УДК 004 DOI https://doi.org/10.35546/kntu2078-4481.2025.4.3.27

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

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

МОДЕЛЬ ПОСТКВАНТОВОЇ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ З ВИКОРИСТАННЯМ КВАНТОВОГО ГЕНЕРАТОРА ВИПАДКОВИХ ЧИСЕЛ ДЛЯ АВТОНОМНОЇ СИСТЕМИ ДИФЕРЕНЦІАЛЬНОЇ КОРЕКЦІЇ ГЛОБАЛЬНИХ НАВІГАЦІЙНИХ СУПУТНИКОВИХ СИСТЕМ

У статті запропоновано формалізовану модель постквантової інфраструктури відкритих ключів (ІВК) для інформаційно-комунікаційної системи (ІКС) автономної системи диференціальної корекції (АСДК), побудовану на основі використання квантового генератора випадкових чисел (QRNG) та національних криптографічних стандартів ДСТУ 7564:2014 («Купина»), ДСТУ 7624:2014 («Калина»), ДСТУ 8961:2019 («Скеля») і ДСТУ 9212:2023 («Вершина»). Актуальність дослідження зумовлена необхідністю підвищення криптостійкості каналів передавання даних між контрольно-коригуючими станціями (ККС) та центром оброблення даних АСДК, а також підвищенням вимог до автентичності та цілісності корекційних даних, що надаються через веб-сервіс зацікавленим користувачам АСДК, зокрема в умовах постквантових загроз. Запропонована модель ІВК забезпечує автентифікацію ККС та користувачів, захист тунельних каналів, цілісність корекційних даних та довіру до серверних компонентів АСДК шляхом інтеграції квантової ентропії у процеси генерації ключів і підпису. У роботі обґрунтовано роль QRNG як джерела високоякісної ентропії для побудови довготривалих ключових пар за алгоритмами ДСТУ «Скеля», «Вершина» та сеансових ключів симетричного шифрування за алгоритмом ДСТУ «Калина», а також розроблено узагальнену структуру ІВК з одним Root CA та декількома Issuing CA для основного й резервного центрів оброблення даних. Запропонована модель визначає логічну взаємодію компонентів ІВК, механізмів тунелювання, модулів підпису та перевірки сертифікатів, а також демонструє можливість забезпечення постквантової стійкості АСДК без зміни її архітектури. Показано, що використання QRNG у поєднанні з національними криптоалгоритмами дає змогу мінімізувати ризик компрометації ключів, підвищити стійкість до квантових атак та забезпечити довготривалу криптографічну надійність каналів зв'язку і веб-сервісу АСДК. Запропонована методика дозволяє створювати ІВК для інформаційно-комунікаційних систем диференціальної корекції та інших сегментів критичної інфраструктури з підвищеними вимогами до довіри, цілісності та конфіденційності даних, з урахуванням вимог сучасних стандартів кібербезпеки (ISO/IEC 27001, NIST, НД ТЗІ).

Ключові слова: *глобальна навігаційна супутникова система (GNSS); квантовий генератор випадкових чисел (QRNG); кібератака; кібербезпека; система диференціальної корекції (Differential GNSS, DGNSS); інфраструктура відкритих ключів (ІВК); автономна система диференціальної корекції (АСДК, Autonomous DGNSS); постквантова криптографія (PQC).*

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

MODEL OF A POST-QUANTUM PUBLIC KEY INFRASTRUCTURE USING A QUANTUM RANDOM NUMBER GENERATOR FOR AN AUTONOMOUS DIFFERENTIAL CORRECTION SYSTEM OF GLOBAL NAVIGATION SATELLITE SYSTEMS

In the article, a formalized model of a post-quantum public key infrastructure (PKI) for the information-and-communication system (ICS) of the Autonomous Differential GNSS System (Autonomous DGNSS) is proposed, constructed on the basis of the use of a quantum random number generator (QRNG) and the national cryptographic standards DSTU 7564:2014 ("Kupyna"), DSTU 7624:2014 ("Kalyna"), DSTU 8961:2019 ("Skelia"), and DSTU 9212:2023 ("Vershyna"). The relevance of the research is conditioned by the need to increase the cryptographic robustness of data-transmission channels between the control-and-correction stations (CCS) and the data-processing center of the Autonomous DGNSS, as well as by the increased requirements for the authenticity and integrity of correction data provided through the web service to interested users of the Autonomous DGNSS, particularly under post-quantum threats. The proposed PKI model ensures authentication of CCS and users, protection of tunnel channels, integrity of correction data, and trust in the server components of the Autonomous DGNSS by integrating quantum entropy into the processes of key generation and signing. The study substantiates the role of the QRNG as a source of high-quality entropy for constructing long-term key pairs according to the DSTU "Skelia" and "Vershyna" algorithms, as well as session keys of symmetric encryption under the DSTU "Kalyna" algorithm, and also develops a generalized PKI structure with a single Root CA and several Issuing CAs for the primary and backup data-processing centers. The proposed model defines the logical interaction of PKI components, tunneling mechanisms, signature and certificate-verification modules, and demonstrates the possibility of ensuring post-quantum resistance of the Autonomous DGNSS without changing its architecture. It is shown that the use of a QRNG in combination with national cryptographic algorithms makes it possible to minimize the risk of key compromise, increase resistance to quantum attacks, and ensure long-term cryptographic reliability of communication channels and the web service of the Autonomous DGNSS. The proposed methodology allows creating PKI for information-and-communication systems of differential correction and other segments of critical infrastructure with increased requirements for trust, integrity, and confidentiality of data, taking into account the requirements of modern cybersecurity standards (ISO/IEC 27001, NIST, ND TZI).

Key words: *global navigation satellite system (GNSS); quantum random number generator (QRNG); cyberattack; cybersecurity; differential GNSS (DGNSS); public key infrastructure (PKI); Autonomous DGNSS; post-quantum cryptography (PQC).*

Постановка проблеми

Глобальні навігаційні супутникові системи (GNSS) є фундаментальним елементом критичної інфраструктури сучасної держави, забезпечуючи точне позиціювання та високоточну синхронізацію часу у сферах авіації, транспорту, геодезії, енергетики, телекомунікацій, фінансових операцій та інших видів діяльності [1, 2]. Водночас достовірність і захищеність сигналів GNSS обмежена низкою факторів, зокрема впливом кібератак на супутникові сигнали. Для підвищення точності координат і часу в реальному часі застосовуються системи диференціальної корекції (DGNSS), які обчислюють поправки на основі даних, отриманих від контрольно-коригуючих станцій (ККС) та передають їх користувачам через IP-мережі. Системи диференціальної корекції, зокрема автономні системи (АСДК), є програмно-апаратними комплексами [1, 3] та відповідно до Закону України «Про критичну інфраструктуру» № 1882-IX належать до об'єктів критичної інфраструктури у сфері космічних технологій [4].

Через стрімке зростання кіберзагроз за останні роки, спрямованих на системи GNSS [5, 6], а також на пов'язані з ними ІКС оброблення даних [7, 8, 9], стає необхідним переосмислення підходів до захисту ІКС АСДК на криптографічному рівні. До найнебезпечніших загроз належать GPS jamming, GPS spoofing, атаки на програмне забезпечення ККС і серверів оброблення даних, DDoS-атаки, MITM-атаки, компрометація ключів, ін'єкції коду, несанкціоноване втручання у корекційні дані, а також фізичні атаки та інсайдерські порушення. Особливо критичною є можливість віддаленої компрометації каналів передавання даних між ККС та АСДК, підміна або модифікація корекційних даних, а також отримання зловмисниками доступу до криптографічних матеріалів і сертифікатів. Сукупність таких атак може призвести до спотворення координат, втрати часової синхронізації, маніпулювання навігаційними даними або повного порушення роботи GNSS, що становить загрозу для об'єктів критичної інфраструктури та може мати критичні наслідки на державному рівні [10].

Ситуація додатково ускладнюється потенціальними кіберзагрозами у постквантовий період [11]. Із розвитком квантових обчислень класичні криптографічні алгоритми, що використовуються для автентифікації, підпису та встановлення захищених з'єднань, можуть втратити стійкість. Це безпосередньо стосується систем АСДК, у яких критично важливі функції: ідентифікація ККС, захист даних, які передаються, підпис корекцій, захист веб-сервісів та захист даних у стані спокою – повністю залежать від надійності інфраструктури відкритих ключів (ІВК). Таким чином, виникає необхідність побудови постквантової ІВК, стійкої до квантових атак, з використанням квантових джерел ентропії (QRNG) та національних криптоалгоритмів (ДСТУ 7564/7624/8961/9212), яка забезпечуватиме довготривалий захист, автентичність джерел корекцій та унеможливлюватиме компрометацію ключів у майбутньому криптографічному середовищі ІКС АСДК.

У зв'язку з викладеним постає науково-прикладна задача: розробити формалізовану модель постквантової ІВК з використанням QRNG для автономної системи диференціальної корекції, яка забезпечуватиме автентифікацію, цілісність даних, захист тунельних каналів та довіру до серверних компонентів без зміни базової архітектури АСДК.

Аналіз останніх досліджень і публікацій

Проблематиці кіберзахисту інформаційно-комунікаційних систем (ІКС) критичної інфраструктури в постквантовий період присвячені численні наукові праці як закордонних, так і вітчизняних вчених. Ключовим викликом сьогодення є загроза, яку становить квантовий комп'ютер для класичних алгоритмів асиметричного шифрування (RSA, ECC), що обґрунтовує проактивний перехід на постквантові криптографічні алгоритми [12]. За результатами наведених досліджень, перехід до квантово-стійких рішень стає пріоритетним завданням для держав та організацій ще до настання ери fault-tolerant квантових обчислень. Зокрема, науковці наголошують, що вже зараз критична інфраструктура є об'єктом кібератак, а поява квантових обчислювачів тільки посилює ці ризики.

Стає очевидним, що постквантова криптографія має стати невід'ємною частиною кіберзахисту ІКС у найближче десятиріччя [13]. А дослідження, згідно з [14] повідомляють, що на сьогоднішній день вже затверджено перші міжнародні стандарти (наприклад такі, як CRYSTALS-Kyber, Dilithium) для широкого впровадження.

Одним із перспективних шляхів підвищення криптостійкості ІКС є використання квантових генераторів випадкових чисел (QRNG) в ІВК. На відміну від псевдовипадкових генераторів випадкових чисел (PRNG), апаратні QRNG генерують істинні випадкові бітові послідовності на основі квантових явищ, що унеможливлює їх передбачення навіть за наявності суперобчислювальних систем. Як зазначається в [15], впровадження QRNG здатне покращити будь-яку криптосистему, адже якість ключів прямо визначає криптостійкість. Українські науковці також акцентують на тому, що веб-сервіси QRNG відкривають нові можливості підвищення надійності ІВК, забезпечуючи високий рівень непередбачуваності ключових даних [16].

З огляду на криптозахист систем диференціальної корекції GNSS, такі системи традиційно мають відкритий формат передачі даних, що робить їх потенційною ціллю для кібератак типу GPS spoofing. Для вирішення цієї проблеми пропонуються криптографічні механізми автентифікації навігаційних повідомлень. Зокрема, у сигнал можна вбудовувати спеціальні маркери (цифрові підписи, Message Authentication Codes тощо), за якими приймач перевірятиме, чи походить повідомлення від легітимного супутника і чи не було воно спотворене. Загальний висновок – додавання криптографічної автентифікації є дієвим засобом протидії кібератакам типу GPS spoofing без суттєвого погіршення якості сервісу [17]. Дослідження [11, 18] підтверджують, що постквантовий захист для DGNSS доцільно будувати на симетричних схемах (TESLA, HMAC) та геш-ланцюжках, оскільки класичні підписи на еліптичних кривих будуть зламані квантовими алгоритмами, а постквантові криптографічні схеми підпису занадто об'ємні для форматів GNSS-повідомлень. Автори показують, що найперспективнішим перехідним рішенням є протокол TESLA з квантово-стійкими геш-ланцюжками або Merkle-структурами, що забезпечує автентифікацію DGNSS-поправок без збільшення ширини каналу.

Українські симетричні стандарти «Калина» (ДСТУ 7624:2014) та «Купина» (ДСТУ 7564:2014) мають високу надійність у постквантовій ері, оскільки, згідно з теоретичними оцінками, квантовий пошук Гровера знижує їхню ефективну стійкість лише вдвічі, що компенсується використанням 256-бітних ключів і 512-бітних геш-образів [13]. Асиметричні алгоритми нового покоління – «Скеля» (ДСТУ 8961:2019, KEM на основі модульних алгебраїчних решіток) та «Вершина» (проєкт постквантового підпису, побудований на тих самих класах решіток) – демонструють рівні безпеки, співставні з CRYSTALS-Kyber та CRYSTALS-Dilithium, що підтверджено сучасними криптоаналітичними дослідженнями [14, 19, 20]. Окремі роботи також показали можливість інтеграції національних алгоритмів у міжнародні схеми постквантової криптографії, зокрема використання геш-функції Купина у модифікації SPHINCS+ [21]. У підсумку, комплекс українських алгоритмів (Калина, Купина, Скеля, Вершина) вже сьогодні може бути використаний як основа для постквантових ІКС, включно з ІКС критичної інфраструктури, зокрема Autonomous DGNSS.

Аналіз останніх досліджень і публікацій показує, що розвиток постквантової криптографії тісно пов'язаний із завданнями забезпечення кібербезпеки критичних ІКС. Проте, в контексті захисту систем диференціальної корекції GNSS (зокрема, АСДК) питання побудови стійких до квантових атак ІКС залишається недостатньо дослідженим. Таким чином, розробка постквантової ІВК з використанням квантових генераторів випадкових чисел (QRNG) та національних криптоалгоритмів для АСДК є надзвичайно актуальною.

Формулювання мети дослідження

Метою цієї роботи є теоретичне обґрунтування та розроблення формалізованої моделі постквантової інфраструктури відкритих ключів для автономної системи диференціальної корекції GNSS з використанням квантового генератора випадкових чисел, а також формулювання рекомендацій щодо її архітектури та застосування на основі аналізу сучасних наукових публікацій з урахуванням вимог стандартів ISO/IEC 27001, NIST SP 800-53/800-57, IEC 62443 та НД ТЗІ.

Викладення основного матеріалу дослідження

На рис. 1 наведено прототип архітектури інформаційно-комунікаційної системи автономної системи диференціальної корекції (ІКС АСДК). До складу ІКС АСДК входять три основні підсистеми: сегмент контрольно-коригуючих станцій (ККС), центри оброблення даних АСДК та сегмент користувачів.

– ККС, розташовані по території країни, які приймають сигнали GNSS, формують сирі навігаційні вимірювання та передають їх у ЦОД АСДК через захищені VPN-тунелі на основі IPsec. Основний та резервний ЦОД забезпечують агрегацію, оброблення й зберігання даних, розрахунок диференціальних поправок, а також формування коригуючих повідомлень для кінцевих користувачів.

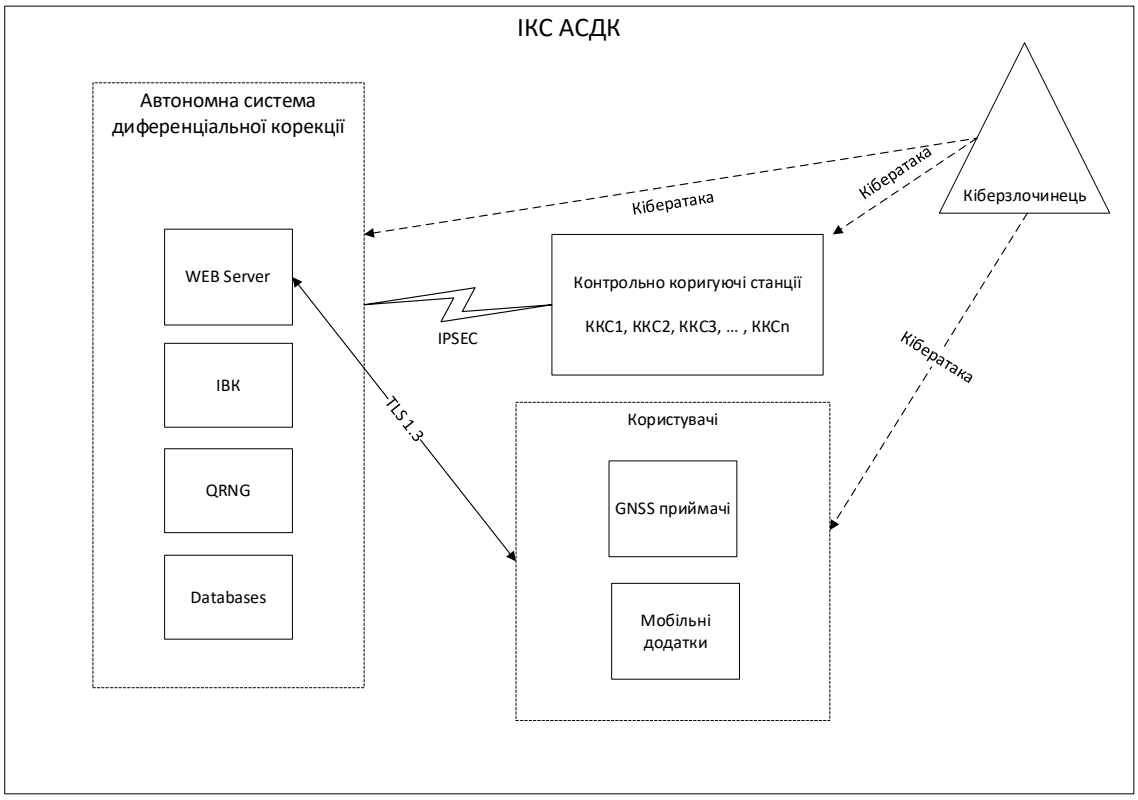

Рис 1. Прототип архітектури ІКС автономної системи диференціальної корекції GNSS

– До внутрішньої архітектури АСДК належать веб-сервер високої доступності, інфраструктура відкритих ключів (ІВК), квантовий генератор випадкових чисел (QRNG) та підсистема баз даних. Веб-сервер надає користувачам коригуючу інформацію через захищені канали TLS 1.3, використовуючи сертифікати, видані ІВК. QRNG інтегровано з компонентами ІВК та криптомодулями ЦОД для формування високоякісної ентропії під час генерації довготривалих і сеансових ключів.

– Сегмент користувачів включає GNSS-приймачі та мобільні додатки, які отримують диференціальні поправки через веб-сервіс АСДК. На рис. 1 пунктирними лініями також схематично показано можливі вектори кібератак на ККС, ЦОД, веб-сервер і кінцевих користувачів з боку зовнішнього порушника, що визначає ІКС АСДК як об’єкт побудови постквантової ІВК.

З урахуванням архітектури, наведеної на рис. 1, ІКС АСДК розглядається як розподілена система, у якій взаємодіють контрольно-коригуючі станції, центри оброблення даних, веб-сервер та кінцеві користувачі. Для кожного з цих сегментів характерні специфічні кіберзагрози, пов’язані як із впливом на сигнали GNSS (GPS jamming, GPS spoofing), так і з атаками на мережеву інфраструктуру та програмне забезпечення ІКС. Окрему небезпеку становить компрометація криптографічних ключів і сертифікатів, що використовується для захисту тунельних каналів між ККС та ЦОД, а також для автентифікації веб-сервісу АСДК та підпису корекційних даних.

У контексті постквантових загроз інфраструктура відкритих ключів АСДК повинна забезпечувати не лише поточну стійкість до класичних атак, а й довготривалий захист ключових матеріалів у разі появи повнофункціональних квантових обчислювачів. Це потребує переходу від класичних алгоритмів асиметричної криптографії (RSA, ECC) до постквантових схем на основі алгебраїчних решіток (ДСТУ «Скеля», «Вершина») та використання квантових генераторів випадкових чисел (QRNG) як джерела високоякісної ентропії для генерації довготривалих

і сеансових ключів. Додатково ІВК має підтримувати симетричні алгоритми «Калина» та геш-функцію «Купина», які вважаються криптостійкими в постквантовій ері завдяки достатній довжині ключів і геш-образів.

На основі аналізу загроз і стандартів кібербезпеки (ISO/IEC 27001, NIST SP 800-53/800-57, IEC 62443, НД ТЗІ) до постквантової ІВК ІКС АСДК формулюються такі ключові вимоги:

– автентифікація суб'єктів ІКС: надійна ідентифікація ККС, серверів ЦОД, веб-сервера та користувачів на основі сертифікатів, виданих постквантовою ІВК АСДК;

– захист каналів зв'язку: встановлення криптографічно стійких тунельних каналів між ККС та ЦОД (IPsec/VPN) та захищених з'єднань між веб-сервером і клієнтами (TLS 1.3) з використанням постквантових механізмів узгодження ключів;

– забезпечення цілісності корекційних даних: використання постквантових алгоритмів підпису для коригуючих повідомлень, що розповсюджуються до GNSS-приймачів та мобільних додатків;

– довготривала криптографічна надійність: застосування QRNG для генерації ключових матеріалів ІВК, суворе розмежування прав доступу до закритих ключів, використання захищених апаратних модулів зберігання (HSM) та регламентованих криптоперіодів;

– підтримка процедур управління життєвим циклом сертифікатів: реєстрація, видача, оновлення, відкликання та публікація статусу сертифікатів (CRL/OCSP) з урахуванням вимог до безперервності надання сервісів АСДК.

Спираючись на класичні підходи до побудови інфраструктур відкритих ключів [22], а також на результати досліджень комбінованих ІВК [23, 24], запропоновано формалізовану модель постквантової інфраструктури відкритих ключів для інформаційно-комунікаційної системи автономної системи диференціальної корекції GNSS (Наведено на Рис. 2).

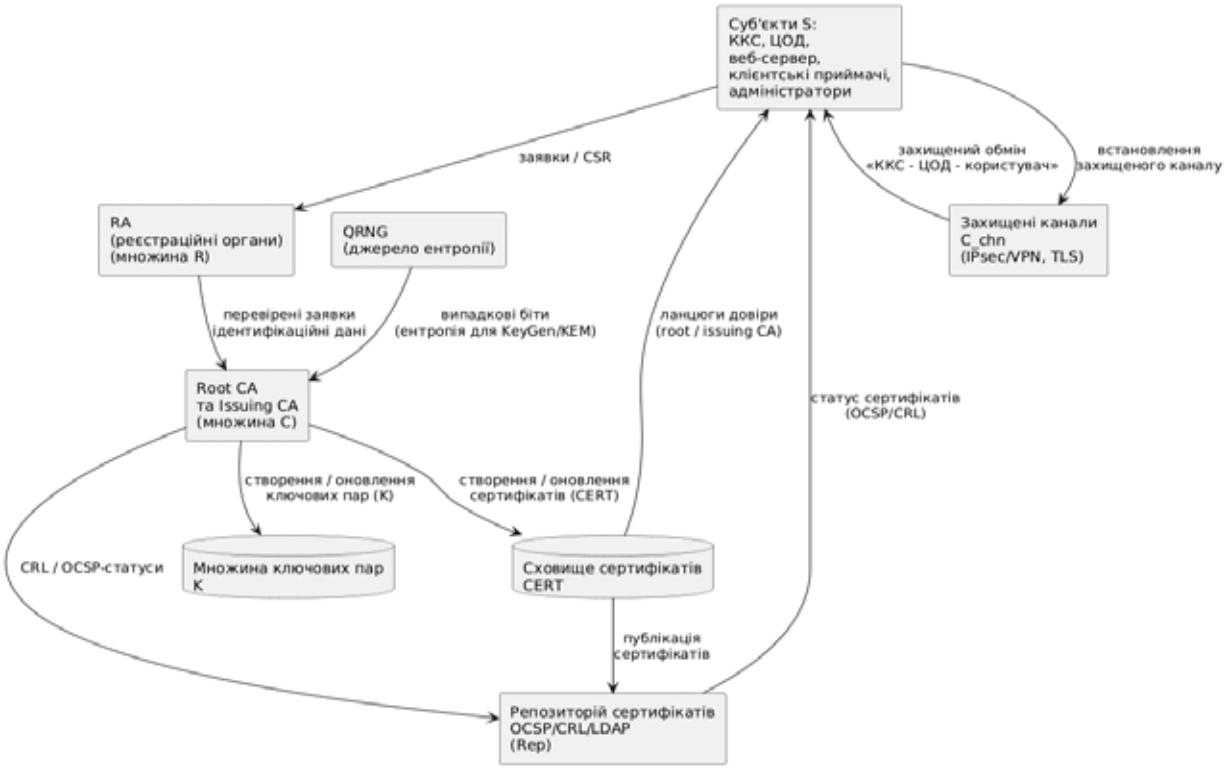

Рис. 2. Формалізована модель постквантової ІВК АСДК – $PKI_{PQ\text{-}ASDK}$

Формально постквантову ІВК для ІКС АСДК можна подати у вигляді кортежу:

$$\left(PKI_{PQ-ASDK} = S, C, R, R_{ep}, A, K, CERT, C_{chn}, QRNG\right) \tag{1}$$

де S – множина суб'єктів (контрольно-коригуючі станції, серверні компоненти основного та резервного ЦОД, веб-сервер, клієнтські приймачі та адміністратори/оператори),

C – множина засвідчувальних центрів (Root CA та Issuing CA),

R – реєстраційні органи (усі операції реєстрації нових контрольно-коригуючих станцій, серверних компонентів та клієнтських приймачів в ІВК виконуються уповноваженими операторами через реєстраційні органи,

що відповідає вимогам до інформаційно-комунікаційних систем об'єктів критичної інфраструктури (Наведено в Рис. 3)),

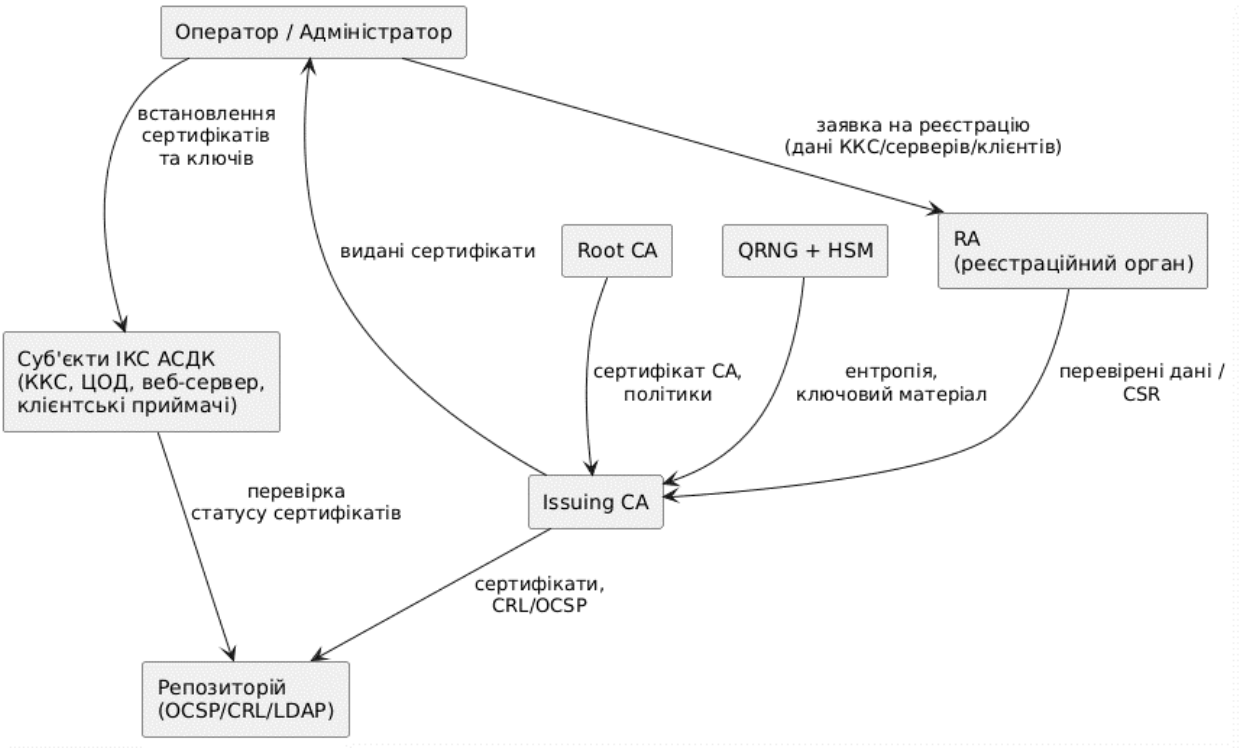

Рис. 3. Процес реєстрації нових ККС/серверів/користувачів АСДК в $PKI_{PQ-ASDK}$

Rep – репозитарії сертифікатів та їх статусів (LDAP/OCSP/CRL),
A – множина національних постквантових криптоалгоритмів («Купина», «Калина», «Скеля», «Вершина»),
K – множина ключових пар,
$CERT$ – множина сертифікатів,
Cchn – множина захищених каналів «ККС – ЦОД – користувач»,
$QRNG$ – квантовий генератор випадкових чисел.

На відміну від класичних ІВК [22-24], у запропонованій моделі квантовий генератор випадкових чисел розглядається як базовий криптографічний ресурс. Його роботу можна описати відображенням:

$$(r = QRNG(n) \in \{0,1\}^n) \tag{2}$$

де n – довжина необхідної бітової послідовності, а r використовується як джерело ентропії для генерації довготривалих та сеансових ключів. Довготривалі ключові пари формуються за постквантовими алгоритмами «Скеля» (KEM) та «Вершина» (цифровий підпис), тоді як сеансові ключі симетричного шифрування обчислюються за схемою:

$$\left(k_{sess} = KDF\left(QRNG\left(n_{sess}\right) \| context\right)\right) \tag{3}$$

де $context$ включає ідентифікатори сторін, параметри тунелю та службові дані протоколів TLS/IPsec.

Співвідношення (1)-(3) є авторським узагальненням відомих моделей класичних та комбінованих інфраструктур відкритих ключів, наведених у працях [22-24], адаптованим до умов постквантових загроз, специфіки автономної системи диференціальної корекції GNSS та вимог національних криптографічних стандартів. Вона створює підґрунтя для забезпечення довготривалої криптографічної стійкості каналів «ККС – ЦОД – користувач» та веб-сервісу АСДК без зміни базової архітектури системи.

На Рис. 4 представлено як $PKI_{PQ-ASDK}$ архітектурно розгортається в основному та резервному ЦОД АСДК і включає кореневий засвідчувальний центр в офлайн-режимі, підлеглі Issuing CA для різних доменів довіри (ККС, сервери ЦОД і веб-сервера, клієнтські приймачі), реєстраційні органи, служби OCSP/CRL та каталог сертифікатів. QRNG інтегрується з апаратними модулями захисту (HSM), які забезпечують генерацію та захищене зберігання ключового матеріалу.

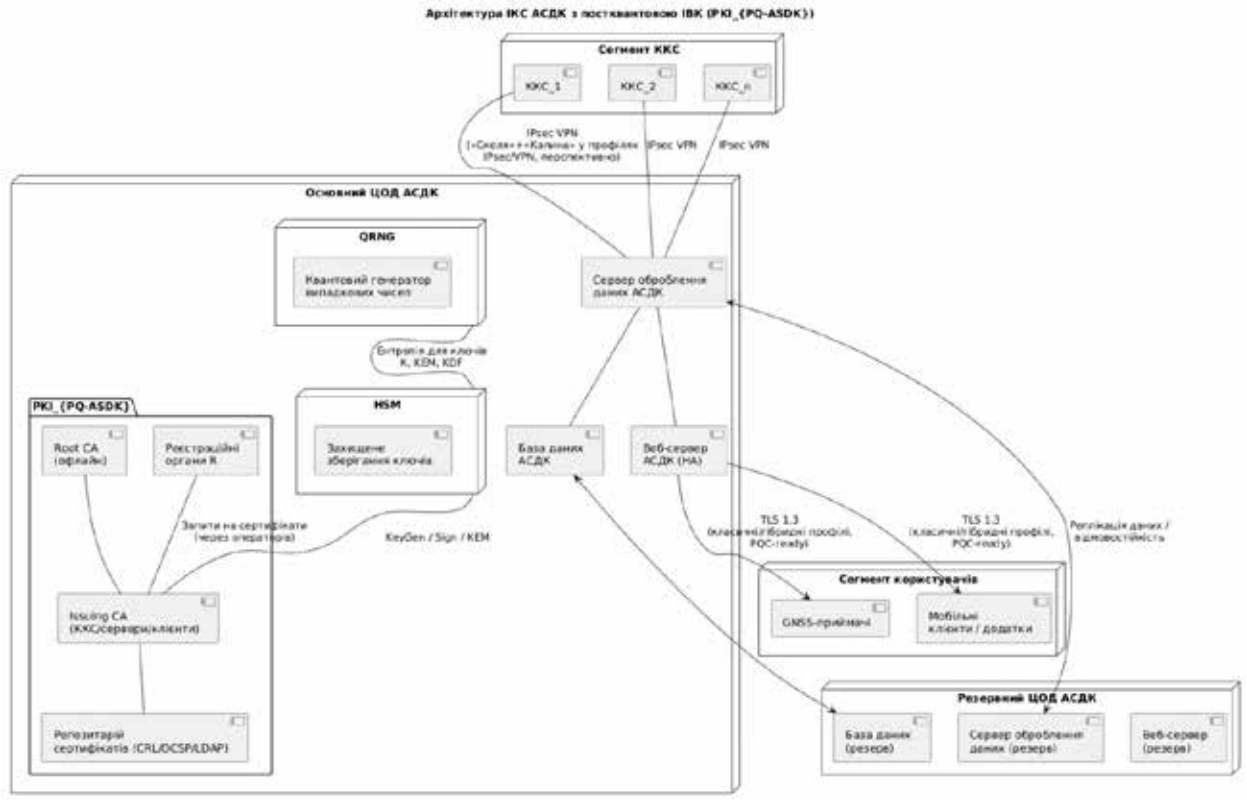

Рис. 4. Архітектура ІКС АСДК з постквантовою ІВК $PKI_{PQ\text{-}ASDK}$

Захищені тунелі між ККС та ЦОД, а також внутрішні канали ЦОД будуються за схемою «Скеля» + «Калина» у профілях IPsec/VPN, тоді як TLS-з'єднання з веб-сервісом АСДК використовують сертифікати, видані постквантовою ІВК, і можуть бути реалізовані як на основі чинних гібридних PQC-профілів TLS 1.3, так і в перспективі – з підтримкою алгоритмів «Скеля» та «Калина» після їх стандартизації в стеку TLS. Корекційні повідомлення та службові артефакти підписуються за алгоритмом «Вершина» і додатково хешуються «Купиною».

Висновки

У роботі обґрунтовано актуальність побудови постквантової інфраструктури відкритих ключів для інформаційно-комунікаційної системи автономної системи диференціальної корекції GNSS як об'єкта критичної інфраструктури. Показано, що класичні криптографічні механізми автентифікації, підпису та встановлення захищених з'єднань є вразливими до квантових атак, а компрометація каналів «ККС – ЦОД – користувач» та криптографічних матеріалів може призвести до спотворення координат, втрати часової синхронізації й порушення роботи систем GNSS.

Запропоновано формалізовану модель постквантової ІВК – $PKI_{PQ-ASDK}$ для ІКС АСДК у вигляді кортежу, яка узагальнює класичні підходи до побудови ІВК і адаптує їх до специфіки Autonomous DGNSS. Модель явно враховує множину суб'єктів (ККС, ЦОД, веб-сервер, клієнти, адміністратори), ієрархію засвідчувальних центрів (Root CA, Issuing CA), реєстраційні органи, репозитарії сертифікатів, захищені канали та інтеграцію квантового генератора випадкових чисел (QRNG). Розроблено архітектурну схему розгортання постквантової ІВК в основному та резервному ЦОД АСДК з виділенням доменів довіри для ККС, серверів ЦОД, веб-сервера та клієнтських приймачів. Показано, як кореневий та підлеглі засвідчувальні центри, RA, служби OCSP/CRL/LDAP, HSM та QRNG інтегруються в єдину інфраструктуру, сумісну з вимогами стандартів ISO/IEC 27001, NIST SP 800-53/800-57, IEC 62443 та НД ТЗІ. Продемонстровано можливість повної побудови криптографічних механізмів ІВК на основі національних постквантових стандартів: «Купина» (ДСТУ 7564:2014), «Калина» (ДСТУ 7624:2014), «Скеля» (ДСТУ 8961:2019) та «Вершина» (ДСТУ 9212:2023). Показано, що використання QRNG як джерела ентропії для процедур KeyGen , KEM , KDF та цифрового підпису дозволяє мінімізувати ризик компрометації ключів, підвищити стійкість до квантових атак та забезпечити довготривалу криптографічну надійність каналів зв'язку і веб-сервісу АСДК без зміни базової функціональної архітектури системи.

Отримані результати мають прикладне значення для проєктування та модернізації національних систем диференціальної корекції GNSS і ширше – для ІКС об'єктів критичної інфраструктури. Запропонована модель може використовуватися як методологічна основа при побудові постквантових ІВК для навігаційних,

телекомунікаційних, енергетичних та інших систем, де критичними є довіра до джерел даних, цілісність інформації та стійкість до довгострокових криптографічних загроз.

Подальші дослідження доцільно зосередити на практичній оцінці продуктивності запропонованої постквантової ІВК в умовах реального часу для інформаційно-комунікаційної системи АСДК. Йдеться насамперед про вимірювання затримок (latency), пропускної здатності (throughput) та обчислювального навантаження під час використання національних криптографічних стандартів ДСТУ 7564:2014 («Купина»), ДСТУ 7624:2014 («Калина»), ДСТУ 8961:2019 («Скеля») та ДСТУ 9212:2023 («Вершина») у протоколах TLS 1.3 та IPsec (включно з експериментальними або модифікованими профілями, які підтримують алгоритми «Скеля» та «Калина») між контрольно-коригуючими станціями, центром оброблення даних і користувачами. Окремим напрямом розвитку роботи є формальне моделювання протоколів встановлення захищених сеансів (TLS/IPsec-handshake) з використанням алгоритмів «Скеля» та «Вершина», побудова їх формалізованих специфікацій і подальша верифікація властивостей безпеки (автентифікація, цілісність, конфіденційність, стійкість до post-quantum атак) із залученням сучасних методів формальної верифікації та інструментів моделювання.

Список використаної літератури

1. Trýb J., Hospodka J. GNSS Interference and Security: Impacts on Critical Infrastructure and Mitigation Strategies. Procedia Computer Science. Вип. 253, 2025. С. 2635-2644. DOI:10.1016/j.procs.2025.01.323.

2. Nicholas Brown 20240620-Hidden_Risk_Report. URL: https://ggim.un.org/UNGGCE/documents/20240620-Hidden_Risk_Report.pdf.

3. Spanghero M., Papadimitratos P. UnReference: analysis of the effect of spoofing on RTK reference stations for connected rovers. arXiv, 2025. DOI:10.48550/arXiv.2503.20364.

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. Шумілова К. НАВІГАЦІЙНІ РИЗИКИ В АСПЕКТІ КІБЕРБЕЗПЕКИ ТРАНСПОРТНИХ СУДЕН І ВІЙСЬКОВИХ КОРАБЛІВ. Scientific Collection «InterConf+». 24(121). С. 391-408. 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. 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). С. 237-250. DOI:10.32631/v.2024.1.20

11. Junquera-Sánchez J., Hernando-Ramiro C., Gamallo-Palomares Ó. et al. Assessment of cryptographic approaches for a quantum-resistant Galileo OSNMA. NAVIGATION: Journal of the Institute of Navigation. Vol. 71, Issue 2. P. navi.648. DOI:10.33012/navi.648.

12. Peña P. A. Quantum randomness reinforces post-quantum cryptography to safeguard large enterprises in the quantum-safe era. QSNP. 17.09.2025. URL: https://qsnp.eu/quantum-randomness-reinforces-post-quantum-cryptography-to-safeguard-large-enterprises-in-the-quantum-safe-era/.

13. Moral J. O. del, iOlius A. deMarti, Vidal G. et al. Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective. arXiv, 2024. DOI:10.48550/arXiv.2401.03780.

14. Gorbenko I., Kandii S. National and International Post-Quantum Standards for Asymmetric Transformations. Cybernetics and Systems Analysis. Vol. 61, 02.08.2025. DOI:10.1007/s10559-025-00800-z.

15. Krelina M. Quantum technology for military applications. EPJ Quantum Technology. Вип. 8, № 1. С. 24. DOI:10.1140/epjqt/s40507-021-00113-y.

16. Morhul D. M., Nariezhnii O. P., Hrinenko T. O. Класифікація атак та вимоги кібербезпеки до веб-ресурсу QRNG. Radiotekhnika. № 220. С. 50-57. DOI:10.30837/rt.2025.1.220.04.

17. Chen Y., Gao W., Chen X. et al. Advances of SBAS authentication technologies. Satellite Navigation. Vol. 2, Issue 1. P. 12. DOI:10.1186/s43020-021-00043-1.

18. E-GIANTS Project Concludes Study on GNSS Authentication and Security Improvements | EU Agency for the Space Programme. 05.08.2025. URL: https://www.euspa.europa.eu/newsroom-events/news/e-giants-project-concludes-study-gnss-authentication-and-security-improvements.

19. Gorbenko I. D., Kachko Y. G., Yesina M. V. та ін. Порівняльна характеристика алгоритмів інкапсуляції ключів Crystals-Kyber та Скеля (ДСТУ 8961-2019). Radiotekhnika. № 210. С. 7-21. DOI:10.30837/rt.2022.3.210.01.

20. Fesenko A., Lytvynenko Y. Cryptanalysis of the «Vershyna» digital signature algorithm. Theoretical and Applied Cybersecurity. Вип. 5, № 2. DOI:10.20535/tacs.2664-29132023.2.288499.

21. Televnyi D. The Kupyna hash function application to SPHINCS+ signatures. Radiotekhnika. № 198. С. 215-219. DOI:10.30837/rt.2019.3.198.17.

22. Інфраструктури відкритих ключів. Електроний цифровий підпис. Теорія та практика :: Державний університет інформаційно-комунікаційних технологій. URL: https://duikt.edu.ua/ua/lib/1/category/2434/view/1822.

23. Горбенко І. Д., Кравченко П. О. Комбінована інфраструктура відкритих ключів та її застосування. Радіоелектронні і комп'ютерні системи. Issue 5. P. 86-90. Also available online, URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=recs_2009_5_17.

24. Горбенко І. Д., Халімов Г. З. Розвиток, стандартизація, уніфікація, удосконалення та впровадження інфраструктури відкритих ключів (включаючи національну систему електронного цифрового підпису) на внутрішньодержавному та міжнародному рівнях. 2012. URL: http://openarchive.nure.ua/handle/document/1064.

References

1. Tryb, J., & Hospodka, J. (2025). GNSS interference and security: Impacts on critical infrastructure and mitigation strategies. Procedia Computer Science, 253, 2635-2644. https://doi.org/10.1016/j.procs.2025.01.323

2. Brown, N. (2024, June 20). Hidden risk report. UN-GGIM. https://ggim.un.org/UNGGCE/documents/20240620-Hidden_Risk_Report.pdf

3. Spanghero, M., & Papadimitratos, P. (2025). UnReference: Analysis of the effect of spoofing on RTK reference stations for connected rovers. arXiv. https://doi.org/10.48550/arXiv.2503.20364

4. Verkhovna Rada of Ukraine. (2024). Law of Ukraine on Critical Infrastructure No. 1882-IX. Official web portal of the Parliament of Ukraine. 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, 16(2), 68-80. 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, 12(2), 1-16. https://doi.org/10.5038/1944-0472.12.2.1720

7. Shumilova, K. (2022). Navigatsiini ryzyky v aspekti kiberbezpeky transportnykh suden i viiskovykh korabliv [Navigation risks in the aspect of cybersecurity of transport vessels and warships]. Scientific Collection "InterConf+", 24(121), 391-408. https://doi.org/10.51582/interconf.19-20.08.2022.037

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

9. Viasat. (2022, March 30). KA-SAT network cyber attack overview. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

10. 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, 104(1), 237-250. https://doi.org/10.32631/v.2024.1.20

11. Junquera-Sanchez, J., Hernando-Ramiro, C., Gamallo-Palomares, O., et al. (2024). Assessment of cryptographic approaches for a quantum-resistant Galileo OSNMA. NAVIGATION: Journal of the Institute of Navigation, 71(2). https://doi.org/10.33012/navi.648

12. Pena, P. A. (2025, September 17). Quantum randomness reinforces post-quantum cryptography to safeguard large enterprises in the quantum-safe era. QSNP. https://qsnp.eu/quantum-randomness-reinforces-post-quantum-cryptography-to-safeguard-large-enterprises-in-the-quantum-safe-era/

13. Del Moral, J. O., de Marti i Olius, A., Vidal, G., et al. (2024). Cybersecurity in critical infrastructures: A post-quantum cryptography perspective. arXiv. https://doi.org/10.48550/arXiv.2401.03780

14. Gorbenko, I., & Kandii, S. (2025). National and international post-quantum standards for asymmetric transformations. Cybernetics and Systems Analysis, 61. https://doi.org/10.1007/s10559-025-00800-z

15. Krelina, M. (2021). Quantum technology for military applications. EPJ Quantum Technology, 8(1), 24. https://doi.org/10.1140/epjqt/s40507-021-00113-y

16. Morhul, D. M., Nariezhnii, O. P., & Hrinenko, T. O. (2025). Klasyfikatsiia atak ta vymohy kiberbezpeky do veb-resursu QRNG [Classification of attacks and cybersecurity requirements for QRNG web resource]. Radiotekhnika, 220, 50-57. https://doi.org/10.30837/rt.2025.1.220.04

17. Chen, Y., Gao, W., Chen, X., et al. (2021). Advances of SBAS authentication technologies. Satellite Navigation, 2(1), 12. https://doi.org/10.1186/s43020-021-00043-1

18. EU Agency for the Space Programme. (2025, August 5). E-GIANTS project concludes study on GNSS authentication and security improvements. https://www.euspa.europa.eu/newsroom-events/news/e-giants-project-concludes-study-gnss-authentication-and-security-improvements

19. Gorbenko, I. D., Kachko, Y. G., Yesina, M. V., et al. (2022). Porivnialna kharakterystyka algorytmiv inkapsuliatsii kliuchiv Crystals-Kyber ta Skelia (DSTU 8961-2019) [Comparative characteristic of key encapsulation algorithms Crystals-Kyber and Skelia (DSTU 8961-2019)]. Radiotekhnika, 210, 7-21. https://doi.org/10.30837/rt.2022.3.210.01

20. Fesenko, A., & Lytvynenko, Y. (2023). Cryptanalysis of the "Vershyna" digital signature algorithm. Theoretical and Applied Cybersecurity, 5(2). https://doi.org/10.20535/tacs.2664-29132023.2.288499

21. Televnyi, D. (2019). The Kupyna hash function application to SPHINCS+ signatures. Radiotekhnika, 198, 215-219. https://doi.org/10.30837/rt.2019.3.198.17

22. State University of Information and Communication Technologies. (n.d.). Infrastruktury vidkrytykh kliuchiv. Elektroniy tsyfrovyi pidpys. Teoriia ta praktyka [Public key infrastructures. Electronic digital signature. Theory and practice]. https://duikt.edu.ua/ua/lib/1/category/2434/view/1822

23. Gorbenko, I. D., & Kravchenko, P. O. (2009). Kombinovana infrastruktura vidkrytykh kliuchiv ta yii zastosuvannia [Combined public key infrastructure and its application]. Radioelectronic and Computer Systems, 5, 86-90. [http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK\&P21DBN=UJRN\&Z21ID=\&S21REF=10\&S21CNR=20\&S21STN=1\&S21FMT=ASP_meta\&C21COM=S&2_S21P03=FILA=&2_S21STR=recs_2009_5_17](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=recs_2009_5_17)

24. Gorbenko, I. D., & Khalimov, G. Z. (2012). Rozvytok, standartyzatsiia, unifikatsiia, udoskonalennia ta vprovadzhennia infrastruktury vidkrytykh kliuchiv na vnutrishnioderzhavnomu ta mizhnarodnomu rivniakh [Development, standardization, unification, improvement and implementation of public key infrastructure at domestic and international levels]. http://openarchive.nure.ua/handle/document/1064

Дата першого надходження рукопису до видання: 23.11.2025
Дата прийнятого до друку рукопису після рецензування: 19.12.2025
Дата публікації: 31.12.2025