Протидія загрозам у космічному середовищі через європейську та євроатлантичну інтеграцію України

Андрій Старчик
аспірант кафедри теорії та історії держави і права,
ВНЗ «Університет економіки і права «КРОК», м. Київ, Україна,
e-mail: StarchykAA@krok.edu.ua,
ORCID: 0009-0003-1348-3822

Сучасна глобальна інфраструктура дедалі більше спирається на супутникові технології, які забезпечують безперервну підтримку зв'язку, навігації, дистанційного зондування Землі та інших критичних сервісів. У різних секторах – від оборони та енергетики до фінансів і транспорту – саме космічні системи гарантують стійкість комунікаційних потоків і координацію складних процесів. Разом з тим, дедалі глибша інтеграція супутникових технологій у критичні процеси створює новий вимір вразливості, адже залежність від орбітальної інфраструктури робить її привабливою ціллю для кібернетичних атак, інспірованих технічних збоїв та навмисного втручання. У цих умовах оцінка потенційних загроз, що формуються в космічному середовищі, стає не лише академічним питанням, а й важливою складовою національної та колективної безпеки.

Проблемність ситуації посилюється тим, що значна частина супутникової інфраструктури традиційно опирається на радіочастотний обмін, який сам по собі є уразливим до перехоплення, глушіння або спуфінгу. Без належних технічних засобів захисту – передусім надійного шифрування командних та телеметричних каналів – сторонні актори можуть отримати доступ до критичних систем або порушити їхню роботу. На це реагує ринок: комерційні оператори все ширше впроваджують наскрізне шифрування від наземних станцій до бортових модулів, а навіть відкриті платформи на кшталт CubeSats розробляють модульні рішення для криптографічного захисту.

Окремий вимір загроз формується у зв'язку з глобальним розгортанням мереж 5G, де супутники виконують ключову роль у забезпеченні покриття у важкодоступних регіонах [1]. Саме тому супутникові канали, що підтримують високошвидкісну передачу даних, стають дедалі більш привабливою ціллю для кіберзлочинних груп, які намагаються порушити роботу життєво важливих сервісів або втрутитися у потоки даних.

Технічні вразливості супутникових систем становлять лише одну частину загального спектру загроз, адже коло потенційних порушників є надзвичайно широким і охоплює різні групи суб'єктів з різними цілями та рівнем підготовки.

До найбільш організованих належать структури, що діють під державним контролем або за підтримки держав, зокрема держав-терористів. Вони використовують ресурси спецслужб та військових відомств, ведуть тривалу розвідку цілей і спеціалізуються на шпигунстві чи дестабілізаційних операціях.

Окрему групу становлять кіберзлочинні угруповання, для яких ключовою

метою є фінансовий прибуток, отриманий шляхом шантажу з використанням викрадених даних (баз даних) або компрометуючих матеріалів, або збуту.

До кола ризиків також входять різноманітні групи хакерів з різним рівнем підготовки – від тих, що мають професійне оснащення та підготовку до аматорів та експериментаторів. Не можна ігнорувати й хакерів-активістів, які керуються ідеологічними чи політичними мотивами і здатні порушувати роботу космічних сервісів для привернення уваги до певного питання.

Іншу категорію становлять працівники та інші особи, які мають доступ до внутрішньої інфраструктури – співробітники, підрядники або колишні працівники, поведінка яких може створювати як умисні ризики, так і загрози через необережність або легковажність [2].

Найрізноманітніший спектр суб'єктів свідчить про те, що деструктивний вплив на супутникові системи може виходити з фундаментально різних джерел, включно з тими, що не мають значної матеріальної чи організаційної бази.

Крім кібернетичних ризиків у космічному середовищі поступово формується і спектр загроз фізичного характеру, що охоплюють можливі напади на наземні станції, космодроми чи інші елементи інфраструктури з перспективами захоплення окремих космічних апаратів або орбітальних платформ. Дедалі більшою проблемою стає й шпигунська активність навколо стратегічних об'єктів, зокрема спроби заволодіти інформацією з обмеженим доступом або проникнути на об'єкти запуску, що вже фіксується в низці європейських країн [3]. Такі прояви демонструють, що загрози на орбіті сьогодні не обмежуються зламом супутників, а можуть реалізовуватися у різних формах – від кібератак до фізичного втручання, що свідчить про зростання складності та багатовимірності ризиків для безпеки космічної інфраструктури.

Космічне середовище також стало ареною геополітичного протистояння. Розвиток космічної інфраструктури не в цілях дослідження Всесвіту, а з метою домінування на Землі стає все більш очевидним пріоритетом окремих держав. Лунають прямі погрози знищення чи пошкодження орбітальних об'єктів, розробляються сценарії збройний конфліктів в космосі, вкладаються чималі ресурси у розробку відповідного обладнання та систем. Активним тестовим майданчиком у цьому стала російська агресія проти України та ширше протистояння рф з країнами Європи та НАТО.

Наведені загрози спонукали до рішень і дій на загальноєвропейському та трансатлантичному рівнях. Так, ухвалена Європейським Союзом Космічна стратегія ЄС щодо безпеки та оборони визначає пріоритети спільного реагування та зміцнення стійкості космічної інфраструктури [4]. Європейські дослідницькі центри також аналізують тенденцію до зближення цивільної космічної політики з оборонними інструментами Союзу, пропонуючи нові рамки для протидії гібридним загрозам у космосі [5]. У трансатлантичному вимірі увагу привертають дослідження, спрямовані на кіберзахист космічних активів держав–членів НАТО, зокрема моделі поетапного підвищення захисту та реагування на супутникові кібератаки [6]. Все це свідчить про те, що

космічна безпека перестала бути периферійною темою та є частиною ширших стратегічних підходів євроатлантичної спільноти.

Сукупність описаних загроз, а також безпекові виклики, з якими Україна стикається в умовах російської збройної агресії, лише підсилюють потребу в глибшій європейській та євроатлантичній інтеграції, зокрема у сферах космічної та кібернетичної безпеки. Така інтеграція не обмежується запозиченням європейських і євроатлантичних підходів, адже Україна, маючи унікальний досвід протидії сучасним технологічним загрозам, здатна робити власний внесок у формування спільних стратегій. Це створює можливість не лише адаптуватися до існуючих стандартів, а й пропонувати нові рішення, що враховують реальні виклики та швидку еволюцію ризиків у космічному середовищі.

Ключові слова: космічна безпека; супутникова інфраструктура; кіберзагрози; євроатлантична інтеграція.

Список використаних джерел

1. Zac Amos. Satellite Infrastructure Is Surprisingly Vulnerable to Cyberattacks. Risk and Resilience HUB. 29.07.2025р. URL : https://riskandresiliencehub.com/satellite-infrastructure-is-surprisingly-vulnerable-to-cyberattacks/?utm_source=chatgpt.com (дата звернення 27.11.2025).

2. ENISA. Space Threat Landscape. European Union Agency for Cybersecurity, 26 March 2025. URL : https://www.enisa.europa.eu/sites/default/files/2025-03/Space_Threat_Landscape_Report_fin.pdf (дата звернення 27.11.2025).

3. Лев Шевченко. Перші атаки почалися: як космічні пірати вже загрожують світу та до чого тут Росія і Китай. URL: https://24tv.ua/kosmichni-pirati-yaki-novi-zagrozi-orbiti-zemli-kosmosi_n2791715?utm_source=chatgpt.com (дата звернення 27.11.2025).

4. European Commission. EU Space Strategy for Security and Defence. 2023. URL : https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en?utm_source=chatgpt.com (дата звернення 27.11.2025).

5. Miglio A., Grossio L., Civitella A., Nota C., Penna M. Space and defence: a hybridisation of EU space policy and CSDP. Centre for Studies on Federalism, 2024. URL : https://www.fondazionecsf.it/images/2024/Research-paper/CSF-RP_EU-Space-Policy_Miglio_Grossio_Civitella_Nota_Penna_Dec2024.pdf (дата звернення 27.11.2025).

6. Julia Cournoyer. Securing the space-based assets of NATO members from cyberattacks. Chatham House 2025. URL : https://www.chathamhouse.org/2025/05/securing-space-based-assets-nato-members-cyberattacks/03-evolution-space-policies-nato-and?utm_source=chatgpt.com (дата звернення 27.11.2025).