DOI: https://doi.org/10.36910/6775-2524-0560-2023-50-22
УДК 621.391
Васильківський Микола Володимирович, к.т.н., доцент,
https://orcid.org/0000-0002-6586-2563
Будаш Михайло Володимирович, аспірант,
Болдирева Ольга Сергіївна, аспірант.
Вінницький національний технічний університет, м. Вінниця, Україна.

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО ЗАХИСТУ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ 6G

Васильківський М.В., Будаш М.В., Болдирева О.С. Забезпечення інформаційного захисту в телекомунікаційних мережах 6G. Розглянуто автономну інформаційну безпеку, яка буде однією з ключових функцій створення благонадійної архітектури телекомунікаційної мережі 6G. Визначено особливості захисту систем і кінцевих користувачів від атак зловмисників у міру їх виникнення із використанням запропонованої архітектури мережі та проактивного підходу. Поєднавши автономні технології інформаційної безпеки з архітектурою системи розглянуто можливість створення динамічного інтелектуального захисту із використанням машинного навчання, штучної імунної системи. Розглянуто перспективи широкого поширення технологій на основі штучного інтелекту та машинного навчання для вирішення проблем інформаційної безпеки. Зокрема, здійснено покращення виявлення проблем інформаційної безпеки, запропоновано рекомендації аналітикам, що дозволить скоротити час відгуку на інцидент із сотень годин до секунд та підвищуючи продуктивність роботи аналітиків з одного або двох інцидентів до тисяч на день.

Розглянуто благонадійність процесу передавання інформаційних даних, як визначальний фактор інформаційного захисту з погляду комунікації. Основні наукові докази для формування правильного висновку про те, чи заслуговує на довіру телекомунікаційна мережа 6G базуються на її функціональних параметрах, які свідчать про рівень благонадійності, яку очікуємо від впровадження технологій 6G. В результаті, визначено, що благонадійність телекомунікаційної мережі 6G успадковує чудові функціональні можливості та передовий досвід мереж попереднього покоління, а також враховує різні дисципліни та соціальні проблеми.

Досліджено вплив надійності глибокої нейронної мережі (DNN) на оцінку систем штучного інтелекту із врахуванням, що для навчання штучного інтелекту використовуються масивні набори реальних даних, які можуть призвести до витоку, підробки, крадіжки та неправомірного використання даних через відсутність належного захисту.

Ключові слова: архітектура телекомунікаційної мережі, динамічний інтелектуальний захист, благонадійність процесу передавання інформаційних даних, глибока нейронна мережа, система штучного інтелекту.

Vasylkivskyi M., Budash M., Boldyreva O. Ensuring information security in 6G telecommunication networks. Autonomous information security, which will be one of the key functions of creating a reliable architecture of the 6G telecommunication network, is considered. Features of system and end-user protection against attacker attacks as they occur using the proposed network architecture and proactive approach are determined. By combining autonomous information security technologies with system architecture, the possibility of creating dynamic intelligent protection using machine learning and an artificial immune system is considered. Prospects for the wide spread of technologies based on artificial intelligence and machine learning for solving information security problems are considered. In particular, the detection of information security problems has been improved, recommendations have been offered to analysts, which will reduce the incident response time from hundreds of hours to seconds and increase the productivity of analysts from one or two incidents to thousands per day.

The reliability of the information data transfer process is considered as a determining factor of information protection from the point of view of communication. The main scientific evidence to form a correct conclusion about whether a 6G telecommunications network is trustworthy is based on its functional parameters, which indicate the level of reliability expected from the implementation of 6G technologies. As a result, it is determined that the reliability of the 6G telecommunication network inherits the excellent functionality and best practices of the previous generation networks, and also takes into account various disciplines and social issues.

The impact of deep neural network (DNN) reliability on the evaluation of artificial intelligence systems is investigated, taking into account that massive real-world data sets are used to train artificial intelligence, which can lead to data leakage, forgery, theft, and misuse due to lack of proper protection.

Keywords: telecommunication network architecture, dynamic intellectual protection, reliability of information data transmission process, deep neural network, artificial intelligence system.

Постановка наукової проблеми. Характеризуючи рівень довіри до чогось, люди найчастіше намагаються описати його за допомогою інженерної мови. В електронній комерції описані чотири загальні індекси довіри: сертифікат конфіденційності від третьої сторони, гарантії конфіденційності, сертифікат безпеки від третьої сторони та функції безпеки [1]. Серед них функції безпеки відіграють найбільшу роль у забезпеченні довіри споживачів до електронної комерції.

Вивчення ризиків почалося після того, як благонадійність почали розглядати як критерій інформаційної безпеки. При аналізі благонадійності будь-якого об'єкта враховують такі три чинники: джерело інформації, саму інформацію та одержувача. Ці три фактори також включають субфактори, наприклад, точність, достовірність. [2].

Результати вищезгаданих досліджень вказують, що благонадійність може бути визначена та виміряна лише за наявності певного сценарію, на який можна спиратися. Навіть за наявності такого сценарію без існування чіткого профілю надійності ставлення до відповідних факторів залежить від окремих осіб. При цьому, «важливість цих факторів може оцінюватися по-різному залежно від людини, яка приймає рішення щодо довіри, а також від ситуації, оскільки така власне суб'єктивна природа довіри» [3].

Зростання важливості благонадійністі інфраструктури інформаційних та комунікаційних технологій (ІСТ) зумовлено технологічним розвитком, що супроводжується співіснуванням фізичного та цифрового світів. Вона значною мірою впливає на бажання користувачів підписувати контракти на послуги, що надаються інфраструктурою. Таким чином, усі зацікавлені сторони у сфері ІСТ потребують благонадійності.

Рекомендація ITU-T X.509 визначила необхідність довіри у сфері ІСТ. «Як правило, можна сказати, що об'єкт "довіряє" другому об'єкту, коли перший об'єкт робить припущення, що другий об'єкт поводитиметься точно так, як очікує перший об'єкт» [4]. Організація ITU проводить стандартизацію довіри в телекомунікаційній галузі з 2015 року, особливо в галузі інтернету речей, послідовно публікуючи технічні звіти, документи та стандарти рекомендацій [1–3]. У документах пропонується концепція довіри та її класифікація як з архітектурної, так і з технічної точки зору. Разом із пропозиціями щодо стратегії забезпечення довіри в системі ІСТ були представлені рекомендації щодо аналізу довіри в мережі, кібербезпеки та IoT. Науковою проблемою є необхідність визначення благонадійності телекомунікаційної мережі 6G із врахуванням інформаційного захисту систем доступу та кінцевих користувачів від атак зловмисників.

Метою роботи є: підвищення інформаційної безпеки телекомунікаційних мереж із використанням штучного інтелекту та машинного навчання за рахунок ключових функцій благонадійної архітектури 6G.

Аналіз досліджень. Дослідження благонадійності почалося з інтернету речей, і тепер охоплює всю екосистему зв'язку. Благонадійність кіберфізичної системи визначається як «доказова ймовірність того, що система працюватиме відповідно до заданої поведінки за будь-якого набору умов, що підтверджується її характеристиками, включаючи безпеку, захищеність, конфіденційність» [4].

Всі галузеві дослідження, визначення та довідкові поняття зрештою спрямовані на забезпечення користувачів надійним комунікаційним середовищем, і тому об'єктивні та суб'єктивні фактори неодноразово ставали предметом суперечок. В результаті, продовжуються дослідження, спрямовані на досягнення благонадійності у сфері ІСТ. При цьому розроблено багато моделей, включаючи засновану на онтології методику, запропоновану для аналізу взаємозалежності і конфліктуючих вимог протягом усього життєвого циклу CPS [5]. Крім того, були проведені дослідження щодо практичного застосування моделі вимірювання довіри на основі теорії ігор, що описує надійність комунікації радарної діаграми, підходу до оцінювання ризиків на основі хмарної моделі та різних інших рішень [6].

Постачальники та інтегратори рішень доклали чимало зусиль для задоволення і навіть перевищення потреб користувачів і постійно коригують вимоги до надійності своїх продуктів, щоб не відставати від запитів користувачів. Наприклад, вимоги споживачів значно розширилися, і тепер недостатньо приділяти увагу довірі лише на етапі розробки, оскільки споживач очікує безперервного впровадження найкращих галузевих практик та стандартів аж до активної участі розробника у створенні здорового екологічного середовища в галузі телекомунікаційних технологій [7].

Визначальним фактором інформаційного захисту є благонадійність процесу передавання даних з погляду комунікації. Основні наукові докази для формування правильного висновку про те, чи заслуговує на довіру телекомунікаційна мережа 6G базуються на її функціональних параметрах, які свідчать про рівень благонадійності, яку очікуємо від впровадження технологій 6G. В результаті, можна скласти уявлення про благонадійність мережі 6G, розглядаючи, як вона успадковує чудові функціональні можливості та передовий досвід мереж попереднього покоління, а також зважаючи на різні дисципліни та соціальні проблеми.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. Без сумніву, мобільний зв'язок як найважливіша інфраструктура, що з'єднує фізичний та цифровий світи. Вона продовжує передавати інформацію між людьми, між речами, а також між людьми та речами. З швидким розвитком комунікаційних технологій можливості передачі стають дедалі більш

просунутими та різноманітними. Люди звикли до інформаційного комфорту, який забезпечують комунікаційні мережі: сімейне спілкування, телеконференції, ведення бізнесу та інші справи, які тісно пов'язані з людьми, а також дослідження незвіданого у Всесвіті.

Єдиним адекватним критерієм збільшення зацікавленості благонадійністю мереж зв'язку є думка звичайних користувачів, оскільки вони очікують, що благонадійні мережі будуть надавати стабільні послуги, захищати особисту інформацію та не завдавати фізичних травм. У свою чергу корпоративні клієнти оцінюють благонадійність своїх мереж з точки зору стабільності роботи, високої якості зв'язку, відсутності витоку конфіденційної інформації, відсутності зловмисних вторгнень [1]. Розмірковуючи про благонадійність мережі 6G необхідно враховувати всі ці фактори, оскільки благонадійність системи зв'язку є багатогранним поняттям.

До аспектів благонадійності можна віднести використання технологій, дотримання законів та постанов, погодження та спільні дії, а також позитивні переконання користувачів. Кожен із цих аспектів має свою характеристику та особливості. Технологія служить сполучною ланкою для інших показників. Отже, необхідно використовувати всі технології, що сприяють створенню надійної мережі, наприклад, криптографію, аналіз даних, машинне навчання та оцінку безпеки. Закони та постанови, оскільки «правила створюються та дотримуються за допомогою соціальних чи урядових інститутів» [2], закони та постанови постійно впливають на стабільність телекомунікаційного ринку. З того моменту, як технологія 5G почала набирати обертів, різні країни почали активно розвивати та доопрацьовувати свої закони та постанови в галузі кібербезпеки, безпеки зв'язку та захисту конфіденційності. При цьому, в індустрію зв'язку було впроваджено відповідні стратегії та заходи щодо тестування, оцінювання та перевірки телекомунікаційного обладнання, станційних пристроїв та цілих мереж. Постійна розробка цих законів визначає обов'язки зацікавлених сторін, а також поступово готує весь технологічний ланцюжок до створення надійнішої мережі [2–4]. Співпраця організацій, які займаються розробкою глобальних стандартів, є важливою рушійною силою співробітництва. За історичний період між технологіями 2G та 5G мережа зв'язку перейшла від простих телефонних дзвінків та служб коротких повідомлень до надання різних галузевих послуг. Цього було неможливо досягти без співпраці всіх зацікавлених сторін екосистеми. Широко відомі спільноти ITU, 3GPP, асоціація GSM (GSMA) та альянс мобільних мереж наступного покоління (NGM-N) надають зацікавленим сторонам можливості вільно обговорювати технології та бізнес. Спираючись на знання та натхнення, отримані від цих платформ, комунікаційна мережа поступово переходить від закритої структури до відкритої. Завдяки відкритості та доступності мережі починає розвиватися міжгалузева співпраця, і різні галузі промисловості співпрацюють між собою, щоб надавати користувачам індивідуалізовані та високоякісні послуги.

Для прикладу можна навести специфікації 3GPP R16, які підтримують два важливі індустріальні сектори (автомобілебудування та промислову автоматизацію). Версія R16 також допомагає «іншим галузям, таким як транспорт (наприклад, майбутня система мобільного зв'язку для залізниць) та ЗМІ (наприклад, широкосмугове мовлення в мережі 5G)» [5].

Прагнення спільноти з інформаційної безпеки розвивати співпрацю пов'язано з тим, що сектор інформаційної безпеки може більш адекватно та ефективно протистояти атакам завдяки аналізу загроз та обміну технологіями, а також спільній роботі членів спільноти. У зв'язку з цим девіз всесвітньо відомого заходу інформаційної безпеки RSA Conference звучав так: «ділитися, вчитися і захищати» [6]. Така співпраця дасть людям можливість «здобути вигоду з ідей та взаємин, які можуть сформувати майбутнє інформаційної безпеки» [7]. Довіра є найефективнішим фактором, оскільки коли користувачі судять про те, чи заслуговує комунікаційна мережа довіри, їх міркування переважають над усіма іншими показниками. В результаті, виникає необхідність у великих наукових та технічних знаннях, які допоможуть досягти погодження щодо розуміння технології та відповідних методик. Іншими словами, конвергенція більшої кількості розумів і рук більшою мірою сприятиме розвитку вдосконалених комунікаційних інновацій у майбутньому.

Достовірність оцінювання благонадійності характеризується факторами: процесом оцінювання, методом оцінювання та невизначеності або несподіваності події [8].

Благонадійність є життєво важливою, оскільки людське суспільство безперервно змінюється, конотації благонадійності та методи, прийняті для її досягнення, залишаються стійкими, якщо вони безперервно оптимізуються, розвиваються та оновлюються.

В основі благонадійності 6G лежать два принципи: початкової благонадійності та балансу.

Принцип 1 полягає в можливості забезпечення благонадійності різноманітності послуг мережі

6G. В результаті, користувачі очікують отримати від мережі 6G найрізноманітніші послуги, починаючи від скануючої мережі та закінчуючи дистанційною системою охорони здоров'я з тактильним зворотним зв'язком та низькоорбітальними супутниками. При цьому, різноманітна структура мережі 6G, її послуги та вимоги користувачів зроблять телекомунікаційну мережу винятковою у всіх сенсах цього слова. Так само різноманітними повинні бути і втілення благонадійності. Мережа 6G, що охоплює різні технічні та ділові аспекти, може вимагати великого набору можливостей забезпечення благонадійності, які можна використовувати як для суворого та централізованого керування доступом у централізованій частині мережі, так і для розпізнавання користувачів, а також їх авторизації у частині автономної периферії. Благонадійність повинна розвиватися протягом усього життєвого циклу 6G, включаючи її проектування, розробку та експлуатацію. На даний момент можливо визначити вимоги благонадійності лише оцінивши їх характеристики на етапі проектування 6G. Отже, при розробці продуктів 6G написання програмного коду та виробництво обладнання відповідатимуть проектним вимогам попереднього етапу. Тому механізм довіри в середовищі 6G слід експлуатувати та розгортати з регулярними та безперервними поліпшеннями на кожному етапі [1].

Принцип 2 пояснює принцип досягнення благонадійності в мережі 6G, який має враховувати три фактори: початкову довіру до клієнтів, вартість атак та швидкість відновлення діяльності. Якщо розробники технології 6G спочатку мало довіряють клієнтам мережі, то навіть якщо вони сподіваються, що вартість атак для зловмисника буде високою/або відновлення буде швидким, їм доведеться передбачити більше контрзаходів і строгих обмежень. Клієнтами мережі 6G можуть бути програми для операцій з ресурсами в мережі 6G, включаючи доступ до мережі для пристроїв, доступ до бази даних додатками, зв'язок між функціональними модулями, доступ до журналу. Вартість атак вказує, що зловмисники атакують тільки тоді, коли їхня вигода перевищує вартість атаки. Механізми, які використовуються для відновлення нормальної роботи або обслуговування, повинні бути здатні швидко нейтралізувати атаки як динамічно, так і безперервно [2].

На практиці надійні архітектури телекомунікаційної мережі зазвичай розробляються разом з певною початковою довірою до клієнтів, виходячи з чого пропонуються рішення щодо керування доступом на ранніх етапах процесу проектування, що ускладнює процес передбачення вартості атак та можливості відновлення.

У деяких сценаріях роботи сучасних телекомунікаційних мереж пред'являються підвищені вимоги до рівня безпеки під час обміну даними з малою затримкою, а це означає, що зловмисники повинні докласти більше зусиль, щоб досягти успіху, тоді як в інших сценаріях це просто звичайні телефонні дзвінки. Очевидно, що ці сценарії по-різному характеризують інформаційний захист від зловмисників, тому співвідношення вартості атаки і вигоди також відрізняється. Крім того, швидкість, з якою може бути відновлено нормальне обслуговування при атаці, у цих двох сценаріях також різниться. З цих причин збалансована довіра може здатися простою, але насправді відповідати всім вимогам складно.

З технологічної точки зору трьома основними характеристиками благонадійності є безпека, приватність та стійкість до відмов, які реалізуються за допомогою технологій криптографії та захисту. Для наочності, їх називають трьома стовпами благонадійності, які спираються на десять блоків (три аспекти безпеки, два аспекти конфіденційності та п'ять аспектів стійкості), як показано на рис. 1. Три стовпи і десять блоків є фундаментом, на якому побудована благонадійність телекомунікаційної мережі 6G [3].

Досягнення благонадійності мережі 6G вимагає вбудованої архітектури благонадійності, яка відповідає характеристикам безпеки, приватності та стійкості до відмов і заснована на інклюзивній моделі довіри. Така архітектура має охоплювати весь життєвий цикл мережі 6G, не залишаючи прогалин. В результаті, визначено три задачі щодо трьох вищезгаданих стовпів та десяти блоків.

Задача 1 полягає в збалансованій безпеці. Так звана тріада AIC – доступність, чесність та конфіденційність є фундаментальними компонентами безпеки. Баланс – це один із принципів вбудованої благонадійності, тобто для різних активів/власності, що захищаються, може знадобитися різний рівень захисту або різна вага кожного аспекту відповідно до різних сценаріїв.

Задача 2 полягає в постійному захисті конфіденційності, оскільки конфіденційність зазвичай передбачає право людей контролювати або впливати на те, яка інформація, пов'язана з ними, може збиратися і зберігатися, а також ким і кому ця інформація може бути розкрита [4]. Для захищення інформації про особу та поведінку користувачів, у їх розпорядження надаються такі технології, як криптографія, яка забезпечує гарантування, що тільки уповноважені користувачами сторони

можуть інтерпретувати зміст інформації, що передається між ними.

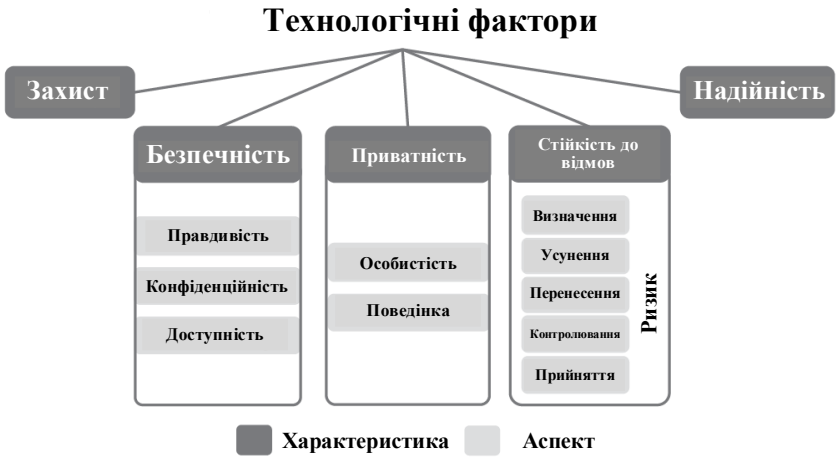

Рис. 1. Технологічні фактори забезпечення благонадійності телекомунікаційної мережі

Задача 3 полягає в розумній стійкості, тобто здатності мережі забезпечувати та підтримувати прийнятний рівень обслуговування перед різними збоями та проблемами, пов'язаними з нормальною роботою. При цьому, аспекти стійкості визначаються набором здібностей та інструментів, що дозволяють визначати та вимірювати ризики. Тому, для виявлення ризиків можуть використовуватися ситуаційна поінформованість та аналітика великих даних, а потім слідують дії, що дозволяють уникнути ризиків. В результаті, можна передавати всі або деякі ризики іншим сторонам, полегшуючи відновлення телекомунікаційної мережі або формувати передумови для мінімізації наслідків. У підсумку, доцільно приймати залишкові ризики, які не завдають шкоди телекомунікаційним мережам [5, 7].

Для підтримання здатності швидкого реагування на загрози та ризики необхідно постійно вимірювати благонадійність телекомунікаційної мережі. Рівень довіри можна виміряти за допомогою кількісного методу, аналогічного тому, що використовується для оцінки якості обслуговування (QoS) або якості досвіду (QoE). Незалежно від підходу, визначення конкретного рівня довіри залежить від зв'язаних служб і додатків. Рівень довіри можна визначити як кількісну оцінку довіри до персони, здібностей, властивостей чи істинності щодо когось чи чогось [8].

Можна здійснювати аналіз ризиків кількісно або якісно. Перший підхід застосовується для присвоєння грошового чи просто числового значення всім елементам процесу аналізу ризиків. Другий використовує рейтингову систему для перегляду різних сценаріїв з різними можливими ризиками та ранжування серйозності загроз та обґрунтованості різних можливих контрзаходів на основі суб'єктивних поглядів людей [3]. За результатами аналізу ризиків можна оцінити ефективність існуючих механізмів безпеки та необхідність вжиття контрзаходів для зниження загального ризику до прийнятного рівня.

Отже, три стовпи та десять блоків є основою архітектури благонадійності мережі 6G і на основі інклюзивної моделі довіри можна розробити вбудовану архітектуру благонадійності. В результаті, почавши зі створення моделі довіри і потім вивчивши відповідні технології, можна побудувати надійну телекомунікаційну мережу 6G.

Довіра користувачів до існуючої мережі формується операторами мобільних мереж (MNO), які купують та розгортають мережне обладнання, що вже пройшло всілякі тести та перевірки. Для керування користувачами оператори мобільних мереж використовують централізовані засоби автентифікації та авторизації. Така модель довіри може зіткнутися з багатьма проблемами на шляху до досягнення трьох задач благонадійності мережі 6G. Наприклад, нелегко забезпечити детальний централізований контроль доступу, який би відповідав як високому рівню безпеки, необхідному для централізованих фінансових сценаріїв, так і полегшеному механізму безпеки для збору локалізованих даних сканування. Крім того, важко встановити миттєву довіру між партнерами, що співпрацюють, і одночасно не вистачає ефективного рішення для керування цифровими ідентифікаційними даними.

Вбудованість різних сервісів мережі 6G визначає перший принцип, пов'язаний з формуванням

благонадійності. У цьому випадку використовується модель багатосторонньої довіри, що відображає різні варіанти довіри, включаючи три режими: міст, погодження та схвалення, як показано на рис. 2.

Основною особливістю моделі є децентралізоване багатостороннє погодження з одночасною централізованою довірою та стороннім схваленням. Режим мосту передбачає встановлення довіреного мосту між об'єктами через структуру авторизації з центральною точкою, такий як центр політики безпеки або керування безпекою профілів користувачів. При цьому, довіра буде отримана з поточної моделі довіри. Погодження передбачає процес створення більш стійких та інтелектуальних систем зв'язку, який зрештою зводиться до довіри між сторонами, які можуть бути компонентами мережі, різними сторонами схеми поставок або ролями промислової екосистеми. У цьому режимі транзакції підтверджуються та відповідальність розподіляється між кількома сторонами. Основними характеристиками даного режиму є висока ефективність та масштабованість, що відповідають гнучким та адаптованим вимогам доступу до мережі 6G. В режимі підтвердження авторитетна третя сторона вимірює та оцінює благонадійність мережі. На рис. 2, показано, що сторона B може запросити третю сторону для визначення, чи заслуговує на довіру сторона A, і третя сторона може підтвердити благонадійність сторони A.

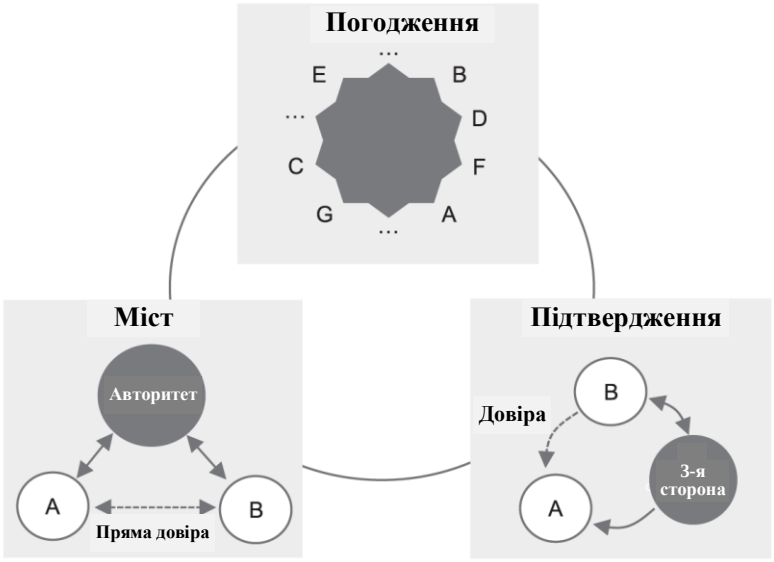

Рис. 2. Модель багатосторонньої довіри до телекомунікаційних технологій

Дані або інформація про транзакцію, які потребують схвалення третьої сторони, можуть бути швидко та справедливо записані та підтверджені у режимі погодження. Крім того, погодження є ключовим доповненням до взаємної довіри у сценаріях граничних автономних послуг.

Три вищезгадані режими взаємопов'язані і можуть спільно використовувати ключові технології, такі як криптографічні алгоритми та протоколи, які адаптовані до нових сценаріїв та архітектури мережі 6G. При цьому, розподіл і повна інтеграція мережевих та обчислювальних ресурсів передбачають гнучку та просту архітектуру безпеки з нульовою довірою, яка застосовується до децентралізованих мереж.

Для кожної сторони розглянутої потрійної моделі (тобто мосту, погодження та схвалення) повинні бути належним чином розв'язані всі завдання (збалансована безпека, постійний захист конфіденційності та інтелектуальна стійкість). Однак нові технології, такі як штучний інтелект та післяквантова криптографія, змінюють глибинні засади благонадійності, побудованої на традиційних механізмах. Тому, для забезпечення благонадійності телекомунікаційної мережі 6G, необхідно використовувати нові методи інформаційного захисту від сучасних кібератак.

В блокчейні із використанням криптографії кожен блок схеми містить криптографічний хеш попереднього блоку, мітку часу та дані транзакції. Розподілений реєстр (distributed ledger) не потребує такої схеми чи доказу роботи, оскільки технологія розподіленого реєстру (DLT) підходить для багатьох сценаріїв, мережевих архітектур та додатків. Дана технологія, по суті, є базою даних активів, яка може використовуватися кількома сайтами, установами або географічними регіонами

[4]. Блокчейн є одним з різновидів розподіленого реєстру, а також існують таблиці розподіленого реєстру, не пов'язані з блокчейном, розподілена криптовалюта та особлива архітектура бази даних [5].

Незважаючи на певні переваги, сучасний блокчейн все ще має обмеження. Недостатня гнучкість зумовленим тим, що блокчейн спочатку спроектований так, щоб бути незмінним, завдяки чому може бути досягнута як висока достовірність доказів несанкціонованого доступу, так і висока стійкість. В багатьох сценаріях ця незмінність забезпечує надійність надання фінансових послуг, однак у численних сценаріях використання зв'язку в реальному часі деякі дані повинні бути зміненими з різних причин, наприклад змінюється або програмований параметр протоколу зв'язку або віртуальної обчислювальної схеми. При цьому, за певних обставин дані вважатимуться дійсними і заноситимуться до розподіленого реєстру блокчейну. Низька швидкодія зумовлена тим, що схема блоків біткоїнів може обробляти лише від трьох до семи транзакцій за секунду на відміну від деяких застарілих систем обробки транзакцій, які можуть обробляти десятки тисяч транзакцій за секунду. Відповідний показник для блокчейну Ethereum [3] складає всього п'ятнадцять транзакцій на секунду, і тому технологія блокчейну не підходить для великомасштабних додатків через її відносно низьку швидкодію.

Неповні моделі безпеки зумовлені тим, що багато сучасних блокчейн-технологій уразливі до різних типів атак. При цьому, деякі проекти покладаються на певні погоджувальні алгоритми (рекурсивні виклики), які, містять уразливості, такі як атаки децентралізованої автономної організації (DAO) у смарт-контракті Ethereum [3]. Іншою проблемою моделі інформаційної безпеки блокчейну є використання квантових обчислень [4], які потенційно можуть зробити вразливими криптографічні механізми та протоколи, що лежать в основі блокчейна.

Погодження може виявитися найважливішим режимом у моделі багатосторонньої довіри, оскільки мережева архітектура 6G матиме тенденцію до розподіленого характеру. В даний час блокчейн-подібна технологія, ймовірно, досягла зрілості, хоча різні нові застосування блокчейну все ще з'являються. Основна проблема полягає в тому, як забезпечити відповідність DLT наступним вимогам технології 6G. Надвисока пропускна здатність та наднизька затримка, оскільки на відміну від традиційного блокчейну, в якому погодження досягається повільно, нові алгоритми та архітектура блокчейна зможуть задовольнити ці вимоги шляхом введення нових погоджувальних та криптографічних алгоритмів. Висока доступність та надійність, оскільки для досягнення високої операційної ефективності мережі 6G потребують простих механізмів керування та функціонування. При цьому показники доступності та надійності не тільки не повинні постраждати, а й мають бути покращені. У зв'язку з цим можна підвищити доступність, запровадивши блокчейн-технологію. Іншими словами, операції мережі 6G повинні бути спроможними витримати певний рівень збоїв або зловмисних атак, не вимагаючи значного втручання людини. Надійний захист конфіденційності та цифровий суверенітет, оскільки коли справа доходить до захисту конфіденційності, необхідно дотримуватись законів та правил захисту персональних даних (наприклад, GDPR), які можуть відрізнятися в різних країнах чи регіонах. Для цього можна використати технологію розподіленого реєстру. Проте більшість законів та правил передбачають право особистості видаляти дані про себе із системи («право на цифрове забуття»), що суперечить обов'язковій незмінності блокчейна [5]. Сучасні структури блокчейнів засновані на схемах хешування, і значення хеш-функції надзвичайно складно змінити після запису транзакції в схему блоків. При цьому, у випадку подальшого внесення змін передбачено запуск хардфорка [2], який створює вразливості в системі інформаційної безпеки. В результаті, хардфорк може вплинути на багато існуючих записаних блоків, і на повторну перевірку транзакції йде багато часу. Тому необхідно дослідити можливість зміни чи редагування транзакцій, не впливаючи на інші блоки.

Квантові комп'ютери можуть ефективно вирішувати складні математичні завдання (наприклад, NP-важкі), тобто цілочисленну факторизацію або дискретне логарифмування, «тим самим роблячи всі криптосистеми з відкритим ключем, що засновані на припущенні складності обчислень, марними» [3].

До появи реальних квантових комп'ютерів необхідно розглянути багато вразливостей традиційних схем. Наприклад, зловмисник може зберегти сьогоднішні повідомлення з обміном ключами та зламати їх у майбутньому. Виходить, що обмін ключами з використанням методу Діфі-Хелмана (DH) вже вразливий. При побудові та використанні великомасштабних квантових комп'ютерів необхідно буде протистояти як квантовим, і класичним комп'ютерним противникам [4]. Національний інститут по стандартизації та технології (NIST) здійснює розробку

квантовобезпечних стандартів криптографії з відкритим ключем, включаючи схеми для шифрування/створення ключів та цифрові підписи [5].

В сфері промисловості основну діяльність у галузі післяквантової криптографії (PQC) здійснюється технологічними гігантами. Наприклад, Google експериментував з реалізацією «нової надії» [6] у версії Canary браузера Chrome протягом кількох місяців, щоб оцінити вплив гібридних схем, а Thales реалізував провідні алгоритми-кандидати та додав їх у популярні криптографічні програми з відкритим вихідним кодом [7] .

Крім того, Microsoft реалізує PQC у рамках відкритого VPN для проекту з відкритим вихідним кодом [8], який включає три різні протоколи PQC: Frodo-KEM, SIKE та Picnic.

Згідно з аналітичним звітом RAND Corporation, «використання квантових комп'ютерів, що здатні виконувати криптографічні програми, очікується в середньому приблизно через 10 років – близько в 2033 р. Проте, за оцінками експертів, це може статися як раніше, так і пізніше» [3]. В епоху 6G, коли стануть доступні великомасштабні квантові розрахунки, доведеться використовувати відповідну архітектуру безпеки. Отже, вже сьогодні потрібно проаналізувати характеристики алгоритмів PQC та оцінити можливості їх адаптації до протоколів 6G. Один із можливих способів вирішення цієї проблеми полягає в розробці спеціалізованих алгоритмів PQC, який зможе гарантувати, що вони забезпечують адекватну гнучкість для застосування в мережах 6G і в той же час зможуть застосовуватися в існуючих платформах. При цьому, алгоритми та протоколи PQC мають підтримувати гнучку структуру мережі 6G, таку як гнучкі рівні безпеки, розміри коду та підписи, які можна адаптувати до встановлених протоколів. Ці алгоритми також повинні забезпечувати підвищену гнучкість керування ключами, щоб відповідати різним розмірам ключів для різних протоколів.

Висновки та перспективи подальшого дослідження. Розглянуто автономну інформаційну безпеку, яка буде однією з ключових функцій створення благонадійної архітектури телекомунікаційної мережі 6G. Визначено особливості захисту систем і кінцевих користувачів від атак зловмисників у міру їх виникнення із використанням запропонованої архітектури мережі та проактивного підходу. Поєднавши автономні технології інформаційної безпеки з архітектурою системи розглянуто можливість створення динамічного інтелектуального захисту із використанням машинного навчання, штучної імунної системи. Розглянуто перспективи широкого поширення технологій на основі штучного інтелекту та машинного навчання для вирішення проблем інформаційної безпеки. Зокрема, здійснено покращення виявлення проблем інформаційної безпеки, запропоновано рекомендації аналітикам, що дозволить скоротити час відгуку на інцидент із сотень годин до секунд та підвищуючи продуктивність роботи аналітиків з одного або двох інцидентів до тисяч на день. Після розгортання в змодельованій мережі 6G модель зможе безперервно навчатися з використанням актуальних даних та покращувати свої показники. Крім того, виконуючи імітацію атак, автономні системи безпеки можуть допомогти операторам своєчасно створювати та налаштовувати ефективні політики безпеки.

Досліджено вплив надійності глибокої нейронної мережі (DNN) на оцінку систем штучного інтелекту із врахуванням, що для навчання штучного інтелекту використовуються масивні набори реальних даних, які можуть призвести до витоку, підробки, крадіжки та неправомірного використання даних через відсутність належного захисту.

Враховуючи відсутність стандартного визначення ключових показників ефективності (KPI) благонадійності доцільно зосереджуватись на технічних показниках, які можна використовувати для подальших наукових досліджень для спрощення процесу визначення KPI благонадійності телекомунікаційної мережі 6G. Розглянуті принципи досягнення благонадійності 6G забезпечать надійну інформаційну безпеку сучасних телекомунікаційних мереж.

Список бібліографічного опису

1. ITU-T, Draft Recommendation X.5Gsec-t, Security framework based on trust relationship for 5G ecosystem, 2019.
2. M. Balduccini, E. Griffor, M. Huth, C. Vishik, M. Burns, and D. Wollman, Ontology based reasoning about the trustworthiness of cyber-physical systems, IET Journal of IoT, June 2018.
3. M. Grieves, Digital twin: Manufacturing excellence through virtual factory replication, White paper, vol. 1, pp. 1–7, 2014.
4. M. J. Vermeer and E. D. Peet, Securing communications in the quantum computing age: Managing the risks to encryption, RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR3102.html.
5. Васильківський, М., Нікітович, Д., & Болдирева, О. (2022). Керування доступом до інформаційних даних в інтелектуальних інфокомунікаційних мережах. Measuring and computing devices in technological processes, (4), 5–17. https://doi.org/10.31891/2219-9365-2022-72-4-1

6. Васильківський, М., Варгатюк, Г., & Болдирева, О. (2022). Дослідження архітектури штучного інтелекту для інфокомунікаційних мереж 6G. Measuring and computing devices in technological processes, (4), 62–70. https://doi.org/10.31891/2219-9365-2022-72-4-7
7. Васильківський, М., Коломієць, А., & Грабчак, Н. (2022). Дослідження функціональних параметрів інфокомунікаційних мереж 6G. Вісник Хмельницького національного університету, (6), 46–52. https://www.doi.org/10.31891/2307-5732-2022-315-6-46-52
8. Васильківський, М., Коломієць, А., & Будаш, М. (2022). Оцінювання параметрів радіотрактів інфокомунікаційних систем 5G/6G. Вісник Хмельницького національного університету, (6), 53–60. https://www.doi.org/10.31891/2307-5732-2022-315-6-53-60

References

1. ITU-T, Draft Recommendation X.5Gsec-t, Security framework based on trust relationship for 5G ecosystem, 2019.
2. M. Balduccini, E. Griffor, M. Huth, C. Vishik, M. Burns, and D. Wollman, Ontology based reasoning about the trustworthiness of cyber-physical systems, IET Journal of IoT, June 2018.
3. M. Grieves, Digital twin: Manufacturing excellence through virtual factory replication, White paper, vol. 1, pp. 1–7, 2014.
4. M. J. Vermeer and E. D. Peet, Securing communications in the quantum computing age: Managing the risks to encryption, RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR3102.html.
5. Vasylkivskyi M., Nikitovych, D., & Boldyreva, O. (2022). Keruvannya dostupom do informatsiynykh danykh v intelektual′nykh infokomunikatsiynykh merezhakh. Measuring and computing devices in technological processes, (4), 5–17. https://doi.org/10.31891/2219-9365-2022-72-4-1
6. Vasylkivskyi M., Varhatiuk, H., & Boldyreva, O. (2022). Doslidzhennya arkhitektury shtuchnoho intelektu dlya infokomunikatsiynykh merezh 6G. Measuring and computing devices in technological processes, (4), 62–70. https://doi.org/10.31891/2219-9365-2022-72-4-7
7. Vasylkivskyi M., Kolomiets, A., & Hrabchak, N. (2022). Doslidzhennya funktsional′nykh parametriv infokomunikatsiynykh merezh 6G. Visnyk Khmel′nyts′koho natsional′noho universytetu, (6), 46–52. https://www.doi.org/10.31891/2307-5732-2022-315-6-46-52
8. Vasylkivskyi, M., Kolomiets, A., & Budash, M. (2022). Otsinyuvannya parametriv radiotraktiv infokomunikatsiynykh system 5G/6G. Visnyk Khmel′nyts′koho natsional′noho universytetu, (6), 53–60. https://www.doi.org/10.31891/2307-5732-2022-315-6-53-60.