УДК 004 DOI https://doi.org/10.35546/kntu2078-4481.2025.3.2.54

О. А. СНЄОСІКОВ
аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій
Харківський національний університет імені В. Н. Каразіна
ORCID: 0009-0001-9468-5965

О. П. НАРЄЖНІЙ
кандидат технічних наук,
доцент кафедри кібербезпеки інформаційних систем, мереж і технологій
Харківський національний університет імені В. Н. Каразіна
ORCID: 0000-0003-4321-0510

МОДЕЛІ ЗАГРОЗ ТА ПОРУШНИКА АВТОНОМНОЇ СИСТЕМИ ДИФЕРЕНЦІАЛЬНОЇ КОРЕКЦІЇ ГЛОБАЛЬНИХ НАВІГАЦІЙНИХ СУПУТНИКОВИХ СИСТЕМ

У статті розроблено формалізовану модель загроз та модель порушника для автономної системи диференціальної корекції (АСДК) глобальних навігаційних супутникових систем (GNSS), яка відноситься до об'єктів критичної інформаційної інфраструктури. Сформовано класифіковану модель порушника, що враховує типи атакуючих суб'єктів, їх мотивацію, технічні ресурси, рівень доступу та потенційні техніки атак. Запропоновано комплексну модель загроз, яка охоплює всі активи системи АСДК, включаючи GNSS-приймачі контрольно-коригуючих станцій (ККС) та АСДК, центри обробки даних, криптографічну інфраструктуру, транспортні канали передачі даних, сервери розповсюдження поправок та кінцевих користувачів. Для побудови моделі загроз використано комбінований методологічний підхід, що об'єднує сучасні методики PASTA (Process for Attack Simulation and Threat Analysis), STRIDE та MITRE ATT&CK (Enterprise та ICS). Розроблено типові сценарії мультивекторних атак з урахуванням GPS spoofing, GPS jamming, атак на інформаційно-комунікаційну інфраструктуру (ІКС), криптосистему, програмне забезпечення та фізичні компоненти системи. Окрему увагу приділено забезпеченню криптостійкості системи в умовах постквантового періоду шляхом впровадження національних постквантових алгоритмів шифрування (Калина, Скеля, Вершина, Купина) та використання квантових генераторів випадкових чисел (QRNG) у системі управління ключами. Проведено аналіз наслідків реалізації атак та обґрунтовано комплекс заходів захисту системи АСДК з урахуванням міжнародних стандартів ISO/IEC 27001, IEC 62443, NIST SP 800-30/53 та національних нормативів НД ТЗІ. Запропонована методика дозволяє створювати практично застосовні захищені архітектури для АСДК GNSS та інших елементів критичної інфраструктури з урахуванням майбутніх криптографічних викликів.

Ключові слова: *глушіння сигналу; спуфінг сигналу; глобальна навігаційна супутникова система; квантовий генератор випадкових чисел; кібератака; кібербезпека; система глобального позиціонування; система диференціальної корекції; інформаційно-комунікаційна система; система виявлення вторгнень; система запобігання вторгненням, модель загроз, модель порушника, автономна система диференціальної корекції (АСДК; Autonomous DGNSS).*

O. A. SNIEOSIKOV
Postgraduate Student at the Department of Cybersecurity
of Information Systems, Networks and Technologies
V. N. Karazin Kharkiv National University
ORCID: 0009-0001-9468-5965

O. P. NARIEZHNII
Candidate of Technical Sciences,
Associate Professor at the Department of Cybersecurity
of Information Systems, Networks and Technologies
V. N. Karazin Kharkiv National University
ORCID: 0000-0003-4321-0510

THREAT AND VIOLATOR MODELS OF THE AUTONOMOUS SYSTEM OF DIFFERENTIAL CORRECTION OF GLOBAL NAVIGATION SATELLITE SYSTEMS

This paper presents the development of a formalized threat model and adversary model for an Autonomous Differential Global Navigation Satellite System (Autonomous DGNSS), which is classified as part of critical information infrastructure. A structured adversary model has been created, incorporating attacker types, motivations, technical resources, access

levels, and potential attack techniques. A comprehensive threat model is proposed, covering all system assets of the Autonomous DGNSS, including GNSS receivers at both control and correction stations and the central system, data processing centers, cryptographic infrastructure, data transmission channels, correction data distribution servers, and end users. The threat model is constructed using a combined methodological approach that integrates modern frameworks such as PASTA (Process for Attack Simulation and Threat Analysis), STRIDE, and MITRE ATT&CK (Enterprise and ICS profiles). Representative multivector attack scenarios have been developed, taking into account GPS spoofing, GPS jamming, attacks on information and communication infrastructure, cryptosystems, software vulnerabilities, and physical components of the system. Particular attention is paid to ensuring the system's cryptographic resilience in the post-quantum era by implementing national post-quantum cryptographic algorithms (Kalyna, Skelia, Vershyna, Kupyna) and utilizing quantum random number generators (QRNG) within the key management infrastructure. The paper includes an impact assessment of potential attack scenarios and provides a comprehensive set of protection measures for the Autonomous DGNSS, incorporating international standards such as ISO/IEC 27001, IEC 62443, NIST SP 800-30/53, as well as national regulations (ND TZI, Ukraine). The proposed methodology enables the design of practically applicable and resilient architectures for Autonomous Differential GNSS systems and other elements of critical infrastructure, with consideration for emerging post-quantum cryptographic challenges.

Key words: *GPS jamming; GPS spoofing; Global Navigation Satellite System (GNSS); quantum random number generator (QRNG); cyberattack; cybersecurity; GPS; Differential GNSS (DGNSS); information and communication system; IDS; IPS; threat model, adversary model, Autonomous DGNSS.*

Постановка проблеми

GNSS є критично важливим фундаментом сучасної критичної інфраструктури, охоплюючи цивільну авіацію, морську навігацію, транспорт, геодезію, енергетику, фінансові системи, телекомунікації, оборонну галузь та інші системи, де потрібно не лише визначення точних координат, а також точне визначення часу [1, 2]. Однак базова точність GNSS-сигналів у відкритому доступі не завжди відповідає сучасним вимогам, особливо у сфері логістики, точного землеробства, інфраструктурного моніторингу та операторів мобільного зв'язку. Таким чином, для забезпечення точності визначення координат, а також визначення точного часу у реальному часі використовуються функціональні доповнення GNSS – системи диференціальної корекції (DGNSS) [3] – програмно-апаратні комплекси, що обчислюють поправки на основі даних від ККС. DGNSS обробляють дані у реальному часі, передають поправки зацікавленим користувачам через IP-мережі (мобільний зв'язок, наземні канали зв'язку, радіоканали), забезпечуючи високоточне позиціювання незалежно від сторонніх сервісів. Системи диференціальної корекції які є частиною GNSS класифікуються як об'єкти критичної інфраструктури, відповідно до Закону України «Про критичну інфраструктуру» № 1882-IX від 15 листопада 2021 року, де до переліку критично важливих сфер включено, зокрема, «15) космічну діяльність, космічні технології та послуги» [4].

Останні роки продемонстрували стрімке зростання кіберзагроз, спрямованих на компоненти GNSS [5, 6], зокрема GPS spoofing, GPS jamming, атаки на програмне забезпечення станцій та серверів [7, 8, 9]. За даними [10, 11, 12], атаки на GNSS стали настільки ефективними та доступними, що потенційно можуть паралізувати об'єкти критичної інфраструктури що несе серйозні наслідки для національної безпеки. Сучасні глобальні навігаційні супутникові системи є вразливими до широкого спектру кіберзагроз. Серед найбільш критичних для функціонування GNSS, так і систем диференціальної корекції (зокрема, автономних систем (АСДК)), виділяють:

– Глушіння сигналу (GPS jamming): використання перешкод для повного блокування прийому сигналів супутників, включаючи сигнали, що надходять на ККС;

– Спуфінг сигналу (GPS spoofing): навмисна генерація фальшивих сигналів навігації з метою введення в оману приймача GNSS, зокрема ККС;

– Кібератаки на наземну та хмарну інфраструктуру GNSS, такі як: DDoS-атаки; MITM-атаки; використання вразливостей ПЗ серверів і веб-інтерфейсів (переповнення буфера, ін'єкції коду, фішинг, тощо …);

– Фізичні атаки на наземні системи: пошкодження або захоплення ККС та ЦОД АСДК;

– Інсайдерські загрози: порушення з боку персоналу або адміністративних користувачів.

У зв'язку з викладеним вище, постає завдання побудови формалізованої моделі загроз і моделі порушника саме для Autonomous DGNSS.

Аналіз останніх досліджень і публікацій

У період 2021–2025 років спостерігається значне зростання досліджень, присвячених виявленню та протидії таким атакам на GNSS як GPS jamming та GPS spoofing. Зокрема, у роботі [13] запропоновано використання методів машинного та глибокого навчання для ідентифікації таких атак з високою точністю. В дослідженні [14] представлено систематичний огляд сучасних методів виявлення перешкод на GNSS, включаючи використання моделей машинного навчання та радіочастотної ідентифікації. Попри це, більшість досліджень зосереджені на загальних аспектах безпеки GNSS сигналів, розглядаючи протидію кібератакам GPS jamming та GPS spoofing, залишаючи поза увагою специфічні загрози для систем диференціальної корекції, а саме наземної інфраструктури DGNSS. Наприклад, у звіті ENISA «Space Threat Landscape» (2025) висвітлюються загрози для космічних систем [15], але детальний аналіз вразливостей

наземної інфраструктури DGNSS відсутній. Варто зазначити, що існуючі моделі загроз, такі як STRIDE, DREAD, VAST, PASTA, OCTAVE, LINDDUN [16–23], хоча й корисні для загального моделювання, не враховують специфіку DGNSS. Стандарт IEC 62443 [24] частково охоплює аспекти безпеки Operational technology систем (OT системи), але не надає конкретних рекомендацій щодо захисту компонентів архітектури DGNSS. Крім того, у звіті CrowdStrike «2025 Global Threat Report» [25] зазначається зростання кількості кібератак на критичну інфраструктуру, зокрема включаючи використання штучного інтелекту для автоматизації атак. Це підкреслює необхідність розробки спеціалізованих моделей загроз для систем, таких як АСДК GNSS, які є частиною критичної інфраструктури. Таким чином, існує очевидна наукова прогалина у дослідженнях, присвячених моделюванню загроз та порушників для систем диференціальної корекції GNSS, які в основному зосереджені на окремих технічних аспектах і не формують комплексної системної моделі кіберзагроз і порушника. Це обґрунтовує необхідність розробки формалізованої моделі загроз та моделі порушника, яка враховує специфіку архітектури автономних DGNSS, протоколів передачі даних, вразливостей програмного забезпечення та можливих сценаріїв атак. Незважаючи на наявність загальних підходів до моделювання кіберзагроз та моделей порушників (зокрема STRIDE, MITRE ATT&CK, PASTA), модель загроз, адаптована до архітектури DGNSS, залишається недостатньо дослідженою, як і об'єкти критичної інфраструктури взагалі [12]. Однак існують дослідження, що використовують STRIDE для моделювання загроз у суміжних сферах, таких як супутникові системи зв'язку, морські кіберфізичні системи та IoT-системи точного землеробства [26–28]. Ці дослідження демонструють застосування моделі STRIDE у різних сферах, що можуть бути релевантними для аналізу загроз у GNSS. Більшість наукових робіт по дослідженню захисту GNSS зосереджено на базовій безпеці самих GNSS-сигналів або захисті користувацьких пристроїв, без урахування особливостей архітектури інформаційно комунікаційної системи (ІКС) АСДК. Оскільки компрометація DGNSS може призвести до катастрофічних наслідків – збоїв у транспортних системах, логістичних маршрутах, аграрній техніці або військових навігаційних платформах, потреба в розробці формалізованої та практично придатної моделі загроз для АСДК є надзвичайно актуальною.

Формулювання мети дослідження

Метою цієї роботи є побудова формалізованої моделі кіберзагроз та моделі порушника, орієнтованих на АСДК. У роботі проаналізовано сучасні методи моделювання кіберзагроз та їхню застосовність до АСДК GNSS. Запропоновано формалізовану модель загроз, яка враховує специфіку протоколів передачі поправок, уразливості ККС, мережевих вузлів, веб-сервера, а також програмного забезпечення користувача. Сформовано модель порушника з урахуванням рівня доступу, технічних можливостей і мотивації. На основі побудованих моделей розроблено типові сценарії атак з оцінкою потенційних наслідків та обґрунтованими контрзаходами. Отримані результати можуть бути використані для побудови систем виявлення загроз, оцінки ризиків та проєктування кіберстійких Autonomous DGNSS. Для побудови формалізованої моделі загроз та моделі порушника було використано міжнародні стандарти ISO/IEC 27001, NIST SP 800-30/53, IEC 62443, а також національні НД ТЗІ 2.5-004-99 та НД ТЗІ 2.5-005-99 [24, 29, 30, 31, 32]. ISO/IEC 27001 надає структуру для ідентифікації активів та загроз; NIST забезпечує детальний підхід до ризик-менеджменту та профілювання атакуючих суб'єктів; IEC 62443 дозволяє врахувати архітектурні особливості OT-систем (OT, Operational Technology Systems), до яких належать автономні системи диференціальної корекції; НД ТЗІ – узгоджує моделі загроз із чинним законодавством України щодо технічного захисту інформації.

Викладення основного матеріалу дослідження

Запропонована архітектура автономної системи диференціальної корекції глобальної супутникової навігації передбачає побудову багаторівневої, захищеної інформаційно-комунікаційної інфраструктури, що має на меті забезпечувати підвищену точність GNSS сигналів та стійкість до кіберзагроз, зокрема у постквантовий період.

Основними компонентами АСДК архітектури є (рис. 1):

– Супутникове угруповання GNSS (GPS, Galileo, GLONASS, BeiDou), що забезпечують передачу навігаційних сигналів до користувачів, ККС та АСДК.

– ККС, рівномірно розташовані по території країни, приймають сигнали GNSS, та передають їх до Центрів Обробки Даних (ЦОД) АСДК через захищені IPSEC-канали з використанням національних криптоалгоритмів.

– Основний та резервний ЦОД, які забезпечують агрегацію, обробку, та зберігання даних, розрахунок диференціальних поправок, а також формування коригуючих повідомлень для кінцевих користувачів. Критичні дані шифруються за алгоритмом «Калина» (≥256 біт). Система управління ключами використовує QRNG; для криптографічних операцій застосовуються національні стандарти «Скеля» (ДСТУ 8961:2019), «Вершина» (ДСТУ 9212:2023) та геш-функція «Купина» (ДСТУ 7564:2014). Автентичність, цілісність і захищений обмін забезпечує інфраструктура відкритого ключа (ІВК).

– Веб-сервер високої доступності, що забезпечує надання коригуючої інформації та стандартизовані потоки поправок кінцевим користувачам через захищені канали зв'язку (TLS 1.3), використовуючи мобільні мережі та інтернет-з'єднання.

– Захищена ІКС, яка включає Security Operation Center (SOC), системи виявлення та протидії вторгненням (IDS/IPS), захист від DDoS-атак, багаторівневу аутентифікацію доступу, аудит операцій та механізми захисту від MITM атак та кібератак на сервіси синхронізації точного часу.

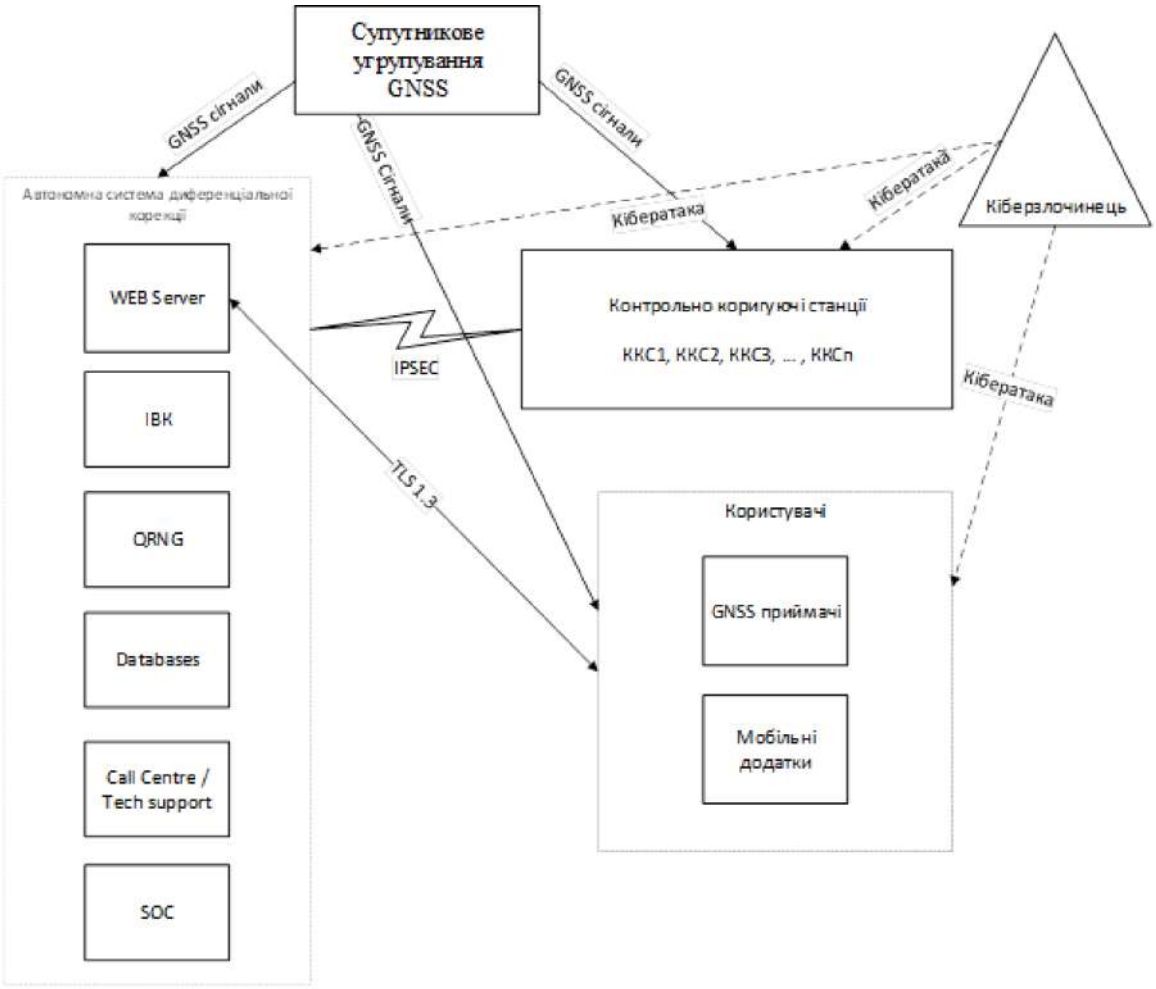

Рис. 1. Прототип архітектури автономної системи диференціальної корекції GNSS

– Кінцеві користувачі отримують коригуючі дані за допомогою сертифікованих GNSS-приймачів та мобільних додатків з можливістю перевірки достовірності отриманих даних за допомогою електронного підпису.

Запропонована архітектура орієнтована на стійкість до широкого спектру кіберзагроз, серед яких: GPS jamming, GPS spoofing, DDoS-атаки, атаки типу MITM, експлуатація вразливостей ПЗ та фізичне проникнення до об'єктів інфраструктури. Інтеграція національних постквантових криптоалгоритмів забезпечує високий рівень криптографічної стійкості як в сучасних, так і у перспективних загрозових сценаріях зокрема у постквантовий період.

Враховуючи особливості архітектури АСДК та проаналізовані підходи (наведено у таблиці 1), пропонується комбінований метод моделювання загроз, що інтегрує переваги кількох моделей:

– PASTA забезпечує сценарне формування атак із врахуванням бізнес-цілей, моделі порушника, технічної архітектури та ризиків, що важливо для критичної інфраструктури;

– MITRE ATT&CK (ICS) надає деталізовану базу знань тактик, технік та процедур (TTPs) реальних атак, особливо актуальних для OT-систем, мережевих та хмарних компонентів ІКС АСДК;

– STRIDE застосовується для початкової класифікації загроз і допомагає визначити базові категорії вразливостей кожного компоненту системи.

Поєднання цих моделей дозволяє одночасно досягти високої деталізації технік атак і комплексного охоплення архітектурних рівнів АСДК. Під час побудови моделі загроз враховано вимоги та рекомендації наступних міжнародних та національних стандартів (наведено у таблиці 2).

Побудова загальної схеми моделювання загроз.

Для побудови моделі загроз АСДК GNSS було застосовано структурний підхід, що передбачає поетапне визначення ключових об'єктів захисту та потенційних точок реалізації кібератак:

На першому етапі здійснено ідентифікацію активів системи, до складу яких віднесено користувацькі та інфраструктурні GNSS-приймачі, ІКС з її мережевими, обчислювальними й криптографічними компонентами, а також програмне забезпечення та механізми забезпечення відмовостійкості й цілісності даних. Такий підхід дозволяє систематизувати об'єкти, що підлягають захисту, і створити основу для подальшої оцінки ризиків.

Таблиця 1

Аналіз основних підходів до моделювання загроз АСДК

Модель	Короткий опис	Переваги та Недоліки	Придатність до АСДК
STRIDE	Класифікація загроз за шістьма категоріями (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)	**Переваги:** простота, структурність; **Недоліки:** без сценаріїв, не для ОТ	Частково – для первинної класифікації загроз
PASTA	Сценарне моделювання атак через 7 етапів (бізнес-цілі, декомпозиція, загрози, вразливості, сценарії, ризики, контрзаходи)	**Переваги:** мотивація, складні атаки; **Недоліки:** багато даних	Висока – базова модель сценаріїв атак
MITRE ATT&CK (ICS)	База знань реальних тактик і технік атакуючих суб'єктів для ОТ-систем	**Переваги:** деталізація, систематизація; **Недоліки:** без ризиків	Висока – деталізація технік атак
OCTAVE	Організаційна модель управління ризиками	**Переваги:** бізнес-процеси, ризики; **Недоліки:** обмежена для технічного моделювання й ОТ	Обмежено – корисна на рівні аналізу активів
LINDDUN	Модель загроз приватності даних	**Переваги:** глибокий аналіз конфіденційності; **Недоліки:** не придатна для GNSS/ОТ	Не придатна для АСДК
DREAD	Кількісна оцінка ризиків (Damage, Reproducibility, Exploitability, Affected Users, Discoverability)	**Переваги:** кількісна оцінка загроз; **Недоліки:** суб'єктивність	Дуже обмежено
VAST	Інструмент для DevOps-орієнтованого моделювання загроз	**Переваги:** agile-підхід; **Недоліки:** не для ОТ	Не придатна для ОТ-систем

Таблиця 2

Перелік стандартів

Стандарт	Основні аспекти використання
ISO/IEC 27001	Ідентифікація активів, категоризація загроз, загальна структура аналізу ризиків
NIST SP 800-30/53	Оцінка ризиків, профілювання атакуючих суб'єктів, побудова сценаріїв загроз
IEC 62443	Особливості захисту ОТ-систем, до яких належить АСДК
НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99	Врахування національних вимог України до моделювання загроз і побудови моделей порушників

Другим етапом визначено точки доступу для потенційних атак (Attack Surface). До них належать канали прийому супутникових сигналів, мережеві тракти обміну інформацією між елементами системи, серверна інфраструктура, підсистеми безпеки, а також фізичний доступ до обладнання й людський фактор у вигляді можливих атак соціальної інженерії. Виявлення таких вразливих місць є необхідною передумовою для формування комплексної моделі загроз.

Третім етапом, що завершує процес, виступає класифікація виявлених загроз за STRIDE, яка узагальнено представлена в Таблиці 3.

Четвертим етапом загальної схеми моделювання загроз є застосування методології PASTA (Process for Attack Simulation and Threat Analysis), що реалізується через послідовні фази:

Фаза 1 – Define the Objectives. Визначаються ключові цілі системи: надання високоточних диференціальних поправок у реальному часі, гарантування достовірності й доступності даних, а також забезпечення стійкості критичної інфраструктури до кіберзагроз.

Фаза 2 – Define the Technical Scope. Формується технічний контур аналізу, що охоплює активи, точки доступу (Attack Surface) та класифікацію загроз за STRIDE.

Фаза 3 – Application Decomposition and Analysis. Система розкладається на основні компоненти: GNSS-приймачі, центри обробки даних, веб-сервер, SOC/SIEM, канали зв'язку (IPSEC, TLS), криптографічну інфраструктуру (QRNG, PKI) та кінцевих користувачів.

Фаза 4 – Threat Analysis. Ідентифікуються та класифікуються загрози: GPS jamming, GPS spoofing, MITM, DDoS, експлуатація уразливостей ПЗ, фізичні атаки, соціальна інженерія, компрометація ключів.

Фаза 5 – Vulnerability & Weakness Analysis. Виконується аналіз уразливостей і слабких місць системи (результати наведено у Таблиці 4).

Фаза 6 – Attack Scenarios (сценарії атак):

Сценарій 1 – мультивекторна атака «GPS Spoofing на ККС та GPS Jamming на АСДК-приймач». Атакуючий організовує GPS spoofing на кілька ККС, паралельно здійснюючи GPS jamming на центральний GNSS-приймач системи. Це призводить до обчислення фальшивих поправок. У разі виявлення невідповідностей механізми sanity-check активують fail-safe, що блокує видачу даних користувачам.

Сценарій 2 – атака MITM на канал «ККС–ЦОД». Порушник здійснює компрометацію або підміну вузла в захищеному каналі (IPSEC), модифікуючи дані від ККС. У результаті ЦОД приймає сфальсифіковані поправки, причому підміна може стосуватися як координат, так і часових міток.

Таблиця 3

Класифікація загроз за STRIDE

Категорія STRIDE	Опис загроз у контексті АСДК
Spoofing (Підміна ідентичності)	– GPS Spoofing на GNSS-приймачі АСДК, ККС та кінцевих користувачів; – Підміна ідентифікації користувачів або адміністраторів при доступі до ІКС АСДК; – Компрометація аутентифікаційних механізмів SOC, SIEM, ІВК
Tampering (Модифікація даних)	– Модифікація GNSS-сигналів при передачі; – Модифікація даних між ККС, ЦОД та веб-сервером; – Модифікація логіки обробки поправок у ПЗ серверів; – Модифікація ключових файлів та баз даних у криптографічній інфраструктурі (QRNG, ІВК)
Repudiation (Відмова від дій)	– Несанкціоновані дії адміністраторів та персоналу SOC без належного логування; – Відмова від відповідальності за зміну конфігурації ІКС АСДК; – Відсутність або компрометація журналів аудиту
Information Disclosure (Розголошення інформації)	– Витік ключової інформації криптографічної інфраструктури (закритих ключів ІВК, QRNG); – Перехоплення даних при передачі поправок між компонентами ІКС; – Несанкціонований доступ до даних ЦОД, SOC, SIEM
Denial of Service (Відмова в обслуговуванні)	– DDoS-атаки на веб-сервер високої доступності; – Перевантаження каналів передачі даних між ККС, ЦОД, веб-сервером; – Блокування SOC через перевантаження або саботаж ПЗ
Elevation of Privilege (Ескалація привілеїв)	– Експлуатація вразливостей у ПЗ серверів ЦОД, SOC, SIEM, веб-сервера; – Отримання повноважень адміністратора системи; – Захоплення контролю над ПЗ обробки поправок

Таблиця 4

Аналіз уразливостей

Компонент	Можливі уразливості
GNSS-приймачі	Відсутність захисту від GPS jamming/GPS spoofing, відсутність верифікації сигналів
Канали передачі	Уразливості IPSEC/TLS, MITM, недостатній захист трафіку
ЦОД	Експлойти ПЗ серверів, вразливості ОС, переповнення буфера
Веб-сервер	Вразливості веб-серверного ПЗ, атаки на API, DDoS
SOC/SIEM	Компрометація облікових записів SOC, некоректна конфігурація моніторингу
Криптоінфраструктура	Компрометація ІВК, генераторів QRNG
Кінцеві користувачі	Атаки на мобільні додатки, витік даних через користувача

Сценарій 3 – комбінована атака DDoS та експлуатація уразливостей ПЗ ЦОД. Виконується масований DDoS на веб-сервер, а паралельно застосовується експлуатація zero-day уразливості в програмному забезпеченні ЦОД. Це створює умови для перехоплення контролю над логікою обробки поправок і може призвести до саботажу або відключення функціоналу системи.

Сценарій 4 – інсайдерська атака на ІВК та SOC. Зловмисні дії адміністратора SOC або іншого інсайдера з доступом до криптографічної інфраструктури створюють ризик передачі критичної інформації третім особам. Наслідком є компрометація електронного підпису та порушення цілісності диференціальних поправок, що призводить до поширення некоректних даних серед користувачів.

Сценарій 5 – фізичне знищення або захоплення ККС. Організація фізичного саботажу ККС може призвести до часткової або повної втрати джерел поправок. Це зумовлює перехід системи в режим fail-safe та створює ризик cascading failure, коли зі зростанням кількості виведених з ладу станцій підтримка працездатності системи стає критично ускладненою.

Фаза 7 – Risk & Impact Analysis

Заключною фазою методології PASTA є оцінка ризиків та наслідків реалізації виявлених загроз. На цьому етапі результати попередніх фаз інтегруються у єдину модель, яка дозволяє співвіднести кожний сценарій атаки з потенційними збитками для системи Autonomous DGNSS.

Оцінювання здійснюється за такими ключовими параметрами:

– імовірність реалізації загрози, що визначається з урахуванням наявних вразливостей та складності експлуатації;

– масштаб впливу на систему, який відображає критичність наслідків для цілісності, доступності та достовірності поправок GNSS;

– системні та cascading effects, що виникають у разі поєднання декількох атак або послідовних відмов елементів (наприклад, виведення з ладу декількох ККС).

Отримані результати дозволяють здійснити ранжування загроз за рівнем ризику та визначити пріоритетність їх нейтралізації. У подальшому це забезпечує основу для розроблення багаторівневих заходів кіберзахисту, орієнтованих на мінімізацію ймовірності успішної атаки та зниження її потенційного впливу на критичну інфраструктуру.

Наступним етапом побудови моделі загроз для АСДК є декомпозиція технік атак з використанням фреймворку MITRE ATT&CK [33–34] (наведено у таблиці 5). На цьому етапі здійснюється ідентифікація конкретних TTPs (Tactics, Techniques, Procedures), характерних для дій атакуючих суб'єктів на різних стадіях життєвого циклу атаки – від розвідки до ексфільтрації даних чи саботажу.

Таблиця 5

Техніки атак за MITRE ATT&CK

Етап атаки (Tactic)	Техніка (Technique)	Реалізація в контексті АСДК
Reconnaissance (Розвідка)	Active Scanning (T1595)	Сканування мережевої інфраструктури ІКС АСДК, SOC, веб-сервера
	Gathering Victim Network Information (T1590)	Збір відомостей про розташування ККС, IP-адреси серверів ЦОД, криптографічну інфраструктуру
Resource Development (Підготовка ресурсів)	Obtain Capabilities (T1588)	Закупівля обладнання для GPS spoofing, jamming, zero-day експлойтів
Initial Access (Початковий доступ)	Supply Chain Compromise (T1195)	Компрометація сторонніх постачальників ПЗ або обладнання ІКС АСДК
	Spearphishing (T1566)	Соціальна інженерія проти адміністраторів SOC, SIEM
	Exploit Public-Facing Application (T1190)	Атаки на веб-сервер високої доступності через уразливості API
Execution (Виконання шкідливого коду)	Exploitation for Client Execution (T1203)	Експлуатація уразливостей серверів ЦОД (переповнення буфера, SQL injection)
Persistence (Закріплення в системі)	Valid Accounts (T1078)	Використання вкрадених або скомпрометованих облікових записів адміністраторів
Privilege Escalation (Ескалація привілеїв)	Exploitation for Privilege Escalation (T1068)	Експлуатація уразливостей ОС серверів, SOC, SIEM
Defense Evasion (Обхід захисту)	Indicator Removal on Host (T1070)	Видалення логів, журналів SOC
	Obfuscated Files or Information (T1027)	Шифрування зловмисного трафіку для обходу IDS/IPS
Credential Access (Доступ до облікових даних)	Credential Dumping (T1003)	Витягування паролів адміністраторів SOC та ІВК
Discovery (Дослідження системи)	Network Service Discovery (T1046)	Сканування внутрішніх мережних сегментів АСДК
Lateral Movement (Горизонтальне пересування)	Remote Services (T1021)	Використання легітимних протоколів для руху між ЦОД, SOC, веб-сервером
Collection (Збір інформації)	Data from Information Repositories (T1213)	Збір даних із серверів поправок, БД, криптоінфраструктури
Command and Control (C2)	Application Layer Protocol (T1071)	Створення прихованих каналів C2 через HTTP(S) API
Exfiltration (Експфільтрація)	Exfiltration Over C2 Channel (T1041)	Передача викрадених даних через приховані C2
Impact (Вплив/порушення роботи)	Service Stop (T1489)	Виведення з ладу серверів обробки поправок
	Data Manipulation (T1565)	Модифікація поправок перед розповсюдженням
	Denial of Service (T1499, T1498)	DDoS-атаки на веб-сервер та мережу передачі поправок
	Inhibit Recovery (T1490)	Знищення резервних копій, шифрування даних
Доповнення для GNSS/АСДК:		
Специфіка	**Техніка**	
GPS Spoofing	У MITRE ATT&CK формально немає окремої категорії для GPS Spoofing (поки що), але зазвичай відносять до « Data Manipulation (T1565, Enterprise); ICS: Spoof Reporting Message (T0856)/Manipulation of View (T0832)/Manipulation of Control (T0831) « в контексті OT	
GPS Jamming	Частково відноситься до « Network DoS (T1498)/Endpoint DoS (T1499); ICS: Denial of Service (T0814)/Denial of View (T0815)/Denial of Control (T0813) (залежно від ефекту) « в MITRE ATT&CK for ICS	

Аналіз наслідків атак (Risk & Impact Analysis) для АСДК виконано відповідно до підходів ISO/IEC 27005 [35], NIST SP 800-30/53, IEC 62443-3-2 та НД ТЗІ 2.5-005-99. Для кожної загрози визначаються: компонент системи, тип і механізм впливу, можливі наслідки та рівень критичності (високий, середній або низький). Узагальнені результати подано в Таблиці 6.

Ключові наслідки атак на АСДК охоплюють:

– втрату точності координат та порушення синхронізації часу (з ризиками для енергетичних, фінансових і телекомунікаційних систем);
– збої у транспортній та логістичній інфраструктурі, точному землеробстві та військовій навігації;
– масові відмови автопілотованого транспорту й блокування служб точного часу;
– вторинні катастрофічні наслідки для економіки, оборони та громадської безпеки.

Узагальнена карта ризиків наведена у таблиці 7.

Таблиця 6

Аналіз наслідків атак на АСДК

№	Компонент	Загроза	Механізм впливу	Наслідки	Критичність
1	GNSS-приймачі ККС та АСДК	GPS Spoofing	Підміна супутникових сигналів	Помилкові поправки, спотворення даних у всій системі	Висока
2	GNSS-приймачі ККС та АСДК	GPS Jamming	Перешкоди в прийомі сигналів	Повна відмова генерації поправок	Висока
3	Канали передачі (ККС – ЦОД – веб-сервер)	MITM	Модифікація даних у процесі передачі	Введення некоректних поправок	Висока
4	ЦОД	Експлойти ПЗ	Захоплення контролю над логікою обробки	Масова генерація хибних поправок	Висока
5	Веб-сервер	DDoS	Перевантаження серверів	Неможливість розповсюдження поправок	Висока
6	IBK, QRNG	Компрометація ключів	Доступ до криптографічної інфраструктури	Порушення цілісності даних	Висока
7	SOC, SIEM	Інсайдерські атаки	Несанкціоновані дії персоналу	Маніпуляції без виявлення	Висока
8	Мобільні додатки користувачів	Атаки на ПЗ	Компрометація додатків	Неправильна інтерпретація даних	Середня
9	Фізичні компоненти (ККС, ЦОД)	Фізичне знищення	Саботаж, диверсія	Втрата частини системи	Висока
10	Мережа управління	Соціальна інженерія	Отримання облікових даних адміністраторів	Отримання доступу до системи	Висока
11	Резервне копіювання	Inhibit Recovery	Знищення резервних копій	Неможливість відновлення	Висока

Таблиця 7

Категорія ризику	Глобальна оцінка
Технічні ризики	Високі
Організаційні ризики	Високі
Людський фактор	Високий
Криптографічні ризики	Критичні
Фізичні ризики	Високі

Побудова моделі порушника:

1) Підходи до формування моделі порушника.

Модель порушника (adversary model, threat actor model) – дозволяє формалізувати та класифікувати потенційних атакуючих суб'єктів, які можуть здійснювати цілеспрямовані впливи на функціонування АСДК GNSS. Вона дозволяє системно описати:

– типи порушників;
– їхні ресурси та можливості;
– цілі та мотивацію;
– потенційні техніки атак.

Побудова моделі порушника базується на методології, закладеній у стандартах:

– ISO/IEC 15408 (Common Criteria) [36];
– NIST SP 800-30/53;
– НД ТЗІ 2.5-005-99 (Україна).

2) Класифікація порушника (надана в Таблиці 8).
3) Мотивація порушника (надана в Таблиці 9).
4) Ресурси порушника (надано в Таблиці 10).
5) Основні цілі атак:

– Порушення точності позиціювання та мітки часу;
– Зрив коректної роботи GNSS користувачів;
– Компрометація інфраструктури ІКС АСДК;
– Блокування розповсюдження поправок (DDoS на веб-сервер);
– Масова дезінформація користувачів через генерацію фальшивих поправок та спотвореної мітки часу;
– Фізичне знищення компонентів системи;
– Порушення довіри до державної системи точного часу та навігації.

6) Зв'язок з моделлю загроз.

Формована модель порушника є основою для побудови конкретної моделі загроз, оскільки визначає:

– рівень складності атак;
– ймовірні вектори атак;

Таблиця 8

Класифікація атакуючих суб'єктів

№	Категорія	Характеристика	Типові техніки (MITRE ATT&CK)	Основні активи атаки
1	Державні актори (APT-групи, розвідслужби)	Висококваліфіковані групи з необмеженими ресурсами, здатні до складних мультивекторних атак, включно із GPS spoofing, GPS jamming, експлуатацією вразливостей ПЗ, атак на криптосистеми, фізичних операцій, соціальний інженерінг, DDoS, MITM, тощо	T1590, T1566, T1190, T1068, T1499, T1565, T1003, ICS T0814	GNSS-приймачі ККС/АСДК, ЦОД, ІКС, (ІВК, QRNG), SOC, користувачі
2	Кіберзлочинні угруповання	Мотивовані фінансовою вигодою. Можуть атакувати АСДК з метою отримання неправомірної переваги в логістиці, агросекторі, транспорті тощо. Використовують доступні експлойти, DDoS, GPS spoofing/ GPS jamming з обмеженим радіусом дії	T1190, T1071, T1499, T1566, T1070	Веб-сервер, API, SOC, фінансові системи
3	Хактивісти (політичні/ідеологічні групи)	Мета – продемонструвати вразливість державної критичної інфраструктури. Основні вектори: DDoS, DoS, соціальна інженерія, спроби зламу веб-сервера	T1499, T1027, T1566	Веб-сервер, API
4	Інсайдери (персонал, адміністратори)	Особи з привілейованим доступом, які можуть навмисно або через помилки створити вразливості. Вектори атак – саботаж, зміна параметрів ПЗ, витік ключової інформації, людський фактор	T1078, T1070, T1003, T1071	SOC, ІВК, ЦОД, Storage, ключові БД
5	Терористичні та диверсійні групи	Мета – фізичне знищення або захоплення компонентів АСДК, зокрема ККС, ЦОД або SOC. Можуть комбінувати фізичні атаки з кібердіями	ICS T0814, ICS T0813/T0815, Physical Sabotage	ККС, ІКС, ЦОД, SOC
6	Низькорівневі зловмисники (script kiddies, аматори)	Використовують готові інструменти для DDoS, доступні вразливості в ПЗ, експлойти нульового дня за умови доступу до них на «чорному ринку»	T1190, T1499, T1071	API, веб-сервер, публічні сервіси

Таблиця 9

Мотивація атакуючих

Тип порушника	Основна мотивація
Державні актори	Геополітичні цілі, ослаблення супротивника, зрив навігаційних сервісів, компрометація національної критичної інфраструктури
Кіберзлочинці	Економічна вигода, шантаж, маніпуляція ринками
Хактивісти	Політичні заяви, демонстрація вразливостей критичних систем, політичний тиск
Інсайдери	Особиста вигода, помста, політичні мотиви
Терористи	Масовий саботаж, підрив критичної інфраструктури
Низькорівневі зловмисники	Навчання, експерименти, прагнення слави

Таблиця 10

Рівень ресурсів атакуючих суб'єктів

Рівень ресурсу	Категорії
Дуже високий	Державні актори
Високий	Терористичні організації, кіберзлочинні угруповання
Середній	Інсайдери, хактивісти
Низький	Низькорівневі зловмисники

– цільові активи системи;
– необхідні сценарії протидії.

Вона лягає в основу сценарного моделювання атак (PASTA), класифікації STRIDE, технічної деталізації MITRE ATT&CK та формування контрзаходів.

Висновки

У даній роботі проведено комплексне дослідження базових моделей загроз та моделей порушника для застосування їх до АСДК GNSS, яка є частиною критичної інформаційної інфраструктури.

Розроблено формалізовану модель порушника, що дозволяє класифікувати атакуючі суб'єкти за рівнем ресурсів, мотивацією, технічними можливостями та типами потенційних атак. Побудовано модель загроз, яка інтегрує сучасні методології моделювання, зокрема:

– класифікацію загроз за STRIDE;
– сценарне моделювання атак за PASTA;
– деталізацію технік атак за MITRE ATT&CK (Enterprise та ICS профілі).

Проаналізовано повний набір активів та зон атак системи АСДК, включаючи GNSS-приймачі ККС та АСДК, інформаційно-комунікаційну інфраструктуру, центри обробки даних, криптографічну інфраструктуру, веб-сервер високої доступності, систему моніторингу SOC та кінцевих користувачів.

Наукова новизна роботи полягає у вперше запропонованому інтегрованому підході до моделювання загроз для АСДК, який об'єднує STRIDE, PASTA та MITRE ATT&CK з урахуванням специфіки GNSS/DGNSS.

Проведено аналіз потенційних сценаріїв мультивекторних атак, які включають комбінації GPS spoofing, GPS jamming, атак на канали зв'язку, компрометації програмного забезпечення, інсайдерських дій, атак на криптоінфраструктуру та фізичного втручання у роботу системи. Встановлено, що особливу небезпеку для АСДК становлять скоординовані атаки з високим рівнем ресурсної підтримки, що здатні одночасно впливати на декілька ключових компонентів архітектури усієї системи. Особливо критичними є атаки, що призводять до генерації некоректних поправок і масового спотворення позиціювання та мітки часу, які можуть мати катастрофічні наслідки для логістичних, енергетичних, фінансових, військових та аграрних секторів. Запропоновано комплексний набір технічних, організаційних, криптографічних та процедурних контрзаходів, який базується на поєднанні міжнародних стандартів ISO/IEC 27001, ISO/IEC 27005, IEC 62443, NIST SP 800-30/53 та національних нормативних документів НД ТЗІ України. Додатково підкреслено важливість використання сучасних засобів автентифікації даних GNSS, захисту каналів розповсюдження поправок та стійкої синхронізації часу, що є визначальними для кіберстійкості АСДК.

Отримані результати можуть бути використані як методологічна основа при:

– проектуванні захищених систем диференціальної корекції GNSS;
– створенні систем виявлення атак;
– розробці нормативних документів щодо кіберстійкості критичної інфраструктури;
– подальших наукових дослідженнях в галузі кібербезпеки GNSS.

Перспективою подальших досліджень є розробка моделей активного виявлення мультивекторних атак на основі машинного навчання, побудова систем прогнозування атак та удосконалення криптографічних протоколів з урахуванням викликів постквантового періоду.

Список використаної літератури

1. European Union Agency for the Space Programme. EUSPA EO and GNSS Market Report. 2024. Iss. 2. LU: Publications Office, 2024. URL: https://data.europa.eu/doi/10.2878/73092

2. Precision Matters: Exploring the Importance of GPS Precision Accuracy. Taoglas. 20.07.2024. URL: https://www.taoglas.com/blogs/precision-matters-exploring-the-importance-of-gps-precision-accuracy

3. DGNSS Fundamentals – Navipedia. URL: https://gssc.esa.int/navipedia/index.php?title=DGNSS_Fundamentals

4. Закон України «Про критичну інфраструктуру», № 1882-IX редакція від 21.09.2024. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/go/1882-20

5. Westbrook T. A. Taxonomy of Radio Frequency Jamming and Spoofing Strategies and Criminal Motives. *Journal of Strategic Security*. 2023. Vol. 16, no. 2. P. 68–80. DOI: https://doi.org/10.5038/1944-0472.16.2.2081

6. Westbrook T. The Global Positioning System and Military Jamming: The geographies of electronic warfare. *Journal of Strategic Security*. Vol. 12, № 2. P. 1–16. DOI:10.5038/1944-0472.12.2.1720

7. Навігаційні ризики в аспекті кібербезпеки транспортних суден і військових кораблів. *ResearchGate*, 2024. doi: 10.51582/interconf.19-20.08.2022.037

8. Garmin outage caused by confirmed WastedLocker ransomware attack. BleepingComputer. URL: https://www.bleepingcomputer.com/news/security/garmin-outage-caused-by-confirmed-wastedlocker-ransomware-attack/

9. KA-SAT Network cyber attack overview. viasat.com. 30.03.2022. URL: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

10. GNSS Interference Monitoring and Classification for Critical Infrastructure Safety. GPSPATRON.com. URL: https://gpspatron.com/gnss-interference-monitoring-and-classification-for-critical-infrastructure-safety.

11. Tauschinski J., Georgiadis P., Wright R. et al. How GPS warfare is playing havoc with civilian life. *Financial Times*. 13.05.2024. URL: https://www.ft.com/content/be9393db-cd63-4141-a4c8-c16b4fe1b6b0

12. Melnyk D. S. Creating a model of threats to Ukraine's national critical infrastructure as a basis for ensuring its security and resilience. *Bulletin of Kharkiv National University of Internal Affairs*. Vol. 104, 1 (Part 1). C. 237–250. DOI:10.32631/v.2024.1.20

13. Ghanbarzade A., Soleimani H. GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning. *arXiv*, 2025. DOI:10.48550/arXiv.2501.02352

14. Radoš K., Brkić M., Begušić D. Recent Advances on Jamming and Spoofing Detection in GNSS. *Sensors*.Vol. 24, № 13. C. 4210. DOI:10.3390/s24134210

15. European Union Agency for Cybersecurity., Space threat landscape. LU: Publications Office, 2025. URL: https://data.europa.eu/doi/10.2824/8841206

16. Naik, Nitin & Jenkins, Paul & Grace, Paul & Naik, Dishita & Phd, Shaligram & Song, Jingping. A Comparative Analysis of Threat Modelling Methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. 2024. DOI:10.1007/978-3-031-74443-3_16

17. Shostack A. Threat modeling: designing for security. Indianapolis, IN : Wiley, 2014. 590 с. [QA76.9.A25 S495 2014]. ISBN 978-1-118-80999-0.

18. UcedaVelez T., Morana M. M. Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. 1st. Wiley Publishing, 2015. 696 p. ISBN 978-0-470-50096-5.

19. Threat Modeling Methodology: PASTA. URL: https://www.iriusrisk.com/resources-blog/pasta-threat-modeling-methodologies

20. Alberts C. J., Behrens S. G., Pethia R. D. та ін. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0: (Fort Belvoir, VA, 01.06.1999). Fort Belvoir, VA : Defense Technical Information Center, 1999. DOI:10.21236/ADA367718. 1999.

21. LINDDUN PRO. linddun.org. URL: https://linddun.org/pro/

22. Threat Modeling with Microsoft DREAD. *Satori*. URL: https://satoricyber.com/glossary/threat-modeling-with-microsoft-dread/

23. VAST Threat Methodology. ThreatModeler. URL: https://threatmodeler.com/glossary/vast-threat-methodology/

24. ISA/IEC 62443 Series of Standards – ISA. isa.org. URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

25. 2025 Global Threat Report. Latest Cybersecurity Trends & Insights. CrowdStrike. CrowdStrike.com. URL: https://www.crowdstrike.com/en-us/global-threat-report/

26. Asif M. R. A., Hasan K. F., Islam M. Z. et al. STRIDE-based Cyber Security Threat Modeling for IoT-enabled Precision Agriculture Systems. *arXiv*, 2022. DOI:10.48550/arXiv.2201.09493

27. Sahay R., Estay D. A. S., Meng W. et al. A Comparative Risk Analysis on CyberShip System with STPA-Sec, STRIDE and CORAS. *arXiv*, 2022. DOI:10.48550/arXiv.2212.10830

28. Sheik A. T., Atmaca U. I., Maple C. et al. Challenges in threat modelling of new space systems: A teleoperation use-case. *Advances in Space Research*. Vol. 70, Issue 8. P. 2208–2226. DOI:10.1016/j.asr.2022.07.013

29. Force J. T. Security and Privacy Controls for Information Systems and Organizations. *National Institute of Standards and Technology*. 2020. DOI:10.6028/NIST.SP.800-53r5. 2020.

30. ISO/IEC 27001:2022. ISO. URL: https://www.iso.org/standard/27001

31. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу – Інформаційна безпека та захист інформації. URL: https://tzi.ua/ua/nd_tz_2.5-004-99.html

32. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу – Інформаційна безпека та захист інформації. URL: https://tzi.ua/ua/nd_tz_2.5-005-99.html

33. Techniques – Enterprise. MITRE ATT&CK®. URL: https://attack.mitre.org/techniques/enterprise/

34. Techniques – ICS. MITRE ATT&CK®. URL: https://attack.mitre.org/techniques/ics/

35. ISO/IEC 27005:2022. ISO. URL: https://www.iso.org/standard/80585.html

36. ISO/IEC 15408-1:2022. ISO. URL: https://www.iso.org/standard/72891.html

References

1. European Union Agency for the Space Programme. (2024) EUSPA EO and GNSS Market Report. 2024. Iss. 2. LU: Publications Office, URL: https://data.europa.eu/doi/10.2878/73092

2. Precision Matters: Exploring the Importance of GPS Precision Accuracy. (2024) Taoglas. 20.07.2024. URL: https://www.taoglas.com/blogs/precision-matters-exploring-the-importance-of-gps-precision-accuracy

3. DGNSS Fundamentals – Navipedia. (2011) URL: https://gssc.esa.int/navipedia/index.php?title=DGNSS_Fundamentals.

4. Zakon Ukrayiny «Pro krytychnu infrastrukturu» № 1882-IX redaktsiya vid 21.09.2024 [Law of Ukraine "On Critical Infrastructure" No. 1882-IX, version dated 09/21/2024]. Official web portal of the Parliament of Ukraine. URL: https://zakon.rada.gov.ua/go/1882-20

5. Westbrook T. A. (2023) Taxonomy of Radio Frequency Jamming and Spoofing Strategies and Criminal Motives. *Journal of Strategic Security*, Vol. 16, no. 2. P. 68–80. DOI: https://doi.org/10.5038/1944-0472.16.2.2081

6. Westbrook T. (2019) The Global Positioning System and Military Jamming: The geographies of electronic warfare. *Journal of Strategic Security*, Vol. 12, № 2. P. 1–16. DOI:10.5038/1944-0472.12.2.1720

7. Navihatsiyni ryzyky v aspekti kiberbezpeky transportnykh suden i viys′kovykh korabliv (2024) [Navigational risks in terms of cybersecurity of transport vessels and warships]. *ResearchGate*, doi: 10.51582/interconf.19-20.08.2022.037

8. Garmin outage caused by confirmed WastedLocker ransomware attack. (2020) BleepingComputer. URL: https://www.bleepingcomputer.com/news/security/garmin-outage-caused-by-confirmed-wastedlocker-ransomware-attack/

9. KA-SAT Network cyber attack overview. (2022) Viasat.com. 30.03.2022. URL: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

10. GNSS Interference Monitoring and Classification for Critical Infrastructure Safety. (2022) GPSPATRON.com. URL: https://gpspatron.com/gnss-interference-monitoring-and-classification-for-critical-infrastructure-safety.

11. Tauschinski J., Georgiadis P., Wright R. et al. (2024) How GPS warfare is playing havoc with civilian life. *Financial Times*, 13.05.2024. URL: https://www.ft.com/content/be9393db-cd63-4141-a4c8-c16b4fe1b6b0

12. Melnyk D. S. (2024) Creating a model of threats to Ukraine's national critical infrastructure as a basis for ensuring its security and resilience. *Bulletin of Kharkiv National University of Internal Affairs*, Vol. 104, 1 (Part 1). C. 237–250. DOI:10.32631/v.2024.1.20

13. Ghanbarzade A., Soleimani H. (2025) GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning. *arXiv*, DOI:10.48550/arXiv.2501.02352

14. Radoš K., Brkić M., Begušić D. (2024) Recent Advances on Jamming and Spoofing Detection in GNSS. *Sensors*, Vol. 24, № 13. C. 4210. DOI:10.3390/s24134210

15. European Union Agency for Cybersecurity. (2025) Space threat landscape. LU: Publications Office. URL: https://data.europa.eu/doi/10.2824/8841206.

16. Naik? Nitin & Jenkins, Paul & Grace, Paul & Naik, Dishita & Phd, Shaligram & Song, Jingping. (2024) A Comparative Analysis of Threat Modelling Methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. DOI:10.1007/978-3-031-74443-3_16

17. Shostack A. (2014) Threat modeling: designing for security. Indianapolis, IN : Wiley, 590 c. [QA76.9.A25 S495 2014]. ISBN 978-1-118-80999-0.

18. UcedaVelez T., Morana M. M. (2015) Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. 1st. Wiley Publishing, 696 p. ISBN 978-0-470-50096-5.

19. Threat Modeling Methodology: PASTA. (2023) URL: https://www.iriusrisk.com/resources-blog/pasta-threat-modeling-methodologies

20. Alberts C. J., Behrens S. G., Pethia R. D. (1999) Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0: (Fort Belvoir, VA, 01.06.1999). Fort Belvoir, VA : Defense Technical Information Center, DOI:10.21236/ADA367718. 1999

21. LINDDUN PRO. linddun.org. URL: https://linddun.org/pro/

22. Threat Modeling with Microsoft DREAD. *Satori*. URL: https://satoricyber.com/glossary/threat-modeling-with-microsoft-dread/

23. VAST Threat Methodology. ThreatModeler. URL: https://threatmodeler.com/glossary/vast-threat-methodology/

24. ISA/IEC 62443 Series of Standards – ISA. isa.org. URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

25. 2025 Global Threat Report. Latest Cybersecurity Trends & Insights. CrowdStrike. CrowdStrike.com. URL: https://www.crowdstrike.com/en-us/global-threat-report/

26. Asif M. R. A., Hasan K. F., Islam M. Z. et al. (2022) STRIDE-based Cyber Security Threat Modeling for IoT-enabled Precision Agriculture Systems. *arXiv*. DOI:10.48550/arXiv.2201.09493

27. Sahay R., Estay D. A. S., Meng W. et al. (2022) A Comparative Risk Analysis on CyberShip System with STPA-Sec, STRIDE and CORAS. *arXiv*. DOI:10.48550/arXiv.2212.10830

28. Sheik A. T., Atmaca U. I., Maple C. et al. (2022) Challenges in threat modelling of new space systems: A teleoperation use-case. *Advances in Space Research*. Vol. 70, Issue 8. P. 2208–2226. DOI:10.1016/j.asr.2022.07.013

29. Force J. T. (2020) Security and Privacy Controls for Information Systems and Organizations. *National Institute of Standards and Technology*. DOI:10.6028/NIST.SP.800-53r5. 2020.

30. ISO/IEC 27001: 2022. (2022) ISO. URL: https://www.iso.org/standard/27001

31. Kryteriyi otsinky zakhyshchenosti informatsiyi v komp″yuternykh systemakh vid nesanktsionovanoho dostupu. [Criteria for assessing the security of information in computer systems from unauthorized access]. *Information security and information protection*. URL: https://tzi.ua/ua/nd_tz_2.5-004-99.html

32. Klasyfikatsiya avtomatyzovanykh system i standartni funktsional′ni profili zakhyshchenosti obroblyuvanoyi informatsiyi vid nesanktsionovanoho dostupu [Classification of automated systems and standard functional profiles of security of processed information from unauthorized access]. *Information security and information protection*. URL: https://tzi.ua/ua/nd_tz_2.5-005-99.html

33. Techniques – Enterprise. MITRE ATT&CK®. URL: https://attack.mitre.org/techniques/enterprise/

34. Techniques – ICS. MITRE ATT&CK®. URL: https://attack.mitre.org/techniques/ics/

35. ISO/IEC 27005:2022. ISO. URL: https://www.iso.org/standard/80585.html

36. ISO/IEC 15408-1:2022. ISO. URL: https://www.iso.org/standard/72891.html

Дата першого надходження рукопису до видання: 24.09.2025
Дата прийнятого до друку рукопису після рецензування: 21.10.2025
Дата публікації: 28.11.2025