УДК 621.317.76.089.68:621.373.82 **DOI:10.30837/rt.2025.1.220.05**

О.А. СНЄОСІКОВ, *О.П. НАРЄЖНІЙ, канд. техн. наук, Т.О. ГРІНЕНКО, канд. техн. наук*

МОДЕЛІ ТА МЕТОДИ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ АВТОНОМНОЇ СИСТЕМИ ДИФЕРЕНЦІАЛЬНОЇ КОРЕКЦІЇ ГЛОБАЛЬНИХ НАВІГАЦІЙНИХ СУПУТНИКОВИХ СИСТЕМ

Вступ

Розвиток глобальних навігаційних супутникових систем (Global navigation satellite systems, GNSS) триває вже понад півстоліття, починаючи з перших експериментальних систем у 1960-х роках до сучасних високоточних глобальних навігаційних систем, що використовуються у всьому світі.

Сучасний ринок GNSS характеризується функціонуванням кількох ключових супутникових навігаційних систем, а саме:

– GPS (Global Positioning System), розроблена Сполученими Штатами Америки (США) – має на орбіті планети близько 31 активних супутників [1, 2];

– GLONASS (Глобальна навігаційна супутникова система), створена Радянським Союзом (тепер Російська Федерація) – має 24 активних супутників [3];

– Galileo – супутникова система навігації Європейського Союзу та Європейського космічного агентства, наразі функціонує з 24 активними супутниками (повна констеляція налічує 30 супутників, враховуючи 6 резервних) [4];

– BeiDou – супутникова система навігації Китайської Народної Республіки, працює з 30 активними супутниками [5].

А також регіональні системи:

– IRNSS (NavIC) – індійська система навігації – має 7 супутників для забезпечення регіонального покриття [6];

– QZSS – японська система навігації – забезпечує регіональне покриття за допомогою 4 супутників [7].

Доповненням до глобальних систем GNSS є супутникові системи корекції та моніторингу, які забезпечують підвищення точності позиціонування за рахунок виправлення похибок супутникових сигналів та моніторингу їх стабільності, забезпечуючи точність до 1-2 метрів.

До таких систем належать:

– WAAS (Wide Area Augmentation System) – система, розроблена у Сполучених Штатах Америки, яка використовує мережу наземних базових станцій для обчислення коригувальних поправок, що передаються супутниками. WAAS дозволяє значно підвищити точність GPS-позиціювання, забезпечуючи горизонтальну точність до 1-2 метрів у багатьох регіонах [8].

– EGNOS (European Geostationary Navigation Overlay Service) – європейська система, що доповнює GPS шляхом передачі коригувальних сигналів із геостаціонарних супутників і наземних базових станцій. EGNOS покращує точність і надійність навігаційних даних у Європі [9].

– СДКМ (Російська система диференційної корекції) – система, що використовується для корекції навігаційних даних супутникової системи GLONASS, забезпечуючи підвищену точність позиціонування в Росії та суміжних регіонах [3].

– GAGAN (GPS Aided Geo Augmented Navigation) – індійська система супутникового підсилення, розроблена для забезпечення високоточних навігаційних послуг в Індії та прилеглих регіонах. GAGAN покращує точність позиціонування завдяки використанню наземної інфраструктури та супутникових сигналів [6].

– MSAS (Multi-functional Satellite Augmentation System) – японська система супутникового підсилення, яка доповнює навігаційні сигнали GPS для забезпечення більшої точності позиціонування в регіоні Японії [10].

Системи корекції і моніторингу значно підвищують ефективність та точність GNSS-систем, дозволяючи користувачам отримувати дані з набагато вищою точністю, що є критично важливим для застосувань у авіації, морській навігації, сільському господарстві, геодезії та інших галузях.

Поєднання GNSS із наземними технологіями, такими як інерційна навігація, диференціальні системи корекції (DGPS, RTK, SBAS), LTE, 5G для передачі поправок, лазерне сканування (LiDAR) та системи машинного зору, відкриває нові можливості для розробки технологій, що забезпечують не лише високу точність, але й підвищену надійність та цілісність навігаційних сигналів.

За прогнозами, встановлена база GNSS-пристроїв буде стрімко зростати: з 5,6 мільярдів одиниць у 2023 р. до майже 9,0 мільярдів одиниць у 2033 р. [9]. Цей суттєвий ріст відображає зростаючу потребу в супутникових навігаційних технологіях у різних секторах економіки, від автомобільної промисловості та землеробства до електронних комунікацій та фінансових послуг.

Очікується, що до 2030 р. глобальний ринок GNSS виросте з рівня 260 мільярдів євро (станом на 2023 р.) до 590 мільярдів євро, що свідчить про суттєве розширення галузі [9].

Екосистема GNSS є багаторівневою та охоплює всі аспекти роботи технології – від супутникових угруповань до кінцевих користувачів. Вона поділяється на три ключові рівні:

1. Інфраструктурний рівень (базовий). Цей рівень включає операторів супутникових систем, таких як GPS (США), GLONASS (Росія), Galileo (Європейський Союз) та BeiDou (Китай). Вони відповідають за розробку, запуск та обслуговування супутників, що забезпечують глобальне покриття навігаційними сигналами.

2. Технологічний рівень (середній). Сюди входять виробники мікросхем та приймачів, які розробляють обладнання для прийому та обробки GNSS-сигналів. Наприклад, компанія Septentrio спеціалізується на високоточних GNSS-приймачах для різних застосувань, включаючи БПЛА.

3. Прикладний рівень (верхній). Цей рівень охоплює кінцеві застосування GNSS-технологій у різних галузях, таких як транспорт, безпека, сільське господарство, геодезія та критична інфраструктура. Наприклад, сервіс високої точності (High Accuracy Service, HAS) від навігаційної системи Galileo надає сантиметрову точність позиціонування в реальному часі, що є критично важливим для геодезичних робіт та точного землеробства [11].

Постановка проблеми

GNSS відіграють ключову роль у забезпеченні стабільної роботи критичних секторів економіки та національної безпеки. Відповідно до Закону України "Про критичну інфраструктуру" № 1882-IX від 15 листопада 2021 р. до критично важливих сфер належать: «15) космічна діяльність, космічні технології та послуги» [12]. Це прямо включає GNSS, оскільки вони є невід'ємною частиною космічних технологій і надають критично важливі послуги для безпеки, економічної та соціальної стабільності держави. Проте, ця технологія стала мішенню для кіберзагроз, що не може не впливати на надійність та безпеку навігаційних систем. Кібератаки на GNSS можуть спричиняти спотворення сигналів, перехоплення даних або навіть повну дезорієнтацію користувачів, що створює значну загрозу функціонуванню критичної інфраструктури.

Транспортні системи, енергетика, аеропорти та морські порти стають об'єктами підвищеного ризику, оскільки їхнє функціонування значною мірою залежить від точних і достовірних даних GPS [13]. Основний перелік споживачів технологій GNSS включає автомобільні навігаційні системи, смартфони та планшети, логістичні та транспортні компанії, повітряну та морську навігацію, туризм і активний відпочинок, сільське господарство, наукові дослідження, аварійно-рятувальні служби, спортсменів та фітнес-програми, банківський сектор, бізнес-корпорації та служби доставки. Враховуючи це, кібератаки на GPS можуть мати значні наслідки для суспільної безпеки та економічної стабільності країни [14]. У зв'язку з

цим забезпечення захисту GPS-систем стає надзвичайно важливим для підтримки функціонування цих критично важливих сфер та забезпечення національної безпеки.

Найбільш відомими прикладами кібератак на GNSS за останні роки є:

– 2017 р. – Кібератака NotPetya та WannaCry. Масштабні кібератаки на інформаційно-комунікаційні системи (ІКС), зокрема ІКС GNSS, вразили навігаційні системи транспортних суден і портів, викликавши перебої в роботі логістичних ланцюгів [15];

– 2017 – 2018 рр. – перешкоди GPS під час військових навчань "Захід-2017" та "Єдиний тризуб-2018". Було здійснено глушіння сигналів GPS у Латвії та Норвегії під час військових навчань, що вплинуло на цивільні авіаційні системи [16];

– 2020 р. – Кібератака на сервери Garmin. Хакерська група Evil Corp здійснила атаку вірусом-вимагачем WastedLocker, що вивело з ладу сервіси ІКС Garmin Connect та інші онлайн-служби. Вимагали викуп у 10 млн. доларів [17];

– 2022 р. – Атака на супутникову мережу KA-SAT. Перед початком повномасштабного вторгнення в Україну була здійснена атака на супутникову мережу KA-SAT, що призвело до перебоїв у роботі інтернет-з'єднання в Україні та Європі [18];

– 2024 р. – Глушіння сигналів GPS у Балтійському регіоні. Велика кількість авіарейсів до Великої Британії зазнала навігаційних проблем через глушіння сигналів GPS у Балтійському регіоні [19].

За період з 2022 – 2025 роки Україна також стала свідком серії інцидентів, пов'язаних із кібератаками на системи глобального позиціонування (GPS). Спостереження приватних компаній бізнес-сегменту держави вказують на різке збільшення відхилень у моніторингу GPS-приймачів, що свідчить про зростання кібератак на GPS у 2022 – 2025 роках (рис. 1).

Рис. 1. Кібератаки на GPS

На сьогодні кібератаки на супутникові навігаційні системи можуть здійснювати як приватні криптоаналітики, так і криптоаналітики третього рівня, використовуючи найпотужніші засоби для кібератак. Таким чином, кібератаки на супутникові системи навігації в Україні вимагають негайної уваги та вивчення через потенційно серйозні наслідки для національної безпеки та економіки.

У цій роботі розглядається реалізація концепції «Створення системи координатно-часового та навігаційного забезпечення України з використанням інформації, отриманої від глобальних навігаційних супутникових систем різних держав» [20]. Відповідно до Концепції реалізації державної політики у сфері космічної діяльності до 2032 р. [21], затвердженої

Розпорядженням КМУ № 238-р від 30 березня 2011 р., планується створення національної системи геоінформаційного забезпечення та проведення моніторингу надзвичайних ситуацій. Ця система буде складовою частиною європейської програми Copernicus, яка до 2012 року мала назву Global Monitoring for Environment and Security (GMES) [22], та світової Global Earth Observation System of Systems (GEOSS), яка буде забезпечувати експлуатацію її інформаційних сервісів зацікавленими користувачами [23].

Проблема, яка набуває особливої актуальності в межах цього дослідження, пов'язана з тим, що на сьогодні ще недостатньо врегульоване на законодавчому рівні питання щодо впровадження діяльності у сфері супутникової навігації, зокрема щодо [24]:

- забезпечення безпечного використання інформації GNSS;
- розроблення та застосування національних стандартів і технічних регламентів щодо виробництва апаратури, засобів супутникової навігації, спеціалізованого програмного забезпечення, надання супутникових навігаційних інформаційних послуг;
- обміну інформацією між вітчизняними та іноземними функціональними доповненнями;
- захисту інформації у сфері супутникової навігації відповідно до вимог Закону України "Про захист інформації в інформаційно-комунікаційних системах" [25];

Очікувані результати після ухвалення проєкту Закону України "Про державне регулювання у сфері супутникової навігації" [24] передбачають такі переваги, як підвищення рівня безпеки та надійності транспортно-логістичного комплексу, розвиток його інфраструктури, а також підвищення якості надання навігаційних послуг користувачам навігаційних послуг України.

Діяльність у сфері супутникової навігації здійснюється за такими напрямами [24, 26]:

1. Моніторинг з використанням функціональних навігаційних інформаційних систем для об'єктів супутникової навігації в галузях будівництва, енергетики та транспортної інфраструктури з метою своєчасного запобігання виникненню надзвичайних ситуацій та ліквідації їх наслідків.

2. Створення, розвиток і експлуатація функціональних доповнень та навігаційних інформаційних систем, а також надання супутникових навігаційних інформаційних послуг користувачам. Це включає обмін інформацією між вітчизняними та іноземними функціональними доповненнями на основі вимог законодавства та міжнародних договорів.

Відповідно до проєкту Закону України "Про державне регулювання у сфері супутникової навігації" користувачі глобальних навігаційних супутникових систем можуть бути тимчасово обмежені в супутникових навігаційних визначеннях власною апаратурою та засобами супутникової навігації (повністю або з бажаним рівнем точності) та в отриманні інших супутникових навігаційних інформаційних послуг у певних районах та/або на певних об'єктах, де існує військова загроза або небезпека терористичної діяльності. Це положення регламентує впровадження заходів протидії атакам по типу GPS spoofing та GPS jamming на GNSS, а також захист від інших хакерских кібератак на ІКС GNSS.

Захист інформації у сфері супутникової навігації в обов'язковому порядку має здійснюватися відповідно до вимог Закону України "Про електронні комунікації" [27]. Захисту підлягає інформація, яка:

- постачається у складі супутникових навігаційних інформаційних послуг користувачам функціональних доповнень та навігаційних інформаційних систем, що виконують завдання у сфері оборони та національної безпеки, цивільного захисту населення та об'єктів інфраструктури, а також охорони правопорядку;
- опрацьовується у функціональних навігаційних інформаційних системах.

Зокрема, проєктом Закону України "Про затвердження Загальнодержавної цільової науково-технічної космічної програми України на 2021 – 2025 роки" (реєстр. № 6129 від 04.10.2021) [28] передбачено захід "Розвиток Системи координатно-часового та навігаційного забезпечення України та забезпечення використання інформаційних сервісів європейської

навігаційної супутникової системи EGNOS/Galileo на території України" з фінансуванням у розмірі 40,78 млрд. гривень до 2025 р.

Аналіз основних досліджень і публікацій.

Проблематиці кіберзахисту супутникового зв'язку присвячено численні наукові праці. Зокрема, у [29] висвітлюються сучасні технології захисту від GPS spoofing, серед яких: аналіз потужності сигналу та його характеристик, застосування диференційного GPS (DGPS), використання мультичастотних та багатосистемних приймачів, автентифікація сигналів, фільтрація на основі методів машинного навчання, а також інтеграція з інерційними навігаційними системами (ІНС). В роботі [30] надано аналіз методів захисту безпілотних літальних апаратів (БПЛА) від атак типу GPS spoofing для забезпечення безпечної навігації. Розглядаються різні підходи до підвищення функціональної ефективності БПЛА в умовах кіберзагроз, а саме, направлені на оптимізацію польотів алгоритми та методи, що дозволяють швидше та точніше вирішувати задачі планування польотів, визначення аномалій у навігаційних даних, інтеграцію штучного інтелекту (генеративний дизайн, алгоритми керування роєм, комп'ютерний зір і метод інформаційно-екстремального навчання), запропоновано використання схеми 2+2, яка складається із ІНС, GNSS, радарів та оптичних систем для підвищення надійності пілотажно-навігаційного обладнання. Додатково автори зазначають, що у науковій літературі існує досить мало робіт, присвячених аспектам надійності та відмовостійкості GNSS пристроїв проти кібератак. В роботі [31] запропоновано комплексний підхід для підвищення стійкості та якості супутникового приймального обладнання до впливу завад типу GPS spoofing та GPS jamming з використанням приймальних антен на базі фазованих антенних решіток. В роботі [32] наголошується, що маніпуляція часом GNSS є серйозною загрозою для навігаційних систем, оскільки атаки можуть здійснюватися як синхронно, так і асинхронно, змінюючи мітку часу приймача GNSS. Дані дослідження підтверджують, що використання комбінації локальних і віддалених джерел міток часу дозволяє ефективно виявляти такі атаки. У роботі [33] дослідники спроєктували та розробили атаку, яка дозволяє підробляти місцезнаходження або рух приймача-жертви без зміни змісту навігаційного повідомлення реального сигналу шляхом ретрансляції сигналів GNSS. В зв'язку з необхідністю запобігання кібератакам, що загрожують цілісності даних диференціальних поправок в автономній системі диференціальної корекції (СДК), науковці запропонували [34] вирішення цієї проблеми шляхом усунення вразливості даних СДК, яка виникає при використанні MD5 у протоколі NTP. Запропоновано модифікацію NTP-сервера часу СДК відповідно до схеми ANSI X9.95 із застосуванням криптографічно стійкої імітовставки (MAC). Також проведено метрологічне дослідження макету NTP-сервера СДК із використанням криптографічно стійкої MAC.

Метою статті є аналіз та дослідження існуючих моделей та методів захисту від кіберзагроз на GNSS шляхом надання та обґрунтування рекомендацій щодо впровадження сучасних рішень в інформаційно-комунікаційні системи автономних СДК з урахуванням вимог національних стандартів до рівня безпеки в постквантовий період.

Основні кіберзагрози для автономної СДК GNSS

1. Глушіння сигналу (GPS jamming).

Використання потужних радіочастотних перешкод може повністю блокувати приймачі GNSS, змушуючи системи втрачати сигнал і припиняти навігацію. Це особливо небезпечно для авіації, морського транспорту та військових операцій. Доступні на ринку пристрої для глушіння GNSS-сигналів, які коштують до 100 $ [14], можна ефективно використовувати для дестабілізації навігаційної інфраструктури.

2. Спуфінг сигналу (GPS spoofing).

Це атака, при якій створюється фальшивий GNSS-сигнал, що змушує приймач визначати неправильне місцеположення або час. Використовується для шахрайських схем, наприклад, викрадення вантажів або введення в оману навігаційних систем автономного транспорту.

У військовій сфері така атака може спричинити дезорієнтацію військових дронів або зброї з супутниковим наведенням.

3. Кібератаки на наземну інфраструктуру GNSS.

GNSS-сигнали слабкі, тому наземні системи корекції та моніторингу мають важливе значення для забезпечення корегувальною інформацією споживачів. Хакерські атаки можуть вивести з ладу ІКС автономної СДК, що суттєво спричинить викривлення навігаційних даних у критичних галузях.

Моделі та методи кібератак на автономну СДК GNSS

1. GPS spoofing. Атака спуфінгу базується на передачі сигналів з параметрами, схожими на справжні сигнали GNSS, але з модифікованими даними навігації. Математично базовий приклад сигналу спуфінга можна описати наступним чином.

Спуфер повинен відтворити радіочастотну (RF – Radio frequency) несучу, псевдовипадковий код (PRN – pseudo-random code) розширення спектра, а також потік бітів даних кожного відкритого супутникового GNSS-сигналу, який він має намір підробити. Типовий прийнятий сигнал GNSS має вигляд [35]:

$$y(t) = Re\left\{\sum_{i=1}^{N} A_i D_i[t-\tau_i(t)] C_i[t-\tau_i(t)]\, e^{j[\omega_c t-\varphi_i(t)]}\right\}, \quad (1)$$

де N – кількість сигналів, кожен з яких відповідає певному супутнику (з унікальним кодом); A_i – амплітуда сигналу i-го супутника; $D_i(t)$ – потік бітів даних сигналу i-го супутника; $C_i(t)$ – код розширення спектра (наприклад, BPSK PRN або BOC/PRN); $\tau_t(t)$ – кодова затримка (тобто, коли приймач "бачить" цей сигнал); $\omega_c t$ – несуча частота; $\varphi_i(t)$ – фазовий зсув (beat carrier phase) для i-го сигналу.

Спуфер передає набір фальшивих сигналів, подібних до:

$$y_s(t) = Re\left\{\sum_{i=1}^{N_s} A_{si} \widehat{D}_i[t-\tau_{si}(t)] C_i[t-\tau_{si}(t)]\, e^{j[\omega_c t-\varphi_{si}(t)]}\right\}, \quad (2)$$

де параметри фейкових сигналів (для $i = 1, \dots, N_s$): A_{si} – амплітуда, τ_{si} – кодова затримка, $\varphi_{si}(t)$ – фаза несучої.

Номінально $N_s = N$, тобто кількість фейкових сигналів дорівнює кількості справжніх. Кожен спуфінговий сигнал повинен мати той самий код $Ci(t)$, що і відповідний справжній сигнал, щоб обдурити приймач. Зазвичай передають найкращу оцінку бітового потоку $\widehat{D}_i(t)$, який мав би бути. Ці параметри можуть трохи відрізнятись від справжніх, оскільки залежні від положення антени спуфера.

Повна модель прийнятого сигналу:

$$y_{tot}(t) = y(t) + y_s(t) + v(t), \quad (3)$$

де $v(t)$ – шум (в основному – білий гаусівський).

У деяких випадках цей шум є основним джерелом перешкод. В інших – саме спуфер створює значну частину сигналу, включаючи як дані, так і шум.

2. GPS jamming. Глушіння реалізується шляхом передачі шумового або узгодженого сигналу з високою потужністю, що перевищує рівень корисного сигналу GNSS. Математично базовий приклад сигналу глушіння можна описати як [36]:

$$x_j(t) = A_j exp\left(j\theta_0 + j2\pi \int_0^{t-\tau_p} f_i(u)du\right), \quad (4)$$

де A_j – амплітуда сигналу глушіння, τ_p – затримка поширення сигналу від генератора заглушення до приймача, θ_0 – фазове зміщення сигналу заглушення, f_i – миттєва частота з періодичним характером.

3. Хакерські атаки на автономну СДК:

– DDoS-атаки на сервери автономної СДК. Розподілені атаки типу "відмова в обслуговуванні" (DDoS) спрямовані на перевантаження серверів автономної СДК

численними запитами, що призводить до їхньої недоступності. DDoS-атаки характеризуються інтенсивним трафіком із багатьох джерел до цільового сервера.

DDoS-атака на сервер-жертву виснажує ресурси цільового сервера, що змушує сервер відмовляти у з'єднанні новим легітимним клієнтам. Виснаження ресурсів сервера може стосуватися як пропускної здатності, так і буферної пам'яті сервера-жертви. Наступне рівняння надає визначення загальної ймовірності виснаження ресурсів на сервері-жертві [37]:

$$Total_{attack} = 1 - \left(1 - P^{\beta}\right)(1 - P^{M}), \tag{5}$$

де $Total_{attack}$ – ймовірність повного виснаження ресурсів жертви внаслідок атаки, P^{β}– ймовірність виснаження пропускної здатності, P^{M} – ймовірність виснаження пам'яті.

Для опису моделі атаки розглянемо два різні випадки в контексті виснаження пропускної здатності та оперативної пам'яті [37].

В и п а д о к А : ймовірність виснаження пропускної здатності визначається рівнянням [37]:

$$P^{\beta} = \frac{\left(\frac{\alpha^{C}}{C!}\right)}{\sum_{i=0}^{C} \frac{\alpha^{i}}{i!}}, \tag{6}$$

де

$$\alpha = \frac{\beta_A + \beta_N}{\beta_{Total}} = \frac{\left(\frac{\delta_{BA}}{\tau_{BA}} + \frac{\delta_{BN}}{\tau_{BN}}\right)}{\beta_{Total}}, \tag{7}$$

C – кількість відкритих каналів або невикористаної пропускної здатності; β_A – пропускна здатність, що споживається атакуючими клієнтами; β_N – пропускна здатність, що споживається легітимними клієнтами; β_{Total} – загальна пропускна здатність; δ_{BA} – розмір переданого пакета для атакуючих клієнтів у контексті пропускної здатності; δ_{BN} – розмір переданого пакета для легітимних клієнтів у контексті пропускної здатності; τ_{BA} – частота прибуття (інтервал) пакетів атакуючих клієнтів; τ_{BN} – частота прибуття (інтервал) пакетів легітимних клієнтів.

Припускаючи, що розмір пакетів подібний у випадках атаки й звичайного трафіку, тобто: $\delta_{BA} = \delta_{BN} = \delta_B$, маємо:

$$\alpha = \frac{\delta_B}{\beta_{Total}}\left(\frac{1}{\tau_{BA}} + \frac{1}{\tau_{BN}}\right) = K \times \frac{1}{\tau_{BA}}, \text{ оскільки } \frac{\delta_\beta}{\beta_{Total}} = K;\ \frac{1}{\tau_{BN}} \to 0, \tag{8}$$

де K – деяка константа. Тобто:

$$\alpha \propto \frac{1}{\tau_{BA}}\ . \tag{9}$$

Інтервал між прибуттям пакетів визначається як час між двома суміжними пакетами від одного клієнта. Використовуючи рівняння (6) та (9), отримуємо два висновки [37]:

$$P^{\beta} \propto \frac{1}{C} \tag{10}$$

та

$$P^{\beta} \propto \alpha \propto \frac{1}{\tau_{BA}}\,. \tag{11}$$

В и п а д о к В : ймовірність виснаження пам’яті або буфера задається рівнянням [37]:

$$P^M = \frac{\left(\frac{\gamma^{M_{Total}}}{M_{Total}}\right)}{\sum_{i=0}^{M_{Total}} \frac{\gamma^i}{i!}}\ , \tag{12}$$

де

$$\gamma = M_A + M_N = \frac{\delta_{MA}}{\tau_{MA}} + \frac{\delta_{MN}}{\tau_{MN}}\left[since\ M_A = \frac{\delta_{MA}}{\tau_{MA}}\ and\ M_N = \frac{\delta_{MN}}{\tau_{MN}}\right],$$

тобто

$$\gamma = \delta_M\left(\frac{1}{\tau_{MA}} + \frac{1}{\tau_{MN}}\right) = \frac{\delta_M}{\tau_{MA}}[since\ \delta_{MA} = \delta_{MN} = \delta_M\ and\ since\ \frac{1}{\tau_{MN}} \to 0].$$

Маємо:

$$\gamma \propto \frac{1}{\tau_{MA}}. \tag{13}$$

Використовуючи рівняння (12) та (13), отримаємо два висновки [37]:

$$P^M \propto \frac{1}{M_{Total}}\ . \tag{14}$$

$$P^M \propto \gamma \propto \frac{1}{\tau_{MA}}\ . \tag{15}$$

Атаки типу "людина посередині" (Man-in-the-Middle, MitM). Такий вид атаки спрямований на перехоплення та можливу модифікацію даних, що передаються між двома сторонами, без їхнього відома. У контексті автономних СДК GNSS це може означати перехоплення даних між приймачем та наземними станціями корекції, що дозволяє зловмиснику змінювати або підробляти навігаційні дані. Така атака ставить під загрозу конфіденційність, цілісність та автентичність переданої інформації.

Припустимо, що дані d передаються від відправника A до отримувача B через канал зв'язку. Зловмисник M перехоплює ці дані, змінює їх на d' і передає B. Математично це можна описати як: $A \to M: d; M(d) = d'; M \to B: d'$. Це призводить до того, що B отримує модифіковані дані d' замість оригінальних d, що може викликати неправильне визначення координат або інших параметрів.

Атаки на програмне забезпечення (ПЗ) автономної СДК GNSS. Криптоаналітики можуть використовувати вразливості в програмному забезпеченні автономної СДК для виконання несанкціонованих дій, таких як виконання шкідливого коду, проникнення в ІКС та отримання доступу до конфіденційних даних. Наприклад, припустимо, що в програмному забезпеченні веб ресурсу автономної СДК є вразливість, яка дозволяє виконати переповнення буфера. Зловмисник надсилає спеціально сформований сигнал $s_{exploit}$, який викликає переповнення буфера і дозволяє виконати шкідливий код. Математично це можна описати як

$$s_{exploit} = \{s_1, s_2, \dots, s_n\}\ , \tag{16}$$

де s_i – частини сигналу, які разом перевищують розмір буфера приймача. Це може призвести до виконання зловмисного коду на стороні веб-ресурса автономної СДК, що може порушити його роботу або сприяти порушенню цілісності даних.

Атаки на фізичне проникнення або пошкодження автономної СДК. Кіберзлочинці можуть здійснювати атаки на наземні станції GNSS, виводячи їх з ладу через фізичне пошкодження. Така атака більш спроможна здійснити саботаж автономної СДК, результатом якої є обмеження до коригувальної інформації певних регіонів СДК. Математичну модель (стійкість автономної СДК до саботажу) можна розрахувати на основі концепції класичної k-out-of-n структури надійності, яка реалізується через біноміальну модель, де для успішної

роботи необхідно, щоб функціонували принаймні k із n компонентів [38,39]. Припустимо, що система має N наземних станцій, і для корекції сигналу потрібно одночасне функціонування N_{req} станцій. Ймовірність нормальної роботи станції після атаки визначається як

$$P_{work} = 1 - P_{fail} \ , \tag{17}$$

де P_{fail} – ймовірність успішного виведення станції з ладу.

Якщо атаки незалежні між станціями, ймовірність того, що хоча б $Nreq$ станцій залишаться працездатними:

$$P_{survive} = \sum_{k=Nreq}^{N} \binom{N}{k} P_{work}^{k} (1 - P_{work})^{N-k} \ . \tag{18}$$

Якщо $P_{survive}$ падає нижче певного значення P_{crit}, система вважається недієздатною, що порушує доступність даних.

Якщо зловмисник одночасно атакує M станцій, то ймовірність знищення кожної:

$$P_{fail} = \frac{M}{N}. \tag{19}$$

Визначення мінімальної кількості станцій M_{crit}, які треба атакувати для виведення системи з ладу:

$$M_{crit} = N - min_k \left(\sum_{k=Nreq}^{N} \binom{N}{k} P_{work}^{k} (1 - P_{work})^{N-k} \leq P_{crit} \right). \tag{20}$$

Моделі та методи захисту автономної СДК GNSS від кібератак

1. *Автентифікація GNSS на рівні сигналу*.

Commercial Authentication Service (CAS) – це сервіс автентифікації сигналів, що надається європейською навігаційною системою Galileo. CAS забезпечує користувачам можливість перевіряти автентичність отриманих навігаційних сигналів, що підвищує захист від спуфінгу та інших видів атак на системи позиціонування.

Основні характеристики CAS. Сигнал E6-C: CAS використовує пілот-компонент сигналу E6 (E6-C), який передається на частоті 1278,75 МГц. Цей компонент може бути зашифрований для забезпечення контрольованого доступу та автентифікації (рис. 2) [40].

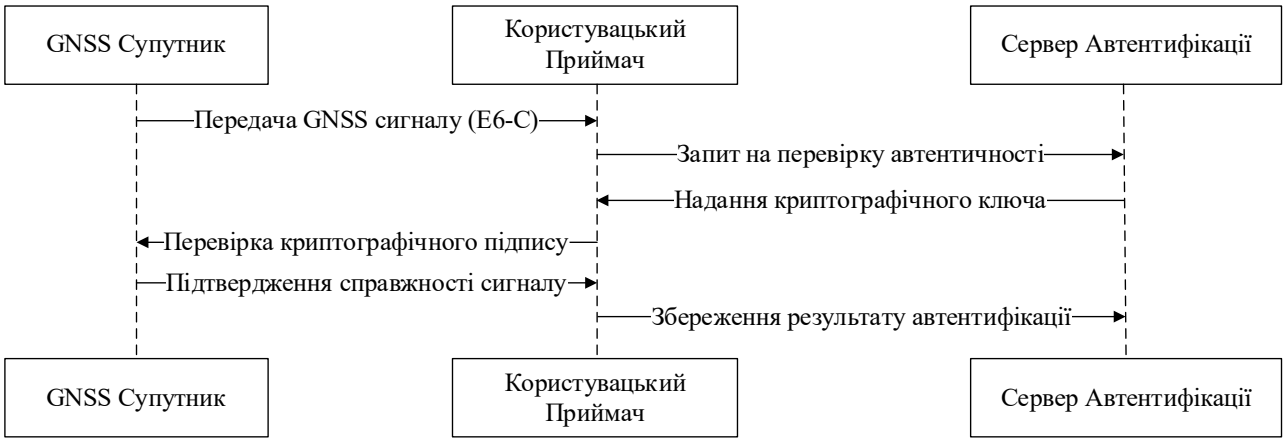

Рис. 2. Автентифікація GNSS на рівні сигналу

2. *Аналіз потужності та його характеристик для виявлення атаки GPS spoofing.*

Принцип аналізу потужності сигналу сигналу та його характеристик для виявлення атаки GPS spoofing наведено на рис. 3.

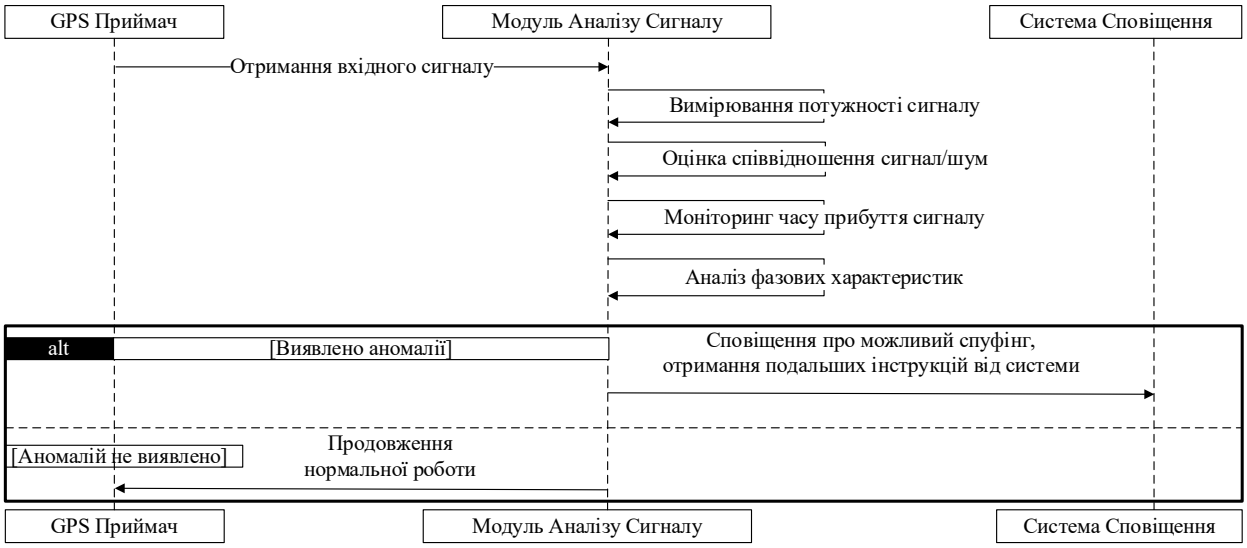

Рис. 3. Аналіз потужності сигналу та його характеристик для виявлення атаки GPS spoofing

Під час спуфінгової атаки дозволяє виявляти такі аномалії. Середня потужність сигналу GPS (L1 C/A) на поверхні Землі ≈ −130 dBm. Спуфінгові сигнали зазвичай мають потужність від −100 dBm зловмисник може передавати сигнали з потужністю, вищою за потужність реальних супутникових сигналів, щоб змусити приймач приймати підроблені дані. Моніторинг вхідної потужності сигналу до −80 dBm, що значно вище від справжнього супутникового сигналу. Допустиме відхилення потужності для автентичного сигналу не більше ±3 dB, що є стандартним допуском у багатьох радіочастотних системах.

Оцінка співвідношення сигнал/шум (SNR – Signal-to-noise ratio). Вимірювання SNR допомагає визначити граничні значення, перевищення яких може вказувати на спуфінгову атаку. Нормальне значення SNR для автентичного GPS-сигналу становить 30 – 50 dB-Hz. Спуфінгові сигнали можуть мати SNR > 55 dB-Hz, що вказує на потенційну атаку. Виявлення аномальних значень > 10 dB вище середнього рівня може свідчити про спуфінг. SNR визначається як відношення потужності сигналу (P_{signal}) до потужності шуму (P_{noise}):

$$SNR = \frac{P_{signal}}{P_{noise}}. \tag{21}$$

Це відношення виражається в децибелах (dB) за допомогою формули

$$SNR_{dB} = 10 \times \log_{10}\left(\frac{P_{signal}}{P_{noise}}\right). \tag{22}$$

(TOA) коливається в межах 10 – 100 нс. При атаці спуфінгом затримки можуть бути від 500 нс до кількох мс, оскільки сигнали передаються зі значно ближчої відстані. Відстеження часу приходу сигналів дозволяє Моніторинг часу прибуття сигналів (Time of Arrival, TOA). Для звичайних супутників затримка сигналу виявляти відхилення, які можуть бути спричинені спуфінгом.

Різницю часу прибуття можна обчислити за формулою [41]:

$$\Delta d = c \times (\Delta t), \tag{23}$$

де c – швидкість світла; Δt – різниця у часі прибуття сигналу в кожну референсну точку.

У двовимірному просторі маємо наступне рівняння:

$$\Delta d = \sqrt{((x^2 - x)^2 + (y^2 - y)^2)} - \sqrt{((x^1 - x)^2 + (y^1 - y)^2)}, \tag{24}$$

де (x_1, y_1) та (x_2, y_2) – відомі координати референсних точок (маяків).

Використовуючи методи нелінійної регресії, це рівняння можна перетворити у форму гіперболи. Після обчислення достатньої кількості таких гіпербол положення цілі можна визначити шляхом знаходження точки їхнього перетину.

Аналіз фазових характеристик. Порівняння фазових характеристик вхідних сигналів допомагає виявити несумісності з реальними супутниковими сигналами. Допустиме відхилення фазової затримки справжніх GNSS-сигналів < 1 рад. Спуфінгові сигнали можуть мати аномальні зміни фазового кута > 3 рад у коротких часових інтервалах.

3. *Інтеграція ІНС з GNSS.* Такий метод є ефективним для підвищення надійності та безпеки навігаційних даних рухомих об'єктів. Ця комбінація дозволяє виявляти та протидіяти атакам типу спуфінгу та глушіння, які можуть спотворювати або блокувати сигнали GNSS. Для поєднання двох систем широко використовується Фільтр Калмана, оскільки від дозволяє вимірювати безперервні вимірювання ІНС (які накопичують похибки з часом) та періодичні, але точні дані від GNSS (які можуть мати перешкоди або спуфінг-атаки). Основна ідея такої інтеграції складається з акселерометрів і гіроскопів, які забезпечують відносне переміщення та орієнтацію рухомого об'єкта. GNSS дає абсолютні координати, які можуть бути хибними через кібератаки. Фільтр Калмана дозволяє компенсувати недоліки обох систем:

ІНС забезпечує безперервність навігації навіть при втраті сигналу GNSS;

GNSS коригує ІНС, зменшуючи накопичення помилок;

ІНС допомагає виявляти атаки на GNSS (якщо дані GNSS не відповідають ІНС, це може бути ознакою спуфінгу).

На рис. 4 наведено приклад інтеграції ІНС та GNSS [42].

4. *Забезпечення захисту ІКС автономної СДК. Захист ІКС автономної СДК є критично важливим для забезпечення надійності та безпеки навігаційних даних*. Моделі та методи захисту ІКС автономної СДК від кібератак мають відповідати вимогам міжнародних стандартів, таких як ISO/IEC 27001, NIST, IEC 62443, та національних НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99 для забезпечення комплексного та системного захисту від хакерських кіберзагроз [43, 44].

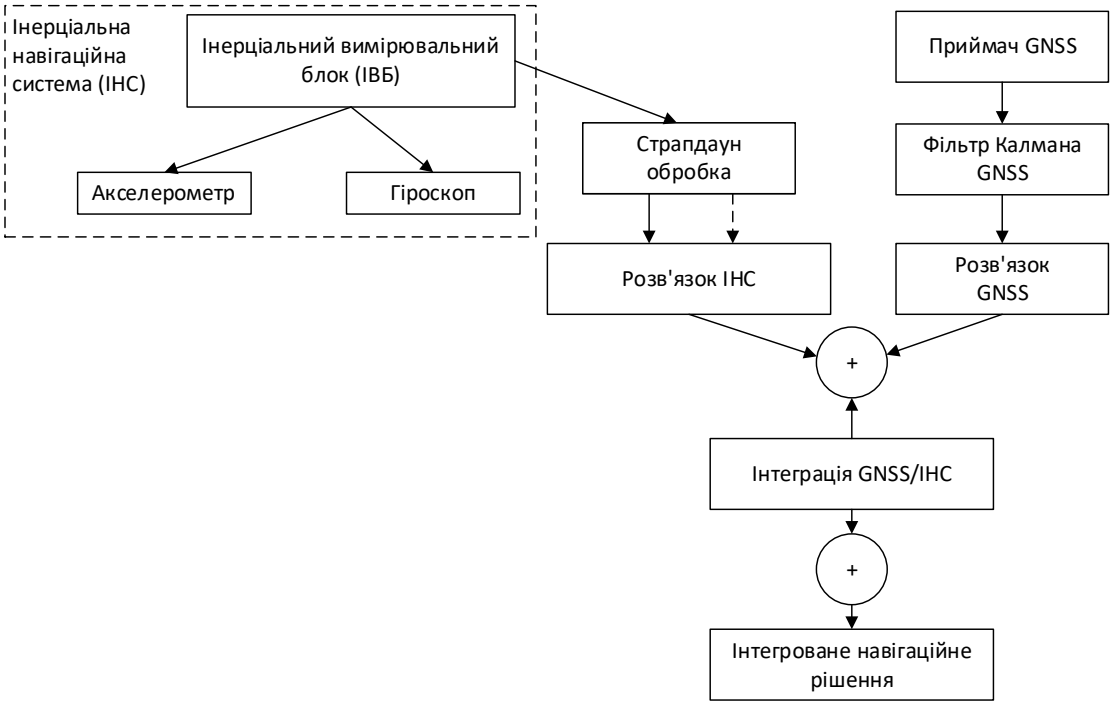

Рис. 4. Приклад інтеграції ІНС та GNSS

4.1. *Захист від DDoS-атак на сервери автономної СДК*. Для захисту веб-сервера автономної СДК від перевантаження шляхом атаки на відмову в обслуговуванні можуть бути розглянуті наступні методи захисту:

Балансування навантаження шляхом розподілу вхідного трафіку між декількома серверами для запобігання перевантаження окремих вузлів. Математично це можна описати як розподіл інтенсивності запитів λ на кількість серверів N:

$$\lambda_{\text{сервер}} = \frac{\lambda}{N}. \tag{25}$$

Фільтрація трафіку за допомогою використання міжмережевих екранів (фаєрволів) для блокування підозрілого трафіку. Ефективність фільтрації визначається коефіцієнтом α, який показує частку заблокованого шкідливого трафіку:

$$\lambda_{\text{ефективна}} = (1 - \alpha)\lambda. \tag{26}$$

Конфігурацію фаєрвола можна представити у вигляді примітивної бінарної матриці доступу A:

$$\begin{bmatrix} A_{1,1}A_{1,2} & \cdots & A_{1,j} \\ A_{2,1}A_{2,2} & \cdots & A_{2,j} \\ \vdots & \ddots & \vdots \\ A_{i,1}A_{i,2} & \cdots & A_{i,j} \end{bmatrix}, \tag{27}$$

де $A_{i,j} = 1$ – означає дозволений трафік між сегментами i та j, а $A_{i,j} = 0$ – заборонений, де $i \in [1, n], j \in [1, m]$; n – кількість сегментів-джерел, m – кількість сегментів-призначень.

Обмеження швидкості запитів (Rate Limiting). Встановлення максимального числа запитів від одного джерела за одиницю часу, щоб запобігти перевантаженню.

4.2. *Захист від атак типу "людина посередині" (MitM).* Для запобігання перехопленню та модифікації даних, що передаються між компонентами автономної СДК, застосовується шифрування даних під час передавання, яке реалізується через функції шифрування E та дешифрування D з використанням ключа K:

$$\mathrm{C} = E_k(M), M = D_k(C). \tag{28}$$

де M – оригінальне повідомлення, C – зашифроване повідомлення.

4.3. *Криптографічний захист інформації шляхом використання протоколів та алгоритмів шифрування для забезпечення конфіденційності та цілісності даних*:

– для цифрових підписів можуть застосовуватися алгоритми RSA, ECDSA і ін.;

– для гешування та перевірки цілісності – SHA-2 (SHA-256, SHA-384, SHA-512).

– управління криптографічними ключами відповідно до стандартів ISO/IEC 11770, 14888, 9796, 27002. Основними вимогами є: генерація ключів з використанням криптографічно стійких генераторів випадкових чисел; зберігання ключів у захищених апаратних модулях (HSM – Hardware Security Module); заміна або оновлення ключів через певні інтервали часу або при підозрі на компрометацію; використання ключів для різних криптографічних систем; реєстрування та аудит діяльності, пов’язаної з управлінням ключами.

– захист каналів зв'язку – наприклад, за допомогою сучасних протоколів шифрування трафіку таких як TLS 1.3, VPN (IPSec, WireGuard, OpenVPN). Забезпечення обов’язкового шифрування між серверами автономної СДК, базами даних та клієнтськими пристроями.

– захист даних у спокої (на дисках, у базах даних, в резервних копіях) доцільно використовувати AES (Advanced Encryption Standard) з ключами не менше 256 біт.

4.4. *Впровадження інфраструктури відкритих ключів (ІВК) для автентифікації та управління цифровими сертифікатами*.

4.5. *Захист від атак на програмне забезпечення автономної СДК* – потрібне для

забезпечення захисту від несанкціонованих дій, таких як впровадження шкідливого коду або отримання несанкціонованого доступу.

Методи захисту:

– регулярне оновлення та патчинг програмного забезпечення;

– використання антивірусних засобів;

– системи виявлення та запобігання вторгнень (IDS/IPS) для моніторингу мережевого трафіку та активності для виявлення підозрілої поведінки в елементах автономної СДК.

4.6. *Захист від атак на фізичну інфраструктуру автономної СДК.* Необхідний для запобігання ризику фізичного доступу до конфіденційних даних. Для запобігання несанкціонованому доступу доречно встановлення систем контролю доступу, відеоспостереження та охорони, а також використання резервних серверів та каналів зв'язку для забезпечення безперервності роботи автономної СДК у разі виходу з ладу основних вузлів.

4.7. *Контроль доступу* – важливий аспект захисту від несанкціонованого доступу до автономної СДК неавторизованих користувачів. Рекомендується впровадження механізмів мультифакторної автентифікації.

4.8. *Розмежування доступу* – використання політик доступу на основі ролей (RBAC – role-based access control). Модель ролей визначає, що кожний користувач U_i має одну або кілька ролей R_k, які визначають доступ до ресурсів P_m: $U_i \in R_k, \quad R_k \in P_m$.

Модель може бути представлена матрицею прав доступу:

$$\begin{bmatrix} P_{1,1}P_{1,2} & \cdots & P_{1,m} \\ P_{2,1}P_{2,2} & \cdots & P_{2,m} \\ \vdots & \ddots & \vdots \\ P_{n,1}P_{n,2} & \cdots & P_{n,m} \end{bmatrix}. \tag{29}$$

де $P_{i,j} = 1$, якщо користувач має доступ, і $P_{i,j} = 0$ – якщо не має доступу.

4.9. *Контроль активності користувачів та адміністраторів*. Обов'язковий елемент ІКС, який включає логування та моніторинг дій користувачів автономної СДК з використанням засобів інтелектуального аналізу поведінкових аномалій.

4.10. *Сегментація мережі* автономної СДК на логічні зони з певними вимогами безпеки та визначення контрольованих каналів зв'язку між ними.

4.11. *Регулярні аудит та тестування всіх елементів безпеки* – сканування ПЗ автономної СДК на наявність вразливостей та тестування на проникнення для проактивного виявлення потенційних кіберзагроз.

На виконання вимог Проєкту Закону України "Про державне регулювання у сфері супутникової навігації" № 10198 від 29.03.2019 [24] щодо застосування національних стандартів, вектор подальших досліджень спрямований на дослідження можливості використання квантового генератора випадкових чисел (QRNG – Quantum Random Number Generation) для управління криптографічними ключами в ІКС автономної СДК, а також застосування постквантових національних стандартів, таких як:

– ДСТУ 7624:2014 – для захисту даних у спокої та для передачі даних. Доцільним є впровадження алгоритму «Калина» з ключами не менше 256 біт;

– ДСТУ 8961:2019 – алгоритм асиметричного шифрування та інкапсуляції ключів «Скеля».

– ДСТУ 9212:2023 – алгоритм електронного підпису «Вершина», заснований на алгебраїчних решітках із відхилами;

– ДСТУ 7564:2014 – алгоритм гешування «Купина».

На рис. 5 представлено прототип загальної схеми архітектури автономної СДК з використанням контрольно коригуючих станцій (ККС), з веб сервісом, який надає користувачам відкориговану GNSS інформацію. На рис. 6 представлено запропонований прототип мережевої архітектури автономної СДК.

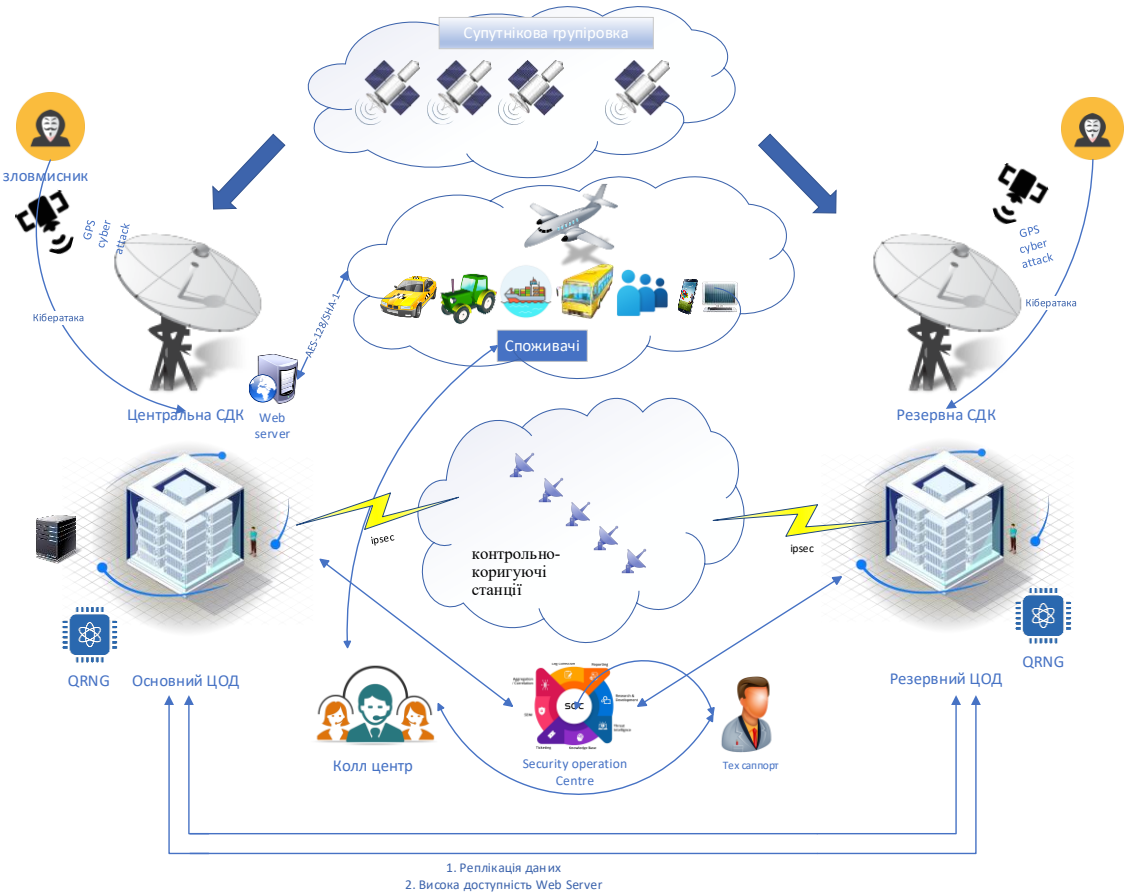

Рис. 5. Прототип архітектури СДК

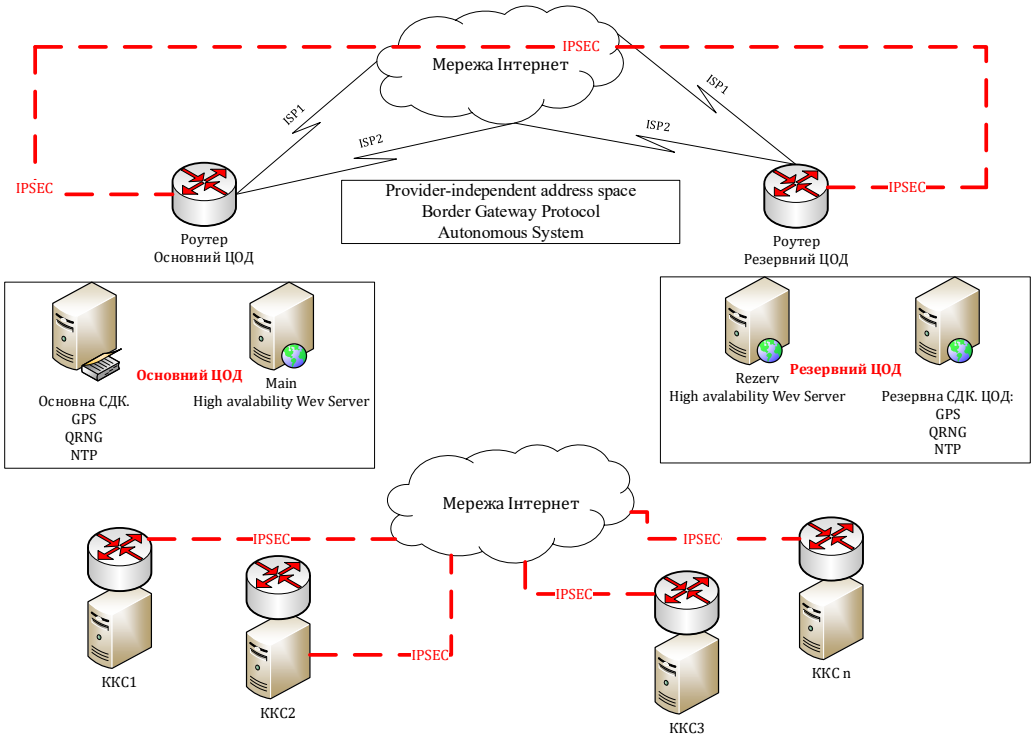

Рис. 6. Прототип мережевої архітектури автономної СДК

Висновки

Зростання використання GNSS супроводжується збільшенням кіберзагроз, які можуть спричиняти фінансові втрати, порушення роботи критичної інфраструктури та створювати небезпеку для життя людей. Атаки на навігаційні системи, такі як спуфінг і глушіння сигналів, а також хакерські атаки на ІКС автономної СДК, є серйозним викликом для транспорту, логістики, військових операцій і комерційних застосувань, що може призводити до значних ризиків використання GNSS.

Забезпечення стабільної, точної та безпечної супутникової навігації вимагає не лише інвестування у системи кібербезпеки GNSS, а ще й постійного дослідження та вивчення нових загроз, а також пошуку ефективних методів їх нейтралізації, зокрема у постквантовий період. Серед ключових механізмів захисту слід виділити: захищені протоколи передачі сигналів, що запобігають перехопленню та підробці даних; механізми автентифікації, які дозволяють ідентифікувати легітимні супутникові сигнали; анти-спуфінгові технології, що виявляють та нейтралізують спроби маніпуляції навігаційними даними; технології захисту ІКС автономних СДК для забезпечення конфіденційності, цілісності та доступності GNSS даних кінцевим користувачам.

Додатково необхідно досліджувати та вивчати можливості застосування автономних СДК, які підвищують точність GNSS і зменшують вплив кібератак, зокрема постквантових. Важливим напрямом є впровадження штучного інтелекту для моніторингу та виявлення загроз та резервних навігаційних технологій для підвищення надійності GNSS у майбутньому.

Отже, ефективний кіберзахист GNSS потребує не лише фінансування, а й активного дослідження, вивчення загроз та розробки інноваційних методів протидії. Комплексний підхід та міжнародна співпраця є ключовими факторами для забезпечення надійної роботи супутникових навігаційних систем у критично важливих сферах.

Проведені дослідження та запропоновані заходи безпеки можуть бути використані як основа для реалізації національної системи координатно-часового та навігаційного забезпечення України. Впровадження відповідного законодавчого регулювання та стандартів дозволить забезпечити кіберстійкість навігаційних систем та інтегрувати їх у європейську супутникову інфраструктуру.

Список літератури:

1. F. T. McClure and R. B. Kershner. The Legacy of Transit: A Dedication // JOHNS HOPKINS APL TECHNICAL DIGEST, vol. 19, no. 1, 1998. URL: https://secwww.jhuapl.edu/techdigest/content/techdigest/pdf/V19-N01/19-01-Pisacane.pdf
2. Department of Defense. Department of Transportation and Department of Homeland Security, 2021 Federal Radionavigation Plan. URL:https://www.navcen.uscg.gov/sites/default/files/pdf/2021_ Federal_Rdionavigation_Plan.pdf
3. V. Vdovin. National Reference Systems of the Russian Federation, used in GLONASS including the user and fundamental segments, 2013. URL: https://www.unoosa.org/pdf/icg/2013/icg-8/wgD/D3_3_2.pdf
4. Redactie De Ingenieur. After 13 years, Galileo satellite navigation complete at last, 2018. URL:https://deingenieur.nl/artikelen/after-13-years-galileo-satellite-navigation-complete-at-last
5. J.A. Ávila Rodríguez. University FAF Munich, Germany. BeiDou Signal Plan – Navipedia. URL: https://gssc.esa.int/navipedia/index.php/BeiDou_Signal_Plan.
6. K.S. Parikh, Deputy Director. IRNSS / GAGAN and its Potential Applications. URL: https://geospatialworld.net/gsi/2016/presentations/benifits-of-IRNSS-GAGAN-satellite-navigation-systems-and-its-potential-applications.pdf.
7. N. S. P. S. C. O. Kenji NUMATA Government of Japan // QZSS System and service Updates. Quasi-Zenith Satellite System, Japanese Regional Navigation Satellite System. URL: https://www.unoosa.org/documents/pdf/icg/2023/ICG-17/icg17.01.06.pdf
8. Greg Thompson. Wide Area Augmentation System (WAAS) – Program Overview. URL: https://www.faa.gov/sites/faa.gov/files/about/office_org/headquarters_offices/ato/WAAS_Program_Status_Update_Jun_2021.pdf
9. 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

10. J. Siu. Global Navigation Satellite System Overview and Support for PBN Implementation. URL: https://www.icao.int/nacc/documents/meetings/2012/pbngnss2012workshop/pbngnss2-1.pdf

11. Galileo HAS: точність в режимі реального часу – SystemNET – ‘Систем Солюшнс’. URL: https://systemnet.com.ua/galileo-has-tochnist-v-rezhymi-realnoho-chasu/

12. Про критичну інфраструктуру // Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/go/1882-20

13. 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.

14. 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.

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

16. Litvinov N. GPS та його значення у сучасних військових конфліктах // Universe Space Tech. 2022. URL: https://universemagazine.com/borotba-za-koordynaty-globalni-navigaczijni-systemy-ta-yih-znachennya-u-suchasnyh-vijskovyh-konfliktah/

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

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

19. Kauranen A. Finland detects satellite navigation jamming and spoofing in Baltic Sea, Reuters, 31, 2024. URL: https://www.reuters.com/world/europe/finland-detects-satellite-navigation-jamming-spoofing-baltic-sea-2024-10-31/

20. Розпорядження Кабінету Міністрів України; Концепція від 03.01.2013 № 1-р. Про схвалення Концепції проєкту Закону України “Про державне регулювання у сфері супутникової навігації”// Офіційний вебпортал парламенту України. Розпорядження Кабінету Міністрів України; Концепція від 03.01.2013 № 1-р. URL: https://zakon.rada.gov.ua/laws/show/1-2013-%D1%80#Text.

21. Розпорядження Кабінету Міністрів України; Концепція від 30.03.2011 № 238-р. Про схвалення Концепції реалізації державної політики у сфері космічної діяльності на період до 2032 р. // Офіційний вебпортал парламенту України. Розпорядження Кабінету Міністрів України; Концепція від 30.03.2011 № 238-р. URL: https://zakon.rada.gov.ua/laws/show/238-2011-%D1%80#Text.

22. European Commission. Copernicus: new name for European Earth Observation Programme. URL: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_12_1345/IP_12_1345_EN.pdf

23. MS4_GEO Strategic Plan 2016-2025 Implementing GEOSS_approved_by_GEO-XII.pdf. URL: https://old.earthobservations.org/documents/ministerial/mexico_city/MS4_GEO%20Strategic%20Plan%202016-2025%20Implementing%20GEOSS_approved_by_GEO-XII.pdf

24. Офіційний портал Верховної Ради України. Проєкт Закону України “Про державне регулювання у сфері супутникової навігації” № 10198 від 29.03.2019.
URL: https://ips.ligazakon.net/document/view/gh7va00a?an=15&ed=2019_03_29

25. Закон України від 05.07.1994 № 80/94-ВР. Про захист інформації в інформаційно-комунікаційних системах // Офіційний вебпортал парламенту України. Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80

26. Офіційний вебпортал парламенту України. Постанова Кабінету Міністрів України ; Перелік від 07.04.2003 № 486. Про утворення державної мережі моніторингу глобальних навігаційних супутникових систем. URL: https://zakon.rada.gov.ua/go/486-2003-%D0%BF#Text"

27. Офіційний вебпортал парламенту України. Закон України від 16.12.2020 № 1089-IX. Про електронні комунікації. URL: https://zakon.rada.gov.ua/go/1089-20#Text.

28. Проєкт Закону України від 30.09.2021 № 6129. Про затвердження Загальнодержавної цільової науково-технічної космічної програми на 2021–2025 роки. № 6129 від 04.10.2021. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/27922

29. Mustafaiev O. V. Modern technologies of protection against gps spoofing in navigation systems // Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences. 2024. Vol. 1, 5. P. 58–61. DOI: 10.32782/2663-5941/2024.5.1/10.

30. Вадіс Д., Аврутов В. Методи підвищення функціональної ефективності БПЛА // Механіка гіроскопічних систем. 2024. Вип. 48. DOI: 10.20535/0203-3771482024317891.

31. Narytnik T., Prysiazhnyi V., Kapshtyk S., Denysenko M., Narushkevych O. Improvement of the gps signal receiving resistance against electromagnetic interference, jamming, and spoofing is based on the use of the antenna array system with digital beamforming and NORAD TLE information. 2022.
URL: https://ela.kpi.ua/handle/123456789/54188

32. Spanghero M., Papadimitratos P. Time-based GNSS attack detection // IEEE Transactions on Aerospace and Electronic Systems. 2024. P. 1–18. DOI:10.1109/TAES.2024.3516708.

33. Motallebighomi M., Sathaye H., Singh M. et al. Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals. arXiv, 2022. DOI:10.48550/arXiv.2204.11641.
34. Солдатов В. В., Нарєжній О. П., Гріненко Т. О. Модифікація ntp сервера часу системи диференціальної корекції відповідно до схеми ANSI X9.95. Український метрологічний журнал // Ukrainian Metrological Journal. № 3А. С. 98–102. DOI:10.24027/2306-7039.3a.2020.218165.
35. Psiaki M. L., Humphreys T. E. GNSS Spoofing and Detection // Proceedings of the IEEE. Vol. 104, № 6. P. 1258–1270. DOI:10.1109/JPROC.2016.2526658.
36. Ghizzo E., Djelloul E.-M., Lesouple J. та ін. Assessing jamming and spoofing impacts on GNSS receivers: Automatic gain control (AGC) // Signal Processing. Vol. 228, 03.2025. P. 109762. DOI:10.1016/j.sigpro.2024.109762.
37. Johnson Singh K., De T. and. Mathematical modelling of DDoS attack and detection using correlation // Journal of Cyber Security Technology. Vol. 1, Issue 3–4. P. 175–186. DOI:10.1080/23742917.2017.1384213.
38. Seddighighachkanloo, Morteza. RBDs and Analytical System Reliability Series Systems. ResearchGate. URL: ttps://www.researchgate.net/publication/278678509_RBDs_and_Analytical_System_Reliability_Series_Systems
39. Barlow R. Heidtmann Klaus. Computing k-out-of-n System Reliability. ResearchGate. DOI:10.1109/TR.1984.5221843.
40. European Union. Galileo E6-B/C Codes Technical Note // European Union. 2019. Vol. 1. URL: https://www.gsc-europa.eu/sites/default/files/sites/all/files/E6BC_SIS_Technical_Note.pdf
41. O'Keefe B. Finding Location with Time of Arrival and Time Difference of Arrival Techniques. URL: https://sites.tufts.edu/eeseniordesignhandbook/files/2017/05/FireBrick_OKeefe_F1.pdf
42. Li S., Mikhaylov M., Mikhaylov N. et al. Deep Learning Based Kalman Filter for GNSS/INS Integration: Neural Network Architecture and Feature Selection // 2023 International Conference on Localization and GNSS (ICL-GNSS). 2023. P. 1–7. DOI: 10.1109/ICL-GNSS57829.2023.10148914.
43. Департамент спеціальних телекомунікаційних систем та захисту, інформації Служби безпеки України. 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
44. ISO/IEC 27001:2022. ISO: Global standards for trusted goods and services. URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf

Надійшла до редколегії 23.01.2025

Відомості про авторів:
Снєосіков Олег Анатолійович – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій, Україна; e-mail: oleh.snieosikov@student.karazin.ua, ORCID: https://orcid.org/0009-0001-9468-5965
Нарєжній Олексій Павлович – канд. техн. наук, Харківський національний університет імені В. Н. Каразіна, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій, Україна; e-mail: o.nariezhnii@karazin.ua, ORCID: https://orcid.org/0000-0003-4321-0510
Гріненко Тетяна Олексіївна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Україна, e-mail: tetiana.grinenko@nure.ua, ORCID: https://orcid.org/0000-0002-8251-8991