DOI: https://doi.org/10.36910/6775-2524-0560-2026-62-40
УДК 004.056:621.396.946
Зарубінська Ірина Борисівна[1] д.п.н., професор
https://orcid.org/0000-0002-7931-1324
Білоненко Владислав Юрійович[1], викладач
https://orcid.org/0009-0002-7941-7249
Костюк Ігор Юрійович[1], викладач
https://orcid.org/0009-0002-1753-4466
Козловська Діана Валеріївна[1], студент
https://orcid.org/0009-0004-6223-0319
Хвищун Денис Миколайович[2], студент
[1]Національний університет «Київський авіаційний інститут», м. Київ, Україна
[2]Луцький національний технічний університет, м. Луцьк, Україна

МЕТОДИКА ОЦІНКИ ТА ЗНИЖЕННЯ КІБЕРРИЗИКІВ СУПУТНИКОВИХ КАНАЛІВ ЗВ'ЯЗКУ STARLINK В ІНФОРМАЦІЙНІЙ ІНФРАСТРУКТУРІ АВІАЦІЙНИХ ПІДПРИЄМСТВ

Зарубінська І.Б., Білоненко В.Ю., Костюк І.Ю., Козловська Д.В., Хвищун Д.М. Методика оцінки та зниження кіберризиків супутникових каналів зв'язку Starlink в інформаційній інфраструктурі авіаційних підприємств. У статті розроблено формалізовану методику оцінювання та зниження кіберризиків супутникових каналів зв'язку Starlink під час інтеграції в інформаційну інфраструктуру авіаційних підприємств як об'єктів критичної інфраструктури. На відміну від традиційних підходів, що здебільшого орієнтовані на наземні корпоративні мережі та матричні оцінки ризику, запропоновано розглядати супутниковий LEO-канал як автономний динамічний периметр безпеки з власною багаторівневою структурою загроз і топологічними залежностями. Методика поєднує структурну декомпозицію системи на космічний, наземний та інтеграційний сегменти, адаптоване застосування STRIDE для систематизації сценаріїв атак і підхід ISO/IEC 27005 для узгодженого ризик-менеджменту. Інформаційну інфраструктуру подано у вигляді орієнтованого графа, де вузли характеризуються коефіцієнтами критичності, а ребра імовірностями переходів атаки, модифікованими коефіцієнтами ослаблення захисних бар'єрів. Показано каскадний ефект альтернативних шляхів компрометації та продемонстровано, що впровадження сегментації, IDS/IPS та контрольованого доступу дозволяє кількісно зменшити інтегральний структурний ризик приблизно на 93–94% у прикладному сценарії. Запропонований підхід придатний для порівняння альтернативних архітектур захисту та обґрунтування контрольних точок з максимальним внеском у зниження ризику.
Ключові слова: Starlink, супутниковий зв'язок, інформаційна безпека, кібербезпека, авіаційні підприємства, критична інфраструктура, модель загроз

Zarubinska I., Bilonenko V., Kostiuk I., Kozlovska D., Khvyshchun D. Methodology for Assessing and Mitigating Cyber Risks of Starlink Satellite Communication Channels in the Information Infrastructure of Aviation Enterprises. The article develops a formalized methodology for assessing and mitigating cybersecurity risks of Starlink satellite communication channels when integrated into the information infrastructure of aviation enterprises as critical infrastructure objects. Unlike traditional approaches primarily focused on terrestrial corporate networks and matrix-based risk assessment, the proposed approach considers the LEO satellite channel as an autonomous dynamic security perimeter with its own multi-level threat structure and topological dependencies. The methodology combines structural decomposition of the system into space, ground, and integration segments, the adapted use of the STRIDE model for systematic classification of attack scenarios, and the ISO/IEC 27005 approach for consistent risk management. The information infrastructure is represented as a directed graph in which nodes are characterized by criticality coefficients and edges by attack transition probabilities modified by protective barrier attenuation factors. The cascading effect of alternative compromise paths is demonstrated, and it is shown that implementing segmentation, IDS/IPS, and controlled access can quantitatively reduce the integral structural risk by approximately 93–94% in a representative scenario. The proposed approach is suitable for comparing alternative security architectures and substantiating control points with the greatest impact on risk reduction.
Keywords: Keywords: Starlink, satellite communications, information security, cybersecurity, aviation enterprises, critical infrastructure, threat model

Постановка проблеми. Сучасні авіаційні підприємства функціонують в умовах високої цифровізації виробничих, логістичних та управлінських процесів, що обумовлює критичну залежність їх діяльності від стабільності та захищеності телекомунікаційної інфраструктури. Забезпечення безперервності зв'язку, цілісності та конфіденційності даних є необхідною умовою безпеки польотів, ефективного управління ресурсами та виконання регуляторних вимог у сфері авіаційної безпеки.

У цьому контексті супутникові системи низькоорбітального зв'язку, зокрема Starlink, активно інтегруються як резервні або додаткові канали передачі даних. Їх використання дозволяє підвищити доступність мережевих сервісів, зменшити залежність від наземної інфраструктури та забезпечити

функціонування підприємства в умовах надзвичайних ситуацій. Водночас інтеграція супутникового каналу у внутрішню мережу авіаційного підприємства формує нові вектори атак та розширює поверхню кіберзагроз.

Особливістю супутникових LEO-мереж є динамічна топологія, використання складних механізмів маршрутизації та наявність розподіленої інфраструктури, що ускладнює традиційні підходи до оцінки ризику. Існуючі методики аналізу інформаційної безпеки, як правило, орієнтовані на наземні корпоративні мережі та не враховують специфіку космічного та міжсегментного компонентів системи. У результаті відсутня формалізована модель, яка дозволяла б кількісно оцінити інтегральний ризик компрометації критичних активів через супутниковий канал з урахуванням альтернативних сценаріїв атак і каскадних ефектів.

Таким чином, виникає науково-прикладна проблема розроблення методики формалізованої оцінки та зниження кіберризиків супутникових каналів зв'язку в структурі авіаційних підприємств, яка б враховувала топологічні залежності, галузеву критичність активів та ефективність впроваджених засобів захисту.

Аналіз останніх досліджень і публікацій. Авіаційна галузь належить до стратегічно важливих секторів економіки та є критичною інфраструктурою, функціонування якої безпосередньо впливає на національну безпеку, економічний розвиток та соціальну стабільність [1-2]. 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 [2-4]. 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 [5-6].

Функціональні можливості та безпекові характеристики супутникового каналу значною мірою визначаються архітектурою системи Starlink, яка базується на низькоорбітальному супутниковому угрупованні (LEO). На відміну від традиційних геостаціонарних систем, супутники Starlink розміщені на висоті 550–570 км та рухаються зі швидкістю близько 7,5 км/с, що забезпечує істотно меншу затримку сигналу – у межах 20–40 мс проти 500–700 мс для геостаціонарних рішень [5, 7]. Така архітектура формує нову якість телекомунікаційного сервісу, придатного для задач, чутливих до затримок, однак водночас створює складну динамічну структуру мережевої взаємодії.

Система включає космічний сегмент із супутниками, обладнаними фазованими антенними решітками та лазерними міжсупутниковими каналами; наземний сегмент із користувацькими терміналами та шлюзами доступу до глобальної мережі; а також управлінський сегмент, що забезпечує орбітальне позиціювання й маршрутизацію трафіку [8]. Передача даних здійснюється з використанням частотних діапазонів Ku та Ka, а мережеві механізми побудовані за принципами mesh-взаємодії з адаптацією до супутникового середовища [6, 9]. Сукупність цих особливостей визначає складну багаторівневу структуру потенційних загроз.

В умовах авіаційних підприємств супутниковий канал застосовується як резервна або додаткова комунікаційна інфраструктура для підтримки критичних сервісів, віддаленого доступу до виробничих систем, обміну даними між територіально розподіленими об'єктами, а також забезпечення зв'язку в надзвичайних ситуаціях. Інтеграція з системами моніторингу, управління та бортовими інформаційними комплексами розширює функціональні можливості, проте одночасно збільшує поверхню потенційної атаки [2-4]. Високі вимоги до безперервності функціонування, цілісності та конфіденційності інформації в авіаційній галузі зумовлюють необхідність комплексного аналізу ризиків [10-12].

Аналіз загроз показує, що інтеграція супутникового каналу формує багаторівневу модель ризику. Космічний сегмент характеризується можливістю перехоплення радіосигналів, компрометації програмного забезпечення супутників або атак на міжсупутникові з'єднання [13, 14]. Наземний сегмент уразливий до фізичного втручання, логічної компрометації терміналів та атак на шлюзи доступу [15]. На мережевому рівні зберігається ризик атак типу DoS/DDoS, маніпуляцій протоколами маршрутизації та проникнення до внутрішньої мережі через недостатню сегментацію [16-17]. Додатковим фактором виступають ризики ланцюга постачання, пов'язані з оновленням програмного забезпечення та залежністю від зовнішнього провайдера [18].

Формування моделі загроз для авіаційного підприємства потребує врахування галузевої специфіки. Критичними активами є системи управління польотами, аеронавігаційні комплекси та інфраструктура безпеки аеропортів; важливими – логістичні та фінансові системи; стандартними – офісні сервіси [20]. Рівень ризику визначається не лише технічними характеристиками каналу, а й топологією мережі підприємства, наявністю резервування, фізичним захистом обладнання, відповідністю нормативним вимогам та підготовкою персоналу. Саме сукупність цих чинників обумовлює необхідність формалізованого підходу до оцінки кіберризиків супутникового каналу в структурі авіаційного підприємства, що і становить основу методичного розгляду.

Мета дослідження полягає в розробленні формалізованої методики оцінки та зниження кіберризиків супутникових каналів зв'язку Starlink при їх інтеграції в інформаційну інфраструктуру авіаційних підприємств з урахуванням структурних залежностей, альтернативних сценаріїв атак і галузевої критичності активів.

Виклад основного матеріалу. Аналіз архітектури системи Starlink та особливостей її інтеграції в інформаційну інфраструктуру авіаційного підприємства показує необхідність формалізованого підходу до дослідження кіберризиків [5]. Методологія дослідження базується на комплексному системному підході, який поєднує структурний аналіз компонентів супутникової мережі, дослідження технічної документації провайдера, узагальнення відомих вразливостей супутникових систем зв'язку та адаптацію сучасних методів оцінювання ризиків інформаційної безпеки до специфіки низькоорбітальних мереж.

На першому етапі було здійснено структурну декомпозицію архітектури системи з визначенням критичних компонентів і потенційних точок компрометації. Такий підхід дозволяє перейти від абстрактного опису мережі до формального виділення вузлів, що можуть виступати як точки входу для зловмисника або як проміжні елементи каскадного поширення атаки. Далі аналіз загроз проводився із застосуванням підходу STRIDE, адаптованого до умов супутникового сегмента, що дало змогу систематизувати можливі сценарії порушення конфіденційності, цілісності та доступності інформації. Оцінювання ризиків здійснювалося з урахуванням положень ISO/IEC 27005, а також вимог до об'єктів критичної інфраструктури, що забезпечило узгодженість результатів із нормативною базою та міжнародними стандартами [10-12].

Інтеграція супутникового каналу в мережеву інфраструктуру авіаційного підприємства формує багаторівневу модель загроз, яка охоплює космічний, наземний та внутрішньомережевий сегменти. Космічний сегмент характеризується ризиками перехоплення радіосигналів, аналізу метаданих трафіку, потенційної компрометації програмного забезпечення супутників або втручання в міжсупутникові з'єднання [5, 7]. Хоча криптографічні механізми на рівні провайдера знижують імовірність несанкціонованого доступу до змісту переданих даних, сама структура трафіку може бути джерелом інформації про активність та архітектуру мережі підприємства.

Наземний сегмент створює додаткові ризики, пов'язані як із фізичним доступом до обладнання, так і з можливими вразливостями програмного забезпечення терміналів або шлюзів. Компрометація термінала може призвести до зміни конфігурації маршрутизації, впровадження шкідливого коду або встановлення апаратних засобів перехоплення трафіку [13, 20]. Особливої уваги потребує ситуація, коли термінал інтегрований безпосередньо у локальну мережу підприємства без належної ізоляції.

На мережевому рівні актуальними залишаються атаки типу відмова в обслуговуванні, що здатні впливати на доступність каналу, а також ризики компрометації внутрішніх інформаційних систем через супутниковий сегмент у разі недостатньої сегментації мережі [12, 21]. Додатковим фактором виступають загрози ланцюга постачання, пов'язані з оновленнями прошивок, залежністю від зовнішнього провайдера та використанням сторонніх компонентів програмного й апаратного забезпечення [21].

Формування адекватної моделі загроз для авіаційного підприємства неможливе без урахування галузевої специфіки. Критичними активами виступають системи управління польотами, аеронавігаційні комплекси та системи безпеки аеропортів; важливими – логістичні, фінансові та управлінські інформаційні системи; стандартними – допоміжні офісні сервіси. Рівень ризику визначається не лише технічними характеристиками каналу, а й топологією корпоративної мережі, ступенем її сегментації, наявністю резервних каналів, фізичним захистом обладнання, нормативними вимогами та підготовкою персоналу.

Для розробки методики використано системний підхід до аналізу інформаційної безпеки супутникового каналу зв'язку як складової критичної інфраструктури авіаційного підприємства. На

відміну від традиційного розгляду телекомунікаційного каналу як ізольованого транспортного середовища, супутниковий канал розглядається як автономний динамічний периметр безпеки, що має власну багаторівневу структуру загроз, змінну топологію та специфічні вектори атак. Методика ґрунтується на таких ключових принципах.

1. Принцип багаторівневої декомпозиції. Супутниковий канал Starlink розглядається як система, що складається з трьох взаємопов'язаних сегментів:

$$S = \{C_{space}, C_{ground}, C_{integr}\} \quad (1)$$

де C_{space} – космічний сегмент (супутники, міжсупутникові лазерні канали, системи орбітального управління);

C_{ground} – наземний сегмент (користувацькі термінали, шлюзи, канали доступу до мережі провайдера);

C_{integr} – інтеграційний сегмент (демілітаризована зона, міжмережеві екрани, маршрутизатори, внутрішня корпоративна мережа).

Такий поділ дозволяє локалізувати джерела ризику, визначити специфічні вразливості кожного сегмента та врахувати їхній вплив на загальний рівень захищеності системи.

2. Принцип структурно-графового представлення. Інформаційна інфраструктура, інтегрована з супутниковим каналом, подається у вигляді орієнтованого графа взаємодії компонентів. Це дозволяє моделювати не лише окремі загрози, а й каскадні сценарії атак, латеральне переміщення зловмисника та комбіновані впливи на кілька сегментів одночасно.

Графова модель дозволяє визначити всі можливі шляхи проникнення з супутникового каналу до критичних активів; оцінити структурну вразливість мережі; виявити вузли з максимальною центральністю, компрометація яких призводить до найбільшого системного ефекту, що є принципово важливим для об'єктів критичної інфраструктури.

У межах моделі визначаються контрольні точки:

– точка входу супутникового трафіку;
– сегмент DMZ;
– міжмережеві екрани;
– точки автентифікації;
– системи моніторингу (SIEM).

Кожна контрольна точка розглядається як бар'єр, що знижує імовірність проходження атаки вздовж відповідного ребра графа.

3. Принцип кількісної оцінки ризику. Методика передбачає формалізацію ризику як функції критичності активів, імовірності реалізації загрози, наявності вразливостей та потенційного впливу на бізнес-процеси. Це забезпечує: об'єктивність оцінювання; можливість порівняння альтернативних архітектур захисту; кількісне визначення ефективності впроваджених заходів.

4. Принцип урахування динамічності LEO-мережі. Особливістю системи Starlink є використання низькоорбітального супутникового угруповання з динамічною маршрутизацією та постійною зміною конфігурації з'єднань. Тому ризик розглядається як змінна величина, що залежить від поточного стану мережі, інтенсивності трафіку та зовнішніх впливів.

Введення динамічної компоненти дозволяє врахувати тимчасові піки навантаження, сценарії перевантаження каналу та перехід системи до деградованих станів.

5. Принцип галузевої критичності. Авіаційні підприємства належать до об'єктів критичної інфраструктури, для яких допустимий рівень ризику є значно нижчим, ніж для звичайних корпоративних мереж. Тому методика вводить коригувальний коефіцієнт галузевої критичності, що відображає підвищені вимоги до безперервності функціонування, цілісності та конфіденційності інформації.

Для забезпечення кількісного аналізу кіберризиків супутникового каналу запропоновано формалізовану модель, у межах якої інформаційна система авіаційного підприємства, інтегрована із супутниковим сегментом, подається у вигляді орієнтованого графа:

$$G = (V, E) \quad (2)$$

де V – множина вузлів (термінал, шлюз, DMZ, сервер управління польотами, база даних тощо),

E – множина можливих каналів взаємодії або потенційних векторів атак.

Кожне ребро графа характеризується імовірністю реалізації атаки $P(e)$, а кожен вузол – коефіцієнтом критичності C_i. Такий підхід дозволяє відобразити топологічну структуру мережі та потенційні напрямки поширення атаки в межах єдиної математичної конструкції.

Множина вершин $V = \{v_1, v_2, \dots, v_n\}$ відповідає компонентам системи, зокрема супутниковим терміналам, сегментам DMZ, маршрутизаторам, серверам прикладного рівня та іншим інформаційним активам. Орієнтовані ребра $E = \{e_{ij}\}$ відображають можливість переходу атаки від вузла v_i до вузла v_j, тобто наявність технічної або логічної залежності, яка може бути використана зловмисником для подальшого проникнення в систему.

Кожному ребру e_{ij} ставиться у відповідність базова ймовірність успішної реалізації атаки $P(e_{ij})$, що визначається з урахуванням характеру вразливостей, рівня експозиції вузла та статистичних або експертних оцінок. Для врахування впливу засобів захисту вводиться коефіцієнт ослаблення $\beta_{ij} \in [0,1]$, який відображає ефективність міжмережевих екранів, систем виявлення вторгнень, сегментації мережі та інших механізмів контролю.

Ефективна ймовірність переходу атаки набуває вигляду:

$$P_{eff}(e_{ij}) = P(e_{ij}) \cdot (1 - \beta_{ij}) \tag{3}$$

що дозволяє інтегрувати вплив заходів захисту безпосередньо в структуру моделі.

Атака розглядається як послідовність переходів між вузлами, тобто як шлях $path_k$, що складається з набору ребер графа. За припущення статистичної незалежності переходів ймовірність реалізації повного сценарію визначається як добуток ефективних імовірностей усіх ребер уздовж цього шляху:

$$P(path_k) = \prod_{e \in path_k} P_{eff}(e) \tag{4}$$

Таким чином, модель відображає каскадний характер поширення атаки та дозволяє враховувати накопичувальний ефект послідовних компрометацій.

Інтегральний структурний ризик для критичного вузла v_c визначається як сума ймовірностей усіх можливих шляхів його компрометації, зважених на коефіцієнт критичності активу C_c:

$$R_{struct}(v_c) = \sum_{k=1}^{N} P(path_k) \cdot C_c \,. \tag{5}$$

Коефіцієнт C_c відображає значущість активу для безперервності функціонування підприємства, що особливо важливо для авіаційної галузі, де компрометація окремих систем може мати суттєві наслідки для безпеки польотів.

Практична реалізація запропонованої методики здійснюється за таким алгоритмом:

1. Структурна декомпозиція системи. Виділяються сегменти супутникового каналу (космічний, наземний, інтеграційний) та визначаються критичні активи авіаційного підприємства.

2. Побудова графової моделі. Інформаційна інфраструктура подається у вигляді орієнтованого графа, де вузли відповідають компонентам системи, а ребра – можливим напрямкам поширення атаки.

3. Оцінювання базових ймовірностей. Для кожного ребра визначається базова ймовірність реалізації атаки з урахуванням вразливостей і рівня експозиції.

4. Урахування заходів захисту. Вводяться коефіцієнти ослаблення, що відображають ефективність засобів безпеки, та обчислюються ефективні ймовірності переходів.

5. Визначення шляхів компрометації. Обчислюються ймовірності всіх можливих шляхів досягнення критичних активів і формується інтегральний структурний ризик з урахуванням їх критичності.

6. Оптимізація архітектури захисту. Порівнюються альтернативні варіанти захисних заходів за критерієм мінімізації інтегрального ризику та обирається раціональна конфігурація.

Запропонована модель принципово відрізняється від традиційних матричних підходів до оцінки ризику, які розглядають загрози ізольовано та не враховують топологічні залежності між компонентами. Графове представлення дозволяє аналізувати латеральне переміщення зловмисника,

виявляти вузли з високою структурною центральністю та визначати контрольні точки, компрометація яких призводить до максимального зростання інтегрального ризику. Крім того, параметр β_{ij} забезпечує можливість кількісного оцінювання ефективності кожного засобу захисту та оптимізації архітектури безпеки на основі мінімізації сумарного ризику.

Для перевірки застосування запропонованої графово-орієнтованої моделі розглянемо умовну конфігурацію авіаційного підприємства, в якій супутниковий канал Starlink використовується як резервний канал зв'язку. Структура вузлів наведена в таблиці 1.

Таблиця 1 – Перелік вузлів моделі та їх критичність

Позначення вузла	Компонент системи	Тип активу	Коефіцієнт критичності C_c
v_1	Супутниковий термінал	Точка входу	0.4
v_2	DMZ	Мережева інфраструктура	0.6
v_3	Корпоративна мережа	Внутрішній сегмент	0.8
v_4	Сервер управління польотами	Критичний актив	0.9

Критичним активом у даному прикладі є сервер управління польотами v_4 , що має коефіцієнт критичності C_4=0.9.

Нехай зловмисник отримує початкову можливість впливу на вузол супутникового термінала, після чого намагається поширити атаку через сегмент DMZ у корпоративну мережу та досягти сервера управління польотами. У термінах моделі цьому відповідає шлях $v_1 \to v_2 \to v_3 \to v_4$, який формалізується послідовністю ребер e_{12}, e_{23}, e_{34}. Базові ймовірності переходів для кожної ланки цього шляху, що відображають рівень уразливості та імовірність успішної реалізації відповідного кроку атаки за відсутності спеціальних засобів захисту, наведено в таблиці 2.

Таблиця 2 – Ймовірності переходів атаки без додаткових засобів захисту

Ребро графа	Опис переходу	Базова ймовірність $P(e_{ij})$	Коефіцієнт ослаблення β_{ij}	Ефективна ймовірність
e_{12}	Термінал → DMZ	0.4	0	0.4
e_{23}	DMZ → Корпоративна мережа	0.3	0	0.3
e_{34}	Корпоративна мережа → Сервер	0.2	0	0.2

Оскільки на початковому етапі захисні механізми не враховуються, коефіцієнти ослаблення для всіх переходів приймаються нульовими, тобто β_{ij}=0, а ефективні ймовірності збігаються з базовими. За припущення незалежності послідовних переходів імовірність успішної реалізації повного шляху визначається як добуток імовірностей його ланок і становить: $P(path)$=0.4·0.3·0.2=0.024. Для критичного вузла v_4 із коефіцієнтом критичності структурний ризик у цій конфігурації дорівнює $R_{initial}=P(path)\cdot C_4$=0.024·0.9=0.0216, що інтерпретується як зважена оцінка ймовірнісної досяжності критичного активу заданим сценарієм проникнення.

Далі оцінюється вплив впровадження комплексу захисних заходів, які зменшують імовірність проходження атаки на кожній ланці шляху. В моделі цей вплив враховується через коефіцієнти ослаблення β_{ij}, що характеризують ефективність відповідних контрольних механізмів. Нехай для переходу «термінал → DMZ» реалізовано фільтрацію та контроль на рівні міжмережевого екрана з ослабленням β_{12}=0.6, для переходу «DMZ → корпоративна мережа» застосовано механізми виявлення та блокування аномалій (IDS/IPS) з β_{23}=0.5, а для переходу «корпоративна мережа → сервер» впроваджено сегментацію та обмеження доступу з β_{34}=0.7. Розраховані ефективні ймовірності переходів наведено в таблиці 3.

Таблиця 3 – Ймовірності переходів після впровадження захисту

Ребро графа	Базова ймовірність $P(e_{ij})$	β_{ij}	Ефективна ймовірність $P_{eff}(e_{ij})$
e_{12}	0.4	0.6	0.16

e_{23}	0.3	0.5	0.15
e_{34}	0.2	0.7	0.06

За цих умов імовірність реалізації повного шляху знижується до $P(path)$=0.00144, а структурний ризик критичного активу становить $R_{residual}$=0.00144·0.9=0.001296. Порівняльні результати наведено в таблиці 4, з якої випливає, що зменшення ймовірності проходження атаки та відповідного структурного ризику складає 94%.

Таблиця 4 – Порівняння рівня ризику до та після впровадження захисту

Показник	До впровадження	Після впровадження	Зміна
Ймовірність шляху атаки	0.024	0.00144	↓ 94%
Структурний ризик	0.0216	0.001296	↓ 94%

Важливо підкреслити, що отриманий ефект є нелінійним: навіть помірне зниження ймовірності на кожній ланці шляху дає суттєвий сумарний результат за рахунок перемноження переходів. Саме ця властивість робить графову модель придатною для порівняння альтернативних архітектур захисту та для обґрунтованого вибору контрольних точок, вплив яких на інтегральний ризик є найбільшим.

Для оцінювання структурної вразливості мережі важливо враховувати, що компрометація критичного активу може бути досягнута кількома незалежними або частково залежними шляхами. Наявність альтернативних шляхів формує каскадний ефект: навіть за наявності захисту на одному напрямі, зловмисник може обрати інший маршрут, а інтегральний ризик визначається сукупністю всіх можливих сценаріїв.

Розглянемо додатковий шлях атаки, що реалізується через компрометацію сервісу віддаленого доступу в DMZ (наприклад, помилка конфігурації VPN-шлюзу або сервісу адміністрування). Альтернативний шлях атаки: $v_1 \rightarrow v_2 \rightarrow v_4$. Такий сценарій є типовим для конфігурацій, у яких окремі прикладні служби мають прямий мережевий зв'язок із внутрішніми системами. Базові ймовірності переходів для цього шляху наведено в таблиці 5. За відсутності додаткових засобів захисту коефіцієнти ослаблення приймаються нульовими, а ефективні ймовірності збігаються з початковими значеннями.

Таблиця 5 – Ймовірності переходів для альтернативного сценарію

Ребро графа	Опис переходу	Базова ймовірність $P(e_{ij})$	β_{ij}	Ефективна ймовірність $P_{eff}(e_{ij})$
e_{12}	Термінал → DMZ	0.4	0	0.4
e_{24}	DMZ → Сервер (через віддалений доступ/адміністрування)	0.15	0	0.15

За припущення незалежності переходів повна ймовірність реалізації альтернативного шляху визначається як $P(path_2)$=0.4·0.15=0.06. З урахуванням коефіцієнта критичності сервера C_4=0.9 структурний ризик для цього сценарію дорівнює R_{path2}=0.06·0.9=0.054.

Для порівняння, у базовому сценарії було отримано ймовірність шляху 0.024 та відповідний структурний ризик 0.0216. Отже, альтернативний маршрут, незважаючи на меншу кількість переходів, створює вищу загрозу для критичного активу. Інтегральний структурний ризик за наявності двох незалежних шляхів визначається сумою їхніх внесків і становить $R_{struct}(v_4)$=(0.024+0.06)·0.9=0.0756.

Порівняно з початковою оцінкою для одного шляху значення ризику зростає більш ніж утричі, що наочно демонструє каскадний ефект: загальний рівень загрози визначається не окремим найбільш імовірним сценарієм, а сукупністю всіх доступних маршрутів проникнення.

Після впровадження комплексу заходів безпеки ефективність яких уже врахована для базового шляху через коефіцієнти $\beta_{12}=0.6$, β_{23}=0.5 та β_{34}=0.7, для альтернативного ребра e_{24} додатково вводиться контроль доступу з використанням багатофакторної автентифікації, списків контролю доступу та сервісної сегментації, що забезпечує ослаблення β_{24}=0.8. Ефективна

ймовірність переходу «DMZ → сервер» зменшується до 0.03, а ймовірність повного альтернативного шляху становить $P(path_2)$=0.16·0.03=0.0048, таблиця 6.

Таблиця 6 – Ефективні ймовірності після впровадження захисту

Ребро графа	$P(e_{ij})$	β_{ij}	$P_{eff}(e_{ij}) = P(e_{ij}) \cdot (1 - \beta_{ij})$
e_{12}	0.4	0.6	0.16
e_{24}	0.15	0.8	0.03

Залишковий ризик для цього сценарію дорівнює $R_{path2new}$=0.0048·0.9=0.00432.

З урахуванням залишкового ризику базового шляху $R_{path1new}$=0.001296 інтегральний ризик після впровадження захисту зменшується до $R_{structnew}(v_4)$=0.001296+0.00432=0.005616.

Коефіцієнт зниження інтегрального ризику становить:

$$\eta_{struct} = \frac{0.0756 - 0.005616}{0.0756} \approx 0.926,$$

що відповідає скороченню загального ризику приблизно на 93%.

Наведений приклад демонструє, що навіть за ефективної фільтрації одного маршруту атаки (через корпоративну мережу) інтегральний ризик може залишатися високим за наявності альтернативного шляху (через DMZ та віддалений доступ). Тому оптимізація архітектури захисту повинна здійснюватися на основі аналізу сукупності шляхів компрометації, а не окремих загроз або сегментів.

Розроблена графово-орієнтована модель оцінки кіберризику створює формальну основу для визначення напрямів його зниження. Практична реалізація запропонованої методики потребує формування комплексної системи захисту, що охоплює технічні, програмні та організаційні компоненти і функціонує як єдиний керований контур безпеки. У межах такої системи супутниковий канал розглядається не лише як транспортне середовище передачі даних, а як окремий сегмент довіри, інтеграція якого повинна бути строго контрольованою та формалізованою.

Архітектурною основою захисту є логічна та фізична сегментація мережі. Супутниковий термінал має функціонувати в ізольованому підсегменті, інтегрованому в корпоративну інфраструктуру через демілітаризовану зону. Така конфігурація дозволяє локалізувати ризики, мінімізувати можливість прямого доступу до критичних систем і зменшити кількість потенційних ребер у графовій моделі атак. Багаторівневі міжмережеві екрани, налаштовані відповідно до принципу найменших привілеїв, разом із системами виявлення та запобігання вторгненням формують периметровий бар'єр, який математично інтерпретується як збільшення коефіцієнтів ослаблення β_{ij} у відповідних ребрах графа. Використання концепції zero-trust забезпечує перевірку кожної сесії незалежно від її джерела, що особливо важливо для каналів з динамічною топологією.

Оскільки криптографічні механізми провайдера не гарантують повної ізоляції корпоративного трафіку, доцільним є застосування додаткового рівня шифрування на основі VPN або IPsec у режимі тунелювання. Такий підхід забезпечує цілісність і конфіденційність даних навіть у разі потенційної компрометації частини супутникової інфраструктури. Використання сучасних протоколів обміну ключами з підтримкою прямої секретності мінімізує наслідки можливого розкриття криптографічних параметрів у майбутньому.

Ефективність захисту значною мірою залежить від надійності механізмів автентифікації та централізованого контролю доступу. Застосування багатофакторної автентифікації, інтеграція з системами управління ідентифікацією та регулярний аудит прав доступу дозволяють знизити ризик несанкціонованого проникнення через адміністративні інтерфейси. У математичному сенсі це відображається як зменшення імовірності альтернативних шляхів атаки, зокрема тих, що проходять через сегмент DMZ до критичних активів.

Суттєвим елементом комплексної системи є безперервний моніторинг подій безпеки. Централізований збір журналів з усіх компонентів інфраструктури та їх кореляція в системах класу SIEM забезпечують своєчасне виявлення аномалій і скорочують час реагування на інциденти. Використання аналітичних методів, зокрема машинного навчання, дозволяє виявляти нетипові патерни супутникового трафіку, що не фіксуються сигнатурними механізмами. У контексті розробленої моделі це відповідає зменшенню реальної тривалості перебування зловмисника в системі та, відповідно, зниженню ефективної ймовірності реалізації повного шляху атаки.

Процеси управління вразливостями та оновленнями мають забезпечувати контроль за станом програмного забезпечення терміналів, шлюзів і внутрішніх серверів. Регулярне сканування, тестування оновлень у контрольованому середовищі та документування виявлених уразливостей дозволяють мінімізувати ризики, пов'язані з експлуатацією відомих помилок. З позицій формалізованої моделі це означає поступове зменшення базових ймовірностей переходів, пов'язаних із використанням експлойтів.

Організаційні заходи доповнюють технічні механізми та формують середовище керованої безпеки. Регламентування використання супутникового каналу, визначення відповідальності персоналу, регулярне навчання з питань кіберзагроз і наявність планів реагування на інциденти забезпечують зниження людського фактора як джерела ризику. Систематична оцінка ризиків і періодичне оновлення моделі загроз дозволяють підтримувати актуальність захисної архітектури в умовах еволюції технологій.

Забезпечення відповідності національному законодавству та міжнародним стандартам є необхідною умовою експлуатації супутникових каналів у сфері авіації. Виконання вимог законів України щодо кібербезпеки та захисту інформації, впровадження системи управління інформаційною безпекою відповідно до ISO/IEC 27001, а також урахування положень NIST Cybersecurity Framework та галузевих стандартів ICAO, EASA і IATA створюють нормативну основу функціонування захисної системи. Наявність процедур контролю відповідності, документування заходів захисту та підготовки звітності для регуляторних органів забезпечує прозорість і відтворюваність процесів управління ризиком.

Таким чином, концептуальні засади забезпечення безпеки супутникового каналу інтегрують результати формалізованого аналізу ризику з практичними механізмами його зниження. Запропонований підхід дозволяє не лише мінімізувати інтегральний структурний ризик, але й створити адаптивну систему захисту, здатну реагувати на зміну топології супутникової мережі та еволюцію кіберзагроз у середовищі критичної інфраструктури авіаційного підприємства.

Висновки та перспективи подальших досліджень. У статті розроблено формалізовану методику оцінки та зниження кіберризиків супутникових каналів зв'язку Starlink в інформаційній інфраструктурі авіаційних підприємств. На відміну від традиційних підходів, супутниковий канал розглянуто як автономний динамічний периметр безпеки з власною структурою загроз та топологічними залежностями, що потребує окремого моделювання та кількісної оцінки ризику.

Запропоновано структурну модель інтеграції супутникового та розроблено графово-орієнтовану модель атак, у межах якої інформаційна система подається як орієнтований граф, а ризик визначається як сукупність імовірностей усіх можливих шляхів проникнення до критичних активів. Показано, що інтегральний ризик формується не окремою загрозою, а множиною альтернативних сценаріїв атак, що створюють каскадний ефект. Наведений формальний приклад продемонстрував, що наявність додаткового шляху компрометації може суттєво збільшити структурний ризик навіть за часткового захисту основного маршруту. Введення коефіцієнтів ослаблення для кожного переходу графа дозволило кількісно оцінити вплив конкретних засобів захисту на зниження інтегрального ризику.

У статті обґрунтовано концептуальні засади побудови комплексної системи захисту супутникового каналу, що поєднує мережеву сегментацію, додатковий криптографічний захист, централізований контроль доступу, безперервний моніторинг та управління вразливостями. Показано, що інтеграція технічних і організаційних заходів дозволяє кількісно зменшити структурний ризик у межах розробленої графової моделі та забезпечити відповідність вимогам критичної інфраструктури й галузевим стандартам авіації. Запропонований підхід формує адаптивну архітектуру безпеки, здатну враховувати динамічність LEO-мереж та еволюцію кіберзагроз.

Список бібліографічного опису:

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України № 447/2021 від 26 серп. 2021 р.
2. ICAO Aviation Cybersecurity Strategy. Montréal: International Civil Aviation Organization, 2019.
3. European Union Aviation Safety Agency. Cybersecurity in Aviation – Overview. 2023.
4. International Air Transport Association. Aviation Cyber Security Position Paper. 2019.
5. Yue P., An J., Zhang J., Ye J. Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead. *IEEE Communications Surveys & Tutorials.* 2023. Vol. 25, No. 3. P. 1604–1652. DOI: 10.1109/COMST.2023.3296160.

6. Roddy D. Satellite Communications. 5th ed. New York: McGraw-Hill Education, 2020.
7. Handley M. Delay is Not an Option: Low Latency Routing in Space. *Proceedings of the 17th ACM Workshop on Hot Topics in Networks (HotNets'18).* 2018. P. 85–91. DOI: 10.1145/3286062.3286075.
8. Mohan N., Ferguson A. E., Cech H., Bose R., Renatin P. R., Marina M. K., Ott J. A Multifaceted Look at Starlink Performance. *Proceedings of the ACM Web Conference 2024 (WWW '24)*. New York: ACM, 2024. P. 2723–2734. DOI: 10.1145/3589334.3645328.
9. Radio Regulations. Geneva: International Telecommunication Union, 2020.
10. ISO/IEC 27005:2022. Information security risk management. Geneva: ISO/IEC, 2022.
11. ISO/IEC 27001:2022. Information security management systems – Requirements. Geneva: ISO/IEC, 2022.
12. NIST. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg: NIST, 2018.
13. 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: 10.1016/j.comnet.2022.109246.
14. McDowell J. C. The Low Earth Orbit Satellite Population and Impacts of the SpaceX Starlink Constellation. *The Astrophysical Journal Letters.* 2020. Vol. 892, No. 2. Article L36. DOI: 10.3847/2041-8213/ab8016.
15. Barker W. et al. Guidelines for Securing Wireless Local Area Networks (WLANs). NIST SP 800-153. Gaithersburg: NIST, 2012.
16. Mirkovic J., Reiher P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. *ACM SIGCOMM Computer Communication Review.* 2004. Vol. 34, No. 2. P. 39–53. DOI: 10.1145/997150.997156.
17. Dierks T., Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. IETF, 2018.
18. ENISA. ENISA Threat Landscape 2021. Luxembourg: European Union Agency for Cybersecurity, 2021.
19. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST SP 800-207. Gaithersburg: NIST, 2020.
20. Common Vulnerabilities and Exposures (CVE). URL: https://cve.mitre.org
21. ISO/IEC 27002:2022. Information security controls. Geneva: ISO/IEC, 2022.

References:

1. On the Decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine No. 447/2021 of August 26, 2021.
2. ICAO Aviation Cybersecurity Strategy. Montréal: International Civil Aviation Organization, 2019.
3. European Union Aviation Safety Agency. Cybersecurity in Aviation – Overview. 2023.
4. International Air Transport Association. Aviation Cyber Security Position Paper. 2019.
5. Yue P., An J., Zhang J., Ye J. Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead. *IEEE Communications Surveys & Tutorials.* 2023. Vol. 25, No. 3. P. 1604–1652. DOI: 10.1109/COMST.2023.3296160.
6. Roddy D. Satellite Communications. 5th ed. New York: McGraw-Hill Education, 2020.
7. Handley M. Delay is Not an Option: Low Latency Routing in Space. *Proceedings of the 17th ACM Workshop on Hot Topics in Networks (HotNets'18).* 2018. P. 85–91. DOI: 10.1145/3286062.3286075.
8. Mohan N., Ferguson A. E., Cech H., Bose R., Renatin P. R., Marina M. K., Ott J. A Multifaceted Look at Starlink Performance. *Proceedings of the ACM Web Conference 2024 (WWW '24)*. New York: ACM, 2024. P. 2723–2734. DOI: 10.1145/3589334.3645328.
9. Radio Regulations. Geneva: International Telecommunication Union, 2020.
10. ISO/IEC 27005:2022. Information security risk management. Geneva: ISO/IEC, 2022.
11. ISO/IEC 27001:2022. Information security management systems – Requirements. Geneva: ISO/IEC, 2022.
12. NIST. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg: NIST, 2018.
13. 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: 10.1016/j.comnet.2022.109246.
14. McDowell J. C. The Low Earth Orbit Satellite Population and Impacts of the SpaceX Starlink Constellation. *The Astrophysical Journal Letters.* 2020. Vol. 892, No. 2. Article L36. DOI: 10.3847/2041-8213/ab8016.
15. Barker W. et al. Guidelines for Securing Wireless Local Area Networks (WLANs). NIST SP 800-153. Gaithersburg: NIST, 2012.
16. Mirkovic J., Reiher P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. *ACM SIGCOMM Computer Communication Review.* 2004. Vol. 34, No. 2. P. 39–53. DOI: 10.1145/997150.997156.
17. Dierks T., Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. IETF, 2018.
18. ENISA. ENISA Threat Landscape 2021. Luxembourg: European Union Agency for Cybersecurity, 2021.
19. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST SP 800-207. Gaithersburg: NIST, 2020.
20. Common Vulnerabilities and Exposures (CVE). URL: https://cve.mitre.org
21. ISO/IEC 27002:2022. Information security controls. Geneva: ISO/IEC, 2022.

Історія статті:
Отримано: 20.01.2026 Доопрацьовано: 05.02.2026 Прийнято до друку: 23.03.2026 Опубліковано: 29.03.2026