DOI: https://doi.org/10.36910/6775-2524-0560-2024-54-29
УДК 621.396
Кудряшов Андрій Сергійович, аспірант
https://orcid.org/0009-0008-6087-3248
Державний університет інтелектуальних технологій і зв'язку, м. Одеса, Україна

ШТУЧНИЙ ІНТЕЛЕКТ ТА БЕЗПЕКА У МОБІЛЬНИХ ТЕХНОЛОГІЯХ 5G ТА 6G

Кудряшов А.С. Штучний інтелект та безпека у мобільних технологіях 5G та 6G. У межах статті проведено дослідження штучного інтелекту та безпеки у мобільних технологіях 5G та 6G. Підкреслено, що у 5G використовуються технології, такі як програмні мережі (SDN), віртуалізація мережевих функцій (NFV), штучний інтелект (ШІ) і хмарні мережі, які є новими у сфері телекомунікацій. Разом ці ключові технології допомагають реалізувати мобільну мережу 5G та 6G, здатну надавати послуги, що виходять далеко за межі високошвидкісного широкосмугового підключення з малою затримкою в будь-який час і в будь-якому місці, однак вони також призводять до збільшення кількості загроз кібербезпеці, ніж будь-коли раніше. Детально описано особливості архітектури безпеки технології 6G, зазначається, що архітектура безпеки 6G повинна підтримувати базову концепцію безпеки нульової довіри (ZT) у мережі мобільного зв'язку, щоб мінімізувати проблему захисту мережі від зовнішніх атак у зв'язку зі знаженням потужності IPsec і брандмауерів. Наголошується, що особиста інформація користувачів повинна зберігатися та використовуватися відповідно до протоколів, узгоджених між постачальником послуг, оператором мобільної мережі (MNO), абонентом і MNO, щоб забезпечити їх безпеку. Підкреслено, що система 6G повинна позбутися існуючих методів шифрування з асиметричним ключем, оскільки квантові комп'ютери зроблять їх небезпечними, а рішення постквантової криптографії (PQC), такі як криптографія на основі решітки, криптографія на основі коду, багатоваріантна поліноміальна криптографія та підпис на основі хешу сформують надійне підґрунтя для захисту та належного рівня безпеки. Розкрито функції безпеки та механізми підвищення безпеки майбутньої архітектури 6G. Очікувана інтелектуальна система 6G призначена для вдосконалених механізмів і методів штучного інтелекту для підтримки високих вимог до послуг, необхідних можливостей і нових вимог до різновидів використання.
Ключові слова: мобільні технології, захист, атака, штучний інтелект, машинне навчання, безпека.

Kudriashov A. Artificial Intelligence and Security in 5g and 6g Mobile Technologies. The article examines artificial intelligence and security in 5G and 6G mobile technologies. It is highlighted that 5G uses technologies such as software-defined networking (SDN), network functions virtualization (NFV), artificial intelligence (AI) and cloud networks that are new to the telecommunications industry. Together, these key technologies help realize a 5G and 6G mobile network capable of providing services that go far beyond high-speed, low-latency broadband anytime, anywhere, but they also lead to more cybersecurity threats than ever before. The features of the security architecture of 6G technology are described in detail, and it is noted that the security architecture of 6G must support the basic concept of zero trust (ZT) security in the mobile communication network to minimize the problem of protecting the network from external attacks due to the increase in IPsec power and firewalls. It is emphasized that users' personal information must be stored and used in accordance with protocols agreed between the service provider, the mobile network operator (MNO), the subscriber and the MNO to ensure their security. It is emphasized that the 6G system must get rid of existing asymmetric key encryption methods, as quantum computers will make them insecure, and post-quantum cryptography (PQC) solutions such as lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, and signature-based hash will form a reliable basis for protection and an appropriate level of security. The security features and security enhancement mechanisms of the future 6G architecture are disclosed. The expected 6G intelligent system is designed for advanced mechanisms and methods of artificial intelligence to support high service requirements, necessary capabilities, and new demands for varieties of use.
Key words: mobile technologies, protection, attack, artificial intelligence, machine learning, security.

Вступ та постановка проблеми. В останні роки радіомережі п'ятого покоління (5G) були впроваджені в усьому світі реалізуючи такі функції як: масове підключення, надзвичайна надійність і гарантована низька затримка [1]. З іншого боку, враховуючи постійний розвиток цифрових технологій, 5G, не зможе задовольнити всі майбутні потреби. Передбачається, що технологія бездротової мережі шостого покоління (6G) запропонує ширше покриття, менше споживання енергії, повний спектр і економічну ефективність із покращеною безпекою. Мережі 6G задовольнять ці потреби шляхом розгортання нових технологій, таких як множинний доступ, схеми кодування каналів, численні технології антен і хмарні периферійні обчислення. 6G впливає на чотири важливі майбутні зміни. По-перше, він пропонує інтегровану комунікаційну мережу повітря–земля–космос–море шляхом розгортання безлічі мереж. По-друге, нові радіодіапазони покращать пропускну здатність мережі та швидкість передачі даних, включаючи міліметрові хвилі (mmwave) та оптичний зв'язок. По-третє, 6G забезпечить нове покоління інтелектуальних програм і послуг, що використовують технології штучного інтелекту (ШІ) і великих даних у відповідь на масивні набори даних, створені гетерогенними мережами з різними сценаріями зв'язку, широкою смугою пропускання і більшою кількістю антен. По-четверте, мережева безпека та конфіденційність повинні бути зміцнені та вдосконалені для технологій та програм 6G. Обробка даних, виявлення

загроз, аналіз трафіку та шифрування даних вважаються найбільш критичними проблемами в мережах 6G.

Аналіз останніх досліджень і публікацій. Науковий підхід у сфері мобільних технологій 5G та 6G є різнорідним та масштабним. У сучасній науковій площині з'являються роботи присвячені дослідженням каналів пропускання та ураження, підвищення рівня кібербезпеки технологій 5G та 6G, тощо.

М.В. Васильківський, М.В. Будаш та О.С. Болдирева [2] розглянули автономну інформаційну безпеку, яка буде однією з ключових функцій створення благонадійної архітектури телекомунікаційної мережі 6G. Авторами визначено особливості захисту систем і кінцевих користувачів від нападу зловмисників у міру їх виникнення із використанням запропонованої архітектури мережі та про активного підходу.

У [3] розглянуто шлях розвитку 6G і подальше зростання технологій. Досліджено найсучасніші технології 5G і зазначено необхідність вивчення 6G. Беручи до уваги поточний і новий розвиток безпроводового зв'язку, передбачено, що 6G охоплюватиме три основні аспекти, а саме: мобільний ультраширокий зв'язок, суперінтернет речей (IoT) і штучний інтелект (ШІ). Терагерцевий (ТГц) зв'язок можна використовувати для підтримання мобільного ультраширокосмугового зв'язку, симбіотичне радіо та супутниковий зв'язок можна використовувати для досягнення суперінтернету речей, а методи машинного навчання є перспективними кандидатами для ШІ.

У роботі [4] розглянута мобільна мережа 6G, включно з мотиваціями, сценаріями використання, вимогами, підтримуваними дослідницькими проектами та технологіями. Було детально проаналізовано еволюцію і розширені функції 5G, щоб передбачити критичні вимоги до 6G і підкреслити їх можливості. Було запропоновано кілька потенційних застосувань, їхні переваги, концепції та напрямки досліджень 6G.

Із зарубіжних авторів варто відмітити роботи таких науковців як: Сяоху Ю, Ван Чен-Сян, Хуан Цзе, Гао Сіці, Чжан Цзайчен, Ван Майкл, Хуан Юнмін, Чжан Чуань, Цзян Яньсян, Ван Цзяхен, Чжу Мінь, Шен Бінь, Ван Дунмін, Пан Чживень, Чжу Пенчен, Ян Ян, Лю Зенінг, Дін Чжан, Тао Сяофен, Лян Ін-Чанг [5], Еміліано Лейте Хосе Роберто, Урсіні Едсон, Хмелевскі Адао, Сілва Антоніу [6], Шарма Гурав, Патель Друвін, Сакс Йоахім, Андраде Марілет, Фаркас Янош, Хармат Янош, Варга Балаш, Бернхард Х.-П., Музаффар Рахіб, Ахмед Махін, Дюрр Франк, Брукнер Дітмар, Монтесдеока Едгардо, Уатра Дрісса, Чжан Хунвей, Гросс Джеймс [7], Шарац Марко, Павлович Нікола, Баканін Турджман Фаді, Адамович Саша [8], Мітра Рупендра, Ронг Бо [9], Джаханхані Хамід, Кендзьєрський Стефан, Хуссейн Усама [10], Мухейдат Фаді, Даджані Халіл, Тавалбе Лоай [11], Чхабра Соня, Ейден Манпріт , Сабхар , Аль-Асаді Мустафа [12], Оунза Джайрус [13], Фатіма Зайнаб, Аршад Садія, Андліб Марія, Зардарі Шахніла [14], Хан Шах Халід, Шивакоті Ніраджан, Стасінопулос Пітер, Уоррен Метью [15] та інших.

Однак незважаючи на масштабність наукових досліджень питання актуальності даної роботи не викликає сумнівів.

Постановка завдання. Метою роботи є дослідження штучного інтелекту та безпеки у мобільних технологіях 5G та 6G.

Викладення основного матеріалу дослідження. Архітектура безпеки технології 6G є головною умовою сьогодення. Оскільки 6G має бути більш відкритою мережею, ніж 5G, межа між внутрішньою та зовнішньою мережею буде поступово стиратися. У результаті поточні заходи безпеки мережі, такі як IPsec і брандмауери, не будуть достатньо потужними, щоб захистити мережу від зовнішніх атак. Архітектура безпеки 6G повинна підтримувати базову концепцію безпеки нульової довіри (ZT) у мережі мобільного зв'язку, щоб мінімізувати цю проблему. ZT – це парадигма безпеки, яка наголошує на захисті системних ресурсів. Архітектура нульової довіри (ZTA) – це архітектура безпеки, яка використовує концепцію ZT і містить зв'язки між об'єктами мережі (NE), процесами протоколів і правилами доступу. Тому ZTA має бути основою архітектури безпеки 6G.

Проблеми безпеки віртуалізації потребують використання системи з безпечним рівнем віртуалізації, який включає технологію безпеки, що ідентифікує приховане шкідливе програмне забезпечення. Крім того, гіпервізор повинен забезпечувати повне розділення обчислень, сховищ і мереж різних мережевих служб за допомогою захищених протоколів, таких як TLS, SSH, VPN і так далі. Інтроспекція віртуальної машини (VMI) – це функція гіпервізора, яка перевіряє та виявляє ризики безпеки, аналізуючи інформацію реєстру vCPU, файли вводу-виводу та пакети зв'язку

кожної віртуальної машини (VM), щоб запобігти проникненню. Під час використання контейнеризації операційна система повинна відповідним чином установити привілеї різних контейнерів і запобігти монтуванню основних системних каталогів і прямому доступу до файлового контейнера головного пристрою.

Керування вразливими місцями, спричиненими використанням, оновленням і видаленням відкритих вихідних кодів, є найважливішою справою при вирішенні питань безпеки з відкритим вихідним кодом. Ось чому швидке виявлення загроз вимагає автоматизованої системи керування, яка може виявляти вразливості та застосовувати виправлення. Потрібен додатковий крок, щоб забезпечити швидке та безпечне застосування виправленого програмного забезпечення за допомогою безпечної технології. Крім того, необхідно створити структуру управління безпекою для обробки:

- вразливостей відкритого коду з довгострокового погляду,
- змін у сприйнятті розробника,
- розгортання Security рішення.

Безпека даних за допомогою штучного інтелекту ґрунтується на принципі гарантованого захисту від атак. Створення моделей ШІ в надійній системі є першим кроком у цьому процесі. Крім того, необхідно використовувати такий метод, як цифрові підписи, щоб перевірити рівень якості захисту. Якщо виявлено шкідливу модель штучного інтелекту, система повинна виконати операції самовідновлення або автовідновлення. Система також повинна обмежити збір даних для навчання штучного інтелекту.

Особиста інформація користувачів повинна зберігатися та використовуватися відповідно до протоколів, узгоджених між постачальником послуг, оператором мобільної мережі (MNO), абонентом і MNO, щоб забезпечити їх безпеку. Особиста інформація зберігається в надійному середовищі виконання (TEE) і надійному програмному забезпеченні за допомогою системи 6G, яка також зменшує або робить анонімним обсяг інформації, яка стає загальнодоступною під час її використання. Автентичність і авторизація повинні бути перевірені, перш ніж MNO оприлюднить особисту інформацію. Іншим варіантом є використання гомоморфного шифрування під час роботи з інформацією користувача, щоб дані могли бути доступні в зашифрованому вигляді. Рішення на основі штучного інтелекту, такі як схема розвантаження з урахуванням конфіденційності на основі навчання, також можуть використовуватися для збереження конфіденційності місцезнаходження користувача та шаблонів використання.

Система 6G повинна позбутися існуючих методів шифрування з асиметричним ключем, оскільки квантові комп'ютери зроблять їх небезпечними. Рішення постквантової криптографії (PQC), такі як криптографія на основі решітки, криптографія на основі коду, багатоваріантна поліноміальна криптографія та підпис на основі хешу, були в центрі уваги багатьох дослідників. У порівнянні з Рівестом–Шаміром–Адлеманом (RSA), довжина ключа, яка зараз розглядається у PQC буде у багато разів більшою. PQC, ймовірно, матиме більшу обчислювальну вартість, ніж поточний метод RSA. Як наслідок, дуже важливо, щоб PQC був належним чином інтегрований у продуктивність апаратного/програмного забезпечення мережі 6G і потреби в обслуговуванні.

Дизайн мережі 6G значно відрізнятиметься від 5G. По-перше, 6G може забезпечити автоматизацію мережі та мережу як послугу (NaaS). NaaS дозволяє абонентам налаштовувати мережі. Ключові технології включають мережу на основі намірів, наскрізне програмне забезпечення, хмаризацію та глибоку віртуалізацію функцій. По-друге, швидке впровадження хмарних мереж і програмного забезпечення з відкритим кодом для мережевих компонентів core/RAN передбачає «повну відкритість» майбутнього 6G. 6G може бути першою стільниковою системою, яка повністю підтримує штучний інтелект. Це бачення перетворить «підключені речі» 5G на «підключений інтелект» 6G, причому штучний інтелект зрештою контролюватиме більшість мережевих операцій і вузлів.

Архітектуру безпеки 6G потрібно буде адаптувати, щоб увімкнути нові додатки та інтеграцію моделі мережі космос–повітря–земля–море. Поточна архітектура безпеки 3GPP може потребувати суттєвих змін. Оператори мережі будуть критично важливими гравцями для оновлення доступу до мережі та архітектури безпеки. Постачальники послуг надають додаткові послуги (онлайн-розваги) і платформи (хмарне зберігання, аналітика даних) для розробників і користувачів. Постачальники послуг оновлять безпеку домену додатків і архітектури на основі послуг. Розробникам ігор XR/AR доведеться посилити безпеку для хмарних/граничних програм або

ввімкнути нові API безпеки (відповідно до послуг сторонніх постачальників). Мережі 6G можуть пропонувати мобільне сховище та інші послуги. Таким чином, вони можуть допомогти покращити безпеку служби багатьма способами. Нарешті, користувачі можуть не вплинути на зміни, якщо вони замінять пристрої або зареєструють нові SIM-карти. Архітектуру безпеки 6G можна розділити на рівні, щоб охопити всі питання безпеки та виклики для всіх об'єктів 6G. Вона складається з фізичного рівня, рівня підключення та рівня додатків. Кожен рівень покращує нові функції безпеки, які можуть покращити безпеку мереж 6G.

Функції безпеки та механізми підвищення безпеки майбутньої архітектури 6G:

1. Безпека доступу до мережі: 6G вимагає нових систем автентифікації та криптографії. Це 6G-AKA, квантово-безпечна криптографія та безпека фізичного рівня. Мотивація для хмарних і відкритих програмованих мережевих технологій у 6G вимагає нової автентифікації, щоб 6G міг використовувати концепції безпеки 5G, такі як єдина платформа автентифікації для мереж відкритого доступу. Для їх виконання потрібні численні додаткові функції. Наприклад, протокол 6G-AKA має гарантувати, який компонент, функція сервера автентифікації (AUSF) або функція прив'язки безпеки (SEAF), визначатиме автентифікацію в міжзрізовому зв'язку. 6G-AKA повинна мати можливість автентифікувати заявлену ідентифікацію кінцевої точки в програмованій мережевій інфраструктурі з глибокими фрагментами. Безпека фізичного рівня може захистити мережі 6G IoT від небезпек, включаючи атаки уособлення, і покращити керування доступом до мережі. Найсуттєвішою відмінністю в адмініструванні абонентів 6G порівняно з 5G є впровадження нового підходу до керування ідентифікацією користувачів.

2. Безпека мережевого домену: виникне потреба в нових відкритих методах автентифікації через поширення 6G на неземні мережі, такі як супутниковий і морський зв'язок.

3. Безпека домену користувача: автентифікація за допомогою біометрії або служби без пароля для механізмів контролю доступу була довгоочікуваною функцією безпеки 6G. Багато програм десятиліттями покладалися на методи безпеки на основі паролів. На жаль, є кілька недоліків. Деякі з них легко зламати, зберігати їх дорого та важко запам'ятати. Автентифікація на основі мозкової хвилі або серцевого ритму може забезпечити більш безпечний і покращений механізм роботи з користувачем у майбутньому.

4. Безпека домену програми: обидві сторони повинні пройти автентифікацію, щоб довірчі мережі 6G працювали. Взаємна автентифікація за допомогою симетричного ключа все ще використовується в 5G. Проте мережі 6G можуть виграти від блокчейну та технологій DLT.

5. Безпека архітектури на основі послуг: коли справа доходить до 6G, архітектура безпеки на основі послуг, яка використовується в 5G, оновлюється до наскрізної архітектури безпеки на основі послуг і політики. Безпека домену є основою архітектури безпеки 5G, побудованої на архітектурі на основі послуг. Виводячи цю функцію на наступний рівень, 6G використовуватиме наскрізну архітектуру на основі послуг або, можливо, безпеку домену на основі архітектури, щоб задовольнити потреби персоналізації та гнучкості мікророзгортання, зберігаючи високий рівень безпеки.

Деякі важливі технології вже довели свою ефективність у важливих основних секторах мереж 6G. Вони забезпечують високий рівень безпеки, надійність із низькою затримкою та ефективні послуги зв'язку з мережами 6G. Однак більшість нових технологій 6G мають вищі ризики для безпеки та конфіденційності.

Запропоновані методи захисту фізичного рівня залежать від випадкових фізичних характеристик і шуму, що оточує бездротові мережі. Однак гнучкість механізмів PLS, особливо в умовах обмежених ресурсів, з можливостями проривних технологій 6G може прокласти шлях для нової ери PLS в епоху 6G.

Терагерцовий зв'язок (ТГц) поєднує оптичні хвилі з широким спектром і мікрохвилі, які можуть підтримувати високі швидкості передачі, надійний захист від перешкод і просту інтеграцію зондування та зв'язку. ТГц зв'язок спочатку використовується для задоволення системних потреб у швидкості передачі в порядку Тбіт/с. ТГц зв'язок стане цінним продовженням існуючих методів передачі. Вони, по суті, будуть використовуватися для зв'язку з латентними голографічними комунікаціями, маломасштабні комунікації, дані надвисокої ємності та передача на короткі відстані з надвисокою швидкістю – це лише деякі з можливостей застосування.

Існує три типові архітектурні конструкції трансивера: архітектура прямої модуляції, архітектура модуляції твердотільного частотного змішування та архітектура оптоелектронної модуляції. Основними проблемами проектування для архітектури є відмінна сумісність, відмінна

енергоефективність і економічна ефективність. Що стосується компонентів RFend, основні елементи ТГц системи включають джерело ТГц сигналу, змішувач, помножувач, детектор і підсилювач.

На даний момент робочі частоти ТГц і вихідна потужність не задовольняють комерційним критеріям високої ефективності системи, низького енергоспоживання і збільшеного терміну служби. Потрібно досліджувати передові напівпровідникові матеріали, такі як германід кремнію (SiGe) і фосфід індію (InP). Крім того, ТГц системи потребують швидкості передачі в режимі реального часу Тбіт/с при обробці базового сигналу. Таким чином, розробка технологій високошвидкісної обробки сигналів базової смуги є простою та споживає мало енергії. З точки зору антен, більшість антен з високим коефіцієнтом посилення сьогодні мають масивні рефлектори, що сприяє розвитку технології надвеликомасштабних ТГц антен зі зменшеними габаритами. Проте радіодіапазони мм-хвиль широко використовуються в мережах 5G. Вимога щодо дуже високих швидкостей передачі в середовищі 6G робить такі діапазони достатніми. У зв'язку з цим радіочастотні діапазони практично реалізовані і не можуть бути використані для майбутніх технологій.

Комунікації видимим світлом (VLC) – це практична технологія, яка може відповідати вимогам бездротової мережі 6G. Крім того, VLC протягом тривалого часу досліджувався в багатьох областях, наприклад, у рішеннях для локалізації в приміщеннях і мережі Vehicle-Ad-Hoc-Network (VANET). Технологія VLC має широку смугу пропускання, що робить її толерантною до перешкод у порівнянні з радіочастотами із серйозними перешкодами та значною затримкою. Стандарти безпеки VLC відповідають основним вимогам безпеки для всіх бездротових мереж. Критерії конфіденційності, цілісності, автентичності, доступності (CIAA) описуються як:

1. Конфіденційність: обмежує доступ до даних лише для призначених одержувачів і запобігає розголошенню інформації стороннім організаціям.

2. Цілісність: щоб забезпечити правильність надісланої інформації, перевіряється ідентифікація мережевого вузла.

3. Автентифікація: залежить від автентифікації особистості та інформації. Перша – це забезпечення ідентифікації особи, яка має доступ, тоді як достовірність інформації передбачає, що ніхто не змінює передану інформацію. Обидві частини автентифікації необхідні для забезпечення безпеки інформації та ресурсів.

4. Доступність: це можливість користувачів підключатися до бездротової мережі в будь-який час і з будь-якого місця.

Крім того, накладання сигналів може призвести до накладення різних сигналів передавача; тому автентичність, цілісність і доступність можуть бути під загрозою. На фізичні характеристики світлового середовища зв'язку в основному впливають два найнижчі рівні (рівень PHY і рівень MAC). Атаки в цій технології спрямовані на фізичний рівень шляхом підслуховування, глушіння та захоплення переданих даних. Інші атаки контролю доступу відбуваються через авторизований доступ до бездротового середовища з атаками автентифікації.

Техніка молекулярного зв'язку є перспективною технологією 6G. Однак метод ще знаходиться на початковій стадії. Фундаментальним принципом технології молекулярної комунікації є передача інформації за допомогою біологічних сигналів.

Нещодавно штучний інтелект і машинне навчання були відзначені як необхідні компоненти мережевої архітектури всіх технологій мереж 6G. Штучний інтелект в мережах 5G реалізується в місцях з величезною кількістю навчальних даних і ефективними обчислювальними ядрами. Однак штучний інтелект / машинне навчання стало основою мереж 6G. Штучний інтелект та машинне навчання використовуються для захисту різних фреймів безпеки та захисту 6G. Використання штучного інтелекту та машинного навчання в безпеці робить рішення безпеки більш автономними та точнішими з можливостями прогнозування для аналітики безпеки.

До проблем, пов'язаних зі штучним інтелектом / машинним навчанням у системі 6G варто віднести:

1. Надійність. Надійність моделей і компонентів машинного навчання стає важливою, коли штучний інтелект забезпечує безпеку мережі.

2. Видимість. Моніторинг функцій безпеки на основі штучного інтелекту та машинного навчання у режимі реального часу для забезпечення контролю та надійності.

3. Етичні та правові аспекти. Методи оптимізації на основі штучного інтелекту можуть обмежити роботу деяких клієнтів або програм. Рішення безпеки на основі штучного інтелекту є однаковими щодо захисту всіх користувачів контрольованих ШІ.

4. Розширюваність і життєздатність. Масштабованість необхідних обчислювальних, комунікаційних і сховищ є проблемою для штучного інтелекту.

5. Контрольовані завдання безпеки. Великі накладні витрати можуть виникнути, коли рішення безпеки штучного інтелекту пов'язані зі значними процесами обробки даних.

6. Гнучкість моделей. Має бути безпечним та гнучким на етапах навчання та висновків.

Очікувана інтелектуальна система 6G призначена для вдосконалених механізмів і методів штучного інтелекту для підтримки високих вимог до послуг, необхідних можливостей і нових вимог до випадків використання.

Висновки. Очікувана інноваційна система 6G включає технології ШІ для підвищення безпеки та захисту мережі. Рівні архітектури безпеки включають інтелектуальний рівень зондування, інтелектуальний крайовий рівень, інтелектуальний рівень керування та інтелектуальний прикладний рівень. Кожен рівень підтримує різні функції та запроваджує деякі атаки. Більшість нових технологій 6G створюють значні загрози безпеці та конфіденційності. Ці провідні технології були виділені, уточнюючи їхні проблеми безпеки та атаки, а також рішення для запобігання безпеці. Кожне нове покоління мережевих технологій представляє інноваційні програми. Пошук рішення для захисту 6G є критичним питанням, яке потрібно буде дослідити в майбутньому.

Список бібліографічного опису

1. Santiago Adrian, Cerio Andoni, Sanchoyerto Martinez Aitor, Liberal Fidel. Analysis of Mission Critical Services Radio Access Network Capacity Limitations Over 5G. IEEE Access. 2024. P. 1-1. DOI: 10.1109/ACCESS.2024.3350902.
2. Васильківський М.В., Будаш М.В., Болдирева О.С. Забезпечення інформаційного захисту в телекомунікаційних мережах 6G. Науковий журнал "Комп'ютерно-інтегровані технології: освіта, наука,виробництво" Луцьк, 2023. Випуск № 50. С. 142-150.
3. Дослідження мобільного широкосмугового зв'язку із застосуванням штучного інтелекту / Н.В. Руденко, Л.В. Дакова, С.Ю. Даков, І.І. Пархоменко, Н.В. Блаженний // Проблеми розвитку та вдосконалення єдиної національної системи зв'язку. Зв'язок, Київ, 2023. № 2. С. 3-9. DOI: 10.31673/2412-9070.2023.020309
4. Одарченко Р. С. Ключові напрямки досліджень стільникових мереж на шляху до 6G (огляд) / Р. С. Одарченко, Т. В. Дика, О. В. Жарова, М. С. Одарченко, В. М. Жога, О. П. Слободян // Наукоємні технології. 2022. № 3. С. 215-228. Режим доступу: http://nbuv.gov.ua/UJRN/Nt_2022_3_8

References

5. Xiaohu You, Wang Cheng-Xiang, Huang Jie, Gao Xiqi, Zhang Zaichen, Wang Michael, Huang Yongming, Zhang Chuan, Jiang Yanxiang, Wang Jiaheng, Zhu Min, Sheng Bin, Wang Dongming, Pan Zhiwen, Zhu Pengcheng, Yang Yang, Liu Zening, Ding Zhang, Tao Xiaofeng, Liang Ying-Chang. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. Science China Information Sciences. 2021. № 64. DOI: 10.1007/s11432-020-2955-6.
6. Emiliano Leite José Roberto, Ursini Edson, Chmielewski Adão, Silva Antônio. New Technological Waves Emerging in Digital Transformation: Internet of Things IoT/IoE, 5G/6G Mobile Networks and Industries 4.0/5.0. 2023. DOI: 10.1007/978-3-031-31007-2_30.
7. Sharma Gourav, Patel Dhruvin, Sachs Joachim, Andrade Marilet, Farkas Janos, Harmatos János, Varga Balazs, Bernhard H.-P., Muzaffar Raheeb, Ahmed Mahin, Duerr Frank, Bruckner Dietmar, Montesdeoca Edgardo, Houatra Drissa, Zhang Hongwei, Gross James. Toward Deterministic Communications in 6G Networks: State of the Art, Open Challenges and the Way Forward. IEEE Access. 2023. P. 1-1. DOI: 10.1109/ACCESS.2023.3316605.
8. Šarac Marko, Pavlović Nikola, Bacanin Nebojsa, Al-Turjman Fadi, Adamović Saša. Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT Device Security Gateway Architecture. Energy Reports. 2021. № 7. DOI: 10.1016/j.egyr.2021.07.078.
9. Mitra Rupendra, Rong Bo. From 5G to 6G: Technologies, Architecture, AI, and Security. IEEE Wireless Communications. 2023. № 30. P. 16-26. DOI: 10.1109/MWC.2023.10355088.
10. Jahankhani Hamid, Kendzierskyj Stefan, Hussien Osama. (2023). Approaches and Methods for Regulation of Security Risks in 5G and 6G. 2023. DOI: 10.1007/978-3-031-33631-7_2.
11. Muheidat Fadi, Dajani Khalil, Tawalbeh Lo'ai. Security Concerns for 5G/6G Mobile Network Technology and Quantum Communication. Procedia Computer Science. 2022. № 203. P. 32-40. DOI: 10.1016/j.procs.2022.07.007.
12. Chhabra Sonia, Aiden Manpreet, Sabharwal Shweta, Al-Asadi Mustafa. 5G and 6G Technologies for Smart City. 2023. DOI: 10.1007/978-3-031-22922-0_14.

13. Ounza Jairus. A Taxonomical Survey of 5G and 6G Security and Privacy Issues. 2023. №14. P. 42–60. DOI: 10.30574/gjeta.2023.14.3.0047.
14. Fatima Zainab, Arshad Sadia, Andleeb Maria, Zardari Shehnila. Network Privacy and Security Issues in 5G and 6G. 2023. DOI: 10.22541/au.167930311.15785905/v1.
15. Khan Shah Khalid, Shiwakoti Nirajan, Stasinopoulos Peter, Warren Matthew. Security assessment in Vehicle-to-Everything communications with the integration of 5G and 6G networks. 2021. P. 154-158. DOI: 10.1109/ISCSIC54682.2021.00037.