УДК 004.056:621.396.946 DOI: 10.18372/2073-4751.84.20892

Білоненко В.Ю.,
orcid.org/0009-0002-7941-7249
vladyslav.bilonenko@npp.kai.edu.ua
Зарубінська І.Б.
orcid.org/0000-0002-7931-1324
iryna.zarubinska@npp.kai. edu.ua
Костюк І.Ю.
orcid.org/0009-0002-1753-4466
ihor.kostiuk@npp.kai.edu.ua
Кутінов О.М.
orcid.org/0009-0000-5559-502X
alexeykutinov@i.ua

ОЦІНЮВАННЯ РИЗИКІВ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУПУТНИКОВИХ КАНАЛІВ STARLINK В АВІАЦІЙНИХ ПІДПРИЄМСТВАХ

Державний університет «Київський авіаційний університет»

Вступ

Авіаційна галузь належить до стратегічно важливих секторів економіки та є критичною інфраструктурою, функціонування якої безпосередньо впливає на національну безпеку, економічний розвиток та соціальну стабільність. Сучасні авіаційні підприємства характеризуються високим рівнем цифровізації виробничих процесів, систем управління та логістики, що передбачає інтенсивне використання телекомунікаційних систем для передачі технологічної, комерційної та службової інформації.

Традиційні наземні телекомунікаційні мережі мають обмеження щодо географічного охоплення, стійкості до природних катастроф та швидкості розгортання в умовах надзвичайних ситуацій. У цьому контексті супутникові системи зв'язку набувають особливої актуальності як альтернативний або резервний канал комунікації.

Система Starlink, розроблена компанією SpaceX, представляє низькоорбітальну супутникову мережу, що забезпечує широкосмуговий доступ до Інтернету з низькою затримкою сигналу. Архітектура системи базується на великій кількості супутників на висоті 550-570 км, що забезпечує глобальне покриття та високу пропускну здатність. Станом на 2025 рік мережа налічує понад 9357 активних супутників, а планується розгортання до 42000 супутників.[1]

Інтеграція супутникових каналів Starlink у інформаційну інфраструктуру авіаційних підприємств створює нові можливості для забезпечення безперервності діяльності, однак водночас формує додаткові вектори кібератак та потребує перегляду традиційних підходів до забезпечення інформаційної безпеки.

Мета і постановка завдання

Метою статті є дослідження особливостей оцінювання ризиків та забезпечення інформаційної безпеки супутникових каналів зв'язку Starlink при їх використанні в інформаційній інфраструктурі авіаційних підприємств як об'єктів критичної інфраструктури з урахуванням архітектурних характеристик системи, сегментної

структури та галузевих вимог до безперервності функціонування.

Для досягнення поставленої мети у статті передбачено вирішення таких завдань: проведення структурного аналізу архітектури системи Starlink; ідентифікація та систематизація загроз інформаційній безпеці у космічному, наземному та мережевому сегментах; формування адаптованої моделі загроз для авіаційних підприємств; розроблення формалізованого підходу до кількісного оцінювання ризиків інтеграції супутникового каналу; обґрунтування концептуальних засад побудови багаторівневої системи захисту.

Основна частина

Система Starlink базується на низькоорбітальному супутниковому угрупованні (Low Earth Orbit, LEO), що відрізняється від традиційних геостаціонарних супутників значно меншою висотою орбіти та більшою щільністю покриття. Супутники розміщені на висоті 550-570 км над поверхнею Землі та рухаються зі швидкістю близько 7,5 км/с, що забезпечує низьку затримку сигналу (latency) у діапазоні 20-40 мс порівняно з 500-700 мс для геостаціонарних супутників.[2]

Архітектуру системи можна розглянути на рисунку 1.:

- Космічний сегмент: супутники з фазованими антенними решітками та лазерними міжсупутниковими зв'язками;
- Наземний сегмент: термінали користувачів (User Terminals) з активними фазованими антенними решітками та шлюзи (Gateways), що забезпечують підключення до наземної інфраструктури Інтернету;
- Управлінський сегмент: центри управління та контролю, що здійснюють орбітальне позиціювання та маршрутизацію трафіку.

Архітектура системи передбачає використання принципів мереж із динамічною маршрутизацією та міжвузловою взаємодією, що за своєю логікою наближені до mesh-підходів, однак адаптовані до специфіки низькоорбітальної супутникової інфраструктури.[3]

На авіаційних підприємствах супутникові канали Starlink можуть застосовуватися для наступних сценаріїв:

1. Резервування основних каналів зв'язку: забезпечення резервного каналу для критичних систем у разі виходу з ладу наземної інфраструктури або під час планового обслуговування.
2. Організація віддаленого доступу: забезпечення безпечного доступу до виробничих систем, систем управління

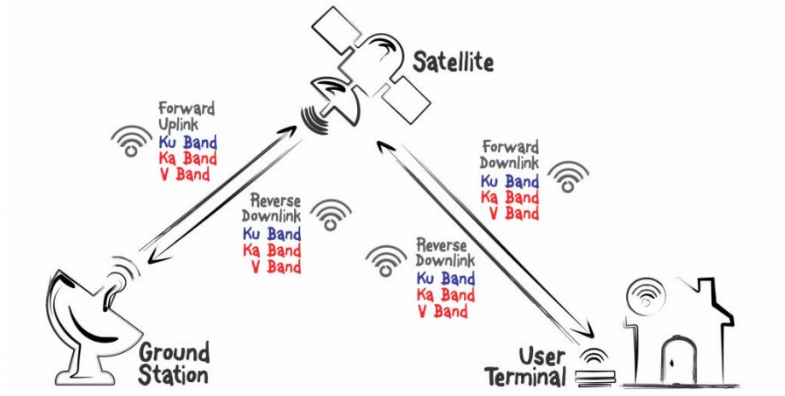

Рис. 1 Архітектурна модель системи Starlink

З рисунку 1 зрозуміло, що у системи можна виділити 3 компоненти:

повітряним рухом та інших критичних інформаційних систем для персоналу,

що працює віддалено або перебуває у відрядженні.
3. Обмін даними між філіями та віддаленими об'єктами: забезпечення зв'язку між центральним офісом та віддаленими аеропортами, складськими комплексами та іншими об'єктами інфраструктури.
4. Забезпечення зв'язку в умовах надзвичайних ситуацій: швидке розгортання комунікаційної інфраструктури у разі природних катастроф, техногенних аварій або інших надзвичайних ситуацій, що призводять до порушення роботи наземних мереж.
5. Інтеграція з системами моніторингу та управління: передача даних від систем моніторингу стану літаків, систем управління логістикою та інших IoT-пристроїв.
6. Забезпечення зв'язку на борту літаків: використання авіаційних терміналів Starlink для забезпечення інтернет-зв'язку пасажирів та передачі телеметричних даних.

Специфіка авіаційної галузі полягає у високій вимогливості до безперервності функціонування, цілісності та конфіденційності інформації. Будь-яке порушення роботи телекомунікаційних систем може вплинути на виробничі процеси, безпеку польотів, логістичні операції та фінансову діяльність підприємства.

Методи дослідження

Дослідження базується на системному підході до аналізу безпеки супутникових каналів зв'язку, що поєднує структурне моделювання архітектури системи, ризик-орієнтований аналіз та формалізацію загроз. На першому етапі здійснено структурний аналіз архітектури системи Starlink із виокремленням космічного, наземного та мережевого сегментів, визначенням їх функціональних ролей та потенційних поверхонь атаки. Це дозволило сформувати базову сегментну модель системи як багаторівневого периметра безпеки.

На другому етапі проведено ідентифікацію загроз із використанням методології STRIDE, адаптованої до специфіки супутникових мереж низької навколоземної орбіти. Особливу увагу приділено врахуванню нетипових для класичних корпоративних мереж векторів атак, зокрема міжсупутникової взаємодії, динамічної маршрутизації та залежності від провайдера супутникової інфраструктури.

Оцінювання ризиків здійснювалося на основі підходів ISO/IEC 27005 із подальшою формалізацією взаємозв'язку активів, загроз та вразливостей у вигляді математичної моделі. Для кількісного представлення ризику використано ймовірнісну інтерпретацію реалізації загроз та умовної експлуатації вразливостей із урахуванням критичності активів авіаційної інфраструктури. Запропоновано введення сегментних коефіцієнтів уразливості та коефіцієнта ефективності заходів захисту, що дозволяє оцінити залишковий ризик інтеграції супутникового каналу.

Додатково здійснено аналіз нормативно-правових вимог у сфері кібербезпеки критичної інфраструктури, міжнародних стандартів управління інформаційною безпекою та галузевих вимог авіаційної безпеки. Це забезпечило узгодження розробленої моделі з чинними регуляторними та стандартними підходами

Аналіз загроз інформаційній безпеці

Інтеграція Starlink у мережеву інфраструктуру авіаційного підприємства формує багаторівневу модель загроз, яка включає космічний, наземний та мережевий сегменти. Кожен сегмент має власні характеристики та вектори атак. Схему інтеграції можна побачити на рисунку 2.

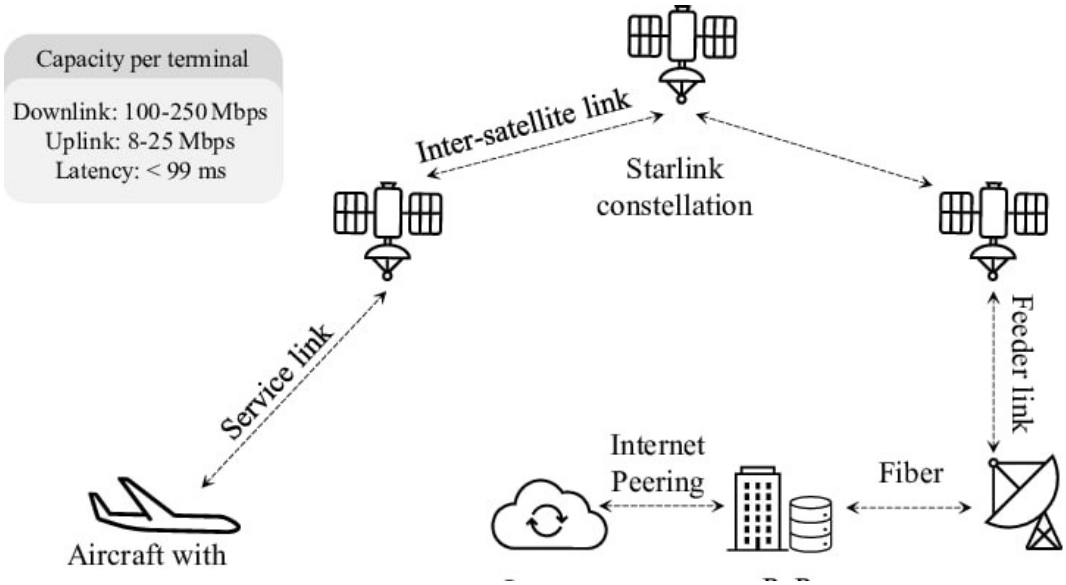

Рис. 2 Мережева архітектура супутникової системи Starlink з інтеграцією в авіаційну інфраструктуру

З точки зору інформаційної безпеки, архітектура системи є багаторівневою та формує декілька потенційних поверхонь атаки:

– рівень радіодоступу (User Terminal ↔ Satellite),

– міжсупутниковий рівень (Inter-satellite links),

– рівень шлюзів та peering-центрів,

– інтеграція в локальну мережу підприємства.

Така багаторівневість зумовлює необхідність розгляду кожного сегмента як окремого периметра безпеки.

Космічний сегмент включає супутники та міжсупутникові зв'язки. Основні загрози:

Незважаючи на використання криптографічних механізмів на рівні провайдера, теоретично можливе перехоплення радіосигналів між супутниками та терміналами з використанням спеціалізованого обладнання. Аналіз метаданих трафіку (обсяги переданих даних, частота зв'язку, тривалість сесій) може дозволити зловмисникам визначити структуру мережі підприємства, типи використовуваних сервісів та активність користувачів.

Теоретично можливі атаки на програмне забезпечення супутників через канали оновлення прошивок або через експлуатацію вразливостей у системах управління орбітальним угрупованням. Компрометація супутника може призвести до перехоплення або модифікації трафіку, що проходить через нього.

Лазерні міжсупутникові зв'язки можуть бути об'єктом атак типу "людина посередині" (man-in-the-middle) за умови фізичного доступу до траєкторії сигналу або через компрометацію системи маршрутизації.

Наземний сегмент включає термінали користувачів, шлюзи та інфраструктуру підключення до Інтернету.

Наземні термінали Starlink можуть бути об'єктом фізичного компрометування. Несанкціонований доступ до обладнання дозволяє зловмисникам:

- Встановлювати апаратні закладки (hardware implants) для перехоплення трафіку;
- Змінювати налаштування маршрутизації та конфігурацію безпеки;
- Впроваджувати шкідливе програмне забезпечення через інтерфейси налагодження;

- Виконувати атаки типу "evil maid" для компрометації системи під час її відсутності.

Вразливості у прошивках терміналів або у веб-інтерфейсах управління можуть дозволити зловмисникам отримати несанкціонований доступ до системи навіть без фізичного доступу. Це особливо актуально для терміналів, що підключені до локальної мережі підприємства.

Шлюзи Starlink, що забезпечують підключення до наземної інфраструктури Інтернету, можуть бути об'єктом атак з боку зловмисників, що мають доступ до наземних мереж.

Атаки типу "відмова в обслуговуванні" (DoS/DDoS)

Спроби перевантаження каналу або цілеспрямоване створення перешкод можуть призвести до зниження якості зв'язку або його повної втрати. Особливо небезпечні розподілені атаки (DDoS), що координуються через мережу зомбованих пристроїв.

За відсутності належної сегментації мережі супутниковий канал може стати точкою входу для атак на внутрішні інформаційні системи підприємства. Зловмисники можуть використовувати супутниковий канал як альтернативний вектор атаки, обходячи традиційні заходи захисту, налаштовані для наземних мереж.

Мережа Starlink використовує динамічну маршрутизацію для оптимізації шляху трафіку через супутникове угруповання. Компрометація протоколів маршрутизації може призвести до перенаправлення трафіку через зловмисні вузли або до створення петель маршрутизації.

Ризики пов'язані з програмним забезпеченням, оновленнями прошивок та залежністю від зовнішнього провайдера супутникової інфраструктури:

- Компрометація оновлень прошивок під час їх розповсюдження;
- Залежність від провайдера щодо конфігурації безпеки та політик доступу;
- Ризики, пов'язані з використанням обладнання та програмного забезпечення від постачальників з невідомою репутацією безпеки.

Формування моделі загроз та ризиків для авіаційних підприємств повинно враховувати специфіку галузі та вимоги до об'єктів критичної інфраструктури.

Для побудови моделі загроз необхідно провести класифікацію активів інформаційної системи за рівнем критичності:

- Критичні активи: системи управління повітряним рухом, системи управління польотами, системи безпеки аеропортів;
- Важливі активи: системи управління логістикою, фінансові системи, системи управління персоналом;
- Стандартні активи: офісні системи, системи електронної пошти, веб-сервіси.

Формування моделі загроз повинно враховувати наступні фактори:

1. Критичність переданих даних: рівень конфіденційності та важливості інформації, що передається через супутниковий канал.
2. Топологія мережі підприємства: структура локальної мережі, наявність сегментації, розміщення критичних систем відносно точки входу супутникового каналу.
3. Наявність резервних каналів: можливість переключення на альтернативні канали зв'язку у разі компрометації або виходу з ладу супутникового каналу.
4. Рівень фізичного захисту обладнання: наявність заходів фізичного захисту терміналів та іншого обладнання від несанкціонованого доступу.
5. Нормативні вимоги: вимоги законодавства у сфері захисту інформації та критичної інфраструктури, стандарти кібербезпеки (ISO/IEC 27001, NIST Cybersecurity Framework, тощо).

6. Рівень кваліфікації персоналу: наявність навчальних програм та рівень обізнаності персоналу щодо кіберзагроз.

Формалізація моделі оцінювання ризиків супутникового каналу

Для переходу від якісного аналізу загроз до кількісної оцінки рівня ризику інтеграції супутникового каналу Starlink у інформаційну інфраструктуру авіаційного підприємства пропонується формалізована модель, що враховує взаємозв'язок активів, загроз, вразливостей, сегментної структури системи та рівня впроваджених заходів захисту.

Нехай $A=\{a_1,a_2,...,a_n\}$— множина активів авіаційного підприємства, $T=\{t_1,t_2,...,t_m\}$— множина потенційних загроз, а $V=\{v_1,v_2,...,v_k\}$— множина вразливостей, що можуть бути експлуатовані зловмисником. У цьому випадку ризик для окремого активу a_i може бути поданий у вигляді

$$R_i=\sum_{j=1}^{m} P(t_j)\sum_{l=1}^{k} P(v_l\vee t_j)\cdot I(a_i),$$

де $P(t_j)$характеризує ймовірність реалізації загрози t_j, величина $P(v_l\vee t_j)$ відображає умовну ймовірність успішної експлуатації відповідної вразливості за наявності цієї загрози, а $I(a_i)$визначає масштаб впливу на актив і може оцінюватися за нормалізованою шкалою критичності. Формула дозволяє врахувати не лише сам факт існування загрози, але й її потенційну реалізованість через конкретні технічні або організаційні слабкі місця.

З огляду на те, що система Starlink має багаторівневу архітектуру, доцільно врахувати сегментну структуру, яка включає космічний, наземний та мережевий сегменти. Введемо множину сегментів $S=\{s_1,s_2,s_3\}$, де кожному сегменту відповідає коефіцієнт уразливості $\alpha_s\in[0,1]$, що відображає його внесок у загальний ризик. Тоді ризик для активу з урахуванням конкретного сегмента можна записати у вигляді

$$R_{i,s}=R_i\cdot\alpha_s. \quad ¿$$

Формула дозволяє врахувати той факт, що одна й та сама загроза може мати різну вагу залежно від того, через який сегмент системи вона реалізується. Наприклад, мережевий сегмент, інтегрований у внутрішню інфраструктуру підприємства, зазвичай має більший коефіцієнт α_s, ніж космічний сегмент.

Інтегральний ризик супутникового каналу для підприємства визначається як сума ризиків для всіх активів та сегментів:

$$R_{sat}=\sum_{i=1}^{n}\sum_{s=1}^{3} R_{i,s}. \quad ¿$$

Вираз відображає системний характер ризику та дозволяє перейти від локальної оцінки окремих активів до оцінки загального рівня небезпеки інтеграції супутникового каналу.

Оскільки авіаційні підприємства належать до об'єктів критичної інфраструктури, доцільним є введення коефіцієнта стратегічної важливості активу $w_i\in[0,1]$, що відображає його роль у забезпеченні безпеки польотів та безперервності діяльності. З урахуванням цього інтегральний ризик для критичної інфраструктури можна подати як

$$R_{crit}=\sum_{i=1}^{n} w_i\sum_{s=1}^{3} R_{i,s}. \quad ¿$$

Таким чином, формула дозволяє посилити внесок найбільш критичних активів у загальний показник ризику та адекватно відобразити специфіку галузі.

З метою оцінки ефективності впроваджених заходів захисту вводиться коефіцієнт ефективності безпеки $\beta\in[0,1]$, який узагальнює рівень реалізації технічних, криптографічних та організаційних механізмів захисту. У цьому випадку залишковий ризик визначається як

$$R_{res}=R_{crit}(1-\beta). \quad ¿$$

Формула відображає зменшення ризику пропорційно рівню впроваджених засобів захисту. При $\beta\to 1$залишковий ризик наближається до мінімального

значення, тоді як при відсутності заходів захисту ($\beta=0$) він дорівнює початковому критичному ризику.

Запропонована модель забезпечує перехід від якісної оцінки загроз до кількісного аналізу ризиків інтеграції супутникових каналів Starlink у мережу авіаційного підприємства. На відміну від традиційних підходів до оцінювання ризиків інформаційної безпеки, які розглядають телекомунікаційні канали як однорідний периметр, у запропонованій моделі враховується сегментна структура низькоорбітальної супутникової системи та її інтеграція у внутрішню інфраструктуру підприємства. Це дозволяє диференціювати внесок космічного, наземного та мережевого сегментів у формування загального ризику та адаптувати оцінювання до специфіки архітектури LEO-систем.

Наукова новизна запропонованого підходу полягає у поєднанні класичної ризик-орієнтованої моделі з урахуванням умовної реалізованості вразливостей, сегментних коефіцієнтів уразливості та вагових коефіцієнтів критичності активів об'єктів авіаційної інфраструктури. Введення коефіцієнта ефективності захисту βдозволяє формалізувати вплив впроваджених технічних і організаційних заходів безпеки на зниження залишкового ризику та перейти до задач оптимізації структури системи захисту.

Практична значущість моделі полягає у можливості її використання для проведення сценарного аналізу, оцінювання наслідків реалізації конкретних типів атак, а також для обґрунтування доцільності впровадження додаткових механізмів захисту, зокрема сегментації мережі, криптографічного тунелювання, багатофакторної аутентифікації та систем моніторингу безпеки. Модель може бути застосована як інструмент підтримки прийняття управлінських рішень при інтеграції супутникових каналів зв'язку в інформаційні системи авіаційних підприємств та інших об'єктів критичної інфраструктури.

Концептуальні засади забезпечення безпеки

Комплексна система забезпечення інформаційної безпеки супутникових каналів Starlink на авіаційних підприємствах повинна базуватися на багаторівневому підході, що поєднує технічні, програмні та організаційні заходи.

Супутниковий канал повинен інтегруватися через демілітаризовану зону (DMZ) з використанням міжмережевих екранів (firewalls) та систем виявлення/запобігання вторгнень (IDS/IPS). Рекомендована архітектура включає:

- Виділений підмережу для супутникового терміналу з обмеженим доступом до внутрішньої мережі;
- Багаторівневий firewall з правилами, що базуються на принципі найменших привілеїв;
- Системи IDS/IPS з сигнатурами, адаптованими для виявлення аномалій у супутниковому трафіку;
- Використання технологій zero-trust для контролю доступу до критичних ресурсів.

Необхідне застосування додаткового шифрування на рівні VPN або IPsec поверх базових механізмів шифрування провайдера. Рекомендації включають:

- Використання VPN-тунелів з симетричним шифруванням AES-256 або вище;
- Застосування протоколів IPsec у режимі tunnel для забезпечення конфіденційності та цілісності даних;
- Використання сучасних протоколів обміну ключами (IKEv2, WireGuard) з стійкими алгоритмами;
- Реалізація forward secrecy для забезпечення захисту минулих сесій у разі компрометації ключів;

- Регулярна ротація криптографічних ключів згідно з політикою безпеки.

Багаторівнева аутентифікація та контроль доступу

Доступ до управління терміналами та критичними системами повинен здійснюватися із застосуванням багатофакторної Аутентифікації (MFA) та централізованих систем контролю доступу:

- Використання MFA з комбінацією паролів, токенів, біометричних даних або сертифікатів;
- Інтеграція з системами Identity and Access Management (IAM) для централізованого управління доступом;
- Реалізація принципу найменших привілеїв з наданням доступу лише до необхідних ресурсів;
- Регулярний аудит прав доступу та їх ревізія;
- Використання протоколів Single Sign-On (SSO) для зручності та безпеки.

Постійний моніторинг трафіку, аналіз журналів подій та інтеграція із системами Security Information and Event Management (SIEM) дозволяють своєчасно виявляти аномалії та реагувати на інциденти:

- Збір та аналіз журналів від усіх компонентів системи (терміналів, firewall, IDS/IPS, серверів);
- Використання систем SIEM для кореляції подій та виявлення складних атак;
- Застосування технологій машинного навчання для виявлення аномалій у трафіку;
- Налаштування системи сповіщень для критичних подій безпеки;
- Регулярний аналіз метрик безпеки та оцінка ефективності заходів захисту.

Управління вразливостями та оновленнями

Необхідно впровадити процеси управління вразливостями та оновленнями програмного забезпечення:

- Регулярне сканування систем на наявність вразливостей з використанням автоматизованих інструментів;
- Моніторинг бюлетенів безпеки від провайдера Starlink та інших постачальників;
- Тестування оновлень на тестовому середовищі перед впровадженням у продуктивну систему;
- Ведення реєстру вразливостей з оцінкою критичності та планами усунення;
- Забезпечення резервного копіювання конфігурацій перед оновленнями.

Організаційні заходи є невід'ємною частиною комплексної системи захисту:

1. Регламентація використання: розробка політик та процедур використання супутникового каналу з визначенням дозволених сценаріїв використання та обмежень.
2. Обмеження прав доступу: впровадження процедур надання та відкликання прав доступу з регулярною ревізією.
3. Навчання персоналу: проведення регулярних тренінгів з кібербезпеки, зокрема щодо специфіки супутникових мереж та соціальної інженерії.
4. Плани реагування на інциденти: розробка детальних планів реагування на різні типи інцидентів безпеки з визначенням ролей та відповідальності.
5. Регулярні аудити безпеки: проведення внутрішніх та зовнішніх аудитів безпеки для оцінки ефективності заходів захисту та виявлення слабких місць.
6. Управління ризиками: регулярна оцінка ризиків інформаційної безпеки з оновленням моделі загроз та планів захисту.

Нормативно-правові аспекти

Авіаційні підприємства підпадають під вимоги законодавства у сфері захисту інформації та критичної інфраструктури. Використання супутникових каналів зв'язку повинно відповідати вимогам щодо захисту службової та конфіденційної інформації, а також стандартам кібербезпеки.

Українське законодавство визначає вимоги до захисту інформації та критичної інфраструктури через низку нормативно-правових актів:
- Закон України "Про основні засади забезпечення кібербезпеки України" визначає вимоги до об'єктів критичної інфраструктури;
- Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" встановлює вимоги до захисту інформації;
- Вимоги Державної служби спеціального зв'язку та захисту інформації України щодо використання криптографічних засобів захисту інформації.

Необхідним є дотримання міжнародних стандартів кібербезпеки:
- ISO/IEC 27001:2022 "Information security management systems" - система управління інформаційною безпекою;
- ISO/IEC 27002:2022 "Information security controls" - набір контролів безпеки;
- NIST Cybersecurity Framework - фреймворк кібербезпеки від Національного інституту стандартів та технологій США;
- IEC 62443 "Security for industrial automation and control systems" - стандарти безпеки для промислових систем управління.

Авіаційна галузь має специфічні вимоги до безпеки:
- Стандарти ІКАО (ICAO) щодо забезпечення безпеки авіаційних систем;
- Вимоги Європейського агентства з безпеки повітряного руху (EASA) щодо кібербезпеки авіаційних систем;
- Стандарти IATA (International Air Transport Association) щодо захисту даних авіакомпаній.

Необхідним є проведення оцінки ризиків, розроблення внутрішніх політик безпеки та впровадження процедур контролю відповідності:
- Регулярна оцінка відповідності вимогам законодавства та стандартів;
- Розробка та оновлення внутрішніх політик та процедур безпеки;
- Ведення документації щодо заходів захисту та інцидентів безпеки;
- Підготовка звітів для регуляторних органів та аудиторів.

Висновки

Супутникові канали зв'язку Starlink відкривають нові можливості для забезпечення безперервності діяльності авіаційних підприємств, особливо в умовах надзвичайних ситуацій або при необхідності швидкого розгортання комунікаційної інфраструктури. Низька затримка сигналу, глобальне покриття та висока пропускна здатність роблять цю технологію привабливою для використання в авіаційній галузі.

Водночас інтеграція супутникових каналів у внутрішню інфраструктуру авіаційних підприємств створює додаткові кіберризики, що потребують системного підходу до забезпечення інформаційної безпеки. Багаторівнева модель загроз, що включає космічний, наземний та мережевий сегменти, вимагає комплексних заходів захисту на всіх рівнях.

Комплексний захист повинен базуватися на поєднанні технічних, програмних та організаційних заходів, формуванні актуальної моделі загроз та постійному моніторингу безпекового стану мережі. Особливу увагу слід приділити сегментації мережі, додатковому криптографічному захисту, багатофакторній аутентифікації та інтеграції з системами моніторингу безпеки.

Література

1. Maral G., Bousquet M., Sun Z. Satellite Communications Systems: Systems, Techniques and Technology. 6th ed. Chichester : Wiley, 2020. 768 p.
2. Kodheli O., Guidotti A., Vanelli-Coralli A. Integration of satellites in 5G through LEO mega-constellations // *IEEE Network*. 2017. Vol. 32, No. 5. P. 44–51.

3. Handley M. Delay is not an option: Low latency routing in space // *Proceedings of ACM SIGCOMM 2018*. Budapest, 2018. P. 411–426.
4. Pavur J., Martinovic I. Security and privacy implications of satellite internet // *IEEE Symposium on Security and Privacy Workshops (SPW)*. 2020. P. 232–241.
5. Bhattacherjee D., Singla A., et al. Characterizing the security and privacy risks of LEO satellite networks // *USENIX Security Workshop*. 2021.
6. Shostack A. Threat Modeling: Designing for Security. Indianapolis : Wiley, 2014. 624 p.
7. Alberts C., Dorofee A. Managing Information Security Risks: The OCTAVE Approach. Boston : Addison-Wesley, 2003. 480 p.
8. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
9. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks.
10. NISTIR 8270. Introduction to Cybersecurity for Space Systems. National Institute of Standards and Technology, 2020.
11. ENISA. Cybersecurity for Critical Infrastructure Protection. European Union Agency for Cybersecurity, 2021.
12. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 12.12.2025).
13. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР (зі змін.). URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 12.12.2025).
14. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 12.12.2025).
15. Повітряний кодекс України : Закон України від 19.05.2011 № 3393-VI. URL: https://zakon.rada.gov.ua/laws/show/3393-17 (дата звернення: 02.03.2026).
16. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017 (дата звернення: 15.12.2025).
17. Деякі питання об’єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п (дата звернення: 15.12.2025).

Білоненко В.Ю., Зарубінська І.Б., Костюк І.Ю. Кутінов О.М.

ОЦІНЮВАННЯ РИЗИКІВ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУПУТНИКОВИХ КАНАЛІВ STARLINK В АВІАЦІЙНИХ ПІДПРИЄМСТВАХ

У статті досліджено особливості оцінювання ризиків та забезпечення інформаційної безпеки супутникових каналів зв’язку Starlink при їх використанні в інформаційній інфраструктурі авіаційних підприємств як об’єктів критичної

інфраструктури. Проведено структурний аналіз архітектури системи Starlink та визначено основні вектори загроз у космічному, наземному та мережевому сегментах. На основі методологій STRIDE та ISO/IEC 27005 сформовано адаптовану модель загроз для авіаційної галузі. Запропоновано формалізований підхід до кількісного оцінювання ризиків інтеграції супутникового каналу з урахуванням сегментної структури, критичності активів та ефективності заходів захисту. Обґрунтовано концептуальні засади побудови багаторівневої системи захисту, що включає сегментацію мережі, криптографічний захист, багатофакторну аутентифікацію та інтеграцію із системами моніторингу безпеки. Отримані результати можуть бути використані при впровадженні супутникових каналів зв’язку в інформаційну інфраструктуру підприємств авіаційної галузі.

Ключові слова: Starlink, супутниковий зв'язок, оцінювання ризиків, інформаційна безпека, кібербезпека, авіаційні підприємства, критична інфраструктура, формалізована модель, низькоорбітальні супутники.

Bilonenko V.Y., Zarubinska I.B., Kostiuk I.Y., Kutinov A.M.

RISK ASSESSMENT AND INFORMATION SECURITY ENSURING OF STARLINK SATELLITE COMMUNICATION CHANNELS AT AVIATION ENTERPRISES

The article investigates the specific features of risk assessment and information security ensuring of Starlink satellite communication channels when integrated into aviation enterprises as critical infrastructure objects. A structural analysis of the Starlink architecture was conducted, and key threat vectors in the space, ground, and network segments were identified. Based on STRIDE and ISO/IEC 27005 methodologies, an adapted threat model for aviation enterprises was developed. A formalized approach to quantitative risk assessment considering segment architecture, asset criticality and security control effectiveness is proposed. Conceptual principles of a multi-layered protection system are substantiated, including network segmentation, additional cryptographic protection, multi-factor authentication and integration with security monitoring systems. The results can be applied during the integration of satellite communication channels into aviation enterprise information infrastructures.

Keywords: Starlink, satellite communications, risk assessment, information security, cybersecurity, aviation enterprises, critical infrastructure, formalized model, low-orbit satellites**.**

Стаття подана до редакції: 28/11/2025
Стаття прийнята до опублікування:9/12/2025
Стаття опублікована:30/12/2025