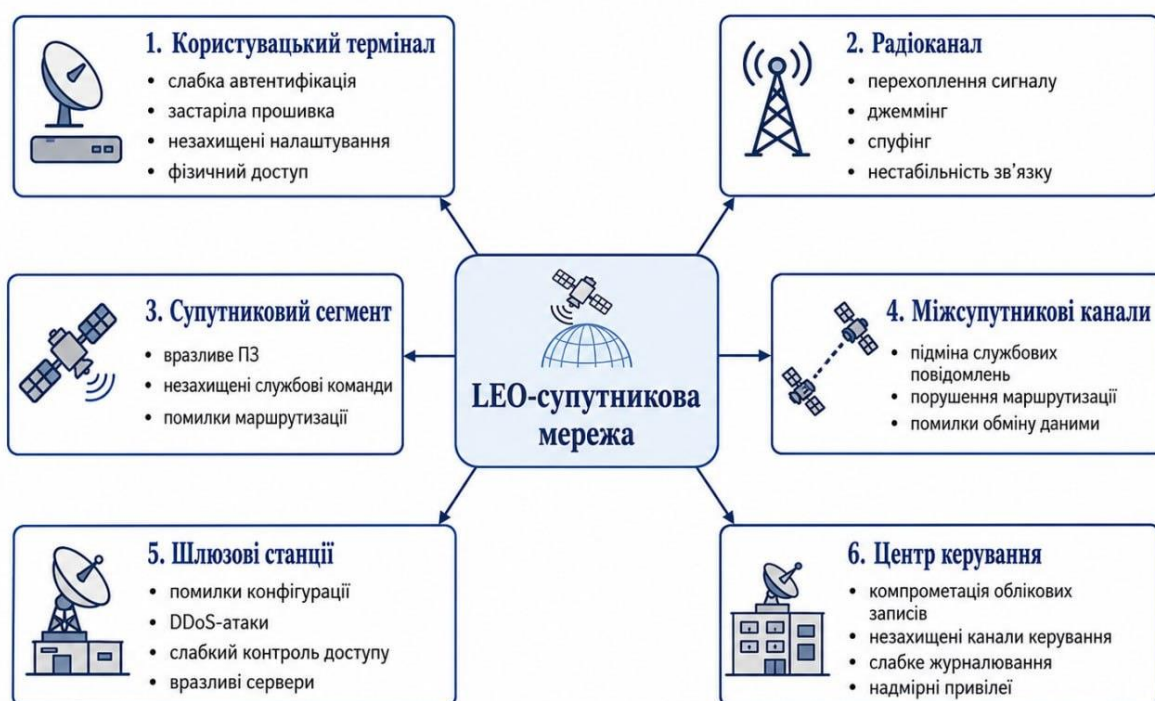
Окремо слід виділити організаційні загрози. Вони виникають через слабкі паролі, помилки адміністрування, недостатній контроль доступу, відсутність регулярного аудиту, несвоєчасні оновлення або слабку підготовку персоналу. Для супутникових мереж такі помилки особливо небезпечні, бо неправильне налаштування наземного сегмента або систем керування може вплинути на велику кількість користувачів [19].

Загрози для LEO-супутникових мереж потрібно розглядати не окремими списками, а у взаємозв'язку між сегментами. Компрометація терміналу може стати першим кроком атаки на мережеві ресурси, а збій або захоплення шлюзової станції здатні вплинути на доступність сервісу в регіоні. Такий погляд допомагає точніше визначати критичні точки архітектури і добирати методи захисту для кожного рівня [23].

2.2. Аналіз вразливостей основних компонентів LEO-супутникової мережі

Вразливості LEO-супутникової мережі пов'язані з її неоднорідністю. У ній поєднуються термінали користувачів, радіоканал, супутниковий сегмент, міжсупутникові канали, наземні шлюзи, центри керування та зовнішня мережева інфраструктура. Порушення безпеки одного елемента може відбитися на всьому маршруті передавання даних, тому аналіз потрібно проводити за сегментами [12].

Основні вразливості компонентів LEO-супутникової мережі



Складено автором

Рисунок 2.1 — Основні вразливості компонентів LEO-супутникової мережі

Користувацький термінал є одним із найбільш доступних для атаки елементів мережі. Він розміщується у користувача, тому може стати об'єктом фізичного доступу, неправильного налаштування або компрометації ПЗ. Типові вразливості — слабка автентифікація, застаріла прошивка, відсутність перевірки цілісності оновлень, незахищений локальний інтерфейс і слабкі паролі [16].

Радіоканал між терміналом і супутником уразливий через сам характер середовища передавання. Сигнал поширюється у просторі, тож його можуть намагатися перехопити, заглушити або підмінити. Навіть коли зміст даних зашифрований, зловмисник здатний аналізувати час передавання, інтенсивність трафіку, параметри сигналу або впливати на доступність каналу [9].

Супутниковий сегмент має власні обмеження: невеликі ресурси бортового обладнання, складність оновлення ПЗ і залежність від команд керування. Супутник може ретранслювати, маршрутизувати і обробляти службові повідомлення. Якщо службові канали або програмне забезпечення захищені недостатньо, виникає ризик порушення маршрутизації, помилкової обробки даних або втручання в роботу мережі [11].

Міжсупутникові канали дають змогу передавати дані між апаратами без негайного виходу на наземну станцію. Це підвищує гнучкість мережі, але водночас додає ризики для маршрутизації та цілісності службових повідомлень. Уразливими можуть бути механізми встановлення з'єднання, автентифікації вузлів, оновлення маршрутної інформації та обробки відмов [22].

Наземні шлюзові станції є вузлами, через які супутникова мережа взаємодіє з наземними телекомунікаційними системами та Інтернетом. Їхні вразливості нагадують проблеми традиційної мережевої інфраструктури: помилки конфігурації, незахищені адміністративні інтерфейси, вразливості серверів, недостатня фільтрація трафіку, слабкий контроль доступу і ризик DDoS-атак

Центр керування є одним із найчутливіших елементів LEO-мережі. Через нього здійснюються моніторинг супутників, обробка телеметрії, передавання команд, оновлення програмного забезпечення та керування параметрами мережі. Найнебезпечнішими тут є компрометація облікових записів адміністраторів, слабе розмежування прав, відсутність багатофакторної автентифікації, незахищені канали керування і недостатнє журналювання

Зовнішня мережева інфраструктура також впливає на загальну безпеку LEO-мережі. Після виходу зі шлюзової станції трафік може проходити через магістральні канали, хмарні сервіси, DNS-інфраструктуру і системи

автентифікації. Якщо ці компоненти налаштовані неналежно, рівень безпеки передачі даних знижується навіть за надійного захисту супутникового каналу [3].

Вразливості різних сегментів часто посилюють одна одну. Наприклад, слабкий захист терміналу може бути використаний для несанкціонованого доступу до мережі, а помилка в конфігурації шлюзу — для перенаправлення або перехоплення трафіку. Тому під час аналізу потрібно враховувати не лише окремі компоненти, а й зв'язки між ними

Практичний сенс такого аналізу полягає у визначенні найбільш критичних точок захисту: терміналів, радіоканалу, службових каналів керування, шлюзових станцій і систем адміністрування. Подальший вибір методів захисту має залежати від того, які саме вразливості найбільше впливають на конфіденційність, цілісність і доступність даних у конкретному сегменті [18].

2.3. Методи захисту передачі даних у LEO-супутникових мережах

Захист передачі даних у LEO-супутникових мережах має будуватися не на одному засобі, а на поєднанні кількох груп методів. Саме шифрування є необхідним, але воно не закриває ризики радіоканалу, маршрутизації, керування мережею, користувацьких терміналів і наземної інфраструктури. Така логіка відповідає підходу NIST до вибору контролів безпеки [15].

Перший базовий метод — криптографічний захист. Його завданням є забезпечення конфіденційності й цілісності інформації під час передавання через супутниковий канал. Для цього використовують симетричне шифрування, асиметричну криптографію, цифрові підписи, хеш-функції та захищений обмін ключами. У LEO-мережах ці механізми мають бути стійкими, але не створювати надмірної затримки для динамічної топології

Другий метод — автентифікація учасників обміну. Вона потрібна для перевірки терміналів, супутників, шлюзових станцій, адміністраторів і службових сервісів. Якщо перевірка слабка, виникає ризик підміни вузла, спуфінгу сигналу

або несанкціонованого доступу до ресурсів. Для зменшення цих ризиків застосовують сертифікати, криптографічні ключі, апаратні модулі безпеки, багатфакторну автентифікацію та мінімальні привілеї [21].

Третій напрям — захист радіоканалу. Оскільки LEO-мережі працюють у відкритому середовищі, потрібно забезпечувати стійкість до перехоплення, спуфінгу та радіоелектронного придушення. Для цього застосовують спрямовані антени, формування променя, завадостійке кодування, резервування частот, контроль рівня сигналу і виявлення аномалій у радіоефірі [9].

Четвертий метод — захист маршрутизації. У LEO-мережах маршрути змінюються через рух супутників, завантаження каналів і стан шлюзових станцій. Якщо маршрутна інформація не захищена, зломисник може спробувати перенаправити трафік, створити хибний маршрут або погіршити якість зв'язку. Тому потрібні автентифікація маршрутних повідомлень, контроль цілісності таблиць, резервні маршрути і моніторинг нетипових змін [9].

Окреме значення має захист наземної інфраструктури. Шлюзові станції, центри керування, сервери автентифікації та системи адміністрування потрібно захищати так само ретельно, як і супутниковий сегмент. Основні заходи — сегментація мережі, фільтрація трафіку, IDS/IPS, контроль доступу адміністраторів, журналювання, резервне копіювання та регулярні оновлення

Важливим методом є безпечне оновлення програмного забезпечення. Супутники, шлюзові станції і термінали використовують програмні компоненти, в яких можуть з'являтися вразливості. Оновлення мають бути підписані, перевірятися на цілісність і надходити лише з довірених джерел. Додатково потрібні безпечне завантаження, контроль версій і можливість відновлення після помилкового або скомпрометованого оновлення [17].

Моніторинг і виявлення аномалій є обов'язковими, бо масштабну LEO-мережу неможливо контролювати вручну. Система безпеки має аналізувати спроби автентифікації, зміну маршрутів, рівень сигналу, навантаження на шлюзи, службові повідомлення і поведінку терміналів. У разі відхилень вона повинна формувати сповіщення або запускати захисні дії

Отже, захист передачі даних у LEO-супутникових мережах має бути багаторівневим. Криптографія забезпечує конфіденційність і цілісність, автентифікація обмежує доступ, захист радіоканалу підтримує доступність, а моніторинг дає змогу швидше помічати атаки. Найкращий результат дає поєднання цих методів, бо кожен із них закриває свою групу ризиків

2.4. Порівняльна оцінка методів захисту даних у LEO-мережах

Методи захисту передачі даних у LEO-мережах відрізняються за призначенням, впливом на безпеку та складністю впровадження. Одні засоби захищають конфіденційність, інші — автентифікацію, доступність, маршрутизацію або контроль стану мережі. Тому оцінювати їх потрібно не ізольовано, а за тим, які саме загрози вони зменшують і як працюють разом [23].

Таблиця 2.1

Порівняльна оцінка методів захисту даних у LEO-мережах

Метод захисту	Основне призначення	Обмеження
Шифрування даних	Захист конфіденційності трафіку	Не усуває завади та атаки на доступність
Автентифікація вузлів	Перевірка легітимності терміналів, супутників і шлюзів	Потребує надійного керування ключами
Захист радіоканалу	Протидія спуфінгу, перехопленню та придушенню сигналу	Залежить від апаратних можливостей обладнання
Безпечна маршрутизація	Захист від перенаправлення або підміни маршрутів	Ускладнюється динамічною топологією LEO-мережі
Моніторинг і IDS/IPS	Виявлення аномалій, атак і підозрілої активності	Потребує якісного журналювання та аналізу подій
Безпечне оновлення ПЗ	Захист прошивок і службового програмного забезпечення	Потребує перевірки підписів і контролю версій

З таблиці видно, що жоден метод не забезпечує повний захист самостійно. Шифрування потрібне для захисту змісту даних, але воно не запобігає

радіоелектронному придушенню або DDoS-атакам. Автентифікація зменшує ризик підміни вузлів, однак її ефективність залежить від безпечного зберігання ключів і своєчасного відкликання скомпрометованих облікових даних [20].

Захист радіоканалу для LEO-мереж має особливе значення, бо передача даних відбувається через відкрите середовище. Спрямовані антени, завадостійке кодування, контроль параметрів сигналу і резервування частот допомагають знизити ризик втрати зв'язку. Водночас ці методи не замінюють криптографію, оскільки переважно працюють на доступність і стійкість каналу [9].

Безпечна маршрутизація важлива через постійний рух супутників і зміну маршрутів передавання даних. Якщо службові маршрутні повідомлення не захищені, зловмисник може створити умови для перенаправлення трафіку або погіршення якості зв'язку. Тому маршрутизація має поєднувати автентифікацію повідомлень, контроль цілісності і резервні шляхи

Моніторинг, журналювання та системи виявлення вторгнень потрібні для своєчасного виявлення інцидентів. Вони дають змогу аналізувати спроби входу, зміну маршрутів, аномалії трафіку, навантаження на шлюзи та порушення параметрів радіоканалу. Ефективність таких засобів залежить від якості зібраних даних і здатності відрізнити реальну атаку від штатної зміни стану мережі

Для LEO-супутникових мереж найбільш доцільним є комбінований підхід: шифрування захищає дані, автентифікація перевіряє вузли, захист радіоканалу підтримує доступність, безпечна маршрутизація стабілізує доставку трафіку, а моніторинг допомагає виявляти інциденти. Така модель зменшує ризики на різних рівнях архітектури і підвищує загальну стійкість передачі даних [15].

2.5. Оцінка ризиків реалізації загроз у LEO-супутникових мережах

Оцінка ризиків у LEO-супутникових мережах потрібна для того, щоб відрізнити справді критичні загрози від другорядних. Не всі події мають однаковий вплив: одні лише тимчасово погіршують якість зв'язку, інші можуть

спричинити витік даних, втрату керованості або порушення роботи значної частини мережі. Такий підхід відповідає загальній логіці NIST SP 800-30 та ISO/IEC 27005

Ризик доцільно оцінювати за двома параметрами: ймовірністю реалізації загрози та рівнем її наслідків. Ймовірність залежить від доступності цілі, складності атаки, наявних вразливостей і чинних контролів. Наслідки визначаються впливом на конфіденційність, цілісність і доступність даних. Для класифікації критичності також можна враховувати підходи FIPS 199 та ETSI TVRA [23].



Рисунок 2.2 — Узагальнена схема ключових ризиків у LEO-супутникових мережах

Найвищий рівень ризику мають атаки на наземну інфраструктуру та центр керування. Шлюзові станції, сервери, системи адміністрування й облікові записи персоналу зазвичай доступніші для кіберзлочинців, ніж космічний сегмент. Компрометація таких елементів може вплинути на маршрутизацію, автентифікацію користувачів, обробку трафіку або передавання службових команд

Високий ризик мають і атаки на доступність: радіоелектронне придушення, DDoS на шлюзові станції та перевантаження каналів. Для LEO-мереж доступність є критичною, бо такі системи можуть підтримувати зв'язок у віддалених регіонах,

у критичній інфраструктурі, військових задачах і аварійному реагуванні. Навіть коротка втрата зв'язку може мати суттєві наслідки [19].

Загрози, пов'язані з перехопленням трафіку, зазвичай мають середній рівень ризику, якщо в мережі використовується сучасне шифрування. Сам факт перехоплення сигналу не обов'язково розкриває зміст даних. Проте зловмисник може аналізувати метадані, інтенсивність трафіку, часові характеристики або структуру з'єднань, тому навіть зашифрований трафік потребує додаткового захисту від кореляційного аналізу

Окрему групу ризиків становить компрометація користувацьких терміналів. Її ймовірність відносно висока через фізичну доступність обладнання, типові конфігурації або несвоєчасне оновлення прошивки. Наслідки часто є локальними, але без сегментації та належного контролю доступу скомпрометований термінал може стати стартовою точкою для подальших атак [16].

Ризики для супутникового та міжсупутникового сегментів мають нижчу ймовірність, але потенційно високі наслідки. Атаки на службові повідомлення, маршрутизацію або бортове програмне забезпечення складніші у виконанні, однак у разі успіху можуть порушити роботу окремих маршрутів або стабільність обміну між супутниками

Для зменшення ризиків потрібен пріоритетний підхід. Передусім слід захищати наземні шлюзи, центр керування, системи автентифікації, канали керування і механізми оновлення ПЗ. Далі посилюються захист радіоканалу, безпечна маршрутизація, моніторинг аномалій і контроль користувацьких терміналів. Така послідовність відповідає логіці управління ризиками та реагування на інциденти [19].

Оцінювання ризиків показує, що для LEO-супутникових мереж небезпечними є не лише технічно складні атаки на космічний сегмент. Часто більш реалістичними є атаки на наземну інфраструктуру, керування, доступність і кінцеві пристрої. Тому система захисту має враховувати ймовірність атак, можливі наслідки та критичність кожного компонента для безперервної передачі даних [25].

Висновки до розділу 2

У другому розділі проаналізовано основні загрози, вразливості та методи захисту передачі даних у LEO-супутникових мережах. Показано, що ризики формуються не тільки в радіоканалі, а й у користувацькому, супутниковому, міжсупутниковому та наземному сегментах. Найбільш небезпечними є загрози, які одночасно зачіпають конфіденційність, цілісність і доступність.

Аналіз показав, що вразливості терміналів, шлюзових станцій, центрів керування, маршрутизації та систем оновлення можуть суттєво знижувати загальний рівень захищеності LEO-мережі. Особливу увагу слід приділяти наземній інфраструктурі, бо вона доступніша для типових кібератак і водночас виконує критичні функції керування, автентифікації та оброблення трафіку.

Визначено, що ефективний захист має спиратися на поєднання криптографічних, мережевих, радіотехнічних, програмних та організаційних заходів. До пріоритетних методів належать шифрування, автентифікація вузлів, контроль доступу, сегментація, захист маршрутизації, моніторинг аномалій, резервування каналів і захищене оновлення програмного забезпечення.

Результати розділу підводять до потреби формалізовано оцінювати ризик, а не лише перелічувати загрози. Тому в третьому розділі обґрунтовується алгоритм оцінювання ризику передачі даних у LEO-мережі та реалізується програмний засіб, який показує рівень небезпеки і формує практичні рекомендації щодо підвищення захищеності каналу зв'язку.

РОЗДІЛ 3 НАУКОВЕ ОБҐРУНТУВАННЯ ПРОПОЗИЦІЙ І РОЗРОБКА ПРОГРАМНОГО ЗАСОБУ

3.1. Постановка задачі та функціональні вимоги до LEO Shield Analyzer

Практична частина роботи присвячена створенню LEO Shield Analyzer — невеликого програмного засобу для попереднього оцінювання ризику передачі даних у LEO-мережі. Його логіка спирається не на загальне враження про «безпечність» системи, а на конкретні контрольні параметри. У попередніх розділах було показано, що слабе місце може з'явитися в радіоканалі, терміналі, шлюзовій станції, каналі керування, автентифікації або процедурах оновлення. Тому програма працює як проста система підтримки рішення: користувач задає умови, а застосунок показує рівень ризику [25].

LEO Shield Analyzer не є інструментом технічного сканування і не підключається до реального супутникового обладнання. Його призначення інше: зібрати в одному інтерфейсі ключові фактори безпеки, дати їм зрозумілу оцінку і сформулювати рекомендації. Через це програму можна використовувати для навчального аналізу, порівняння сценаріїв і демонстрації того, як окремі засоби захисту впливають на підсумковий ризик.

Користувач працює не з абстрактною анкетой, а зі сценаріями, наближеними до реального використання LEO-зв'язку. У програмі передбачено чотири варіанти: цивільний доступ до мережі, канал критичної інфраструктури, службовий канал керування та мобільна група реагування. Для кожного сценарію важливі різні акценти: масовість і стабільність сервісу, безперервність, цілісність команд або швидке розгортання в нестабільних умовах.

Після вибору сценарію користувач оцінює вісім контролів безпеки. Такий набір не перевантажує інтерфейс, але охоплює основні сторони захисту LEO-каналу: шифрування, автентифікацію, термінал, радіоканал, наземний сегмент, моніторинг, резервування і безпечне оновлення ПЗ. Для кожного контролю

використовується шкала 0-3, де 0 означає відсутній або дуже слабкий захист, а 3 — належно реалізований контроль [15].

Головне завдання програми — перетворити ці оцінки на інтегральний показник ризику. При цьому результат не має бути сухим числом. Користувач повинен бачити рівень ризику, розуміти, які контролю найбільше погіршують ситуацію, і отримувати підказку, що варто покращити першочергово. Саме це робить LEO Shield Analyzer ближчим до практичного аналітичного інструмента, ніж до звичайної таблиці з балами.

Таблиця 3.1

Функціональні вимоги до програмного засобу LEO Shield Analyzer

Вимога	Зміст вимоги
Вибір сценарію	Користувач обирає один із типових сценаріїв використання LEO-каналу: цивільний доступ, критична інфраструктура, службовий канал керування або мобільна група реагування.
Оцінювання контролів	Програма приймає оцінки восьми контролів безпеки за шкалою від 0 до 3.
Розрахунок ризику	Система перетворює оцінки контролів на інтегральний показник ризику з урахуванням ваг.
Визначення рівня	Показник ризику класифікується як низький, середній, високий або критичний.
Пояснення результату	Користувач бачить, які контролю найбільше вплинули на підсумкову оцінку.
Рекомендації	Програма формує практичні поради щодо зменшення ризику для вибраного сценарію.
Порівняння	Користувач може порівняти сценарії між собою та побачити, де ризик є найбільшим.

Нефункціональні вимоги пов'язані з простим запуском, зрозумілим інтерфейсом і локальною роботою без передавання даних у зовнішні сервіси. Оскільки засіб має демонстраційне й аналітичне призначення, він повинен відкриватися у браузері як звичайний HTML-файл, не вимагати серверної частини та не залежати від спеціального обладнання.

Отже, задача полягає у створенні легкого вебзастосунку, який дає змогу вибрати сценарій, оцінити вісім контролів безпеки, розрахувати ризик, визначити його рівень і отримати рекомендації. Така постановка природно переходить в архітектуру програми: інтерфейс збирає дані, модулі обробки їх аналізують, а блок звіту перетворює результат на практичний висновок.

3.2. Проектування архітектури програмного засобу

Архітектура LEO Shield Analyzer спроектована так, щоб кожна частина програми виконувала свою функцію і не змішувала введення даних, розрахунків та виведення результатів. Для невеликого вебзастосунку це теж важливо: у майбутньому можна додати нові сценарії, змінити ваги контролів або розширити рекомендації без повного переписування коду.

Логіка роботи програми є послідовною. Спочатку користувач відкриває інтерфейс і вибирає сценарій. Потім програма завантажує типові ваги та стартові параметри. Далі користувач оцінює контролі безпеки, а модуль розрахунку визначає інтегральний ризик. На завершення модуль рекомендацій формує висновок, а блок звіту показує результат у вигляді тексту, таблиці та порівняння.

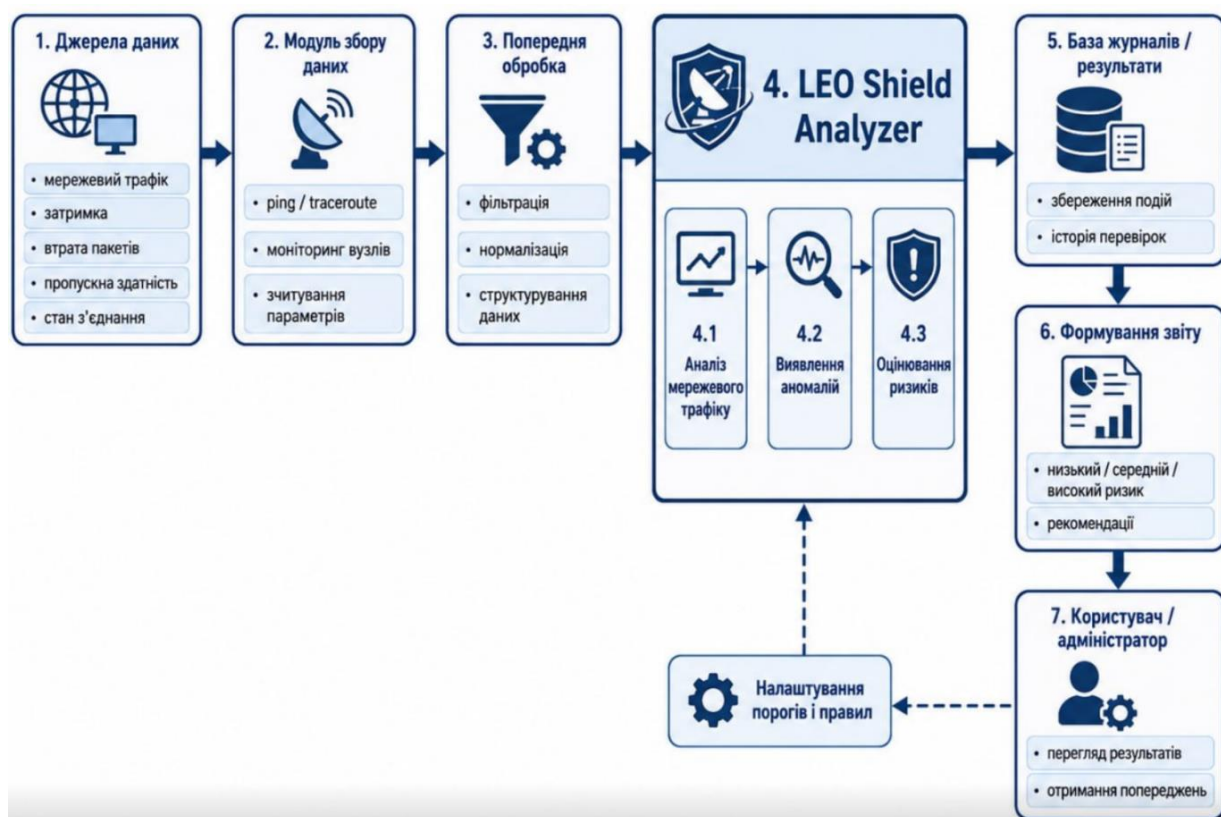


Рисунок 3.1 — Структурна схема роботи програмного засобу LEO Shield Analyzer

Інтерфейс користувача відповідає за взаємодію з програмою. У ньому розміщено вкладки, вибір сценарію, елементи керування оцінками контролів і блоки результатів. Користувач одразу бачить, який сценарій обрано, які контролі оцінюються і як змінюється підсумковий ризик після коригування параметрів.

Модуль вибору сценарію зберігає типові профілі. Сценарій змінює не лише назву ситуації, а й ваги контролів. Наприклад, для службового каналу керування важливішими є автентифікація, цілісність команд і захист наземного сегмента. Для мобільної групи реагування більшу роль відіграють доступність, резервування і стійкість радіоканалу.

Модуль оцінювання контролів приймає значення від 0 до 3. Така шкала достатньо проста для ручного введення, але дозволяє відрізнити повну відсутність захисту від частково реалізованого або достатнього контролю. У програмі кожна оцінка має коротке пояснення, щоб користувач не вгадував, що саме означає вибране значення.

Модуль розрахунку ризику переводить оцінки контролів у числовий показник. Оскільки вища оцінка означає кращий захист, ризик для контролю визначається як різниця між максимальним балом і фактичною оцінкою. Далі цей ризик множиться на вагу контролю, після чого програма отримує нормований відсоток ризику. Такий підхід відповідає базовій логіці зваженого оцінювання ризиків [13].

Модуль рекомендацій аналізує слабкі контролі і добирає поради, які мають практичний сенс саме для обраного сценарію. Якщо слабким місцем є шифрування, рекомендація стосується сучасних протоколів і керування ключами. Якщо проблемним є резервування, програма радить підготувати альтернативний маршрут або канал зв'язку. Завдяки цьому рекомендації не виглядають однаковими для всіх ситуацій.

Таблиця 3.2

Основні модулі програмного засобу LEO Shield Analyzer

Модуль	Призначення	Результат роботи
Інтерфейс користувача	Забезпечує вибір сценарію, зміну оцінок контролів і перегляд результатів.	Користувач бачить панель оцінювання та підсумковий рівень ризику.
Модуль вибору сценарію	Завантажує профіль сценарію та ваги контролів.	Програма враховує специфіку цивільного, критичного, службового або мобільного сценарію.
Модуль оцінювання контролів	Приймає бали восьми контролів за шкалою 0-3.	Формується набір вхідних даних для розрахунку ризику.
Модуль розрахунку	Обчислює інтегральний показник ризику з	Отримується числовий відсоток ризику та його

Модуль	Призначення	Результат роботи
ризик	урахуванням ваг.	рівень.
Модуль рекомендацій	Визначає найслабші контролю та підбирає поради.	Користувач отримує практичні напрями зменшення ризику.
Звіт і порівняння	Подає результати у вигляді підсумку, матриці та порівняння сценаріїв.	Результати можна використати для аналізу та пояснення висновків.

Отже, архітектура LEO Shield Analyzer повторює логіку реального аналітичного процесу: від вибору ситуації до висновку. Це робить програму зрозумілою для користувача і водночас залишає простір для подальшого розвитку.

3.3. Алгоритм оцінювання ризику передачі даних у LEO-мережі

Алгоритм оцінювання ризику поєднує дві ідеї: бальну оцінку контролів і вагове врахування їх важливості. Бал показує, наскільки добре реалізований конкретний контроль, а вага — наскільки цей контроль важливий у вибраному сценарії. Тому однакова слабкість може мати різний вплив: наприклад, відсутність резервування критичніша для мобільної групи реагування, ніж для звичайного домашнього доступу [13].

У програмі використано шкалу від 0 до 3. Значення 0 означає, що контроль відсутній або майже не працює. Значення 1 відповідає мінімальному рівню, коли певний механізм є, але його недостатньо для стійкого захисту. Значення 2 означає прийнятний стан, а 3 — добре реалізований контроль. Така шкала проста для введення і не створює ілюзії надмірної точності, що важливо для експертного попереднього оцінювання [23].

Таблиця 3.3

Шкала оцінювання контролів безпеки

Бал	Стан контролю	Пояснення
0	Відсутній або слабкий	Контроль фактично не захищає канал або реалізований формально.
1	Мінімальний	Механізм є, але має суттєві обмеження або залежить від ручних дій.
2	Достатній	Контроль працює у типовому режимі, але має простір для посилення.
3	Сильний	Контроль реалізований повно, регулярно перевіряється і підтримується.

Ризик за окремим контролем визначається за принципом зворотної оцінки. Якщо контроль має високий бал, його внесок у ризик менший; якщо оцінка низька, внесок зростає. Для цього використовується нормована величина: $r_i = (3 - c_i) / 3$, де c_i — оцінка контролю від 0 до 3, а r_i — частковий ризик за цим контролем [18].

Підсумковий ризик розраховується як нормована зважена сума часткових ризиків: $R = (\sum(w_i \cdot r_i) / \sum w_i) \cdot 100$, де w_i — вага контролю у вибраному сценарії. Ділення на суму ваг є важливим, бо формула залишається коректною навіть тоді, коли вагові коефіцієнти згодом будуть уточнені або змінені.

Таблиця 3.4

Вісім контролів безпеки, використаних в алгоритмі

Контроль	Що оцінюється
Шифрування даних	Наявність захищених протоколів, актуальність алгоритмів і керування ключами.
Автентифікація та	Перевірка користувачів, терміналів, адміністраторів і

Контроль	Що оцінюється
доступ	службових вузлів.
Користувацький термінал	Стан прошивки, локальні налаштування, фізична доступність і захищене завантаження.
Радіоканал	Стійкість до перехоплення, спуфінгу, завад і деградації сигналу.
Наземний сегмент	Захист шлюзів, центрів керування, серверів і адміністративних інтерфейсів.
Моніторинг	Збір подій, виявлення аномалій, журналювання та реагування.
Резервування	Наявність альтернативного каналу, маршруту або шлюзової станції.
Оновлення ПЗ	Регулярність оновлень, цифровий підпис і контроль цілісності.

Таблиця 3.5

Рівні інтерпретації інтегрального показника ризику

Діапазон	Рівень	Зміст результату
0-24 %	Низький	Сценарій має прийнятний рівень захисту; потрібна підтримка поточного стану.
25-49 %	Середній	Є слабкі місця, але вони не формують критичної ситуації за умови своєчасного усунення.
50-74 %	Високий	Кілька важливих контролів працюють недостатньо; потрібне пріоритетне посилення захисту.
75-100 %	Критичний	Конфігурація небезпечна для використання без негайного усунення

Діапазон	Рівень	Зміст результату
		основних недоліків.

Алгоритм також визначає слабкі місця. Для цього програма сортує контролі за внеском у ризик і вибирає ті, які найбільше погіршують результат. Це корисно, бо два сценарії з однаковим відсотком ризику можуть мати різну природу проблем: в одному випадку слабким є наземний сегмент, в іншому — радіоканал або резервування.

Отже, запропонований алгоритм не просто підсумовує бали. Він враховує контекст сценарію, вагу контролів і пояснюваність результату. Завдяки цьому LEO Shield Analyzer можна використовувати як інструмент попереднього аналізу, де користувач бачить не тільки рівень ризику, а й причини його виникнення.

3.4. Реалізація програмного засобу LEO Shield Analyzer

LEO Shield Analyzer реалізовано як локальний вебзастосунок на HTML, CSS і JavaScript. Для практичної частини це зручний вибір: програма не потребує серверної інфраструктури, бази даних або підключення до реальної супутникової мережі. Користувач відкриває index.html у браузері й одразу працює з інтерфейсом.

HTML задає структуру сторінки: заголовок програми, вкладки, вибір сценарію, блоки оцінювання контролів і області результатів. CSS відповідає за вигляд панелі, таблиць, шкал ризику та адаптацію інтерфейсу до різної ширини екрана. JavaScript містить основну логіку: сценарії, ваги контролів, розрахунок ризику, класифікацію результату, рекомендації та перемикання вкладок.

Інтерфейс поділено на чотири вкладки: «Панель», «Матриця», «Звіт» і «Порівняння». На «Панелі» користувач вибирає сценарій і задає оцінки восьми контролів. «Матриця» показує внесок контролів у ризик. «Звіт» формує текстовий висновок і рекомендації. «Порівняння» дає змогу зіставити сценарії між собою.

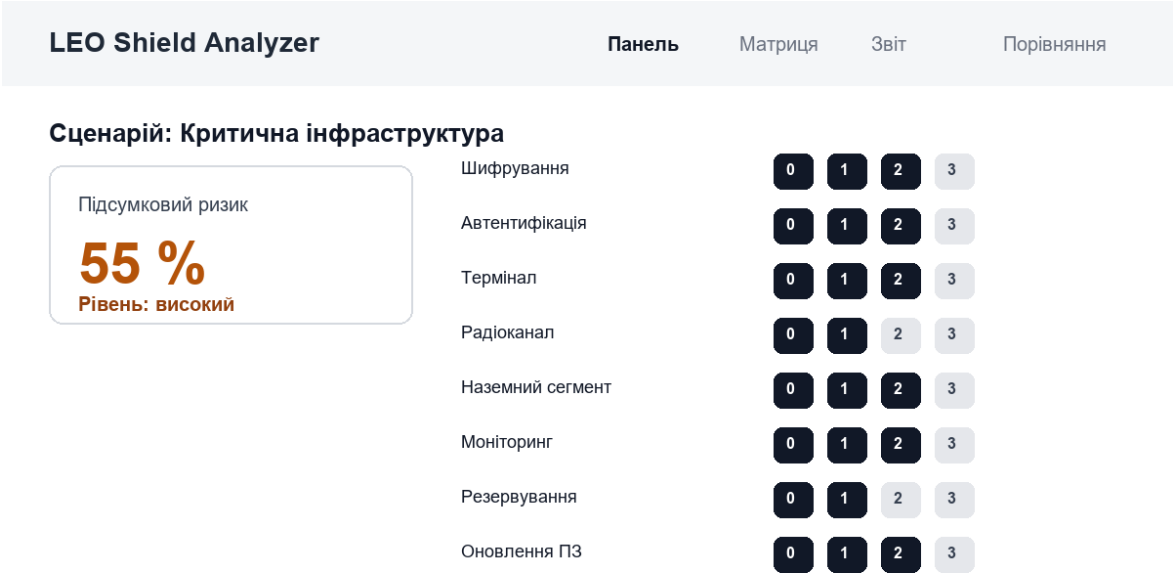


Рисунок 3.2 — Головна панель LEO Shield Analyzer для вибору сценарію та оцінювання контролів

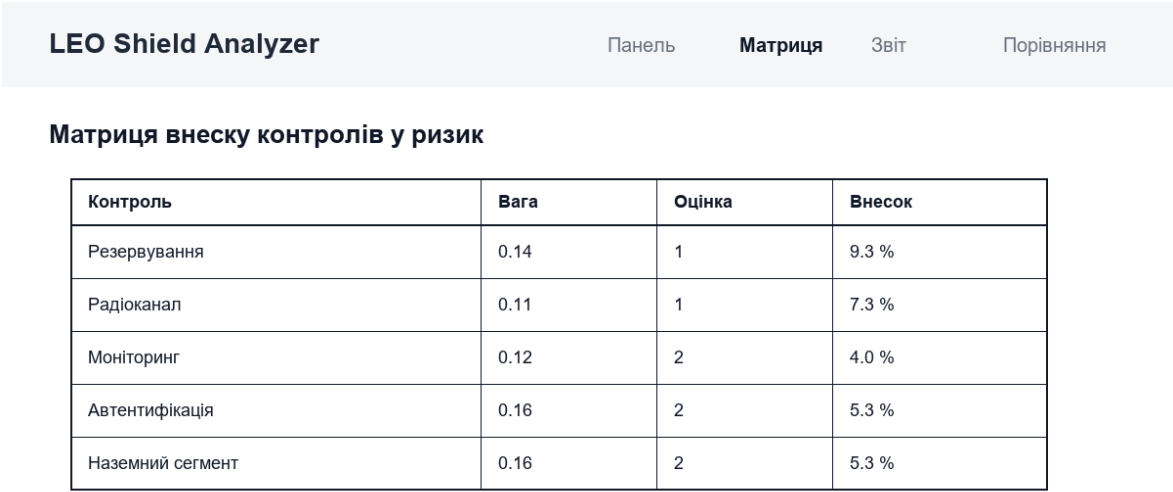


Рисунок 3.3 — Вкладка «Матриця» з внеском контролів у підсумковий ризик

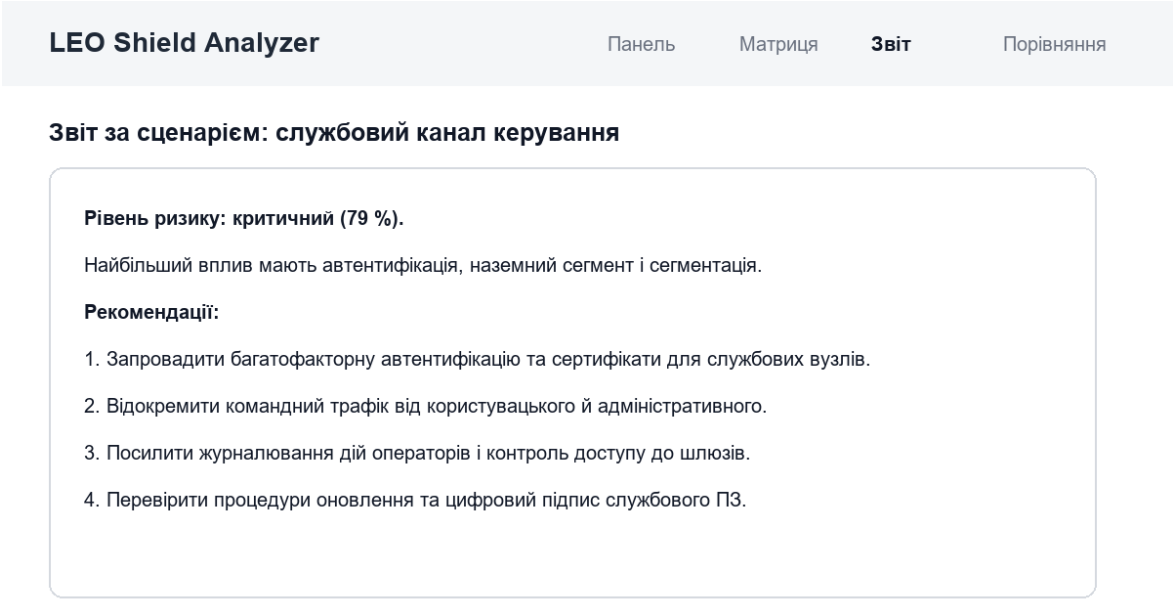


Рисунок 3.4 — Вкладка «Звіт» із текстовими рекомендаціями

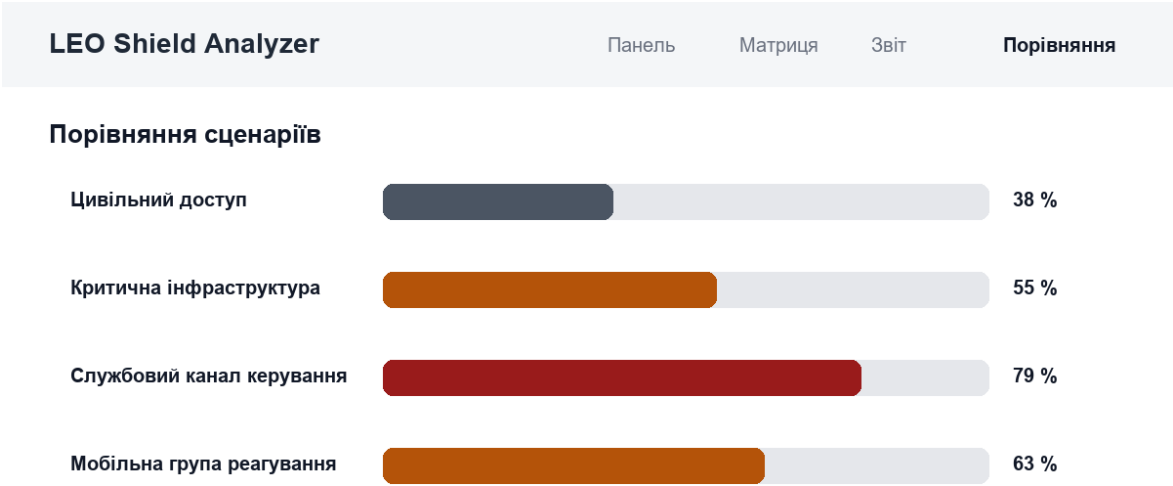


Рисунок 3.5 — Вкладка «Порівняння» для зіставлення сценаріїв

Таблиця 3.6

Призначення вкладок інтерфейсу LEO Shield Analyzer		
Вкладка	Призначення	Що бачить користувач

Вкладка	Призначення	Що бачить користувач
Панель	Основна робоча область для вибору сценарію та оцінювання контролів.	Назву сценарію, вісім контролів, поточний відсоток ризику та рівень небезпеки.
Матриця	Деталізація внеску кожного контролю у підсумковий ризик.	Таблицю контролів, оцінки, ваги та частковий внесок у ризик.
Звіт	Пояснення результату у текстовій формі.	Короткий висновок, слабкі місця і рекомендації для обраного сценарію.
Порівняння	Порівняння типових сценаріїв між собою.	Список сценаріїв із підсумковим ризиком і пріоритетами посилення захисту.

У коді сценарії зручно зберігати як масив об'єктів JavaScript. Кожний об'єкт містить назву сценарію, короткий опис, ваги контролів і типові стартові оцінки. Завдяки такій структурі новий сценарій можна додати без зміни основної логіки застосунку.

Лістинг 3.1 — Приклад опису сценарію у JavaScript

```
const scenarios = [
  {
    id: "critical",
    name: "Критична інфраструктура",
    weights: {
      encryption: 0.14,
      auth: 0.16,
      terminal: 0.09,
      radio: 0.11,
      ground: 0.16,
      monitoring: 0.12,
      redundancy: 0.14,
      updates: 0.08
    },
    scores: {
      encryption: 2,
      auth: 2,
      terminal: 2,
      radio: 1,
```

```

        ground: 2,
        monitoring: 2,
        redundancy: 1,
        updates: 2
    }
}
];

```

Функція розрахунку ризику проходить по всіх контролях, визначає частковий ризик за формулою $(3 - \text{оцінка}) / 3$ і множить його на вагу. Далі результат переводиться у відсотки. Окремо виконується класифікація рівня ризику та підготовка списку найслабших контролів.

Лістинг 3.2 — Фрагмент функції розрахунку ризику

```

function calculateRisk(scores, weights) {
    let risk = 0;
    for (const key of Object.keys(weights)) {
        const controlRisk = (3 - scores[key]) / 3;
        risk += controlRisk * weights[key];
    }
    const weightSum = Object.values(weights).reduce((sum, value) => sum + value, 0);
    return Math.round((risk / weightSum) * 100);
}

function classifyRisk(value) {
    if (value < 25) return "низький";
    if (value < 50) return "середній";
    if (value < 75) return "високий";
    return "критичний";
}

```

Лістинг 3.3 — Фрагмент формування рекомендацій

```

function buildRecommendations(scores) {
    const weakControls = Object.keys(scores)
        .filter((key) => scores[key] < 2);

    return weakControls.map((key) => recommendations[key]);
}

```

Рекомендації у програмі прив'язані до конкретних контролів. Якщо найслабшим є радіоканал, користувач бачить пораду щодо моніторингу сигналу, завадостійких режимів і резервного маршруту. Якщо проблемним є оновлення ПЗ, програма звертає увагу на цифровий підпис, перевірку цілісності та регулярність оновлень. Такий підхід відповідає ідеї адресного добору контролів безпеки [15].

Для підвищення надійності реалізації варто передбачити перевірку коректності вхідних оцінок, уніфікувати назви контролів у всіх модулях, нормалізувати вагові коефіцієнти і винести сценарії та рекомендації в окремі

структури даних. Це спростить додавання нових сценаріїв LEO-зв'язку без зміни основної логіки розрахунку ризику.

Отже, реалізація LEO Shield Analyzer поєднує простий запуск, зрозумілий інтерфейс і прозору JavaScript-логіку. Вебформат дає змогу швидко демонструвати роботу програми, а поділ на вкладки робить її ближчою до повноцінного аналітичного інструмента.

3.5. Тестування програмного засобу та аналіз результатів

Тестування LEO Shield Analyzer виконувалося для перевірки того, як програма реагує на різні сценарії використання LEO-зв'язку. Для цього обрано не випадкові набори балів, а чотири ситуації з різним характером ризику: цивільний доступ, критична інфраструктура, службовий канал керування і мобільна група реагування. Такий сценарний підхід узгоджується з методиками попереднього аналізу загроз і ризиків [23].

Під час тестування перевірялися три речі: чи правильно програма приймає оцінки восьми контролів; чи відповідає підсумковий рівень ризику логіці сценарію; чи формуються рекомендації саме за тими напрямками, які є слабкими в обраній конфігурації. Така перевірка також важлива для майбутнього реагування на інциденти, бо допомагає бачити пріоритетні слабкі місця [19].

Таблиця 3.7

Контрольні результати тестування LEO Shield Analyzer

Сценарій	Вхідні умови	Очікуваний рівень	Отриманий результат
Цивільний доступ	Шифрування і автентифікація на достатньому рівні, але резервування та	Середній	Ризик 38 %, рівень середній; рекомендовано посилити моніторинг і резервування.

Сценарій	Вхідні умови	Очікуваний рівень	Отриманий результат
	моніторинг обмежені.		
Критична інфраструктура	Базові засоби захисту присутні, однак радіоканал і резервування мають недостатні оцінки.	Високий	Ризик 55 %, рівень високий; програма виділила доступність і захист радіоканалу як пріоритет.
Службовий канал керування	Слабка автентифікація, недостатній захист наземного сегмента і відсутня сегментація службового трафіку.	Критичний	Ризик 79 %, рівень критичний; рекомендовано посилити автентифікацію, контроль доступу і захист командного контуру.
Мобільна група реагування	Канал швидко розгортається, але має нестабільний радіозв'язок, слабе резервування і нерегулярні оновлення.	Високий	Ризик 63 %, рівень високий; рекомендації стосуються резервного каналу, оновлень і контролю якості сигналу.

Результати тестування показали, що програма змінює рівень ризику відповідно до змісту сценарію. У цивільному доступі ризик не є критичним, бо базові засоби захисту присутні, але слабкий моніторинг не дозволяє назвати ситуацію низькоризиковою. У сценарії критичної інфраструктури ті самі слабкі місця мають більшу вагу, тому підсумковий рівень стає високим.

Найсудовішу оцінку отримав службовий канал керування. Це очікувано, адже компрометація командного контуру може вплинути не лише на окремого користувача, а й на керування вузлами мережі. Програма правильно показала, що слабка автентифікація і недостатній захист наземного сегмента в цьому сценарії є критичними факторами.

Для мобільної групи реагування програма змістила акцент на доступність і роботу в нестабільних умовах. Найбільший внесок у ризик дали резервування, радіоканал та оновлення програмного забезпечення. Це відповідає практичній логіці: під час аварійного або польового розгортання канал корисний лише тоді, коли він стійкий до втрати основного маршруту і швидко відновлюється після збоїв.

Окремим напрямом удосконалення програмного засобу є збереження результатів оцінювання у файл звіту, додавання експорту в PDF або CSV, розширення бази сценаріїв та інтеграція з реальними параметрами мережі: рівнем сигналу, втратами пакетів, подіями автентифікації і телеметрією шлюзової станції.

Отже, тестування підтвердило працездатність LEO Shield Analyzer. Програма не видає однаковий висновок для різних сценаріїв, а змінює оцінку відповідно до ваг контролів і введених балів. Це свідчить, що запропонований підхід можна застосовувати для попереднього аналізу ризику передачі даних у LEO-мережах і демонстрації впливу окремих засобів захисту на загальний рівень безпеки [5].

Висновки за розділом 3

У третьому розділі розроблено практичну логіку програмного засобу LEO Shield Analyzer. На відміну від загального опису методів захисту, програма переводить аналіз у прикладну площину: користувач обирає сценарій, задає оцінки восьми контролів і отримує підсумковий рівень ризику.

Запропонована архітектура містить інтерфейс користувача, модуль вибору сценарію, модуль оцінювання контролів, модуль розрахунку ризику, модуль рекомендацій і блок звіту/порівняння. Така структура є зрозумілою, розширюваною і близькою до реального аналітичного процесу.

Алгоритм оцінювання побудовано на шкалі 0-3, вагових коефіцієнтах і формулі зваженого ризику. Завдяки цьому результат враховує не лише стан окремих контролів, а й їхню важливість для конкретного сценарію. Реалізація на HTML, CSS і JavaScript дозволяє запускати програму локально та працювати з вкладками «Панель», «Матриця», «Звіт» і «Порівняння».

Тестування на сценаріях цивільного доступу, критичної інфраструктури, службового каналу керування і мобільної групи реагування показало, що LEO Shield Analyzer розрізняє характер ризику та формує рекомендації відповідно до слабких місць. Це підтверджує доцільність використання програмного засобу як допоміжного інструмента попереднього оцінювання безпеки передачі даних у LEO-мережах.

ВИСНОВКИ

У дипломній роботі досліджено методи забезпечення безпеки передачі даних у низькоорбітальних супутникових мережах. Актуальність теми пояснюється тим, що LEO-системи дедалі частіше використовуються для доступу до Інтернету, підтримки критичної інфраструктури, службового зв'язку, мобільних підрозділів і віддалених об'єктів. Разом із цим зростає потреба у зрозумілому оцінюванні ризиків, які виникають у таких мережах.

У першому розділі було розглянуто особливості побудови LEO-мереж і визначено, що безпека передачі даних залежить від взаємодії користувацького, космічного, міжсупутникового, наземного та зовнішнього мережевого сегментів. Захист у такій системі не може обмежуватися одним механізмом, оскільки загрози виникають на різних рівнях і часто посилюють одна одну.

У другому розділі проаналізовано загрози, вразливості та методи захисту LEO-супутникових мереж. Встановлено, що особливої уваги потребують наземні шлюзи, центри керування, користувацькі термінали, радіоканал, автентифікація, моніторинг і резервування. Саме ці елементи мають найбільший вплив на конфіденційність, цілісність і доступність передачі даних.

У третьому розділі розроблено програмний засіб LEO Shield Analyzer. Він дає змогу вибрати сценарій використання LEO-зв'язку, оцінити вісім контролів безпеки, розрахувати інтегральний ризик і отримати рекомендації. Така реалізація робить практичну частину роботи більш наочною, оскільки показує зв'язок між теоретичними загрозами і конкретними рішеннями щодо зниження ризику.

Практичне значення роботи полягає у можливості використання запропонованого підходу для навчального аналізу, попереднього порівняння сценаріїв і формування рекомендацій щодо посилення захисту LEO-каналу. LEO Shield Analyzer не замінює повноцінний технічний аудит, але допомагає швидко побачити слабкі місця і пояснити, чому саме вони впливають на рівень ризику.

Подальший розвиток роботи може передбачати уточнення ваг для різних типів LEO-сервісів, підключення фактичних журналів подій, аналіз реальних конфігурацій обладнання, автоматичне формування звітів і розширення моделі ризику. Це дозволить перетворити програмний засіб на більш повну систему підтримки рішень у сфері кібербезпеки супутникового зв'язку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. NASA. Commercial Space Frequently Asked Questions. Low Earth Orbit Economy. URL: <https://www.nasa.gov/leo-economy/faqs>
2. Lightman S., Suloway T., Brule J. NIST IR 8401: Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control. National Institute of Standards and Technology, 2022. DOI: <https://doi.org/10.6028/NIST.IR.8401>
3. McCarthy J., Mamula D., Brule J., Meldorf K. та ін. NIST IR 8441: Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN). National Institute of Standards and Technology, 2023. DOI: <https://doi.org/10.6028/NIST.IR.8441>
4. Consultative Committee for Space Data Systems. The Application of Security to CCSDS Protocols. CCSDS 350.0-G-3. Green Book, 2019. URL: <https://ccsds.org/publications/allpubs/entry/3130/>
5. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper, 2024. DOI: <https://doi.org/10.6028/NIST.CSWP.29>
6. ENISA. ENISA Space Threat Landscape 2025. European Union Agency for Cybersecurity, 2025. URL: <https://www.enisa.europa.eu/publications/enisa-space-threat-landscape-2025>
7. Viasat. KA-SAT Network cyber attack overview. 2022. URL: <https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview>
8. National Institute of Standards and Technology. Post-Quantum Cryptography Project. FIPS 203, FIPS 204, FIPS 205. URL: <https://csrc.nist.gov/projects/post-quantum-cryptography>
9. Threat analysis for space information network based on network security attributes: a review. Complex & Intelligent Systems, 2022. URL: <https://link.springer.com/article/10.1007/s40747-022-00899-z>
10. 3GPP. Non-Terrestrial Networks (NTN). Technical overview. URL: <https://www.3gpp.org/technologies/ntn-overview>
11. Consultative Committee for Space Data Systems. Space Data Link Security Protocol. CCSDS 355.0-B-2. Recommended Standard, 2022. URL: <https://ccsds.org/publications/allpubs/entry/3258/>

12. Souppaya M., Scarfone K. NIST IR 8270: Introduction to Cybersecurity for Commercial Satellite Operations. National Institute of Standards and Technology, 2022. DOI: <https://doi.org/10.6028/NIST.IR.8270>
13. Joint Task Force Transformation Initiative. NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments. National Institute of Standards and Technology, 2012. DOI: <https://doi.org/10.6028/NIST.SP.800-30r1>
14. Joint Task Force. NIST SP 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations. National Institute of Standards and Technology, 2018. DOI: <https://doi.org/10.6028/NIST.SP.800-37r2>
15. Joint Task Force. NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology, 2020. DOI: <https://doi.org/10.6028/NIST.SP.800-53r5>
16. Rose S., Borchert O., Mitchell S., Connelly S. NIST SP 800-207: Zero Trust Architecture. National Institute of Standards and Technology, 2020. DOI: <https://doi.org/10.6028/NIST.SP.800-207>
17. Boyens J., Smith A., Bartol N., Winkler K., Holbrook A., Fallon M. NIST SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. National Institute of Standards and Technology, 2022. DOI: <https://doi.org/10.6028/NIST.SP.800-161r1-upd1>
18. National Institute of Standards and Technology. FIPS 199: Standards for Security Categorization of Federal Information and Information Systems. 2004. DOI: <https://doi.org/10.6028/NIST.FIPS.199>
19. Cichonski P., Millar T., Grance T., Scarfone K. NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide. National Institute of Standards and Technology, 2012. DOI: <https://doi.org/10.6028/NIST.SP.800-61r2>
20. Barker E. NIST SP 800-57 Part 1 Rev. 5: Recommendation for Key Management. National Institute of Standards and Technology, 2020. DOI: <https://doi.org/10.6028/NIST.SP.800-57pt1r5>
21. 3GPP TS 33.501: Security architecture and procedures for 5G System. 3rd Generation Partnership Project. URL: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169>
22. 3GPP TR 38.821: Solutions for NR to support non-terrestrial networks (NTN). 3rd Generation Partnership Project. URL: https://www.3gpp.org/ftp/Specs/archive/38_series/38.821/
23. ETSI TS 102 165-1: CYBER; Methods and protocols; Part 1: Method and proforma for Threat, Vulnerability, Risk Analysis (TVRA). European Telecommunications

- Standards Institute. URL: https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/
24. The White House. Space Policy Directive-5: Cybersecurity Principles for Space Systems. 2020. URL: <https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/>
25. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. International Organization for Standardization, 2022. URL: <https://www.iso.org/standard/80585.html>
26. ENISA. Low Earth Orbit (LEO) Satcom Cybersecurity Assessment. European Union Agency for Cybersecurity, 2024. URL: <https://www.enisa.europa.eu/publications/low-earth-orbit-leo-satcom-cybersecurity-assessment>
27. Consultative Committee for Space Data Systems. Security Architecture for Space Data Systems. CCSDS 351.0-M-1. Magenta Book, 2012. URL: <https://ccsds.org/Pubs/351x0m1.pdf>
28. Cybersecurity and Infrastructure Security Agency. Recommendations to Space System Operators for Improving Cybersecurity. CISA, 2024. URL: <https://www.cisa.gov/sites/default/files/2024-06/Recommendations%20to%20Space%20System%20Operators%20for%20Improving%20Cybersecurity%20%28508%29.pdf>
29. Cybersecurity and Infrastructure Security Agency. Space Systems and Services. CISA. URL: <https://www.cisa.gov/topics/risk-management/space-systems>
30. European Cooperation for Space Standardization. ECSS-E-ST-80C: Space engineering — Security in space systems lifecycles. ECSS, 2024. URL: <https://ecss.nl/standard/ecss-e-st-80c-space-engineering-security-in-space-systems-lifecycles/>
31. Falco G. Minimum Requirements for Space System Cybersecurity: Ensuring Cyber Access to Space. IEEE Space Mission Challenges for Information Technology, 2024. URL: <https://www.computer.org/csdl/proceedings-article/smc-it/2024/845100a078/22NQJn8CIHS>
32. Kang M., Park S., Lee Y. A Survey on Satellite Communication System Security. Sensors, 2024. Vol. 24, No. 9. Article 2897. DOI: <https://doi.org/10.3390/s24092897>
33. Tedeschi P., Sciancalepore S., Di Pietro R. Satellite-based communications security: A survey of threats, solutions, and research challenges. Computer Networks, 2022. Vol. 216. Article 109246. DOI: <https://doi.org/10.1016/j.comnet.2022.109246>
34. Zhang Y., Zhao S., He J., Zhang Y., Shen Y., Jiang X. A Survey of Secure Communications for Satellite Internet Based on Cryptography and Physical Layer Security. IET Information Security, 2023. Article 5604802. DOI: <https://doi.org/10.1049/2023/5604802>

35. Peled R., Aizikovich E., Habler E., Elovici Y., Shabtai A. SoK: Evaluating the Security of Satellite Systems. arXiv, 2023. DOI: <https://doi.org/10.48550/arXiv.2312.01330>
36. Yue P., An J., Zhang J., Ye G., Pan G., Wang S., Xiao P., Hanzo L. Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and Future Directions. IEEE Communications Surveys & Tutorials, 2023. DOI: <https://doi.org/10.1109/COMST.2023.3296160>
37. Wang J., Jiang C., Zhang H., Ren Y. A Survey on Authentication in Satellite Internet. International Journal of Electronics and Communications Engineering, 2022. URL: <https://iecsce.org/jpapers/128>
38. Rescorla E. RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3. Internet Engineering Task Force, 2018. DOI: <https://doi.org/10.17487/RFC8446>
39. Kent S., Seo K. RFC 4301: Security Architecture for the Internet Protocol. Internet Engineering Task Force, 2005. DOI: <https://doi.org/10.17487/RFC4301>
40. Bundesverband der Deutschen Luft- und Raumfahrtindustrie. Security for Space Systems. BDLI Position Paper, 2024. URL: https://www.bdli.de/sites/default/files/2024-05/240508_Positionspapier_Security_in_Space.pdf
41. Lin P., Abney K., DeBruhl B., Abercromby K., Danielson H., Jenkins R. Outer Space Cyberattacks: Generating Novel Scenarios to Avoid Surprise. arXiv, 2024. DOI: <https://doi.org/10.48550/arXiv.2406.12041>
42. Ellis T., Hitaj B., Lindqvist U., Shands D., Tinnel L., DeBruhl B. Critical Infrastructure Security Goes to Space: Leveraging Lessons Learned on the Ground. arXiv, 2023. DOI: <https://doi.org/10.48550/arXiv.2309.15232>

ДОДАТОК А

Програмний код LEO Shield Analyzer

Лістинг А.1 — Функція розрахунку ризику

```
function calculateRisk(scores, weights) {  
  let total = 0;  
  for (const key of Object.keys(weights)) {  
    const partialRisk = (3 - scores[key]) / 3;  
    total += partialRisk * weights[key];  
  }  
  const weightSum = Object.values(weights).reduce((sum, value) => sum + value,  
0);  
  return Math.round((total / weightSum) * 100);  
}
```

Лістинг А.2 — Масив сценаріїв

```
const scenarioNames = [  
  "Цивільний доступ",  
  "Критична інфраструктура",  
  "Службовий канал керування",  
  "Мобільна група реагування"  
];
```

Лістинг А.3 — Приклад формування рекомендацій

```
const recommendations = {  
  encryption: "Увімкнути сучасне шифрування та контроль життєвого циклу  
ключів.",  
  auth: "Посилити автентифікацію, додати сертифікати та багатофакторну  
перевірку.",  
  radio: "Передбачити моніторинг сигналу, завадостійкі режими та резервний  
маршрут.",  
  ground: "Обмежити адміністративний доступ і посилити захист шлюзових  
станцій."  
};
```

Лістинг А.4 — Основна логіка оновлення інтерфейсу програми

```
function updateDashboard() {  
  const scenario = scenarios.find((item) => item.id === selectedScenarioId);  
  const scores = readControlScores();  
  const risk = calculateRisk(scores, scenario.weights);  
  const level = classifyRisk(risk);  
  const advice = buildRecommendations(scores);  
  
  renderRiskValue(risk);  
  renderRiskLevel(level);  
  renderMatrix(scores, scenario.weights);  
  renderRecommendations(advice);  
}
```

Повний програмний код засобу LEO Shield Analyzer складається з файлів `index.html`, `styles.css` та `app.js` і подається в електронному додатку до кваліфікаційної бакалаврської роботи.

ДОДАТОК Б

Інструкція користувача

1. Відкрити файл index.html у браузері Google Chrome, Microsoft Edge або Mozilla Firefox.
2. На вкладці «Панель» обрати сценарій використання LEO-каналу.
3. Перевірити або змінити оцінки восьми контролів безпеки за шкалою від 0 до 3.
4. Переглянути підсумковий відсоток ризику та його рівень.
5. Відкрити вкладку «Матриця», щоб побачити внесок кожного контролю у ризик.
6. Перейти на вкладку «Звіт» і прочитати рекомендації щодо зменшення ризику.
7. За потреби відкрити вкладку «Порівняння» і зіставити різні сценарії між собою.

ДОДАТОК В

Контрольні тестові сценарії

Таблиця В.1

Вхідні оцінки контролів і очікуваний рівень ризику

Сценарій	Оцінки контролів	Очікуваний рівень
Цивільний доступ	2, 2, 2, 2, 2, 1, 1, 2	Середній
Критична інфраструктура	2, 2, 2, 1, 2, 2, 1, 2	Високий
Службовий канал керування	1, 0, 2, 1, 0, 1, 1, 2	Критичний
Мобільна група реагування	2, 2, 1, 1, 2, 1, 0, 1	Високий

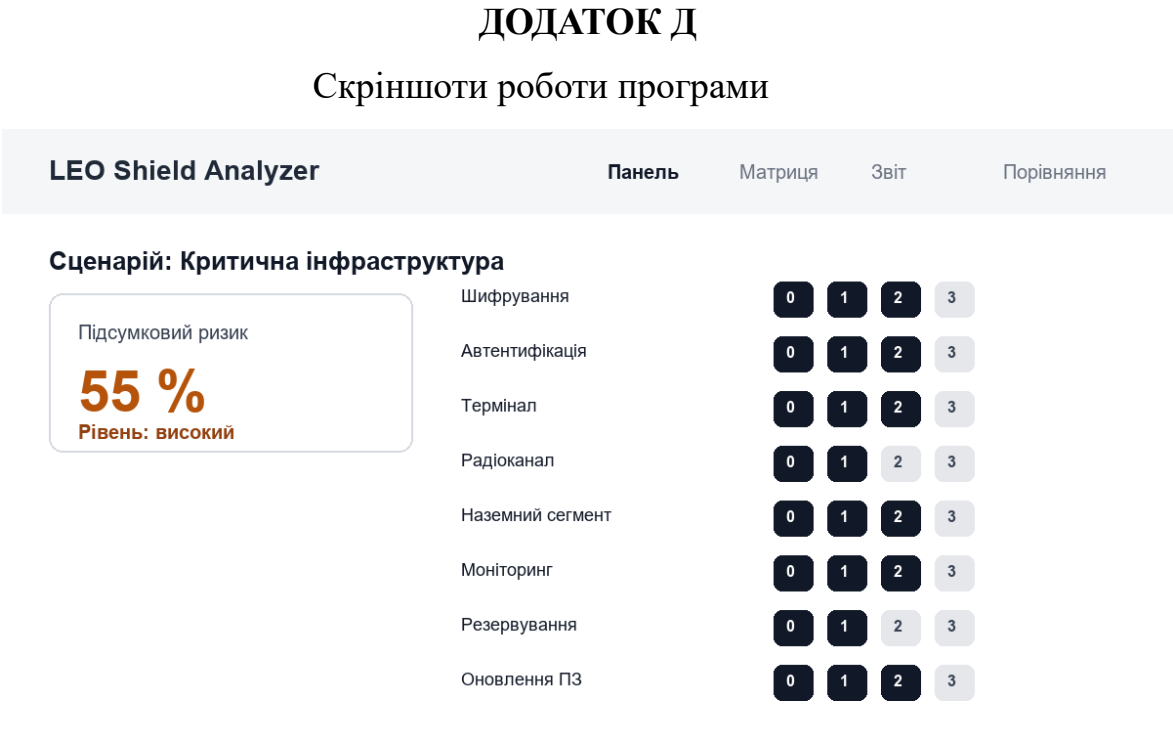


Рисунок Д.1 — Головна панель програмного засобу LEO Shield Analyzer

LEO Shield Analyzer

ПанельМатрицяЗвітПорівняння

Матриця внеску контролів у ризик

Контроль	Вага	Оцінка	Внесок
Резервування	0.14	1	9.3 %
Радіоканал	0.11	1	7.3 %
Моніторинг	0.12	2	4.0 %
Автентифікація	0.16	2	5.3 %
Наземний сегмент	0.16	2	5.3 %

Рисунок Д.2 — Вкладка «Матриця» з внеском контролів у підсумковий ризик

Звіт за сценарієм: службовий канал керування

Рівень ризику: критичний (79 %).

Найбільший вплив мають автентифікація, наземний сегмент і сегментація.

Рекомендації:

- Запровадити багатофакторну автентифікацію та сертифікати для службових вузлів.
- Відокремити командний трафік від користувацького й адміністративного.
- Посилити журналювання дій операторів і контроль доступу до шлюзів.
- Перевірити процедури оновлення та цифровий підпис службового ПЗ.

Рисунок Д.3 — Вкладка «Звіт» із текстовими рекомендаціями

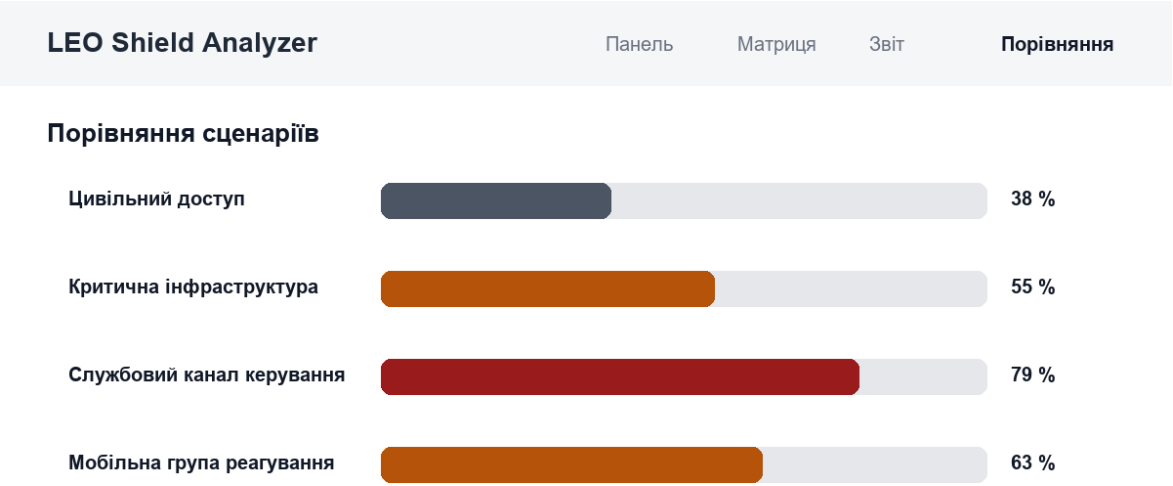


Рисунок Д.4 — Вкладка «Порівняння» для зіставлення сценаріїв

0

Інтернет		0
Мікропробіли		0
Білі знаки		0
Парафрази (SmartMarks)		0

Джерела

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз

Колір тексту

#	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
---	--	--

1	Ct27wSuSjgFG0oEsNSaPuQdleIDTp5AO 4/29/2025 Vinnytsia Humanities Pedagogical College (Vinnytsia Humanities Pedagogical College)	12 (0.13 %)
База даних RefBooks		
#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
Домашня база даних		
#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
Програма обміну базами даних (0.13 %)		
#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

1	Ct27wSuSjgFG0oEsNSaPuQdleIDTp5AO 4/29/2025 Vinnytsia Humanities Pedagogical College (Vinnytsia Humanities Pedagogical College)	12 (1) (0.13 %)
Інтернет		
#	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

Список прийнятих фрагментів

#	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)
---	-------	---------------------------------------