РАДІОЕЛЕКТРОНІКА ТА РАДІОЕЛЕКТРОННЕ АПАРАТОБУДУВАННЯ

https://doi.org/10.31649/1997-9266-2025-180-3-178-186

УДК 621.391

Д. М. Розенвассер[1]
В. В. Педяш[1]
О. П. Русу[1]
Ю. О. Стрелковська[2]

ВРАЗЛИВОСТІ ТА КІБЕРБЕЗПЕКА STARLINK

[1]Міжнародний гуманітарний університет, Одеса, Україна;
[2]Worthing College, Вортінг, Велика Британія

Комплексно проаналізовано вразливості та проблеми кібербезпеки супутникової мережі Starlink, яка забезпечує глобальний доступ до інтернету через мережу низькоорбітальних супутників. Розглянуто технологічні аспекти функціонування системи, зокрема архітектуру мережі, принципи передачі даних, а також взаємодію між супутниками, наземними станціями та користувацькими терміналами. Окреслено ключові компоненти системи, які можуть стати об'єктами потенційних кібератак, зокрема супутники, наземні шлюзи та клієнтські термінали. Особливу увагу приділено аналізу основних загроз, таких як перехоплення сигналу, DDoS-атаки, несанкціонований доступ до даних, глушіння сигналу та фізичні збої в роботі супутників. Досліджено можливі наслідки таких атак для приватних користувачів, бізнесу, військової інфраструктури та глобальної комунікаційної мережі. Проаналізовано поточний стан кібербезпеки Starlink, зокрема використання шифрування, автентифікації, протоколів захищеної передачі даних та систем раннього виявлення загроз. Дано рекомендації для поліпшення кіберзахисту, зокрема впровадження механізмів динамічного шифрування, підвищення стійкості мережі до зовнішніх атак, вдосконалення стратегій реагування на інциденти та інтеграцію передових технологій, таких як квантова криптографія та мережі нульової довіри. Оцінено загальний рівень безпеки системи, включно з показниками стійкості до атак, часу реагування на інциденти та доступністю мережі. Окреслено перспективні напрями для зниження ризиків і забезпечення стабільної роботи інфраструктури Starlink в умовах сучасних кіберзагроз. На основі чисельних показників оцінено рівень захищеності системи, зокрема стійкість до зовнішніх загроз і здатність відновлюватися після атак.

Ключові слова: Starlink, вразливості, кібербезпека, атаки, супутники, інтернет, шифрування.

Вступ

Супутниковий інтернет-сервіс Starlink, розроблений компанією SpaceX, є революційною технологією, що має на меті забезпечити доступ до швидкісного інтернету в найвіддаленіших куточках світу. Використовуючи групу супутників на низькій навколоземній орбіті (LEO), Starlink пропонує новий підхід до вирішення проблеми цифрового розриву, що є особливо важливим для регіонів з обмеженою або взагалі відсутньою інфраструктурою наземного інтернету [1], [4].

Проте разом з перевагами цієї технології постають нові виклики, пов'язані з її кібербезпекою. Використання супутникових систем створює унікальні ризики, які включають як можливість кібератак на рівні супутників та наземних станцій, так і загрози для кінцевих користувачів [12], [13]. Потенційні вразливості можуть мати серйозні наслідки, від порушень у роботі мережі і до ризиків національної безпеки.

До того ж оскільки Starlink розширює свою базу користувачів та інтегрується з наявними наземними мережами, поверхня атаки для кіберзагроз тільки розширюється. Кіберзлочинці можуть використовувати вразливості в мережевих протоколах, програмних застосунках або пристроях користувача, щоб проникнути в інфраструктуру Starlink і зламати її. Від атак програм-вимагачів до розподілених атак типу «відмова в обслуговуванні» (DDoS), ландшафт потенційних загроз різноманітний і розвивається.

Метою роботи є аналіз вразливостей супутникового інтернету Starlink та оцінювання заходів кібербезпеки, які реалізує SpaceX. Зокрема, дослідження зосереджене на визначенні основних загроз, поточних способів їхнього усунення та рекомендаціях щодо підвищення захищеності системи.

Ця тема має велике значення не лише з технічної точки зору, але й у контексті глобальної кібербезпеки та забезпечення стійкості інтернет-інфраструктури в умовах постійно зростаючих викликів цифрової епохи.

Огляд технології Starlink

Starlink — це глобальна система супутникового інтернету, створена компанією SpaceX, яка базується на використанні сузір'я супутників, розташованих на низькій навколоземній орбіті (LEO). Її основна мета — забезпечити високошвидкісний доступ до інтернету навіть у найвіддаленіших та важкодоступних регіонах світу [1], [6].

Система Starlink складається з трьох основних компонентів: сузір'я супутників, наземні станції та клієнтські термінали.

Сузір'я складається з тисяч малих супутників, які знаходяться на висоті від 340 до 1200 км над поверхнею Землі. Завдяки їхній низькій орбіті система має значно нижчу затримку передачі даних (латентність) порівняно з традиційними геостаціонарними супутниками [5], [15].

Наземні шлюзи є важливим елементом системи, які забезпечують обмін даними між супутниками та глобальною мережею інтернет. Ці станції використовують передові технології зв'язку для забезпечення стабільності сигналу [3], [21].

Термінали, що встановлюються у клієнтів, є компактними антенами типу фазованої решітки. Вони автоматично налаштовуються для з'єднання з супутниками, забезпечуючи простоту використання для споживачів [6], [25].

Starlink використовує Ku- і Ka-діапазони частот для передачі даних, а також передові протоколи шифрування для забезпечення безпеки комунікацій [15], [21]. До того ж, супутники оснащені лазерними системами зв'язку, що дозволяють передавати дані між супутниками без участі наземних станцій, підвищуючи гнучкість та швидкість мережі [3].

На відміну від геостаціонарних супутників, які розташовані на висоті приблизно 35 786 км, супутники Starlink на LEO забезпечують меншу затримку (20–40 мс) і стабільнішу якість зв'язку. Проте це потребує більшої кількості супутників для забезпечення глобального покриття [5], [22].

Станом на 2024 рік система Starlink налічує понад 5000 активних супутників на орбіті, через що вона є найбільшим угрупованням такого типу у світі. SpaceX планує збільшити це число до 12 000 супутників у найближчі роки [6], [25].

Система Starlink демонструє високу ефективність у забезпеченні інтернет-послуг для приватних користувачів, бізнесу та урядів. Водночас, її інноваційна архітектура породжує низку викликів, зокрема у сфері кібербезпеки, які потребують ретельного аналізу та вирішення.

Також SpaceX отримала контракт від уряду США на розширення доступу України до Starshield — нової програми, орієнтованої на національну безпеку. Starshield розроблено для підтримки військових та урядових потреб, забезпечуючи захищену передачу даних, висококласне шифрування і можливість інтеграції з іншими державними супутниковими системами. Проєкт також включає функції зображення, комунікацій і підтримки сторонніх корисних навантажень, таких як сенсори чи інші пристрої, які можуть бути розміщені на супутниках SpaceX [29].

Можливі вразливості

Хоча система Starlink є передовою технологією у сфері супутникового інтернету, вона також має вразливості, які можуть стати ціллю для кіберзагроз. Враховуючи масштаб системи та її критичне значення для глобальної комунікаційної інфраструктури, виявлення та аналіз потенційних ризиків є надзвичайно важливими.

Кілька конкретних загроз і векторів атак потенційно можуть бути спрямовані на Starlink, створюючи значні ризики для його операцій і користувачів.

Супутникова система Starlink забезпечує глобальний інтернет-зв'язок, через що вона є критично важливою для багатьох сфер, включно з комунікаціями, національною безпекою, медициною та бізнесом. Атаки на Starlink можуть мати серйозні наслідки як для окремих користувачів, так і для суспільства в цілому.

Однією з таких загроз є розподілені атаки на відмову в обслуговуванні (DDoS), які можуть перевантажити інфраструктуру Starlink величезним обсягом трафіку, спричиняючи збої в роботі послуг і через що мережа може бути недоступною для законних користувачів.

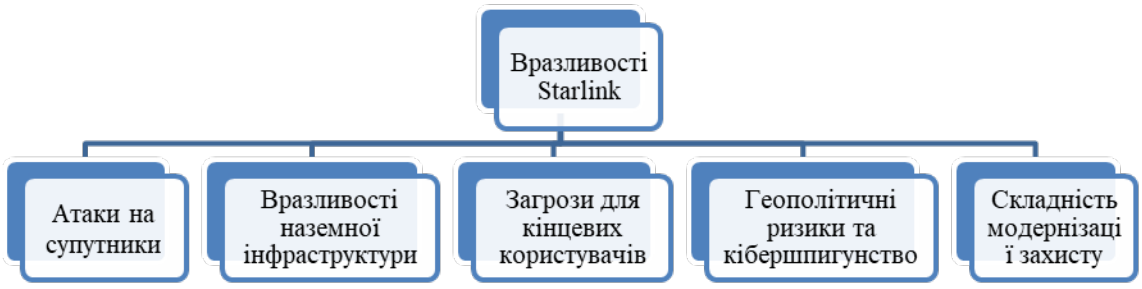

Рис. 1. Вразливості Starlink

Іншою небезпекою є спуфінг, коли зловмисники маніпулюють супутниковими сигналами, вводячи в оману термінали користувачів або наземні станції, що може призвести до несанкціонованого доступу, маніпуляцій з даними або їх перехоплення. Перешкоди, спрямовані на супутниковий зв'язок шляхом передачі сигналів, що перекривають законні, здатні погіршити якість з'єднання або зробити його недоступним для цілих регіонів.

Передача даних між супутниками та користувачами здійснюється через відкритий простір, що створює ризик перехоплення сигналів. Хоча Starlink використовує протоколи шифрування, атаки типу "man-in-the-middle" можуть загрожувати конфіденційності даних.

Радіочастотне глушіння може призвести до тимчасової втрати зв'язку для користувачів у певному регіоні. Цей вид атаки є особливо небезпечним у зонах конфліктів або під час надзвичайних ситуацій.

Якщо зловмисники отримають доступ до програмного забезпечення, яке контролює супутники, вони можуть змінити маршрути сигналу або навіть вивести супутник з експлуатації.

Наземні шлюзи є важливим елементом системи Starlink, і їхнє пошкодження або злам можуть спричинити значні перебої у роботі мережі. Наприклад, фізичні атаки або зараження шкідливим програмним забезпеченням становлять серйозну загрозу. Хакери можуть намагатися отримати доступ до даних користувачів, збережених у наземних центрах обробки даних, що використовуються для обробки трафіку Starlink.

Термінали Starlink, які використовують кінцеві користувачі, також можуть бути об'єктом атак. Зокрема, можливі злами для перенаправлення трафіку або отримання доступу до пристроїв у локальній мережі. Користувацькі термінали можуть бути вразливими до фізичного пошкодження або несанкціонованого втручання, що порушить роботу зв'язку.

Starlink, як система, що використовується військовими та державними установами, може бути мішенню для атак з боку державних або пов'язаних з державами груп. У разі військового протистояння або кіберконфліктів супутникові інтернет-мережі, зокрема Starlink, можуть бути використані як ціль для атак, спрямованих на порушення критичної інфраструктури, дестабілізацію комунікацій чи зниження військового потенціалу.

Також існує ризик перехоплення сигналів, який дозволяє зловмисникам підслуховувати супутниковий зв'язок, що порушує конфіденційність і цілісність переданих даних. Отримана інформація може бути використана для шпигунства, стеження чи інших злочинних цілей. Starlink може стати об'єктом кібершпигунства, організованого державними або кримінальними групами для викрадення конфіденційної інформації чи отримання стратегічної переваги.

У табл. 1 подано можливі сценарії атак та їхні наслідки.

Таблиця 1

Можливі сценарії атак та їхні наслідки

Тип атаки	Можливі наслідки
DDoS-атаки	Перевантаження наземних станцій або терміналів, що призведе до втрати доступу до інтернету
Перехоплення сигналів	Викрадення або підробка даних, що передаються через супутники
Глушіння радіочастот	Локальне відключення зв'язку в стратегічно важливих регіонах
Атаки на програмне забезпечення	Компрометація оновлень системи, що може призвести до поширення шкідливого ПЗ серед користувачів
Фізичні атаки	Знищення наземних станцій або запуск супутників, що імітують Starlink, для втручання в роботу системи

Зважаючи на глобальний масштаб системи та високу кількість активних супутників, оновлення систем захисту або виправлення вразливостей у програмному забезпеченні може бути тривалим процесом.

Аналіз цих потенційних загроз свідчить про необхідність постійного вдосконалення кібербезпеки Starlink для мінімізації ризиків, що можуть мати як локальні, так і глобальні наслідки.

Поточна кібербезпека та рекомендації

Компанія SpaceX приділяє значну увагу забезпеченню безпеки системи Starlink, адже вона є однією з найважливіших глобальних інфраструктур для надання інтернет-зв'язку. Однак швидкий розвиток технології супутникових мереж та зростаюча кількість кібератак вимагають безперервного вдосконалення кіберзахисту.

Поточна служба Starlink вже забезпечує наскрізне шифрування даних користувачів, але версія для національної безпеки матиме «додаткові криптографічні можливості високої надійності» для безпечної обробки та доставки секретних даних.

Україна вже використовує Starlink для забезпечення зв'язку на полі бою, але новий контракт розширює можливості шляхом інтеграції цих технологій в інфраструктуру Starshield. Це є відповіддю на стратегічну потребу забезпечення надійного зв'язку для підтримки військових операцій.

Рис. 2. Поточні методи захисту Starlink

Starlink пропонує багато функцій, які враховують безпеку в Інтернеті та встановлюють приватне з'єднання. По-перше, це децентралізована платформа, тобто наявність багатьох супутників по всій земній кулі значно зменшує одну точку збою та допомагає запобігти мережевим атакам, які є поширенішими в централізованій інфраструктурі [31].

Starlink використовує сучасні протоколи шифрування для захисту переданих даних. Це зменшує ймовірність перехоплення інформації зловмисниками під час передачі між супутниками, наземними станціями та користувацькими терміналами [12].

Впровадження надійних механізмів шифрування має важливе значення для захисту даних, що передаються в супутникових мережах Інтернету. Наскрізне шифрування гарантує, що дані шифруються під час передачі, захищаючи їх від перехоплення або підробки зловмисниками.

Розширені стандарти шифрування, такі як AES (Advanced Encryption Standard) з надійними методами керування ключами, можуть допомогти зменшити ризик несанкціонованого доступу до конфіденційної інформації [21]. Starlink використовує розширений стандарт шифрування (AES) з довжиною ключа 256 біт, найпоширеніший алгоритм шифрування, який вважається дуже безпечним. Це шифрування кодує дані, унеможливлюючи їх прочитання для неавторизованих сторін. Для захисту передачі даних від перехоплення на глобальному рівні можна застосовувати квантову криптографію, що забезпечує майже абсолютну безпеку каналів зв'язку.

Starlink стверджує, що вони не мають головних ключів для шифрування даних користувачів. Натомість кожен користувач генерує власні унікальні ключі шифрування, підвищуючи ще більше безпеку та контроль.

Щоб ще більше посилити безпеку, Starlink, як повідомляється, використовує регулярну ротацію ключів, тобто ключі шифрування періодично змінюються, щоб мінімізувати ризик компрометації, навіть якщо доступ до одного ключа.

Для протидії радіочастотному глушінню компанія SpaceX реалізує стратегії адаптивного перемикання частот, що дозволяє підтримувати зв'язок навіть у разі цілеспрямованих атак на сигнали [13].

Компанія регулярно випускає оновлення програмного забезпечення для супутників, терміналів і наземної інфраструктури. Це допомагає оперативно реагувати на виявлені вразливості [9]. Використання штучного інтелекту та машинного навчання для прогнозування потенційних загроз та їх оперативного виявлення є наразі дуже важливим елементом захисту.

Новітні супутники Starlink оснащені лазерними передавачами, що дозволяє зменшити залежність від наземної інфраструктури і знижує ризики атак на наземні шлюзи [15]. Необхідним є розширення використання лазерного зв'язку між супутниками та впровадження резервних каналів для забезпечення стабільності системи під час атак на наземну інфраструктуру.

Наземні станції та інші критичні елементи системи захищені фізичними засобами безпеки, включно з системами спостереження та контролю доступу. Сьогодні розробляються покращені механізми аутентифікації, такі як багатофакторна автентифікація, та інтеграція захисного програмного забезпечення для терміналів користувачів. Розгортання надійних механізмів автентифікації має вирішальне значення для перевірки ідентичності користувачів і пристроїв, які отримують доступ до супутникових мереж Інтернету. Багатофакторна автентифікація (Multi-factor authentication, MFA) підвищує безпеку, вимагаючи кількох форм автентифікації, таких як паролі, біометричні дані або автентифікація на основі маркерів. Це допомагає запобігти несанкціонованому доступу та зміцнює загальну безпеку мережі.

Впровадження систем виявлення вторгнень (Intrusion Detection System, IDS) дозволяє здійснювати моніторинг у реальному часі та виявляти підозрілі дії або спроби несанкціонованого доступу в супутниковій мережі Інтернет. IDS може виявляти аномалії в мережевому трафіку, незвичні шаблони поведінки або відомі сигнатури атак, дозволяючи групам безпеки оперативно реагувати на потенційні інциденти безпеки та зменшувати ризики до їх ескалації.

Розробка та впровадження безпечної мережевої архітектури має важливе значення для мінімізації поверхонь атак і вразливостей у супутникових мережах Інтернету. Сегментація мережевої інфраструктури, забезпечення контролю доступу з найменшими привілеями та впровадження мережевих брандмауерів допомагають запобігти несанкціонованому доступу та боковому переміщенню зловмисників. До того ж розгортання мережевих систем запобігання вторгненням (Intrusion Prevention System, IPS) додає додатковий рівень захисту від зловмисних дій. IPS використовує базу даних сигнатур відомих атак та визначає нормальну поведінку мережі.

Створення надійної системи для безперервного моніторингу та реагування на інциденти дає змогу проактивно виявляти загрози кібербезпеці та реагувати на них у режимі реального часу. Операційні центри безпеки (Security Operations Center, SOC), оснащені розширеними інструментами аналітики безпеки, можуть контролювати мережевий трафік, виявляти аномалії та оперативно реагувати на інциденти безпеки. Реалізація планів реагування на інциденти та проведення регулярних навчань безпеки гарантує, що групи безпеки добре підготовлені для ефективної обробки інцидентів кібербезпеки.

Незважаючи на впроваджені заходи, Starlink стикається з низкою викликів, зокрема атаками, які спрямовані на порушення роботи мережі в стратегічно важливих регіонах.

У шифруванні Starlink використовує протокол безпечного з'єднання, відомий як TLS/SSL (Transport Layer Security / Secure Sockets Layer) для безпечної передачі даних між терміналом користувача та наземними станціями. Це додає ще один рівень захисту під час фази передачі. TLS — це криптографічний протокол, який забезпечує конфіденційність зв'язку та цілісність даних між двома взаємодіючими комп'ютерними програмами. Це означає, що дані, які передаються між супутниками Starlink і пристроєм користувача, зашифровані, що ускладнює перехоплення або доступ до них хакерам. Він також використовує технологію, відому як «Мережа нульової довіри» (Zero-Trust) для захисту даних користувачів. Ця технологія має на меті запобігти зловмисникам отримати доступ до мережі Starlink, відстежуючи всю активність і гарантуючи, що доступ надано лише найнадійнішим користувачам і пристроям.

Starlink наразі підтримує захист за протоколом WPA2, але не пропонує WPA3. WPA3 є новішим стандартом безпеки, представленим у 2018 році. Хоча він пропонує покращений захист, не всі пристрої підтримують цей протокол, особливо старіші моделі. Використання WPA2 забезпечує сумісність з ширшим спектром пристроїв, що є критично важливим для глобальної мережі, такої як Starlink, яка орієнтована на різноманітних користувачів у різних регіонах. Переходячи на WPA3, виробники повинні переконатися, що їх обладнання повністю відповідає вимогам нового стандарту. Це може потребувати не лише оновлення програмного забезпечення, але й модернізації апаратного забезпечення. У випадку Starlink це означало б оновлення всіх маршрутизаторів у ко-

ристувачів або забезпечення сумісності через оновлення прошивки, що може бути технічно та економічно складним. Хоча WPA3 пропонує покращення, зокрема захист від офлайн-атаки методом підбору паролів завдяки одночасній автентифікації рівних (Simultaneous Authentication of Equals, SAE), WPA2 все ще забезпечує достатній рівень безпеки для більшості користувачів, якщо використовуються сильні паролі та інші практики кібербезпеки.

Для зменшення наслідків атак необхідно розробити плани дій на випадок повного або часткового збою роботи системи, передбачивши використання резервних каналів зв'язку. Важливим заходом є впровадження багаторівневої аутентифікації для забезпечення безпечного доступу до супутників і наземних станцій.

Використання компанією протоколів шифрування, мережі Zero-Trust і програми Bug Bounty вказує на зусилля щодо підвищення безпеки та захисту даних користувачів. Starlink вже впровадив низку заходів для забезпечення своєї безпеки, проте через унікальні виклики супутникових мереж необхідно продовжувати інвестувати в інноваційні технології захисту. Реалізація зазначених рекомендацій може сприяти більшої стійкості системи до кіберзагроз та підвищити її надійність у глобальному масштабі.

Показники ефективності

Поточні показники ефективності планів обслуговування для України та середні світові подано у табл. 2 [35].

Таблиця 2

Показники ефективності планів обслуговування

План обслуговування	Середнє по Україні	Фіксований (середнє)	Мобільний (середнє)	Морський (середнє)
Швидкість завантаження даних, Мбіт/с	53...242	40...220	40...220	40...220
Швидкість відправлення даних, Мбіт/с	8...22	8...25	8...25	8...25
Затримка, мс	44...71	25...60	≤ 99	≤ 99

Для аналізу кібербезпеки системи Starlink можна використовувати кількісні показники, які відображають її здатність протистояти різним видам атак. Ця оцінка враховує такі ключові параметри, як рівень шифрування, частота оновлення програмного забезпечення, кількість виявлених атак, швидкість реагування на інциденти та інші аспекти.

Запропоновано оцінку вразливостей та кібербезпеки Starlink на основі загальних критеріїв теорії надійності:

– індекс стійкості системи (System Resilience Index, *SRI*) відображає здатність системи протистояти атакам і відновлюватися після них.

$$SRI = \frac{\text{Кількість успішних відбитих атак}}{\text{Загальна кількість атак}} \cdot 100\,\%;$$

– час реагування на інцидент (Incident Response Time, *IRT*) — середній час, необхідний для виявлення, аналізу та нейтралізації атаки;

– середній час до відмови (Mean Time To Failure, *MTTF*) — це середній час, протягом якого мережа функціонує без збоїв;

– середній час відновлення (Mean Time To Repair, *MTTR*), необхідний для відновлення роботи системи після виникнення відмови;

– середній час між відмовами (Mean Time Between Failures, *MTBF*) включає як час безвідмовної роботи, так і час, необхідний для відновлення.

$$MTBF = MTTF + MTTR.$$

– доступність (Availability, *A*) визначає ймовірність того, що мережа буде готова до роботи в будь-який момент часу

$$A = \frac{MTTF}{MTBF} \cdot 100\,\%;$$

– кількість вразливостей у програмному забезпеченні відображає кількість виявлених і виправ-

лених вразливостей за певний період часу. Темп виявлення вразливостей

$$R_v = \frac{\Delta V}{\Delta t},$$

де ΔV — кількість нововиявлених вразливостей за час Δt;

– навантаження на інфраструктуру — відсоток втрати пакетів (Packet Loss Ratio, *PLR*) або збільшення затримки під час кібератак

$$PLR = \frac{\text{Кількість втрачених пакетів}}{\text{Загальна кількість надісланих пакетів}} \cdot 100\ \%.$$

Статистичні дані щодо показників надійності глобальної мережі інтернет-покриття системи Starlink не публікуються компанією SpaceX у відкритому доступі.

Індекс стійкості системи (SRI) для мережі Starlink становить приблизно 98 %. Це свідчить про високий рівень захисту, оскільки компанії SpaceX вдалося успішно нейтралізувати більшість кібератак на систему [13].

Час реагування на інциденти (IRT) оцінюється приблизно у 2 години. За останній рік близько 1 години. Такий показник забезпечується завдяки впровадженню автоматизованих систем моніторингу, що дозволяє оперативно виявляти та локалізувати загрози. Дані про тривалість відновлення після інцидентів або збоїв подані в табл. 3 [33].

Таблиця 3

Інциденти та збої Starlink за 2024—2025 рр.

Дата	Регіон	Тривалість
7 квітня 2025 р.	США, Канада, Європа	56 хвилин
21 січня 2025 р.	Україна	64 хвилини
9 жовтня 2024 р.	США, Європа	53 хвилини
8 серпня 2024 р.	США, Європа	43 хвилини
18 липня 2024 р.	Україна	31 хвилина
29 травня 2024 р.	США, Європа, Австралія	45 хвилин

Втрати сигналу під час атак (*PLR*) зазвичай не перевищують 1…3 %. Це стало можливим завдяки ефективній протидії загрозам як на рівні супутників, так і на рівні наземних терміналів [34], [35].

Доступність системи (A) перевищує 99 %. У середньому користувачі втрачають доступ до мережі не більше ніж на 87 годин протягом року, що відповідає високим стандартам безперервності обслуговування [36].

Висновки

Чисельна оцінка підтверджує, що Starlink демонструє високу кіберстійкість завдяки сучасній архітектурі, надійному шифруванню та ефективному моніторингу мережевих загроз. Проте інтеграція передових захисних рішень, таких як протоколи нового покоління (WPA3, квантова криптографія), поліпшення механізмів виявлення атак та оптимізація часу реагування на кіберзагрози здатні значно підвищити захищеність системи. Це дозволить мінімізувати ризики, навіть у випадку складних і багатоетапних атак, зберігаючи надійність зв’язку для користувачів у критичних умовах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] “FCC approves SpaceX’s plan to provide broadband services with Starlink satellites,” *GeekWire*. [Electronic resource]. Available: https://surl.li/tansii . Accessed: 02.12.2024.

[2] Anthony Spadafora, *Starlink internet coverage, cost, speeds and the latest news — what you need to know*. [Electronic resource]. Available: https://surl.li/peazry. Accessed: 02.12.2024.

[3] Bernard Sklar, *Digital Communications, Fundamentals and Applications*, Prentice Hall PTR, Second Edition, 2001. ISBN: 0-13-084788-7.

[4] A. Boyle, “SpaceX files FCC application for internet access network with 4,425 satellites,” *GeekWire*. [Electronic resource]. Available: https://www.geekwire.com/2016/spacex-fcc-application-internet-4425-satellites/ . Accessed: 02.12.2024.

[5] S. Cakaj, “The Parameters Comparison of the “Starlink” LEO Satellites Constellation for Different Orbital Shells,” *Frontiers in Communications and Networks*, no. 2(7), 2021.

[6] Catherine McNally. *SpaceX Starlink Satellite Internet Review*, 2023. [Electronic resource]. Available: https://www.reviews.org/internet-service/spacex-starlink-satellite-internet-review/ . Accessed: 02.12.2024.

[7] Denys Rozenvasser, and Kateryna Shulakova. “Estimation of the Starlink Global Satellite System Capacity,” *Proceedings of International Conference on Applied Innovation in IT*, vol. 11, Iss. 1, pp. 55-59, 2023. https://doi.org/10.25673/101912.

[8] Dr. S. Pekhterev “The bandwidth of the StarLink constellation and the assessment of its potential subscriber base in USA,” *SatMagazine*, pp. 54-57, November 2021.

[9] Михайло Року, «SpaceX перекидає ресурси на кібербезпеку, щоб усунути перешкоди в роботі Starlin,» 6 березня 2022. https://surl.li/zxvhiy . Дата звернення: 02.12.2024.

[10] *So you got your new Starlink? Congratulations! Now you need to step up your cyber protection as well*, 2023. [Electronic resource]. Available: https://surl.li/vdipuh . Accessed: 02.12.2024.

[11] *За місцеперебуванням супутників Starlink тепер можна стежити в режимі реального часу*. 2024. [Електронний ресурс]. Режим доступу: https://surl.li/pehndi. Дата звернення: 02.12.2024.

[12] T. McMillan, “Recent Intel Report Reveals New Starlink Vulnerabilities, Increasing Concerns About the Future of Global Satellite Internet,” *The Debrief*, 2023.[Electronic resource]. Available: https://surl.li/xtfpsl . Accessed: 02.12.2024.

[13] Gizem Yılmaz (2024). «Cybersecurity Threats in Global Satellite Internet». [Electronic resource]. Available: : https://www.cyberdefensemagazine.com/cybersecurity-threats-in-global-satellite-internet/ . Accessed: 02.12.2024.

[14] Gerber Christopher John, “Cybersecurity Risk Effects of Starlink on Rural Populations in the United States,” *Capitol Technology University ProQuest Dissertations & Theses*, 2023.[Electronic resource]. Available: https://surl.li/oziqzc Accessed: 02.12.2024.

[15] Humphreys, Todd E., et al. *Signal Structure of the Starlink Ku-Band Downlink.*, 2022. https://doi.org/10.48550/arXiv.2210.11578 .

[16] J. Proakis, and M. Salehi, *Digital communications 5th Edition. McGrawHill*, 2007.

[17] Kim MG, and Jo HS, “Performance Analysis of NB-IoT Uplink in Low Earth Orbit Non-Terrestrial Networks,” *Sensors* (Basel). 2022 Sep 19; 22 (18):7097. https://doi.org/10.3390/s22187097 .

[18] Michael Kan, SpaceX’s Starlink Raises Download Speed Goal From 1Gbps to 10Gbps. [Electronic resource]. Available: https://www.pcmag.com/news/spacexs-starlink-raises-download-speed-goal-from-1gbps-to-10gbps . Accessed: 02.12.2024s.

[19] Mike Dano, *Starlink’s network faces significant limitations, analysts find*. [Electronic resource]. Available: https://surl.li/rpvave . Accessed: 02.12.2024.

[20] Noah Clarke, *Starlink Internet Speeds – Updated For 2023*. [Electronic resource]. Available: https://www.starlinkhardware.com/starlink-internet-speeds/ . Accessed: 02.12.2024.

[21] T. G. R. Reid, et al., Position, “Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications,” *Wiley-IEEE*, vol. 1, ch. Navigation from Low Earth Orbit: Part 1: *Concept, Capability, and Future Promise*., pp. 1359-1380, 2020.

[22] T. G. Reid, A. M. Neish, T. Walter, and P. K. Enge, “Broadband LEO constellations for navigation,” *Navigation*, Journal of the Institute of Navigation, vol. 65, no. 2, pp. 205-220, 2018.

[23] A .Aguilar, P. Butler, J. Collins, and M. Guerster, “Tradespace exploration of the next generation communication satellite,” *AIAA Scitech 2019 Forum*, 2019.

[24] Tyler Cooper, *Starlink Internet Speeds.* [Electronic resource]. Available: https://broadbandnow.com/starlink . Accessed: 02.12.2024.

[25] *World’s most advanced broadband satellite internet.* [Electronic resource]. Available: https://www.starlink.com/technology . Accessed: 02.12.2024.

[26] Z. M. Kassas, “Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications,” *Wiley-IEEE*, 2020, vol. 1, ch. *Navigation from Low Earth Orbit: Part 2: Models, Implementation, and performance*, pp. 1381-1412.

[27] *Китай розпочав розгортання власної глобальної мережі супутникового інтернету*, 2024. [Електронний ресурс]. Режим доступу: https://surl.li/jktqmb . Дата звернення: 02.12.2024.

[28] SpaceX розробляє Marslink – версію Starlink для забезпечення інтернетом Марса, 2024. [Електронний ресурс]. Режим доступу:https://mediasat.info/uk/2024/11/12/spacex-rozroblyaye-marslink/ . Дата звернення: 02.12.2024.

[299] *SpaceX Gets US Contract to Expand Ukraine’s Access to Starshield*, 2024. [Electronic resource]. Available: https://surl.li/xscrez . Accessed: 02.12.2024.

[30] Kareem, Karwan, *Cyber Threat Landscape Analysis for Starlink Assessing Risks and Mitigation Strategies in the Global Satellite Internet Infrastructure*, 2024. 10.48550/arXiv.2406.07562.

31] *What is Starlink Internet? Your Guide to Elon Musk’s Satellite Network*, 2024. [Electronic resource]. Available: https://blog.internxt.com/starlink/ . Accessed: 02.12.2024.

[32] Abhimanyu Ghoshal, *Starlink’s first constellation of direct-to-phone satellites is now in orbit*, 2024. [Electronic resource]. Available: https://newatlas.com/technology/starlink-direct-to-phone-satellites-orbit/ . Accessed: 02.12.2024.

[33] *Is Starlink down?* 2025. [Electronic resource]. Available: https://downforeveryoneorjustme.com/starlink . Accessed: 02.05.2025.

[34] Thomas Kunath, *Cisco Catalyst SD-WAN optimizations for Starlink*, 2024. [Electronic resource]. Available: https://learningnetwork.cisco.com/s/article/cisco-catalyst-sd-wan-optimizations-for-starlink . Accessed: 02.12.2024.

[35] Dominic Laniewski, Eric Lanfer, and Nils Aschenbruck, “Measuring Mobile Starlink Performance,” *A Comprehensive Look*, 2025. [Electronic resource]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10877858 . Accessed: 02.03.2025.

[36] *Starlink Specifications*. URL: https://www.starlink.com/legal/documents/DOC-1138-34130-60 (дата звернення: 02.12.2024).

Рекомендована кафедрою Інфокомунікаційних систем і технологій ВНТУ

Стаття надійшла до редакції 15.04.25

Розенвассер Денис Михайлович — канд. техн. наук, доцент кафедри комп'ютерних наук, e-mail: denysrozenvasser@gmail.com ;

Педяш Володимир Віталійович — канд. техн. наук, доцент, доцент кафедри комп'ютерної інженерії та інтелектуальних технологій;

Русу Олександр Петрович — канд. техн. наук, доцент кафедри комп'ютерних наук.

Міжнародний гуманітарний університет, Одеса, Україна;

Стрелковська Юлія Олександрівна — канд. юр. наук, доцент.

Worthing College, м. Вортінг, Велика Британія

D. M. Rozenvasser[1]
V. V. Pedyash[1]
O. P. Rusu[1]
Yu. O. Strelkovska[2]

Vulnerabilities and cybersecurity of Starlink

[1]International Humanitarian University, Odesa, Ukraine;
[2]Worthing College, Worthing, United Kingdom

The article is devoted to a comprehensive analysis of vulnerabilities and cybersecurity problems of the Starlink satellite network, which provides global access to the Internet through a network of low-orbit satellites. The technological aspects of the system's functioning are considered, including the network architecture, data transmission principles, as well as the interaction between satellites, ground stations and user terminals. The key components of the system that can become objects of potential cyberattacks are outlined, in particular satellites, ground gateways and client terminals. Particular attention is paid to the analysis of the main threats, such as signal interception, DDoS attacks, unauthorized access to data, signal jamming and physical failures in the operation of satellites. The possible consequences of such attacks for private users, businesses, military infrastructure and the global communications network are investigated. The current state of Starlink cybersecurity is analysed, including the use of encryption, authentication, secure data transfer protocols, and early threat detection systems. Recommendations are provided for improving cybersecurity, including the implementation of dynamic encryption mechanisms, increasing network resilience to external attacks, improving incident response strategies, and integrating advanced technologies such as quantum cryptography and zero-trust networks. The overall level of system security is assessed, including attack resilience indicators, incident response time, and network availability. Promising directions for reducing risks and ensuring stable operation of the Starlink infrastructure in the face of modern cyber threats are outlined. The level of system security is assessed based on numerical indicators, including resistance to external threats and the ability to recover from attacks.

Keywords: Starlink, vulnerabilities, cybersecurity, attacks, satellites, internet, encryption.

Rozenvasser Denys M. — Cand. Sc. (Eng.), Associate Professor of the Chair of Computer Sciences, e-mail: denysrozenvasser@gmail.com ;

Pedyash Volodymyr V. — Cand. Sc. (Eng.), Associate Professor, Associate Professor of the Chair of Computer Engineering and Intellectual Technologies;

Rusu Oleksandr P. — Cand. Sc. (Eng.), Associate Professor of the Chair of Computer Sciences.

Strelkovska Yulia O. — Candidate of Law, Associate Professor.