ВСТУП

Актуальність теми. В умовах стрімкої цифрової трансформації суспільства електронні комунікаційні системи перетворилися на критично важливу інфраструктуру, що забезпечує функціонування економіки, державного управління та соціальної взаємодії. Глобальний перехід до хмарних обчислень, масове впровадження Інтернету речей (IoT) та розгортання мереж 5G призвели до експоненційного зростання обсягів даних, що передаються. Однак ця еволюція супроводжується безпрецедентним загостренням кіберзагроз, які ставлять під сумнів надійність традиційних механізмів захисту інформації.

Сучасні комунікаційні мережі, побудовані на класичних централізованих архітектурах та стандартних протоколах (TCP/IP, SMTP, DNS), демонструють суттєві вразливості. Централізація створює «єдині точки відмови» (Single Point of Failure), що робить системи вразливими до DDoS-атак та компрометації серверів баз даних. Крім того, традиційні методи аутентифікації та контролю доступу часто не здатні ефективно протидіяти складним атакам, таким як «людина посередині» (Man-in-the-Middle) або експлойти нульового дня, що призводить до витоків конфіденційної інформації та порушення цілісності даних.

У цьому контексті виникає нагальна науково-практична потреба в пошуку нових парадигм побудови захищених комунікацій. Технологія блокчейн, завдяки своїй децентралізованій природі, пропонує революційний підхід до вирішення зазначених проблем. Використання розподіленого реєстру дозволяє забезпечити незмінність історії транзакцій та унеможливити непомітну модифікацію даних, що є критичним для забезпечення цілісності. Криптографічні механізми блокчейну та технологія смарт-контрактів відкривають можливості для автоматизації процесів безпеки, знижуючи вплив людського фактору та адміністративних помилок.

Незважаючи на значний потенціал, інтеграція блокчейну в системи реального часу пов'язана з викликами масштабованості та швидкодії. Тому розробка та дослідження гібридних архітектур, які поєднують ефективність традиційних комунікацій з гарантіями безпеки блокчейну, є надзвичайно актуальним завданням.

Це дозволить створити стійкі до кіберзагроз системи, що відповідають високим вимогам сучасності щодо прозорості, довіри та захищеності інформаційного обміну.

Метою роботи є підвищення рівня захищеності, прозорості та надійності систем електронних комунікацій шляхом розробки та аналізу архітектури з інтегрованим блокчейн-компонентом.

Об’єкт дослідження — процеси забезпечення інформаційної безпеки в системах електронних комунікацій.

Предмет дослідження — методи та засоби захисту електронних комунікацій з використанням технології блокчейн, смарт-контрактів та криптографічних протоколів.

1. ТЕОРЕТИЧНІ ОСНОВИ БЕЗПЕКИ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

1.1. Сутність та структура електронних комунікаційних систем

У швидкозмінному ландшафті сучасного суспільства системи електронного зв'язку стали основою щоденної взаємодії, ділових операцій та поширення інформації. Ці системи сприяють передачі даних на величезні відстані з безпрецедентною швидкістю та надійністю, забезпечуючи рівень зв'язку, який колись був немислимим. Суть електронних комунікацій полягає в їхній здатності кодувати, передавати та декодувати інформацію електронними засобами, фундаментально змінюючи те, як люди та машини обмінюються знаннями. На відміну від традиційних методів зв'язку, таких як особисті розмови, поштові послуги чи телеграфія, електронні комунікації використовують цифрові та аналогові сигнали, що передаються через складні мережі, роблячи взаємодію більш ефективною та масштабованою. Розуміння структури цих систем передбачає вивчення їхніх основних компонентів, їхньої базової архітектури та того, як вони працюють разом для підтримки безперебійного потоку інформації в різних контекстах, від особистих повідомлень до глобальних фінансів [1].

Суть електронних комунікацій полягає в їхній ролі як основного засобу передачі, обробки та зберігання даних у сучасному інформаційному суспільстві. Ці системи лежать в основі практично кожної цифрової діяльності, незалежно від того, чи це надсилання електронних листів, потокове відео, проведення фінансових транзакцій чи ведення хмарних баз даних. Вони характеризуються здатністю швидко та точно обробляти великі обсяги даних, що є важливим для застосувань у реальному часі, таких як відеоконференції чи торгівля акціями. На відміну від традиційних засобів, таких як поштова пошта чи телефонні дзвінки, електронні комунікації використовують електричні сигнали, що передаються по дротових, бездротових або волоконно-оптичних каналах. Цей перехід забезпечує миттєве підключення між континентами, а пакети даних проходять складні маршрути до місця призначення. Наприклад, хмарні обчислювальні сервіси значною мірою

залежать від електронних комунікаційних систем для зберігання та отримання величезних обсягів даних, підтримуючи такі галузі, як охорона здоров'я, освіта та виробництво. Цифрова природа цих систем також дозволяє використовувати протоколи шифрування та безпеки, які захищають конфіденційну інформацію, що менш можливо за допомогою традиційних методів комунікації. Загалом, електронні комунікаційні системи відіграють центральну роль у функціонуванні сучасної цифрової економіки та суспільства, сприяючи інноваціям, співпраці та доступу до інформації (рис. 1.1) [2].

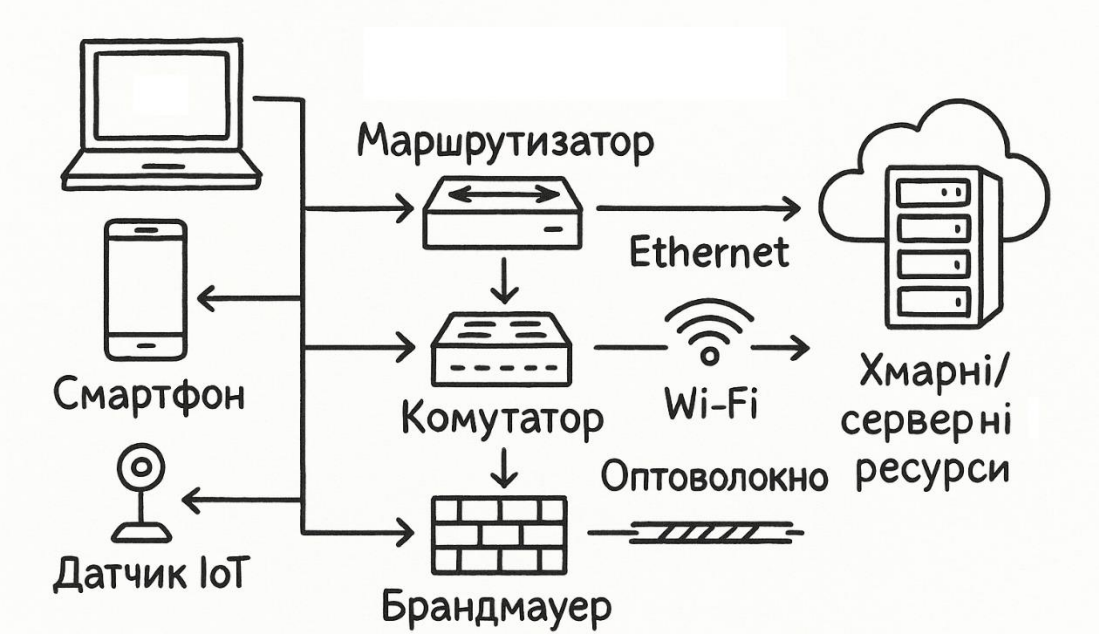


Рис. 1.1. Структурна схема електронної комунікаційної системи

Основними елементами, що складають електронні комунікаційні системи, є кінцеві пристрої, мережеве обладнання та канали зв'язку. Кінцеві пристрої – це обладнання, яке використовується користувачами або системами для надсилання та отримання даних, таке як комп’ютери, смартфони, сервери або датчики, вбудовані в пристрої Інтернету речей. Мережеве обладнання включає маршрутизатори, комутатори, модеми та брандмауери, які сприяють маршрутизації, фільтрації та забезпеченню безпеки даних у мережах. Канали зв’язку – це фізичні або бездротові носії, такі як мідні кабелі, оптоволоконні лінії, Wi-Fi або супутникові канали, які передають сигнали між пристроями та мережевою інфраструктурою. Ці елементи

регулюються набором протоколів, стандартів та інтерфейсів, що забезпечують сумісність та ефективність. Наприклад, пакет протоколів керування передачею/інтернет-протоколу (TCP/IP) є основоположним для інтернет-комунікації, забезпечуючи правила формування пакетів даних, адресації та маршрутизації. Такі стандарти, як Ethernet або Wi-Fi, визначають технічні характеристики, яким має відповідати обладнання для правильного функціонування в мережах, забезпечуючи сумісність та продуктивність. Програмні засоби для управління та моніторингу мережі, такі як брандмауери, системи виявлення вторгнень та мережеві аналізатори, також є життєво важливими, дозволяючи адміністраторам підтримувати справність системи, оптимізувати продуктивність та реагувати на загрози безпеці. Разом ці елементи утворюють складну, але цілісну систему, яка підтримує надійний та безпечний електронний зв’язок у різних середовищах. Архітектура електронних комунікаційних систем складається з різних рівнів та функціональних підсистем, призначених для організації та оптимізації процесів обміну даними. На концептуальному рівні логічна архітектура описує, як дані передаються в мережі, з акцентом на протоколах та форматах даних, тоді як фізична архітектура стосується матеріального обладнання та середовищ передачі. Модель OSI (взаємозв'язок відкритих систем) та модель TCP/IP – це дві фундаментальні структури, що визначають, як різні компоненти взаємодіють у мережі. Модель OSI складається з семи рівнів, від фізичного та канального рівнів до мережевого, транспортного, сеансового, презентаційного та прикладного рівнів, кожен з яких має певні ролі в управлінні передачею даних, виправленні помилок та безпеці. Наприклад, фізичний рівень обробляє передачу необроблених бітів по кабелях, тоді як прикладний рівень забезпечує взаємодію користувачів через веб-браузери або поштові клієнти. І навпаки, модель TCP/IP спрощує ці функції до чотирьох рівнів – канальний, інтернет-, транспортний та прикладний – зосереджуючись на практичній реалізації для Інтернету. Ці моделі ілюструють, як апаратні компоненти, програмні протоколи та інтерфейси користувача взаємодіють злагоджено, забезпечуючи сумісність та масштабованість. Логічна та фізична архітектури є невід'ємною частиною

проектування надійних мереж, таких як корпоративні інтрамережі, центри обробки даних або глобальна інтернет-інфраструктура, де ефективна взаємодія компонентів та багаторівнева організація є важливими для продуктивності та надійності.

Технологічні платформи та середовища, що лежать в основі електронних комунікаційних систем, різноманітні та постійно вдосконалюються, щоб відповідати вимогам взаємопов'язаного світу. Дротові технології, такі як Ethernet та волоконно-оптичні кабелі, забезпечують високошвидкісні та надійні з'єднання, необхідні для центрів обробки даних, корпоративних мереж та магістральної інфраструктури. На противагу цьому, технології бездротового зв'язку, включаючи Wi-Fi, стільникові мережі та супутникові канали, пропонують гнучкість та мобільність, дозволяючи пристроям безперешкодно підключатися до різних мереж. середовища. Поява хмарних середовищ та віртуалізованих платформ революціонізувала способи розміщення, управління та доступу до даних і послуг, що дозволило створити масштабовані, економічно ефективні та стійкі системи, що підтримують віддалену роботу, хмарні обчислення та глобальну співпрацю. Більше того, інтеграція передових технологій, таких як Інтернет речей (IoT), 5G та програмно-визначені мережі (SDN), перетворює традиційні мережі на інтелектуальні, адаптивні екосистеми. Пристрої IoT генерують величезні обсяги даних, що вимагає надійних каналів зв'язку, що забезпечує технологія 5G завдяки високій пропускній здатності та низькій затримці. SDN забезпечує динамічне управління мережею за допомогою централізованого контролю, підвищуючи гнучкість, безпеку та ефективність. Разом ці технологічні платформи та інновації формують майбутнє електронних комунікаційних систем, роблячи їх більш взаємопов'язаними, автоматизованими та здатними підтримувати зростаючі потреби розумних міст, автономних систем та цифрових підприємств.

Розвиток електронних комунікаційних систем відзначився значною еволюцією та постійними тенденціями, що відображають технологічний прогрес та суспільні потреби. Історично комунікаційні технології перейшли від ранніх телеграфних та телефонних систем до радіомовлення, супутникового зв'язку та появи Інтернету, кожен етап яких підвищував швидкість, охоплення та ємність.

Цифрова революція призвела до конвергенції голосових, інформаційних та мультимедійних послуг в єдині платформи, що суттєво змінило способи передачі та споживання інформації. Сьогодні тенденція до цифровізації продовжує прискорюватися, а системи зв'язку стають все більш інтегрованими та інтелектуальними, підтримуючи такі послуги, як відеоконференції, соціальні мережі та хмарні додатки. Ця конвергенція сприяє взаємодії між різними платформами та пристроями, створюючи безперебійний користувацький досвід. Однак ці досягнення також створюють проблеми безпеки, такі як витоки даних, кібератаки та проблеми конфіденційності. Для вирішення цих проблем нові рішення, такі як технологія блокчейн, пропонують багатообіцяючі перспективи, забезпечуючи децентралізовані, захищені від несанкціонованого доступу записи, що підвищують безпеку та надійність. У міру розвитку електронних комунікаційних систем балансування інновацій з безпекою та конфіденційністю залишається першочерговим для використання їхнього повного потенціалу на благо суспільства.

Підсумовуючи, системи електронного зв'язку є основоположними для функціонування сучасного суспільства, забезпечуючи швидку та надійну передачу, обробку та зберігання даних, що лежать в основі численних аспектів повсякденного життя та економічної діяльності. Їхні основні елементи – від кінцевих пристроїв та мережевої інфраструктури до протоколів та архітектурних рамок – працюють разом, щоб забезпечити безперебійну та безпечну взаємодію в різних середовищах. Технологічні платформи, що підтримують ці системи, включаючи дротові та бездротові технології, хмарні середовища та інноваційні інтеграції, такі як Інтернет речей, 5G та SDN, продовжують стимулювати прогрес та забезпечують створення розумніших, більш адаптивних мереж. Їхня еволюція від ранньої телеграфії до складних цифрових екосистем підкреслює постійні тенденції до цифровізації, конвергенції та підвищення безпеки. Оскільки такі проблеми, як кіберзагрози, зберігаються, нові рішення, такі як блокчейн, пропонують перспективні шляхи для захисту інформації та підтримки довіри. Зрештою, розуміння сутності та структури

систем електронного зв'язку висвітлює їхню життєво важливу роль у формуванні взаємопов'язаного, інноваційного та безпечного цифрового майбутнього.

1.2. Основні загрози та вразливості електронних комунікацій

У сучасну цифрову епоху електронні комунікації формують основу особистих, комерційних та урядових взаємодій по всьому світу. Зі зростанням залежності від цих цифрових каналів зростає і спектр загроз і вразливостей, які ставлять під загрозу їхню цілісність, конфіденційність та доступність. Ці загрози є багатогранними, охоплюючи технічні експлойти, атаки на основі програмного забезпечення та тактики соціальної інженерії, всі з яких можуть поставити під загрозу конфіденційну інформацію або порушити роботу комунікаційних послуг. Розуміння різних класифікацій цих загроз, а також їхніх основних вразливостей в архітектурі, протоколах, апаратному та програмному забезпеченні, є важливим для розробки надійних заходів безпеки. У цьому есе досліджуються основні загрози та вразливості, з якими стикаються електронні комунікації сьогодні, підкреслюючи складність та мінливий характер кіберризиків [3].

Ландшафт загроз електронним комунікаціям можна загалом класифікувати на три категорії: технічні загрози, програмні загрози та загрози соціальної інженерії. Технічні загрози, в першу чергу, пов'язані з отриманням зловмисниками несанкціонованого доступу до мереж або перехопленням переданих даних. Наприклад, хакери можуть використовувати вразливості в мережевій інфраструктурі для підслуховування комунікацій або введення неправдивої інформації, тим самим порушуючи цілісність та конфіденційність даних. Перехоплення даних може відбуватися через атаки «людина посередині», коли зловмисник таємно передає або змінює зв'язок між двома сторонами без їхнього відома. Модифікація даних є ще однією критичною проблемою, коли кіберзлочинці змінюють передану інформацію, що призводить до дезінформації або шахрайства. Програмні загрози охоплюють шкідливі програми, такі як віруси, шпигунські програми та шкідливі скрипти, призначені для зараження систем, крадіжки даних

або порушення роботи. Віруси можуть швидко поширюватися через вкладення електронної пошти або заражені веб-сайти, тоді як шпигунські програми приховано відстежують активність користувачів для збору конфіденційної інформації. Шкідливі скрипти, вбудовані в скомпрометовані веб-сайти або електронні листи, можуть виконувати небажані дії на пристрої користувача (табл. 1.1).

Таблиця 1.1.

Основні загрози та вразливості електронних комунікацій

Параметр	Характеристика	Приклад
Технічні загрози	Несанкціонований доступ, перехоплення, модифікація даних	Атака «людина посередині» (MitM)
Програмні загрози	Віруси, шпигунські програми, шкідливі скрипти	Віруси у вкладеннях email; spyware
Соціальна інженерія	Маніпуляція користувачами, інсайдерські ризики	Фішингові листи для викрадення паролів
Вразливості протоколів	Слабкості TCP/IP, DNS, SMTP, SIP	DNS-cache poisoning, підміна SMTP
Маршрутизація та тунелювання	Перехоплення або перенаправлення трафіку	MitM через недоліки маршрутизації
Вразливості шифрування	Слабкі або застарілі реалізації SSL/TLS	Прослуховування трафіку через слабкі TLS-конфігурації
Апаратні вразливості	Помилки прошивки, незахищені пристрої	Botnet Mirai (IoT)
Програмні вразливості	Експлойти ОС та додатків, відсутність патчів	Невиправлені вразливості Windows/Linux
Недоліки оновлень і сертифікації	Відсутність контролю патчів та перевірки обладнання	Невстановлені оновлення безпеки
Організаційні вразливості	Слабкі політики безпеки, поганий контроль доступу	Непослідовне управління аккаунтами
Людський фактор	Помилки користувачів, низька кіберосвіченість	Співробітник відкрив фішинговий лист
Вразливості зберігання та передавання	Незахищені сервери, передача без шифрування	Перехоплення даних під час передачі
Сучасні кіберзагрози	DDoS, MitM, 0-day експлойти, атаки на IoT	DDoS-атаки для зупинки сервісів
Перспективні засоби захисту	Блокчейн для підтвердження цілісності та автентичності	Децентралізована верифікація даних

З іншого боку, загрози соціальної інженерії використовують людську психологію, щоб маніпулювати окремими особами або інсайдерами, змушуючи їх розкривати конфіденційну інформацію або надавати несанкціонований доступ. Фішингові електронні листи, що імітують легітимне спілкування, обманюють користувачів, змушуючи їх розголошувати паролі або фінансові дані. Внутрішні ризики пов'язані з тим, що співробітники чи партнери навмисно чи ненавмисно витікають конфіденційні дані або надають доступ зловмисникам. Поєднання цих категорій загроз підкреслює багатогранний характер ризиків, з якими стикаються системи електронного зв'язку.

Окрім окремих загроз, вразливості, властиві архітектурі та протоколам комунікаційних мереж, значно підривають безпеку. Багато основних мережевих протоколів, таких як TCP/IP, DNS, SMTP та SIP, мають притаманні слабкості, якими можуть скористатися зловмисники. Наприклад, система доменних імен (DNS), яку часто називають телефонною книгою Інтернету, вразлива до атак отруєння кешу, які перенаправляють користувачів на шкідливі веб-сайти без їхнього відома. Аналогічно, простий протокол передачі пошти (SMTP), який використовується для передачі електронної пошти, не має надійних функцій безпеки, що робить його вразливим до підміни та перехоплення. Аутентифікація та керування сеансами також мають критичні вразливості; слабка політика паролів, неправильна реалізація тайм-ауту сеансу або недостатнє шифрування можуть дозволити зловмисникам захоплювати сеанси або видавати себе за легітимних користувачів. Протоколи маршрутизації та тунелювання, життєво важливі для спрямування трафіку через складні мережі, схильні до зловмисних маніпуляцій, таких як перехоплення маршрутів або атаки «людина посередині», які можуть перенаправляти або перехоплювати конфіденційні дані. Протоколи шифрування трафіку, такі як SSL/TLS, хоча й широко поширені, мають відомі слабкі місця, особливо коли використовуються застарілі версії або неправильно налаштовані, що піддає комунікації ризику прослуховування та втручання. Ці вразливості разом створюють середовище, де зловмисники можуть використовувати недоліки протоколу для

порушення цілісності даних та доступності системи, що підкреслює необхідність постійної оцінки та вдосконалення протоколів.

Апаратні та програмні компоненти також містять вразливості, що загрожують системам електронного зв'язку. Такі пристрої, як маршрутизатори, комутатори та кінцеві точки, часто містять помилки у своїй прошивці — низькорівневому програмному забезпеченні, що контролює роботу апаратного забезпечення, — які можуть бути використані зловмисниками для отримання постійного доступу або спричинення збоїв. Наприклад, вразливості прошивки в мережевих пристроях були використані в масштабних атаках, таких як інцидент з ботнетом Mirai 2016 року, в якому незахищені пристрої Інтернету речей використовувалися для запуску масованих розподілених атак типу «відмова в обслуговуванні» (DDoS). Операційні системи та програми постійно стають цілями через вразливості, які можна використовувати віддалено або локально; невиправлені експлойти в популярних ОС-платформах, таких як Windows або Linux, використовувалися для встановлення шкідливого програмного забезпечення або доступу до конфіденційних даних. Більше того, багато організацій нехтують належним контролем оновлень, патчів та сертифікації пристроїв, залишаючи системи вразливими до відомих вразливостей. Нездатність своєчасно застосовувати патчі безпеки або перевіряти автентичність пристроїв може створити прогалини, якими зловмисники легко користуються. Швидкий розвиток технологій вимагає суворого управління оновленнями та процесів сертифікації пристроїв для зменшення цих апаратних та програмних вразливостей, але недоліки в цих сферах створюють постійні загрози для безпеки електронних комунікацій [4].

Організаційні та інфраструктурні вразливості ще більше посилюють ризики, пов'язані з електронними комунікаціями. Багато організацій працюють з політиками безпеки, які є або неповними, або погано застосовуються, що призводить до прогалин у захисті та непослідовного контролю доступу. Слабкі політики щодо автентифікації користувачів, керування паролями та обробки привілейованих облікових записів можуть бути використані зловмисниками, які прагнуть проникнути в системи. Крім того, людський фактор залишається

критичною вразливістю; недостатня підготовка персоналу та обізнаність про найкращі практики кібербезпеки часто призводять до того, що співробітники стають жертвами фішингових схем або ненавмисного впровадження шкідливого програмного забезпечення в мережі. Людські помилки, такі як неправильне налаштування параметрів безпеки або неправильне поводження з конфіденційними даними, можуть бути такими ж руйнівними, як і технічні атаки. Окрім кадрових проблем, вразливості в системах зберігання, резервного копіювання та передачі даних становлять значну загрозу цілісності та доступності даних. Дані, що зберігаються на незахищених серверах або передаються без належного шифрування, можуть бути перехоплені або підроблені, тоді як неадекватні процедури резервного копіювання ускладнюють відновлення після таких атак, як програми-вимагачі або витоки даних. Взаємопов'язаний характер сучасної інфраструктури посилює ці ризики, підкреслюючи важливість комплексних політик безпеки, регулярного навчання персоналу та стійких практик управління даними для захисту систем електронного зв'язку від організаційних вразливостей.

В останні роки методи кібератак, спрямованих на електронні комунікації, швидко розвивалися, відображаючи зростаючу витонченість кіберзлочинців та зловмисників. Розподілені атаки типу «відмова в обслуговуванні» (DDoS) залишаються поширеними, перевантажуючи сервери та мережеву інфраструктуру надмірним трафіком, що порушує роботу сервісів, часто використовуються як відволікаючий маневр для інших зловмисних дій. Атаки типу «людина посередині» (MitM) продовжують викликати серйозне занепокоєння, особливо в незахищених або погано налаштованих мережах, де зловмисники перехоплюють і потенційно змінюють зв'язок між двома сторонами. Крім того, експлойти нульового дня — вразливості, невідомі постачальникам або не виправлені — становлять серйозну загрозу, оскільки зловмисники можуть скористатися цими недоліками до того, як буде запроваджено захист. Поширення пристроїв Інтернету речей (IoT) та систем мобільного зв'язку створило нові вектори атак, коли незахищені пристрої викрадаються для ботнетів або крадіжки даних. Ці вразливості посилюються зростаючою залежністю від мобільних платформ для конфіденційного зв'язку.

Однак нові технології, такі як блокчейн, пропонують перспективні рішення; його децентралізований та стійкий до несанкціонованого доступу характер може бути використаний для виявлення, запобігання або пом'якшення кібератак шляхом підвищення безпеки та цілісності обміну даними. Механізми автентифікації та перевірки транзакцій на основі блокчейну все частіше досліджуються для підвищення стійкості електронних комунікаційних мереж до кіберзагроз, що розвиваються.

Загрози та вразливості, з якими стикаються електронні комунікації сьогодні, є масштабними та багатогранними, охоплюючи технічні експлойти, слабкі місця протоколів, апаратні та програмні недоліки, організаційні недоліки та нові стратегії атак. Технічні загрози, такі як перехоплення та модифікація даних, програмне шкідливе програмне забезпечення та тактики соціальної інженерії, продовжують розвиватися, використовуючи як людські, так і технологічні слабкості. В основі цих загроз лежать фундаментальні вразливості в мережевих архітектурах, протоколах та прошивці пристроїв, на які зловмисники активно націлені, щоб поставити під загрозу цілісність даних та функціональність системи. Крім того, організаційні недоліки, такі як неадекватні політики безпеки, недостатня підготовка персоналу та незахищене управління даними, ще більше посилюють вплив кіберризиків. Ландшафт кіберзагроз є динамічним, а останні тенденції підкреслюють зростаючу складність DDoS-атак, експлойтів MitM, вразливостей нульового дня та нових векторів атак, що з'являються через Інтернет речей та мобільні пристрої. Тим не менш, технологічні інновації, такі як блокчейн, забезпечують перспективні шляхи для підвищення безпеки та виявлення загроз.

1.3. Методи та засоби забезпечення безпеки в сучасних комунікаційних мережах

В епоху, коли цифровий зв'язок лежить в основі майже кожного аспекту особистої, комерційної та урядової діяльності, забезпечення безпеки сучасних комунікаційних мереж стало першочерговим завданням. Оскільки кіберзагрози стають дедалі складнішими, життєво важливо розуміти низку методів та засобів, що використовуються для захисту конфіденційної інформації та підтримки цілісності, конфіденційності та доступності каналів зв'язку. У цьому есе досліджуються три фундаментальні основи безпеки мережі: криптографічні методи безпеки, механізми автентифікації та контролю доступу, а також інструменти захисту мережевої інфраструктури. Детально розглянувши ці стратегії, ми можемо оцінити, як вони разом сприяють створенню стійкого та надійного середовища зв'язку [5].

Криптографічні методи безпеки формують основу безпечного зв'язку, використовуючи різні механізми шифрування та цілісності для захисту даних від несанкціонованого доступу та втручання. Симетричні алгоритми шифрування, такі як Advanced Encryption Standard (AES), використовують один спільний ключ як для шифрування, так і для дешифрування, пропонуючи високошвидкісний захист, що підходить для шифрування великих обсягів даних, наприклад, для безпечної передачі файлів або VPN-зв'язку. І навпаки, асиметричне шифрування спирається на пару ключів — відкритий ключ для шифрування та закритий ключ для дешифрування — що сприяє безпечному обміну ключами та цифровим підписам; RSA та криптографія еліптичних кривих (ECC) є прикладами цього підходу. Цифрові підписи служать цифровими «відбитками пальців» для перевірки автентичності та цілісності повідомлень, дозволяючи одержувачам підтвердити, що дані походять з надійного джерела та не були змінені. Доповнюють ці криптографічні методи хеш-функції, такі як SHA-256, які генерують значення дайджесту фіксованого розміру, що представляють вміст даних; вони мають вирішальне значення для забезпечення цілісності повідомлення, оскільки навіть

незначні зміни створюють дуже різні хеші, попереджаючи одержувачів про потенційні компрометації. Разом ці криптографічні методи створюють багаторівневий захисний механізм, який забезпечує конфіденційність, автентичність та цілісність у сучасних комунікаційних мережах.

Механізми автентифікації та контролю доступу є важливими для перевірки особи користувачів та обмеження доступу до мережі для авторизованих осіб, тим самим запобігаючи зловмисним вторгненням та внутрішнім загрозам. Методи ідентифікації користувачів включають імена користувачів та паролі, біометричну автентифікацію (наприклад, розпізнавання відбитків пальців або обличчя) та цифрові сертифікати, видані довіреними центрами сертифікації (ЦС). Ідентифікація пристроїв додає ще один рівень, розпізнаючи апаратні або програмні облікові дані, гарантуючи, що лише довірені пристрої підключаються до конфіденційних мереж. Для ефективного управління дозволами використовуються різні моделі контролю доступу. Дискреційний контроль доступу (DAC) надає власникам ресурсів повноваження встановлювати права доступу; обов'язковий контроль доступу (MAC) забезпечує дотримання суворих політик на основі рівнів безпеки, часто використовується в урядових або військових контекстах; контроль доступу на основі ролей (RBAC) призначає дозволи на основі ролей користувачів, спрощуючи управління у великих організаціях.

Крім того, багатофакторна автентифікація (MFA) підвищує безпеку, вимагаючи кількох факторів перевірки — чогось, що користувач знає (пароль), чим володіє (токен безпеки) або чим є (біометричні дані), — що значно ускладнює несанкціонований доступ. Наприклад, використання багатофакторної автентифікації (MFA) у банківських додатках або корпоративних VPN значно знижує ризик компрометації облікових даних, тим самим захищаючи конфіденційну інформацію, що передається через комунікаційні мережі.

Захист базової мережевої інфраструктури є фундаментальним для підтримки безпечних каналів зв'язку, особливо в умовах постійного розвитку кіберзагроз. Брандмауери служать воротарями, моніторячи та фільтруючи вхідний і вихідний трафік на основі попередньо визначених правил безпеки для блокування шкідливих

пакетів даних. Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) доповнюють брандмауери, активно аналізуючи моделі трафіку для виявлення та реагування на підозрілу активність, таку як шкідливе програмне забезпечення або атаки типу «відмова в обслуговуванні». Віртуальні приватні мережі (VPN) забезпечують безпечні тунелі для передачі даних через загальнодоступні мережі, шифруючи трафік для запобігання підслуховуванню та атакам «людина посередині» (табл. 1.2) [6].

Бездротові мережі створюють додаткові проблеми через свою широкомовну природу; тому надійні протоколи шифрування, такі як WPA3, разом із надійними політиками паролів, є важливими для захисту бездротових каналів. Методи сегментації та маршрутизації трафіку, такі як VLAN та підмережі, допомагають ізолювати конфіденційні дані та обмежити поверхню атаки. Механізми фільтрації забезпечують дотримання політик, які дозволяють лише легітимний трафік, тоді як протоколи маршрутизації, такі як BGP та OSPF, можна налаштувати для виявлення аномалій та перенаправлення трафіку в обхід скомпрометованих вузлів. Разом ці інструменти захисту інфраструктури створюють зміцнене середовище, яке мінімізує вразливості та забезпечує цілісність даних і конфіденційність під час передачі.

Системи виявлення та моніторингу вторгнень є життєво важливими компонентами в постійних зусиллях щодо виявлення та зменшення кіберзагроз у режимі реального часу. Ці системи розроблені зі складними архітектурами, які аналізують мережевий трафік на наявність аномалій, що свідчать про шкідливу діяльність. Наприклад, системи виявлення аномалій трафіку використовують алгоритми машинного навчання та статистичні моделі для встановлення базової поведінки та позначки відхилень, які можуть сигналізувати про вторгнення, поширення шкідливого програмного забезпечення або витік даних. Такі системи часто інтегруються з іншими інструментами безпеки, щоб забезпечити повний огляд стану та безпеки мережі. Крім того, журнали подій та аналіз журналів відіграють вирішальну роль в аудиті безпеки, фіксуючи детальну інформацію. Записи мережевої активності, дій користувачів та системних подій (табл. 1.2).

Таблиця 1.2.

Методи та засоби забезпечення безпеки сучасних комунікаційних мереж

Метод	Характеристика	Приклад
Криптографічні методи	Захист конфіденційності, цілісності й автентичності даних	AES, RSA, ECC, SHA-256
Симетричне шифрування	Один ключ для шифрування і дешифрування	AES у VPN
Асиметричне шифрування	Пара ключів для шифрування та цифрового підпису	RSA, ECC
Цифрові підписи	Перевірка джерела та незмінності повідомлень	Сертифікат + підпис
Хеш-функції	Контроль цілісності даних	SHA-256
Автентифікація користувачів	Перевірка особи користувача або пристрою	Пароль, біометрія, сертифікати
Контроль доступу	Розмежування доступу до ресурсів	DAC, MAC, RBAC
Багатофакторна автентифікація (MFA)	Комбінація кількох факторів підтвердження	Пароль + токен + біометрія
Брандмауери	Фільтрація та моніторинг мережевого трафіку	Статичні/динамічні правила фільтрації
IDS/IPS	Виявлення та запобігання вторгненням	Виявлення аномального трафіку
VPN	Створення шифрованого тунелю для передачі даних	Захист від MitM
Захист Wi-Fi	Шифрування та політики доступу	WPA3
Сегментація мережі	Ізоляція трафіку та зменшення поверхні атаки	VLAN, підмережі
Моніторинг логів	Виявлення відхилень, аудит дій	Аналіз системних логів
Реагування на інциденти	Ізоляція, очищення, відновлення систем	Відновлення з резервних копій
Блокчейн	Децентралізована перевірка та незмінність	Розподілений реєстр для автентифікації
NFV/SDN	Гнучке керування функціями безпеки	Віртуальні брандмауери
AI/ML у безпеці	Аналіз загроз і виявлення аномалій	Моделі машинного навчання

Регулярний аналіз цих журналів дозволяє командам безпеки виявляти закономірності, відстежувати порушення та розуміти вектори атак, тим самим сприяючи прийняттю обґрунтованих рішень та зміцненню захисту. Після кібератаки оперативне реагування на інциденти та відновлення є вкрай важливими. Це включає ізоляцію уражених систем, видалення шкідливого програмного забезпечення, відновлення даних з резервних копій та застосування виправлень для усунення вразливостей. Ефективні плани реагування на інциденти в поєднанні з постійним моніторингом допомагають організаціям швидко стримувати загрози, мінімізувати збитки та відновлювати нормальну роботу з урахуванням отриманого досвіду для запобігання майбутнім порушенням. Загалом, системи виявлення та моніторингу вторгнень утворюють критичний рівень сучасної комунікаційної безпеки, забезпечуючи проактивний захист та швидке реагування на нові загрози.

Постійно з'являються інноваційні підходи для підвищення безпеки сучасних комунікаційних мереж поза традиційними методами. Технологія блокчейн пропонує багатообіцяючий потенціал для децентралізованої перевірки, забезпечуючи незмінні записи транзакцій, які можуть автентифікувати особи та обмін даними, не покладаючись на централізований орган. Цей підхід розподіленого реєстру значно зменшує кількість точок відмови та підвищує надійність цифрових транзакцій. Технології віртуалізації безпеки, такі як віртуалізація мережевих функцій (NFV) та програмно-визначені мережі (SDN), забезпечують динамічне та гнучке управління мережевою безпекою. NFV дозволяє функціям безпеки, таким як брандмауери та системи запобігання вторгненням, працювати як віртуальні екземпляри, які можна швидко розгортати або масштабувати за потреби, тоді як SDN забезпечує централізований контроль над мережевим трафіком, що дозволяє швидко переналаштовувати політики безпеки у відповідь на загрози. Крім того, інтеграція штучного інтелекту (ШІ) у процеси кіберзахисту трансформує виявлення та реагування на загрози. Системи на базі ШІ можуть аналізувати величезні обсяги даних, щоб виявляти тонкі шкідливі закономірності, адаптуватися до стратегій атак, що розвиваються, та автоматизувати дії реагування швидше, ніж оператори-люди. Ці передові підходи

разом розширюють межі безпеки зв'язку, пропонуючи більш стійкий, адаптивний та інтелектуальний захист від дедалі складніших кіберзагроз.

Забезпечення безпеки сучасних комунікаційних мереж вимагає багатогранного підходу, який охоплює криптографічні методи, надійну автентифікацію та контроль доступу, комплексний захист інфраструктури та інноваційні технологічні досягнення. Криптографічні методи, такі як симетричне та асиметричне шифрування, цифрові підписи та хеш-функції, формують фундаментальний рівень захисту цілісності, конфіденційності та автентичності даних. Механізми автентифікації, включаючи багатофакторну автентифікацію та контроль доступу на основі ролей, допомагають перевірити особу користувачів та обмежити несанкціонований доступ. Інструменти мережевої інфраструктури, такі як брандмауери, системи виявлення вторгнень/IPS та VPN, створюють безпечні канали зв'язку та захищають від зовнішніх загроз. Впровадження систем виявлення та моніторингу вторгнень дозволяє виявляти загрози в режимі реального часу, проводити ефективний аудит безпеки та швидко реагувати на інциденти, мінімізуючи збитки від кібератак. Нарешті, новітні технології, такі як блокчейн, віртуалізація та рішення безпеки на основі штучного інтелекту, революціонізують ландшафт, пропонуючи децентралізовані, гнучкі та інтелектуальні засоби захисту, які адаптуються до швидкозмінного середовища загроз. Разом ці методи та інновації утворюють комплексну систему безпеки, необхідну для підтримки цілісності, конфіденційності та стійкості сучасних комунікаційних мереж у все більш взаємопов'язаному світі [7].

1.4. Аналіз існуючих стандартів і протоколів захисту інформації

В епоху швидкої цифрової трансформації та повсюдного зв'язку, захист конфіденційної інформації став першочерговим завданням як для організацій, урядів, так і для окремих осіб. Складність сучасних інформаційних систем вимагає комплексних стандартів та протоколів, розроблених для забезпечення

конфіденційності, цілісності та доступності даних на різних платформах та мережах. Це есе заглиблюється в ландшафт існуючих стандартів та протоколів захисту інформації, виділяючи ключові структури, що лежать в основі глобальних зусиль у сфері кібербезпеки. Розглядаючи міжнародні стандарти, такі як серія ISO/IEC 27000 та рекомендації NIST, поряд з критично важливими протоколами шифрування та захисту даних, а також механізмами автентифікації та контролю доступу, цей аналіз має на меті забезпечити детальне розуміння структур, що підтримують безпечне управління інформацією в цифрову епоху.

Міжнародні стандарти формують основу систематичних та послідовних підходів до управління інформаційною безпекою в різних галузях та за кордоном. Серія ISO/IEC 27000, комплексний набір стандартів, розроблених Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC), слугує основоположною основою для створення, впровадження, підтримки та постійного вдосконалення систем управління інформаційною безпекою (СУІБ). Ця серія охоплює широку сферу застосування, враховуючи оцінку ризиків, засоби контролю безпеки та вимоги до дотримання вимог, тим самим дозволяючи організаціям адаптувати практику безпеки до своїх конкретних потреб, дотримуючись при цьому всесвітньо визнаних орієнтирів. Наприклад, ISO/IEC 27001 визначає вимоги до створення СУІБ, допомагаючи організаціям ефективно керувати своїми інформаційними активами та захищати їх. Доповнює ці стандарти ISO/IEC 15408, відомий як Загальні критерії, який забезпечує сувору основу для оцінки функцій безпеки IT-продуктів та систем. Його стандартизована методологія оцінки дозволяє зацікавленим сторонам оцінити, чи є заяви про безпеку достовірними та такими, що піддаються перевірці, сприяючи довірі до комерційного та урядового розгортання. Крім того, заслуговує на увагу роль Національного інституту стандартів і технологій (NIST) у формуванні політики безпеки електронних комунікацій. Спеціальна публікація NIST серії 800, включаючи широко прийняту Структуру кібербезпеки NIST, пропонує рекомендації, передовий досвід та технічні стандарти, що впливають на національну та міжнародну політику безпеки. Наприклад, NIST SP 800-53 надає

каталог засобів контролю безпеки та конфіденційності, які організації можуть впроваджувати для захисту своїх інформаційних систем, тим самим гармонізуючи зусилля щодо безпеки в різних секторах та між кордонами.

Шифрування залишається наріжним каменем конфіденційності даних, гарантуючи, що інформація залишається незрозумілою для неавторизованих сторін під час передачі або зберігання.

Такі протоколи, як Secure Sockets Layer (SSL) та Transport Layer Security (TLS), сприяють безпечному обміну даними через Інтернет, встановлюючи зашифровані канали між клієнтами та серверами. Ці протоколи використовують процес рукостискання, який узгоджує алгоритми шифрування та обмінюється криптографічними ключами, тим самим запобігаючи підслуховуванню та втручанню (рис. 1.3) [8].

Окрім безпеки транспортного рівня, розгортання симетричних та асиметричних стандартів шифрування відіграє життєво важливу роль у захисті даних. Симетричні алгоритми шифрування, такі як Advanced Encryption Standard (AES), використовують один спільний ключ як для шифрування, так і для дешифрування, що забезпечує високу ефективність для великих обсягів даних. І навпаки, асиметричні стандарти шифрування, такі як RSA та Elliptic Curve Cryptography (ECC), використовують пари ключів — відкритий та закритий — для забезпечення безпечного обміну ключами та цифрових підписів. Ці криптографічні методи лежать в основі безпечної електронної пошти, цифрових сертифікатів та підпису коду, забезпечуючи автентичність та цілісність. Протоколи на транспортному та мережевому рівнях, включаючи IP Security (IPsec) та Secure Shell (SSH), розширюють захисний охоплення шифрування. IPsec захищає IP-зв'язок, автентифікуючи та шифруючи кожен IP-пакет, що є важливим для віртуальних приватних мереж (VPN), тоді як SSH забезпечує безпечний віддалений вхід та виконання команд, що критично важливо для системного адміністрування та безпечної передачі файлів. Разом ці протоколи утворюють багаторівневий захисний механізм, який захищає конфіденційні дані, що передаються через складні мережеві інфраструктури.

Таблиця 1.3.

Основні стандарти і протоколи захисту інформації

Стандарт	Характеристика	Назва
Міжнародні стандарти ISO/IEC	Системи управління інформаційною безпекою, оцінка ризиків	ISO/IEC 27001, ISO/IEC 15408
Стандарти NIST	Рекомендації та технічні стандарти кібербезпеки	NIST SP 800-53, NIST CSF
Транспортне шифрування	Захист даних під час передавання в Інтернеті	SSL/TLS, HTTPS
Симетричне шифрування	Один ключ для шифрування і дешифрування	AES
Асиметричне шифрування	Пари ключів для шифрування та підпису	RSA, ECC
Протоколи мережевого рівня	Захист пакетів і віддалених підключень	IPsec, SSH
Корпоративні протоколи автентифікації	Централізована перевірка користувачів	Kerberos, RADIUS, TACACS+
Веб-протоколи автентифікації	Єдиний вхід, делегований доступ	OAuth, OpenID Connect, SAML
Управління ключами	Створення і перевірка сертифікатів	PKI, X.509
Стандарти Wi-Fi	Шифрування і автентифікація бездротових мереж	WPA3, EAP
Стандарти мобільних мереж	Захист даних мобільних абонентів	3GPP Security
Стандарти IoT	Безпека пристроїв Інтернету речей	IEEE 802.15.4, OSCORE, ETSI EN 303 645
Стандарти 5G та SDN	Сегментація, шифрування, централізовані політики	5G security, SDN policies
Квантово-стійкі алгоритми	Захист від квантових атак	Ініціативи ISO, NIST, ETSI PQC
Децентралізовані протоколи	Незмінність та прозорість записів	Блокчейн-рішення
Гармонізація національних стандартів	Погодження з міжнародними вимогами	Інтеграція ISO/NIST у нац. політики

Ефективні механізми автентифікації та контролю доступу мають вирішальне значення для перевірки особи користувачів та забезпечення того, щоб лише авторизовані особи мали доступ до конфіденційної інформації та систем. Такі протоколи, як Kerberos, RADIUS та TACACS+, широко використовуються в корпоративних середовищах для керування процесами автентифікації. Kerberos, заснований на криптографії із секретним ключем та системах видачі квитків, забезпечує безпечний єдиний вхід (SSO) у довірених мережах, зменшуючи потребу в багаторазовому введенні паролів та мінімізуючи вразливості. RADIUS (Remote Authentication Dial-In User Service) та TACACS+ (Terminal Access Controller Access-Control System Plus) служать централізованими серверами автентифікації, особливо в мережевих пристроях та сценаріях віддаленого доступу, забезпечуючи гнучку та масштабовану перевірку користувачів [9].

У сфері сучасних веб-сервісів нові протоколи, такі як OAuth, OpenID Connect та Security Assertion Markup Language (SAML), трансформують те, як автентифікація та авторизація керуються в розподілених додатках. OAuth забезпечує делегований доступ, дозволяючи користувачам надавати стороннім додаткам обмежений доступ до своїх ресурсів без спільного використання облікових даних. OpenID Connect базується на OAuth, щоб забезпечити перевірку особи користувача, що сприяє безперешкодному входу. досвід на різних платформах. SAML, стандарт обміну даними автентифікації та авторизації, широко використовується для єдиного входу в корпоративних середовищах, дозволяючи співробітникам отримувати доступ до різних служб за допомогою єдиного набору облікових даних. Доповнюють ці протоколи надійні механізми сертифікації та управління ключами, такі як інфраструктура відкритих ключів (PKI) та сертифікати X.509. PKI забезпечує основу для створення, управління та перевірки цифрових сертифікатів, які служать цифровими паспортами, що підтверджують особу користувачів та пристроїв. Сертифікати X.509, широко поширені в протоколах SSL/TLS, підтримують безпечний зв'язок, прив'язуючи криптографічні ключі до перевірених ідентифікаційних даних, таким чином встановлюючи довіру в цифрових екосистемах. Ці багаторівневі стратегії автентифікації та контролю

доступу разом утворюють стійкий захист від несанкціонованого доступу, витоків даних та атак імперсонації.

Зі зростанням поширення технологій бездротового та мобільного зв'язку забезпечення їхньої безпеки стало критичним пріоритетом. Безпечні протоколи Wi-Fi, такі як WPA3 та розширюваний протокол автентифікації (EAP), знаходяться на передньому краї захисту бездротових локальних мереж (WLAN). WPA3 запроваджує вдосконалені механізми шифрування, включаючи одночасну автентифікацію рівних (SAE), яка зменшує вразливості, пов'язані з попередніми протоколами, такими як WPA2. EAP, з іншого боку, забезпечує гнучку основу для автентифікації користувачів та пристроїв у різних типах мереж, підтримуючи безпеку корпоративного рівня за допомогою кількох методів автентифікації. Мобільні мережі, особливо ті, що регулюються проектом партнерства третього покоління (3GPP), включають надійні стандарти безпеки для захисту даних користувачів та сигналізації. Ці стандарти включають конфіденційність ідентифікації абонента, взаємну автентифікацію та шифрування трафіку, що є життєво важливим для запобігання підслуховуванню та видаванню себе за іншу особу. Інтернет речей (IoT), що характеризується величезним масивом взаємопов'язаних пристроїв, створює додаткові проблеми безпеки. Такі стандарти, як IEEE 802.15.4, який лежить в основі малопотужних бездротових персональних мереж (WPAN), розробили функції безпеки, такі як шифрування на основі AES та автентифікація пристроїв для захисту цілісності даних. Робоча група з питань інтернет-інженерії (IETF) запровадила такі протоколи, як Object Security for Constrained RESTful Environments (OSCORE), що сприяють комплексній безпеці в пристроях IoT з обмеженими ресурсами. Крім того, Європейський інститут телекомунікаційних стандартів (ETSI) видав стандарт EN 303 645, який забезпечує комплексну базову кібербезпеку для споживчих пристроїв Інтернету речей, з акцентом на принципах безпечного проектування, управлінні вразливостями та захисті даних. У контексті передових мережевих архітектур мережі 5G включають такі функції безпеки, як сегментація мережі, надійне шифрування та покращений захист ідентифікаційних даних абонентів. Інфраструктура програмно-визначених

мереж (SDN) ще більше підвищує безпеку, забезпечуючи централізоване керування та динамічне забезпечення дотримання політик, що дозволяє мережам швидко адаптуватися до нових загроз. Ці стандарти, що розвиваються, разом відповідають унікальним вимогам безпеки бездротових, мобільних та Інтернет-екосистем, закладаючи основу для стійких та надійних комунікаційних мереж наступного покоління.

Заглядаючи в майбутнє, розробка стандартів безпеки все більше зосереджується на вирішенні нових загроз та технологічних інновацій. Одним із найважливіших досягнень є інтеграція квантово-стійких алгоритмів у міжнародні стандарти. Оскільки досягнення квантових обчислень загрожують традиційним криптографічним методам, такі органи стандартизації, як ISO, NIST та ETSI, активно оцінюють та стандартизують алгоритми, здатні витримувати квантові атаки. Цей проактивний підхід спрямований на забезпечення майбутнього криптографічних систем та забезпечення довгострокової безпеки даних. Одночасно зростає акцент на розробці децентралізованих протоколів безпеки на основі технології блокчейн. Розподілена система реєстру блокчейну пропонує підвищену прозорість, незмінність та стійкість до несанкціонованого доступу, що робить її привабливою основою для таких застосувань, як безпечне управління ідентифікацією, відстеження ланцюгів поставок та перевірка цілісності даних. Ці децентралізовані протоколи обіцяють зменшити залежність від централізованих органів влади, тим самим зменшуючи появу єдиних точок відмови та підвищуючи стійкість до кібератак. Крім того, докладаються зусилля для гармонізації українських національних стандартів з міжнародними вимогами безпеки, узгоджуючи їх з передовим світовим досвідом для сприяння транскордонній співпраці та економічній інтеграції. Ця гармонізація передбачає прийняття міжнародно визнаних рамок, участь у глобальних ініціативах зі стандартизації та забезпечення дотримання загальних політик кібербезпеки. Такі зусилля не лише зміцнюють безпекову позицію України, але й сприяють глобальним зусиллям створення сумісних, надійних систем безпеки, які можуть адаптуватися до цифрового середовища, що постійно змінюється. У сукупності ці перспективні

напрямки відображають проактивний, інноваційний підхід до вдосконалення стандартів безпеки, забезпечуючи їхню актуальність та ефективність у дедалі складнішому технологічному середовищі.

Ландшафт стандартів та протоколів захисту інформації є величезним та постійно розвивається, щоб відповідати вимогам сучасних цифрових екосистем. Міжнародні стандарти, такі як серія ISO/IEC 27000, ISO/IEC 15408 та рекомендації NIST, створюють міцну основу для систематичного управління безпекою та оцінки продуктів, сприяючи глобальній довірі та сумісності. Протоколи шифрування та захисту даних, такі як SSL/TLS, AES, RSA та IPsec, формують багаторівневий захист, який захищає дані під час передачі та зберігання, тоді як механізми автентифікації та контролю доступу, включаючи Kerberos, OAuth та PKI, забезпечують надійні рамки перевірки користувачів та довіри. Оскільки бездротові, мобільні та Інтернет речей мережі стають невід'ємною частиною повсякденного життя, спеціалізовані стандарти, такі як WPA3, безпека 3GPP та ETSI EN 303 645, усувають їхні унікальні вразливості, забезпечуючи безпечне підключення в різних середовищах.

2. ТЕХНОЛОГІЯ БЛОКЧЕЙНУ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ БЕЗПЕКИ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

2.1. Принципи функціонування технології блокчейн

Технологія блокчейн стала однією з найбільш трансформаційних інновацій цифрової епохи, фундаментально змінивши спосіб запису, зберігання та перевірки даних у різних секторах. По суті, блокчейн працює як децентралізований цифровий реєстр, який записує транзакції на кількох комп'ютерах, гарантуючи, що жодна окрема особа не контролює всю систему. Цей інноваційний підхід сприяє прозорості, безпеці та незмінності, роблячи її дуже стійкою до шахрайства та втручання. Розуміння фундаментальних принципів технології блокчейн є важливим для оцінки її потенціалу революціонізувати такі галузі, як фінанси, управління ланцюгами поставок та охорона здоров'я. У цьому есе досліджуються основні концепції, що лежать в основі блокчейну, включаючи його структуру, формування та механізми перевірки транзакцій, щоб з'ясувати, як ця технологія функціонує як безпечна та прозора система ведення обліку [10].

Фундаментальна ідея технології блокчейн полягає в її залежності від технології розподіленого реєстру (DLT), що означає, що замість єдиного центрального органу, який веде облік, реєстр розповсюджується по глобально мережевій системі комп'ютерів, які називаються вузлами. Кожен вузол містить ідентичну копію всього реєстру, що гарантує, що всі учасники мають доступ до однієї й тієї ж інформації в режимі реального часу. Цей принцип децентралізації усуває потребу в довіреній третій стороні, зменшуючи ризик корупції, цензури або єдиних точок відмови. Наприклад, у криптовалютних транзакціях, таких як Bitcoin, цей розподілений реєстр гарантує, що кожен учасник може самостійно перевіряти та затверджувати транзакції, сприяючи середовищу без довіри, де прозорість є невід'ємною частиною. Прозорість транзакцій ще більше підкріплюється їх неминучістю; після того, як транзакція записана в блокчейні, її майже неможливо змінити або видалити, забезпечуючи постійний та захищений від

несанкціонованого доступу запис. Ця характеристика сприяє довірі серед користувачів, оскільки всі транзакції відкрито доступні для перевірки, що має вирішальне значення в секторах, що вимагають високого рівня підзвітності, таких як фінанси та державні записи (рис. 2.1).

Таблиця 2.1.

Характеристика принципів функціонування технології блокчейн

Параметр	Характеристика	Приклад реалізації
Децентралізація	Відсутність центрального вузла; розподіл повноважень між учасниками мережі	P2P взаємодія у Bitcoin, Ethereum
Розподілений реєстр	Копія блокчейну зберігається на багатьох вузлах; синхронізація через консенсус	Синхронізація вузлів у Ethereum
Невідворотність	Неможливість зміни даних у блоці без зміни всього ланцюга	Хеш-ланцюг SHA-256 у Bitcoin
Механізм консенсусу	Алгоритм визначення дійсного блоку	Proof of Work, Proof of Stake
Криптографічний захист	Хешування та асиметрична криптографія забезпечують автентичність	Підпис транзакцій приватним ключем
Прозорість	Дані транзакцій доступні для перегляду всіма учасниками	Etherscan, Blockchain.com
Безперервність додавання блоків	Нові блоки додаються послідовно за унікальними хеш-посиланнями	Генерація блоків Bitcoin кожні ~10 хвилин

Цілісність та безпека даних блокчейну підтримуються завдяки його унікальній структурі блоків та методу формування ланцюга. Кожен блок у блокчейні складається з кількох компонентів: заголовка, який містить метадані, такі як позначка часу та версія; даних, які включають фактичні транзакції; та хеш-посилання, яке з'єднує його з попереднім блоком. Хеш – це криптографічний відбиток, згенерований з вмісту блоку, який служить унікальним ідентифікатором. Коли створюється новий блок, він пов'язується з існуючим ланцюгом, посилаючись на хеш попереднього блоку, утворюючи нерозривний ланцюг блоків. Цей механізм зв'язування гарантує, що будь-яка зміна в попередньому блоці змінить його хеш, тим самим анулюючи всі наступні блоки та попереджаючи мережу про спроби втручання. Процес додавання нового блоку включає майнерів або валідаторів, які компілюють транзакції в блок, перевіряють його дійсність за допомогою алгоритмів консенсусу, таких як Proof of Work або Proof of Stake, а потім додають його до ланцюга. Цей процес гарантує хронологічну цілісність блокчейну та робить його стійким до зловмисних модифікацій, оскільки зміна будь-якого блоку вимагала б величезної обчислювальної потужності для зміни всього ланцюга [11].

Критичним аспектом технології блокчейн є її механізм перевірки транзакцій, який гарантує, що реєструються лише легітимні транзакції, та запобігає таким проблемам, як подвійні витрати. Коли транзакція ініціюється, її мають перевірити та підтвердити кілька вузлів у мережі. Ці вузли діють як незалежні валідатори, перевіряючи справжність даних транзакції, таких як цифрові підписи та баланси, на відповідність своїм копіям реєстру. Після досягнення консенсусу більшості – залежно від протоколу – транзакція підтверджується та додається до нового блоку. Цей децентралізований процес перевірки усуває залежність від єдиного авторитету та зменшує ризик шахрайської діяльності. Крім того, механізм перевірки блокчейну відіграє важливу роль у запобіганні подвійним витратам, проблемі, поширеній у цифрових валютах, де одна одиниця валюти могла б бути витрачена кілька разів. Вимагаючи підтвердження роботи або консенсусу на основі ставок, система гарантує, що кожна транзакція є унікальною та справжньою, тим самим підтримуючи загальну узгодженість та довіру блокчейну. Приклади з Bitcoin та

Ethereum демонструють, як ці процеси перевірки забезпечують цілісність та безпеку цифрових транзакцій, сприяючи довірі між користувачами та зацікавленими сторонами (рис. 2.1).

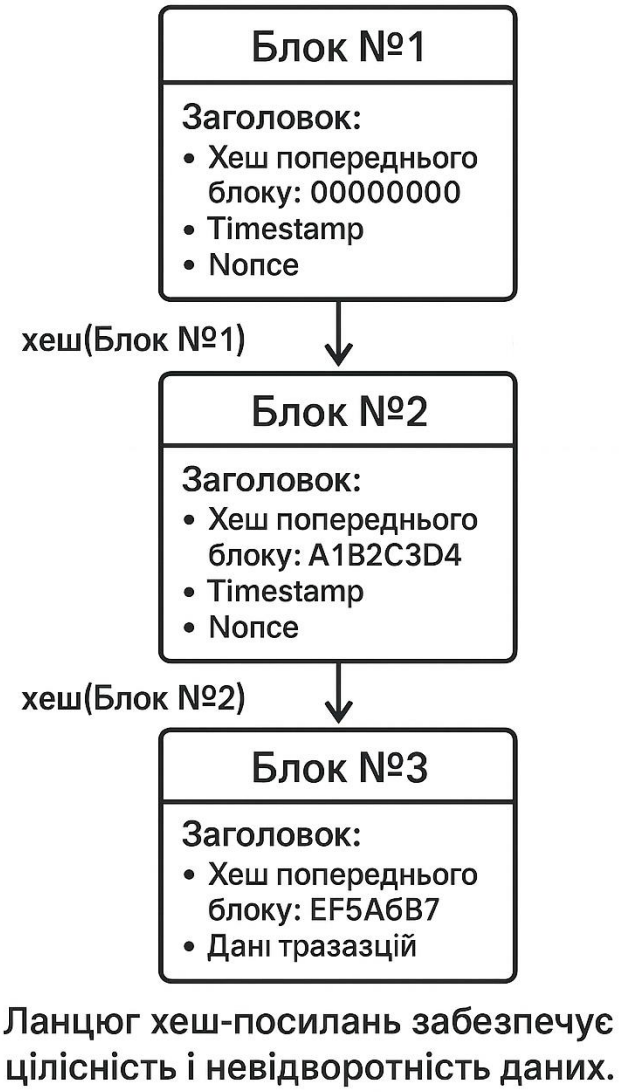


Рис. 2.1. Структура блоку та формування ланцюга блоків

Важливим компонентом, що лежить в основі функціонування мереж блокчейну, є алгоритм консенсусу, який забезпечує згоду між розподіленими вузлами щодо дійсності транзакцій та стану реєстру. Найвідомішими механізмами консенсусу є Proof of Work (PoW) та Proof of Stake (PoS). PoW, що використовується Bitcoin, вимагає від учасників, яких називають майнерами, розв'язувати складні математичні головоломки, процес, який вимагає значної обчислювальної

потужності та енергії. Як тільки майнер успішно розв'язує головоломку, він отримує право додати новий блок до ланцюга, при цьому мережа досягає консенсусу на основі першого дійсного рішення. І навпаки, PoS спирається на валідаторів, яких обирають для створення нових блоків на основі кількості криптовалюти, яку вони мають, і які готові "ставити" як забезпечення. Цей метод зменшує споживання енергії та прискорює обробку транзакцій, зберігаючи при цьому безпеку за рахунок економічних стимулів. Окрім цього, існує кілька альтернативних механізмів консенсусу, таких як Delegated Proof of Stake (DPoS), який запроваджує обраних делегатів для прийняття рішень; Practical Byzantine Fault Tolerance (PBFT), розроблений для мереж з дозволом та відомими учасниками; і підтвердження авторитетності (PoA), де довірені валідатори є попередньо схваленими суб'єктами. Кожен алгоритм консенсусу по-різному впливає на продуктивність, безпеку та масштабованість блокчейну; наприклад, PoW пропонує високий рівень безпеки, але за рахунок швидкості та енергоефективності, тоді як PoS забезпечує швидшу обробку з іншим компромісом безпеки. Таким чином, вибір механізму консенсусу впливає не лише на технічні можливості мережі блокчейн, але й на її придатність для різних застосувань та середовищ [12].

Криптографія є основою безпеки блокчейну, захищаючи цілісність, конфіденційність та автентичність даних за допомогою складних криптографічних механізмів. Хеш-функції, такі як SHA-256, широко використовуються для створення криптографічних дайджестів даних транзакцій фіксованої довжини, гарантуючи, що будь-яка зміна даних призведе до іншого хешу, який сигналізує про втручання. Цей процес гарантує цілісність інформації, що зберігається в кожному блоці. Крім того, для підписання транзакцій використовується асиметричне шифрування, що включає пару ключів – відкритий ключ та закритий ключ. Коли користувач ініціює транзакцію, він цифровим чином підписує її, використовуючи свій закритий ключ, надаючи доказ автентичності та власності, тоді як інші можуть перевірити підпис, використовуючи відкритий ключ відправника. Цей криптографічний підпис гарантує, що лише законний власник міг авторизувати транзакцію. Керування криптографічними ключами має вирішальне значення;

користувачі зазвичай генерують та зберігають свої закриті ключі безпечно, часто використовуючи апаратні гаманці або захищені цифрові гаманці для запобігання несанкціонованому доступу. Правильне управління ключами є життєво важливим для підтримки безпеки та запобігання шахрайству чи крадіжці. Разом ці криптографічні методи створюють надійну систему безпеки, яка захищає від підробки, прослуховування та несанкціонованого доступу, тим самим сприяючи довірі до систем на основі блокчейну.

Однією з найінноваційніших особливостей технології блокчейн є впровадження смарт-контрактів — самовиконуваних угод з умовами, безпосередньо записаними в код, який автоматично полегшує, перевіряє та забезпечує виконання договірних положень. Смарт-контракти працюють на блокчейн-платформах, таких як Ethereum, і структуровані як код, написаний мовами програмування, такими як Solidity або Vyper. Ці мови розроблені для створення складної логіки, яка може обробляти різні умови та автоматизувати процеси без втручання людини. Коли виконуються певні умови, вбудовані в смарт-контракт, контракт виконує заздалегідь визначені дії, такі як переказ коштів або оновлення записів. Ця автоматизація зменшує потребу в посередниках, знижує транзакційні витрати та підвищує ефективність. Розумні контракти широко використовуються в системах зв'язку, управлінні ланцюгами поставок та децентралізованих фінансах, де вони забезпечують прозорі, захищені від несанкціонованого доступу угоди, які надійно виконуються для різних учасників. Наприклад, у застосунках ланцюгів поставок розумні контракти можуть автоматично здійснювати платежі після перевірки доставки товарів, що спрощує процес транзакцій та зменшує затримки. Їхня програмованість та автономний характер роблять розумні контракти потужним інструментом для підвищення прозорості, зменшення шахрайства та автоматизації складних робочих процесів у широкому спектрі галузей.

Масштабованість та енергоефективність є критично важливими факторами в постійному розвитку та впровадженні технології блокчейн. Однією з основних проблем, з якими стикаються багато мереж блокчейн, є їхня обмежена здатність швидко та ефективно обробляти транзакції. Наприклад, мережа Bitcoin може

обробляти близько 7 транзакцій за секунду, що блідне в порівнянні з традиційними платіжними системами, такими як Visa, які здатні обробляти тисячі транзакцій за секунду. Це обмеження пов'язане з такими проблемами, як максимальний розмір блоку та час, необхідний для перевірки та додавання кожного блоку, що призводить до перевантаження та вищих комісій за транзакції в періоди пік. Для вирішення цих проблем було розроблено різні стратегії оптимізації. Рішення другого рівня, такі як Lightning Network для Bitcoin, створюють позаблокчейнові канали, які дозволяють здійснювати швидкі та недорогі транзакції без перевантаження основного блокчейну, тим самим збільшуючи пропускну здатність та зменшуючи затримку. Аналогічно, методи шардування розділяють блокчейн на менші, керовані сегменти, відомі як шарди, що дозволяє паралельну обробку транзакцій та значно покращує масштабованість. Альтернативні підходи включають інші протоколи другого рівня та сайдчейни, які додатково розподіляють обчислювальне навантаження. Однак, зі зростанням блокчейн-систем, їх споживання енергії залишається спірним питанням. Мережі на основі Proof of Work, такі як Bitcoin, вимагають величезних обчислювальних зусиль, що призводить до значного споживання електроенергії та викликає занепокоєння щодо навколишнього середовища. Це спонукало до досліджень більш стійких механізмів консенсусу, таких як Proof of Stake, які різко знижують потреби в енергії, зберігаючи при цьому безпеку. Балансування масштабованості та енергоефективності залишається ключовим пріоритетом для розробників блокчейну, прагнучи зробити технологію більш практичною та екологічно чистою для широкого використання.

На завершення, технологія блокчейн побудована на фундаментальних принципах, таких як децентралізація, прозорість та криптографічна безпека, які разом створюють надійну, стійку до несанкціонованого доступу систему ведення обліку. Її структура, що складається з пов'язаних блоків, перевірених за допомогою алгоритмів консенсусу, забезпечує цілісність даних та запобігає шахрайській діяльності, такій як подвійні витрати. Інтеграція криптографії додатково захищає дані користувачів та транзакції, тоді як смарт-контракти автоматизують складні процеси, зменшуючи залежність від посередників та підвищуючи ефективність.

Тим не менш, проблеми, пов'язані з масштабованістю та споживанням енергії, продовжують впливати на еволюцію мереж блокчейн. Інновації, такі як рішення другого рівня, шардінг та альтернативні механізми консенсусу, є життєво важливими для вирішення цих проблем, роблячи блокчейн більш стійким та здатним підтримувати великомасштабні програми. У міру розвитку технологій розуміння цих основних принципів висвітлює його потенціал для революціонізування багатьох галузей, сприяючи створенню більш прозорих, безпечних та ефективних цифрових систем. Зрештою, постійні зусилля щодо оптимізації продуктивності та впливу на навколишнє середовище блокчейну визначатимуть його роль у формуванні більш пов'язаного та надійного цифрового майбутнього.

2.2. Типи блокчейн-мереж та їх характеристики

Технологія блокчейн революціонізувала спосіб зберігання, перевірки та обміну даними на цифрових платформах, забезпечуючи безпечну та прозору основу, яка лежить в основі різних застосувань у різних галузях. З розвитком технології з'явилися різні типи блокчейн-мереж, кожна з яких розроблена для задоволення конкретних потреб щодо доступності, управління та операційної ефективності. Розуміння відмінностей між публічними, приватними та консорціальними (федеративними) блокчейн-мережами має вирішальне значення для розуміння того, як вони сприяють безпечному зв'язку, обміну даними та організаційній співпраці. У цьому есе досліджуються ключові характеристики, переваги та типові випадки використання цих трьох основних типів блокчейн-мереж, проливаючи світло на їхню роль у формуванні сучасних цифрових взаємодій [13].

Публічні (відкриті) блокчейн-мережі характеризуються відкритим доступом, що дозволяє будь-кому приєднуватися та брати участь без обмежень. Ці мережі працюють за децентралізованою моделлю, тобто немає центрального органу, який би контролював мережу, що підвищує безпеку та прозорість системи. Оскільки

будь-хто може перевіряти транзакції, публічні блокчейни використовують механізми консенсусу, такі як Proof-of-Work або Proof-of-Stake, для забезпечення цілісності даних. Прикладом публічного блокчейну є Bitcoin, який функціонує переважно як децентралізована цифрова валюта. Його прозорість дозволяє користувачам відкрито перевіряти транзакції, сприяючи довірі між учасниками. Аналогічно, Ethereum впроваджує смарт-контракти, які автоматизують та прозоро перевіряють угоди, що дозволяє створювати широкий спектр децентралізованих додатків (dApps). У контексті комунікації публічні блокчейни сприяють створенню безпечних, захищених від несанкціонованого доступу платформ обміну повідомленнями або систем перевірки сертифікатів, де прозорість та незмінність є першочерговими. Однак відкритість публічних мереж також викликає занепокоєння щодо масштабованості та споживання енергії, що є постійними викликами для широкого впровадження.

Приватні (закриті) блокчейн-мережі розроблені для роботи в межах певної організації або консорціуму з обмеженою участю. Доступ обмежений; Тільки уповноважені організації або окремі особи можуть приєднуватися та перевіряти транзакції, що робить ці мережі більш контрольованими та захищеними від зовнішніх загроз. Ідентифікація та автентифікація учасників ретельно контролюються, часто за допомогою цифрових сертифікатів або систем управління ідентифікацією, що підвищує підзвітність. Приватні блокчейни забезпечують значні переваги з точки зору продуктивності та керованості, оскільки не потребують енергоємних механізмів консенсусу, таких як Proof-of-Work. Вони добре підходять для внутрішніх корпоративних комунікацій, управління ланцюгом поставок або фінансових послуг, де конфіденційність та швидкість є важливими. Наприклад, багатонаціональна корпорація може впровадити приватний блокчейн для внутрішнього відстеження походження продукту, забезпечуючи конфіденційність даних, зберігаючи при цьому прозорий запис, доступний лише уповноваженим співробітникам. Ці мережі також сприяють легшому дотриманню нормативних вимог та управлінню даними, що робить їх привабливими для галузей, де захист даних є критично важливим (табл. 2.2).

Таблиця 2.2.

Типи блокчейн-мереж та їх характеристики

Тип мережі	Характеристика	Приклад
Публічна мережа	Повністю відкрита, децентралізована, всі учасники мають рівні права	Bitcoin, Ethereum
Приватна мережа	Доступ контролюється організацією, висока продуктивність та керованість	Hyperledger Fabric
Консорціумна мережа	Керування здійснюється групою організацій, збалансована децентралізація	R3 Corda
Пермісійна мережа	Доступ дозволяється лише авторизованим учасникам	Quorum
Непермісійна мережа	Повністю відкрита участь без дозволу	Ethereum
Гібридна мережа	Поєднання відкритих та закритих механізмів для гнучкості та безпеки	Dragonchain
Спеціалізована мережа	Оптимізована під IoT, телеком та спеціальні комунікаційні задачі	IOTA, Helium

Консорціальні (федеративні) блокчейн-мережі представляють собою гібридний підхід, де кілька організацій спільно керують та експлуатують блокчейн. На відміну від публічних мереж, вони не відкриті для всіх, а включають попередньо обрану групу довірених організацій, таких як фінансові установи, партнери по ланцюжку поставок або державні установи. Відповідальність за управління мережею є спільною, що забезпечує збалансований підхід між децентралізацією та централізованим контролем. Така структура знижує ризик зловмисної діяльності,

зберігаючи при цьому певний рівень прозорості серед учасників. Прикладом консорціального блокчейну є Corda від R3, який використовується фінансовими установами для оптимізації процесів транскордонних платежів та розрахунків. Переваги таких мереж полягають у їхній здатності сприяти безпечній міжорганізаційній взаємодії та обміну даними, що є важливим для галузей, які потребують співпраці без шкоди для конфіденційності чи ефективності. Розподіляючи обов'язки, консорціальні блокчейни також підвищують стійкість та сприяють довірі між учасниками, що робить їх ідеальними для складних екосистем, де багато зацікавлених сторін повинні безперебійно працювати разом [14].

Блокчейн-мережі можуть працювати за різними моделями доступу, які впливають на їхню безпеку, масштабованість та участь користувачів. Дозволені мережі, також відомі як блокчейни з керованим доступом, обмежують участь уповноваженими особами, часто керованими центральним адміністратором або консорціумом. Ці мережі реалізують рольовий контроль, що дозволяє детально керувати дозволами, наприклад, хто може перевіряти транзакції, читати дані або додавати нових учасників. Ця модель підвищує безпеку, запобігаючи несанкціонованому доступу, та сприяє дотриманню нормативних стандартів, що робить її придатною для корпоративних додатків, де конфіденційність та контроль є першочерговими. І навпаки, мережі без дозволів є повністю відкритими, що дозволяє будь-кому приєднуватися, перевіряти транзакції та брати участь у механізмах консенсусу. Ця модель втілює основні принципи децентралізації, сприяючи прозорості та стійкості до цензури. Вона спирається на алгоритми консенсусу, такі як Proof-of-Work або Proof-of-Stake, щоб забезпечити цілісність без центрального нагляду. Вибір між мережами з дозволом та без нього значною мірою залежить від вимог безпеки, проблем конфіденційності та потреб масштабованості певної системи зв'язку. Наприклад, публічні криптовалюти віддають перевагу моделям без дозволів через їхню відкритість, тоді як корпоративні колаборації часто віддають перевагу мережам з дозволом для захисту конфіденційної інформації. та підтримувати операційний контроль.

Гібридні блокчейн-мережі інтегрують функції як публічних, так і приватних блокчейнів, пропонуючи гнучкі конфігурації, адаптовані до складних потреб комунікації та обміну даними. Ці мережі поєднують відкритість публічних блокчейнів з конфіденційністю та контролем приватних мереж, що дозволяє організаціям визначати конкретні рівні доступу та видимості даних. Наприклад, гібридна мережа може дозволити публічний доступ до певних даних, зберігаючи конфіденційні деталі транзакцій обмеженими для уповноважених сторін. Такий підхід сприяє створенню масштабованих та безпечних систем зв'язку, які можуть адаптуватися до змінюваних організаційних вимог. На практиці гібридні мережі використовуються в таких секторах, як охорона здоров'я, де дані пацієнтів можуть безпечно передаватись між уповноваженими постачальниками, зберігаючи при цьому публічну прозорість для цілей аудиту. Налаштування рівнів відкритості та конфіденційності робить гібридні блокчейни особливо ефективними для середовищ з багатьма зацікавленими сторонами, що вимагають як прозорості, так і конфіденційності. Налаштовувані опції включають вибірковий обмін даними, зашифровані транзакції та багаторівневий контроль доступу, що забезпечує гнучкість у проектуванні безпечних та ефективних архітектур зв'язку.

Архітектура блокчейн-мереж також характеризується багаторівневими структурами, зокрема рішеннями рівня 1 та рівня 2, які виконують різні функції та враховують певні обмеження. Перший рівень стосується базового блокчейну, такого як Bitcoin або Ethereum, який відповідає за ведення основного реєстру, перевірку транзакцій та забезпечення дотримання правил консенсусу. Хоча ці мережі є безпечними та децентралізованими, вони часто стикаються з обмеженнями пропускної здатності транзакцій та масштабованості, що призводить до перевантаження та високих комісій у години пік. Щоб подолати ці проблеми, були розроблені рішення другого рівня, що функціонують поверх базового рівня для збільшення обчислювальної потужності без шкоди для безпеки. Прикладами є зведення, які об'єднують кілька транзакцій в одне підтвердження, та канали станів, які дозволяють взаємодію між учасниками поза блокчейном з періодичними розрахунками всередині блокчейну. Ці рішення значно підвищують пропускну

здатність та зменшують затримку, роблячи блокчейн-мережі більш придатними для зв'язку в режимі реального часу та обміну великими обсягами даних. Таким чином, багатошарова архітектура відіграє вирішальну роль у балансуванні безпеки, масштабованості та ефективності, дозволяючи складним комунікаційним системам працювати безперебійно, зберігаючи при цьому надійні заходи безпеки. Такі багаторівневі конструкції сприяють взаємодії та адаптивності, що є важливим для розгортання технології блокчейн у різноманітних, масштабних середовищах.

Спеціалізовані блокчейн-мережі адаптовані до унікальних потреб певних галузей, особливо тих, що вимагають високого рівня безпеки, конфіденційності та довіри. Наприклад, у сфері Інтернету речей (IoT) мережі блокчейн використовуються для забезпечення безпечного автоматизованого зв'язку між взаємопов'язаними пристроями. Ці мережі забезпечують цілісність даних і запобігають несанкціонованому доступу, дозволяючи пристроям перевіряти транзакції та безперешкодно спілкуватися без централізованого контролю. Телекомунікаційні оператори та постачальники комунікаційної інфраструктури також використовують спеціалізовані блокчейни для управління величезними мережами даних, автентифікації користувачів та оптимізації процесів виставлення рахунків та надання послуг. Такі блокчейни оптимізовані для високої пропускної здатності, низької затримки та надійних заходів безпеки для захисту конфіденційних даних користувачів та підтримки цілісності мережі. Крім того, ці мережі часто включають передові криптографічні методи та механізми консенсусу, розроблені спеціально для безпечного зв'язку в режимі реального часу. Зосереджуючись на галузевих вимогах, спеціалізовані мережі блокчейн підвищують операційну ефективність, зміцнюють довіру між зацікавленими сторонами та забезпечують стійку основу для критично важливих систем зв'язку, що лежать в основі сучасного цифрового зв'язку [15].

Підсумовуючи, ландшафт блокчейн-мереж є різноманітним і охоплює різні типи, розроблені для задоволення конкретних організаційних та комунікаційних потреб. Публічні блокчейн-мережі є прикладом децентралізації, прозорості та відкритості, що робить їх ідеальними для застосувань, де довіра та перевірка мають

першочергове значення. Приватні мережі, з іншого боку, пропонують контрольоване середовище, яке надає пріоритет конфіденційності, продуктивності та керованості, що підходить для внутрішніх корпоративних процесів. Консорціумні або федеративні блокчейни досягають балансу, забезпечуючи спільне управління між вибраними організаціями, сприяючи безпечному міжорганізаційному обміну. Різниця між моделями з дозволом та без нього додатково уточнює контроль доступу на основі вимог безпеки та конфіденційності, тоді як гібридні мережі поєднують сильні сторони обох для підтримки складних систем з багатьма зацікавленими сторонами. Багаторівневі архітектури, такі як рішення Layer-1 та Layer-2, підвищують масштабованість та пропускну здатність, забезпечуючи практичність блокчейну для високооб'ємного або реального зв'язку. Нарешті, спеціалізовані мережі, розроблені для Інтернету речей та телекомунікацій, демонструють, як технологію блокчейн можна адаптувати до галузевих викликів, підкреслюючи безпеку та високий рівень довіри. Разом ці різні типи та моделі блокчейн-мереж трансформують ландшафти цифрових комунікацій, пропонуючи безпечні, прозорі та ефективні рішення, адаптовані до потреб галузей промисловості, що постійно змінюються, у всьому світі.

2.3. Механізми консенсусу та шифрування в блокчейні

Технологія блокчейн здійснила революцію в цифровому ландшафті, забезпечивши децентралізований та безпечний метод запису транзакцій. Центральним елементом цієї інновації є механізми, які перевіряють та захищають дані, що зберігаються в розподілених мережах, відомі як механізми консенсусу. Ці протоколи гарантують, що всі учасники блокчейну погоджуються щодо стану реєстру, запобігаючи таким проблемам, як подвійні витрати та шахрайські записи. Поряд з механізмами консенсусу, шифрування відіграє ключову роль у захисті даних транзакцій, збереженні конфіденційності користувачів та забезпеченні цілісності всієї системи. У цьому есе досліджуються основні механізми консенсусу, що використовуються в технології блокчейн, з особливим акцентом на Proof of Work

та Proof of Stake, а також коротко розглядаються інші помітні методи. Крім того, обговорюються основні принципи, переваги та недоліки цих механізмів, підкреслюючи їхній вплив на безпеку, ефективність та децентралізацію.

Ландшафт блокчейну переважно спирається на кілька механізмів консенсусу, кожен з яких розроблений для перевірки транзакцій та підтримки цілісності мережі за допомогою різних процесів. Найвідомішим є Proof of Work (PoW), який лежить в основі функціонування Bitcoin, першої та найвідомішої криптовалюти. PoW вимагає від майнерів розв'язувати складні математичні головоломки, такі як пошук одноразового числа (nonce), яке в поєднанні з даними транзакцій створює хеш нижче певного цільового значення. Цей процес вимагає значної обчислювальної потужності та енергії, оскільки майнери змагаються за те, щоб першими перевірити блок та отримати винагороду. Іншим широко поширеним механізмом є Proof of Stake (PoS), який вибирає валідаторів на основі кількості криптовалюти, яку вони зберігають, і яку готові "закласти" або заблокувати як забезпечення. PoS має на меті зменшити енергетичне навантаження, пов'язане з PoW, обіцяючи швидшу перевірку транзакцій та підвищену масштабованість. Окрім цього, для задоволення конкретних потреб різних блокчейн-систем були розроблені інші механізми, такі як Delegated Proof of Stake (DPoS), де зацікавлені сторони обирають делегатів для перевірки транзакцій, та алгоритми на основі Візантійської відмовостійкості (BFT), які забезпечують консенсус, незважаючи на зловмисних акторів. Ці різноманітні механізми підкреслюють постійні зусилля щодо балансування децентралізації, безпеки та ефективності в мережах блокчейн [16].

Основний принцип Proof-of-Work полягає в тому, що майнери змагаються у вирішенні складних математичних задач, зазвичай методом спроб і помилок, що вимагає значних обчислювальних ресурсів. Цей процес гарантує, що додавання нового блоку до ланцюга є ресурсомістким, тим самим стримуючи зловмисні спроби змінити минулі дані. Безпека мережі принципово залежить від цієї обчислювальної складності, оскільки зміна історичних транзакцій вимагатиме від зловмисника повторного виконання Proof-of-Work для всіх наступних блоків, що є нездійсненним завданням з огляду на поточні обмеження енергії та часу (табл. 2.3).

Таблиця 2.3.

Механізми консенсусу та шифрування в блокчейні

Параметр	Характеристика	Приклад
Proof of Work (PoW)	Алгоритм консенсусу, що ґрунтується на складних обчисленнях, високий рівень захисту	Bitcoin
Proof of Stake (PoS)	Консенсус на основі стейкінгу монет, енергоефективність і швидший блокчейн	Ethereum 2.0
Delegated Proof of Stake (DPoS)	Узгодження через делегатів, висока продуктивність мережі	EOS
Practical Byzantine Fault Tolerance (PBFT)	Захист від збоїв та зловмисних вузлів, підходить для приватних мереж	Hyperledger Fabric
Асиметричне шифрування	Використання пари ключів: приватного й публічного для підпису та автентифікації	ECDSA у Bitcoin та Ethereum
Хешування	Однобічна криптографічна функція, забезпечує цілісність даних	SHA-256, Keccak-256
Управління ключами (PKI)	Система створення, розподілу та зберігання криптографічних ключів	X.509 сертифікати

Однак це споживання енергії є головним недоліком, що викликає занепокоєння щодо навколишнього середовища через високе споживання електроенергії, пов'язане з великомасштабними майнінговими операціями, такими як ті, що спостерігаються на фермах майнінгу біткойнів у регіонах з дешевою електроенергією. Крім того, мережі Proof-of-Work вразливі до атак 51%, коли організація, яка контролює понад половину майнінгової потужності мережі, може маніпулювати перевіркою транзакцій, що потенційно може призвести до подвійних витрат або цензури. Ці вразливості та неефективність спонукали до дослідження

альтернативних механізмів, які пропонують порівнянну безпеку зі зменшеним впливом на навколишнє середовище.

Підтвердження частки (Proof of Stake) пропонує переконливу альтернативу Proof of Work, вибираючи валідаторів на основі кількості криптовалюти, яку вони вкладають як заставу. У цій системі ймовірність бути обраним для перевірки нового блоку корелює з розміром вашої частки, стимулюючи чесну участь для захисту ваших інвестицій. PoS значно зменшує споживання енергії, оскільки усуває потребу в інтенсивній обчислювальній роботі, що забезпечує швидший час підтвердження транзакцій та більшу масштабованість, що є критично важливим для широкого впровадження та корпоративних додатків. Наприклад, криптовалюти, такі як Ethereum 2.0, перейшли на PoS для підвищення ефективності та стійкості. Тим не менш, PoS створює власні проблеми, зокрема ризик централізації, оскільки великі зацікавлені сторони — часто ранні інвестори або організації зі значними активами — можуть здійснювати непропорційний вплив на процес управління та перевірки мережі. Така концентрація влади може підірвати децентралізований дух технології блокчейн, що потенційно може призвести до змови або монополістичної поведінки. Хоча PoS пропонує багатообіцяючі переваги над PoW, поточні дослідження та моделі управління спрямовані на пом'якшення цих ризиків, щоб зберегти основні принципи децентралізації та безпеки блокчейну. Окрім фундаментальних механізмів консенсусу, деякі блокчейн-системи використовують делеговані алгоритми для підвищення ефективності та масштабованості. Делеговане підтвердження частки (DPoS) є яскравим прикладом, коли учасники мережі голосують за обрання обмеженого набору довірених делегатів або свідків, відповідальних за перевірку транзакцій та підтримку блокчейну. Ці делегати діють подібно до обраних посадових осіб, приймаючи рішення від імені ширшої спільноти, що спрощує процес консенсусу та збільшує пропускну здатність транзакцій. DPoS був прийнятий такими платформами, як EOS та Steem, демонструючи його здатність забезпечувати швидший час підтвердження порівняно з традиційними системами PoS або PoW. Однак таке делегування створює потенційні ризики централізації, оскільки влада, як правило,

концентрується серед невеликої кількості делегатів, що може підірвати децентралізовану природу технології блокчейн. Хоча система пропонує значні переваги в швидкості та знижене енергоспоживання, критики стверджують, що це може призвести до змови або впливу з боку впливових осіб. Компроміс між ефективністю та децентралізацією залишається ключовим фактором у впровадженні алгоритмів делегованого консенсусу, що спонукає до постійних дискусій про те, як збалансувати ці конкуруючі пріоритети для підтримки основних принципів блокчейну (рис. 2.2) [17].

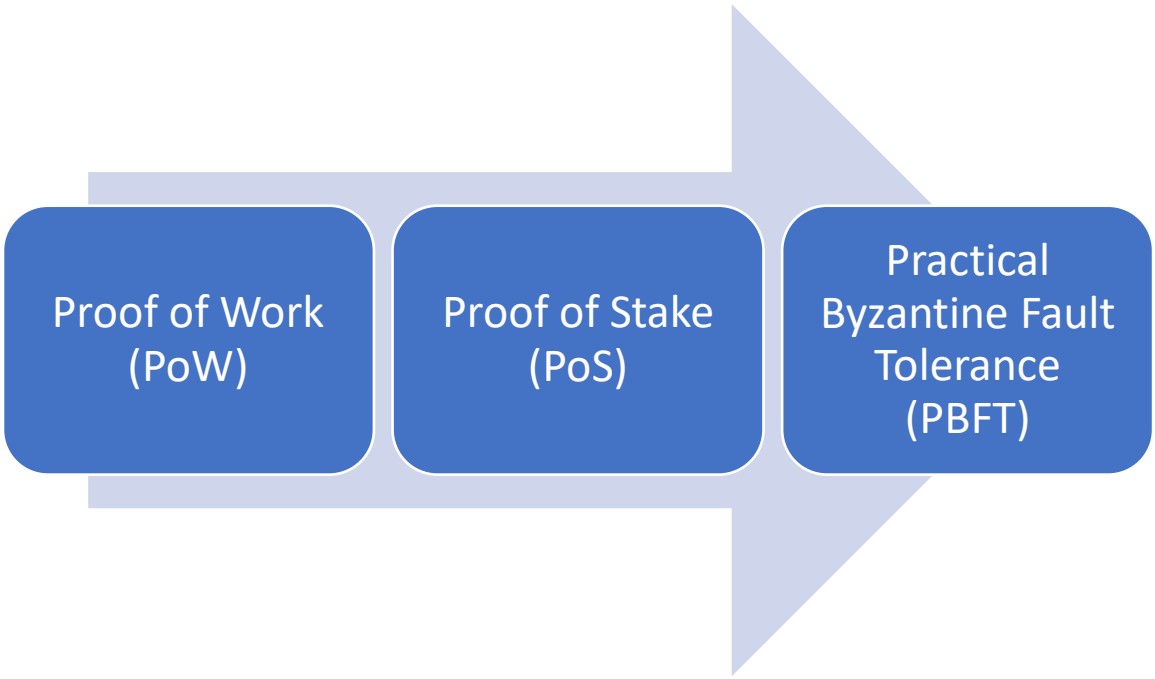


Рис. 2.2. Алгоритми консенсусу в блокчейні: PoW, PoS та PBFT (порівняльна схема)

Технології шифрування утворюють критично важливу основу для захисту даних та забезпечення довіри в мережах блокчейн. Симетричне шифрування, яке використовує один ключ як для шифрування, так і для дешифрування даних, забезпечує швидкий та ефективний спосіб захисту конфіденційної інформації, що зберігається в блокчейні, особливо під час обміну даними поза блокчейном або в приватних каналах. Прикладами є AES (Advanced Encryption Standard), який широко використовується завдяки своїй безпеці та швидкості. З іншого боку,

асиметричне шифрування використовує пару ключів – відкритий ключ та закритий ключ – для забезпечення безпечного зв'язку та перевірки особи. Цей метод лежить в основі цифрових підписів, дозволяючи користувачам автентифікувати транзакції та підтверджувати їх походження без розкриття закритих ключів, таким чином забезпечуючи цілісність даних та їхню невідмовність. Хеш-функції, такі як SHA-256, також є невід'ємною частиною технології блокчейн, забезпечуючи засоби для створення унікальних цифрових відбитків даних фіксованої довжини. Ці функції сприяють цілісності даних, виявляючи будь-які зміни та підтримуючи анонімність користувачів, оскільки вони не розкривають оригінальні дані, але все ще дозволяють їх перевірку. Разом ці криптографічні інструменти дозволяють мережам блокчейн підтримувати надійну безпеку, захищати дані користувачів та сприяти довірі в децентралізованих середовищах.

Застосування шифрування в технології блокчейн суттєво впливає на безпеку та конфіденційність, балансуючи прозорість з конфіденційністю. Механізми шифрування захищають деталі транзакцій та дані користувачів від несанкціонованого доступу, гарантуючи, що конфіденційна інформація залишається конфіденційною, навіть коли записи транзакцій є загальнодоступними в блокчейні. Функції підвищення конфіденційності, такі як докази з нульовим розголошенням (наприклад, zk-SNARK), дозволяють користувачам доводити достовірність твердження, такого як право власності на кошти, не розкриваючи основних даних, тим самим зберігаючи анонімність, зберігаючи при цьому достовірність. Аналогічно, кільцеві підписи, що використовуються в криптовалютах, орієнтованих на конфіденційність, таких як Monero, приховують походження транзакцій, змішуючи підпис користувача з підписами інших у групі, що робить практично неможливим відстеження відправника. Ці методи зміцнюють конфіденційність користувачів, дозволяючи мережі перевіряти легітимність транзакцій. Однак досягнення балансу між прозорістю та конфіденційністю залишається складним; Підвищена прозорість пропонує можливість аудиту та довіру, але може поставити під загрозу анонімність користувачів. І навпаки, розширені функції конфіденційності можуть зменшити здатність виявляти

шахрайську діяльність або дотримуватися нормативних стандартів. Тому постійні інновації спрямовані на узгодження цих контрастних потреб, гарантуючи, що блокчейн-системи є безпечними та поважають конфіденційність користувачів.

Взаємодія між механізмами консенсусу та технологіями шифрування відіграє вирішальну роль у зміцненні загальної цілісності блокчейн-систем. Хоча консенсусні протоколи, такі як Proof of Work та Proof of Stake, встановлюють надійну угоду між учасниками щодо стану реєстру, шифрування додає додатковий рівень безпеки, захищаючи дані транзакцій та ідентичність користувачів від зловмисників. Наприклад, криптографічні методи, такі як цифрові підписи, гарантують, що лише авторизовані користувачі можуть ініціювати транзакції, тоді як хеш-функції перевіряють цілісність даних, що надзвичайно ускладнює для зловмисників зміну інформації непоміченою. Ця синергія підвищує стійкість блокчейн-мереж до різних форм атак, включаючи подвійні витрати, підробку даних та крадіжку особистих даних. Крім того, комплексний підхід до безпеки, який поєднує надійні алгоритми консенсусу з передовими методами шифрування, є важливим для запобігання шахрайству та підтримки довіри між користувачами. Оскільки технологія блокчейн продовжує розвиватися, перспективи подальшого розвитку та інновацій у цій галузі є багатообіцяючими. Дослідники досліджують квантово-стійку криптографію, багаторівневі стратегії шифрування та більш складні консенсусні протоколи, що включають шифрування для посилення безпеки без шкоди для ефективності. Ці досягнення спрямовані на створення більш стійких, масштабованих та конфіденційних блокчейн-мереж, що гарантують їхню життєздатність для різноманітних застосувань у фінансах, ланцюжках поставок, охороні здоров'я тощо [18].

Підсумовуючи, консенсусні механізми, такі як Proof of Work (Протокол роботи), Proof of Stake (Протокол частки) та делеговані алгоритми, лежать в основі фундаментального функціонування блокчейн-мереж, перевіряючи транзакції та підтримуючи децентралізацію. Хоча Proof of Work забезпечує високий рівень безпеки за рахунок неефективності енергоспоживання, Proof of Stake пропонує більш стійку альтернативу, але створює проблеми, пов'язані з централізацією.

Делеговані системи ще більше підвищують масштабованість, але створюють ризики для децентралізації. Технології шифрування, включаючи симетричну та асиметричну криптографію разом з хеш-функціями, є невід'ємною частиною захисту даних, автентифікації користувачів та збереження конфіденційності в цих мережах. Синергія між консенсусними протоколами та шифруванням не тільки зміцнює безпеку блокчейну, але й сприяє його прозорості та надійності. З розвитком технологій інноваційні підходи, що поєднують безпечні консенсусні алгоритми з передовими методами шифрування, мають потенціал для усунення існуючих вразливостей та розширення застосувань блокчейну. Зрештою, комплексний та збалансований підхід, який використовує як консенсусні механізми, так і шифрування, є важливим для реалізації всіх можливостей технології блокчейн — створення систем, які є безпечними, ефективними та справді децентралізованими для майбутнього.

2.4. Потенціал інтеграції блокчейну в системи електронних комунікацій

У швидкозмінному цифровому середовищі системи електронного зв'язку стали невід'ємною частиною особистої, комерційної та урядової взаємодії. Однак занепокоєння щодо безпеки даних, прозорості та ідентифікації користувачів посилилося, що підкреслює необхідність інноваційних рішень для захисту цих систем. Технологія блокчейн, відома своєю децентралізованою та криптографічною природою, має багатообіцяючий потенціал для революціонізування електронних комунікацій. У цьому есе досліджується, як блокчейн може підвищити безпеку, збільшити прозорість та довіру, а також покращити управління ідентифікацією користувачів у рамках електронних комунікацій. Розглядаючи ці аспекти, ми можемо краще зрозуміти трансформаційний вплив, який блокчейн може мати на створення більш безпечних, прозорих та орієнтованих на користувача систем зв'язку (рис. 2.4) [19].

Таблиця 2.4.

Потенціал інтеграції блокчейну в системи електронних комунікацій

Параметр	Характеристика	Переваги для комунікацій
Децентралізація	Відсутність центральної точки відмови	Підвищення стійкості та надійності мереж
Прозорість	Усі транзакції зберігаються у відкритому реєстрі	Спрощення аудиту та контролю цілісності
Криптографічний захист	Стандартизоване хешування та цифрові підписи	Захист від модифікації та підміни даних
Смарт-контракти	Автоматизація взаємодії між вузлами	Зменшення затримок та людських помилок
Масштабованість	Підтримка Layer-2 та шардінгу	Підвищення продуктивності комунікаційних систем

Одна з основних переваг інтеграції блокчейну в електронні комунікації полягає в його здатності посилювати безпеку за допомогою передових криптографічних методів. Блокчейн використовує комбінацію криптографії, такої як алгоритми хешування та цифрові підписи, для шифрування даних, що надзвичайно ускладнює несанкціонований доступ або втручання. Наприклад, на платформах обміну повідомленнями кожне повідомлення може бути підписано цифровим підписом, що гарантує перевірку його походження та цілісності. Крім того, децентралізована архітектура блокчейну розподіляє дані по глобальній мережі вузлів, усуваючи єдину точку відмови. Ця децентралізація значно знижує ризик злому та зловмисних атак, оскільки немає централізованої бази даних, на яку можна було б націлитися. Крім того, системи блокчейну включають надійні механізми автентифікації та авторизації, такі як багатофакторна автентифікація та смарт-контракти, для перевірки особистості користувачів та надання доступу виключно уповноваженим сторонам. Ці функції разом створюють стійке середовище, де

електронні комунікації суттєво захищені від загроз, гарантуючи, що дані залишаються конфіденційними та захищеними від втручання.

Окрім безпеки, здатність блокчейну сприяти прозорості та довірі є не менш переконливою в системах електронних комунікацій. Підтримуючи прозорий, відкритий реєстр усіх транзакцій та обміну повідомленнями, блокчейн дозволяє кожному учаснику самостійно перевіряти історію комунікацій. Наприклад, у комунікаціях у ланцюжку поставок або у переговорах щодо контрактів незмінний запис блокчейну гарантує, що всі сторони мають доступ до незмінної історії, зменшуючи суперечки та непорозуміння. Ця відстежуваність підвищує підзвітність, оскільки стає можливим перевіряти повідомлення та транзакції в будь-який момент часу. Більше того, прозора природа блокчейну може значно зменшити корупцію та шахрайство в комунікаційних службах; оскільки кожна дія записується та публічно перевіряється, зловмисні спроби маніпулювання даними стримуються. Отже, користувачі та постачальники послуг можуть розвинути більшу впевненість у цілісності своїх взаємодій, що призводить до підвищення довіри та надійніших комунікаційних мереж [20].

Нарешті, технологія блокчейн пропонує інноваційні рішення для управління ідентифікацією користувачів в електронних комунікаційних системах. Децентралізовані системи перевірки ідентичності, побудовані на блокчейні, дозволяють користувачам контролювати свої персональні дані, не покладаючись на централізовані органи. Наприклад, користувачі можуть створювати цифрові ідентифікаційні дані, які криптографічно захищені, та вибірково розкривати інформацію за потреби, підвищуючи конфіденційність, зберігаючи при цьому автентичність. Такий підхід не тільки знижує ризик крадіжки особистих даних, але й надає користувачам більший контроль над своїми даними. Крім того, блокчейн сприяє швидким та безпечним процесам автентифікації, усуваючи затримки, пов'язані з традиційними централізованими базами даних. Наприклад, на платформах безпечного обміну повідомленнями або відеоконференцій користувачі можуть швидко перевірити свою особу за допомогою криптографічних доказів, що зберігаються в блокчейні, оптимізуючи доступ, зберігаючи при цьому безпеку. Цей

децентралізований підхід до управління ідентифікацією відповідає очікуванням щодо конфіденційності та нормативним базам, що змінюються, роблячи електронні комунікації більш безпечними, орієнтованими на користувача та ефективними.

Попри численні переваги, впровадження технології блокчейн в системах електронного зв'язку створює значні проблеми та обмеження, які необхідно ретельно враховувати. Однією з головних проблем є високе споживання енергії, пов'язане з мережами блокчейн, особливо тими, що покладаються на механізми консенсусу Proof-of-Work. Ці процеси вимагають значних обчислювальних ресурсів, що призводить до збільшення споживання електроенергії та впливу на навколишнє середовище, що може перешкоджати широкому впровадженню. Крім того, масштабованість мереж блокчейн залишається критичною проблемою; зі зростанням кількості транзакцій або обміну повідомленнями система може сповільнювати обробку та збільшувати комісії, обмежуючи ефективність у середовищах з великим обсягом даних. Це вузьке місце може перешкоджати потребам у зв'язку в режимі реального часу, особливо в сценаріях, що вимагають миттєвої передачі даних, таких як відеодзвінки в реальному часі або обмін миттєвими повідомленнями. Крім того, правові та нормативні перешкоди створюють складні проблеми для інтеграції блокчейну в системи зв'язку. Закони про конфіденційність, правила захисту даних та юрисдикційні розбіжності можуть ускладнювати впровадження блокчейн-рішень, особливо під час транскордонного обміну даними. Питання щодо володіння даними, відповідальності та дотримання стандартів, таких як GDPR, вимагають ретельного вивчення, щоб забезпечити юридичну обґрунтованість комунікаційних платформ на основі блокчейну та захист прав користувачів. Ці обмеження підкреслюють необхідність постійних технологічних удосконалень та продуманих регуляторних баз для ефективного використання потенціалу блокчейну [21].

Трансформаційний потенціал блокчейну виходить за рамки безпеки та прозорості, відкриваючи нові горизонти для інноваційних комунікаційних послуг та бізнес-моделей. Блокчейн може каталізувати розвиток децентралізованих додатків (dApps), які працюють без централізованого управління, дозволяючи

створювати нові платформи для обміну повідомленнями, обміну файлами та співпраці, які надають пріоритет контролю користувачів та конфіденційності. Наприклад, можуть з'явитися децентралізовані соціальні мережі або комунікаційні центри, що пропонуватимуть користувачам право власності на свої дані та взаємодію, одночасно зменшуючи залежність від традиційних постачальників послуг. Більше того, інтеграція блокчейну з Інтернетом речей (IoT) відкриває можливості для безпечної передачі даних у режимі реального часу між взаємопов'язаними пристроями, такими як системи розумного дому або автономні транспортні засоби. Ці мережі вимагають надійних заходів безпеки для запобігання злому та маніпуляціям даними, які блокчейн може забезпечити завдяки своєму захищеному від несанкціонованого доступу реєстру та криптографічному захисту. Крім того, системи голосового та відеозв'язку можуть скористатися функціями безпеки блокчейну, забезпечуючи безпечне наскрізне шифрування та автентифікацію. Інновації, такі як голосові дзвінки або відеоконференції на основі блокчейну, можуть запропонувати підвищену конфіденційність, стійкість до перехоплення та перевірену перевірку особи, тим самим підвищуючи стандарти цифрового спілкування у все більш взаємопов'язаному світі. Широке впровадження технології блокчейн також має значні наслідки для регулювання та політики в секторі зв'язку. Оскільки блокчейн може забезпечити автоматичне виконання контрактів через смарт-контракти, регуляторні бази повинні будуть адаптуватися, щоб врахувати ці нові правові механізми, потенційно зменшуючи адміністративне навантаження та підвищуючи ефективність. Смарт-контракти можуть автоматично забезпечувати дотримання стандартів безпеки та конфіденційності, гарантуючи, що обмін та передача даних відповідають встановленим політикам без ручного втручання. Ця автоматизація може спростити регуляторний нагляд, підвищити прозорість та зміцнити довіру користувачів. Однак вона також викликає занепокоєння щодо нагляду, підзвітності та юридичної застосовності, особливо коли виникають суперечки або коли технологія використовується зловмисно. Урядам та регуляторним органам необхідно буде розробити політику, яка збалансує інновації із захистом прав споживачів, забезпечуючи дотримання законів про

конфіденційність даних, одночасно сприяючи технологічному прогресу. Інтеграція блокчейну в системи зв'язку також може вплинути на майбутнє регулювання захисту даних користувачів, з акцентом на децентралізованому контролі, управлінні згодою та посилених заходах безпеки. Таким чином, політикам буде доручено розробити адаптивні рамки, які підтримують технологічний прогрес, одночасно захищаючи права особистості та суспільні інтереси.

Заглядаючи в майбутнє, майбутній розвиток інтеграції блокчейну в системи електронного зв'язку має бути як динамічним, так і трансформаційним. Одним із перспективних напрямків є розробка гібридних моделей блокчейну, які поєднують сильні сторони як публічних, так і приватних блокчейнів. Ці гібридні системи можуть запропонувати підвищену безпеку та прозорість, зберігаючи при цьому ефективну швидкість транзакцій та контроль конфіденційності, адаптований до конкретних потреб комунікації. Наприклад, гібридний блокчейн може сприяти безпечному обміну повідомленнями в організації, дозволяючи публічно перевіряти певні деталі транзакцій, таким чином балансуючи відкритість та конфіденційність. Крім того, постійне вдосконалення алгоритмічної ефективності є важливим для вирішення проблем масштабованості. Такі інновації, як Proof-of-Stake, шардінг та рішення другого рівня, спрямовані на збільшення пропускної здатності транзакцій та зменшення затримки, що робить блокчейн більш придатним для сценаріїв комунікації в реальному часі, таких як відеодзвінки або обмін миттєвими повідомленнями. Ці досягнення дозволять блокчейн-мережам швидко обробляти величезні обсяги даних, гарантуючи, що безпека та децентралізація не відбуватимуться на шкоду продуктивності. Крім того, оскільки глобальні мережі стають все більш взаємопов'язаними, впровадження блокчейну на макрорівні може забезпечити безпечне та бездоганне спілкування через кордони. Це передбачає розгортання масштабованих, сумісних блокчейн-платформ, здатних захищати цілісність даних та конфіденційність у різних юрисдикціях та інфраструктурних середовищах. Такі розробки матимуть вирішальне значення для створення стійких, безпечних та ефективних міжнародних комунікаційних систем, які зможуть

відповідати вимогам взаємопов'язаного світу, сприяючи інноваціям та довірі в цифрових взаємодіях.

Підсумовуючи, технологія блокчейн має значні перспективи для революціонізування систем електронного зв'язку шляхом підвищення безпеки за допомогою криптографічного захисту та децентралізації, сприяння прозорості та довірі завдяки незмінним записам транзакцій, а також надання користувачам можливостей децентралізованого управління ідентифікацією. Хоча такі проблеми, як високе споживання енергії, проблеми масштабованості та регуляторні перешкоди, залишаються невирішеними, постійні технологічні інновації та продумана розробка політики прокладають шлях для ширшого впровадження. Майбутні перспективи інтеграції блокчейну включають гібридні моделі та вдосконалені алгоритми, спрямовані на підвищення ефективності та масштабованості, а також розширення можливостей безпечного зв'язку в глобальних мережах. У міру розвитку цих досягнень потенціал блокчейну для створення більш безпечних, прозорих та орієнтованих на користувача комунікаційних екосистем стає все більш досяжним, обіцяючи нову еру цифрової взаємодії, заснованої на довірі та інноваціях [22].

3. АНАЛІЗ ТА МОДЕЛЮВАННЯ СИСТЕМИ ЗАХИЩЕНИХ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ З ВИКОРИСТАННЯМ БЛОКЧЕЙНУ

3.1. Архітектура та принципи роботи системи електронних комунікацій з блокчейн-компонентом

У швидкозмінному ландшафті цифрових комунікацій інтеграція технології блокчейн в електронні комунікаційні системи пропонує перспективні шляхи для підвищення безпеки, прозорості та операційної ефективності. Система електронного зв'язку з блокчейн-компонентом розроблена для забезпечення безпечного обміну даними, використовуючи при цьому децентралізовані та незмінні характеристики блокчейну. У цьому есе досліджується фундаментальна архітектура таких інтегрованих систем, зосереджуючись на їхніх ключових функціональних модулях, детальній структурі блокчейн-компонента та основних принципах, що регулюють обробку даних, автентифікацію та маршрутизацію. Розглядаючи ці аспекти, ми отримуємо розуміння того, як блокчейн може доповнити традиційні комунікаційні інфраструктури, забезпечуючи більш надійні та стійкі до несанкціонованого доступу операції [23].

Загальна архітектура системи електронного зв'язку, що включає компонент блокчейн, складається з кількох взаємопов'язаних модулів, які безперебійно працюють для забезпечення безпечного та ефективного обміну даними (рис. 3.1). В основі системи лежать традиційні модулі, такі як інтерфейси користувача, сигнальні сервери, механізми маршрутизації та блоки зберігання даних. Ці модулі виконують основні функції передачі повідомлень, управління сеансами та зберігання даних. У цю структуру вбудований рівень блокчейну, який функціонує як розподілений реєстр, що записує критичні події, такі як ініціювання сеансу, обмін даними та журнали автентифікації. Взаємодія між цими модулями відбувається через чітко визначені протоколи зв'язку, де рівень блокчейну діє як незмінний компонент ведення записів, забезпечуючи журнал аудиту для всіх транзакцій. Потоки зв'язку структуровані таким чином, щоб включати контрольні

точки блокчейну в стратегічних точках, таких як під час автентифікації користувача або встановлення сеансу, що забезпечує цілісність та відстежуваність даних. Точки інтеграції між традиційною інфраструктурою та мережею блокчейн встановлюються за допомогою API та проміжного програмного забезпечення, які сприяють синхронізації та перевірці даних, забезпечуючи безперебійну сумісність.

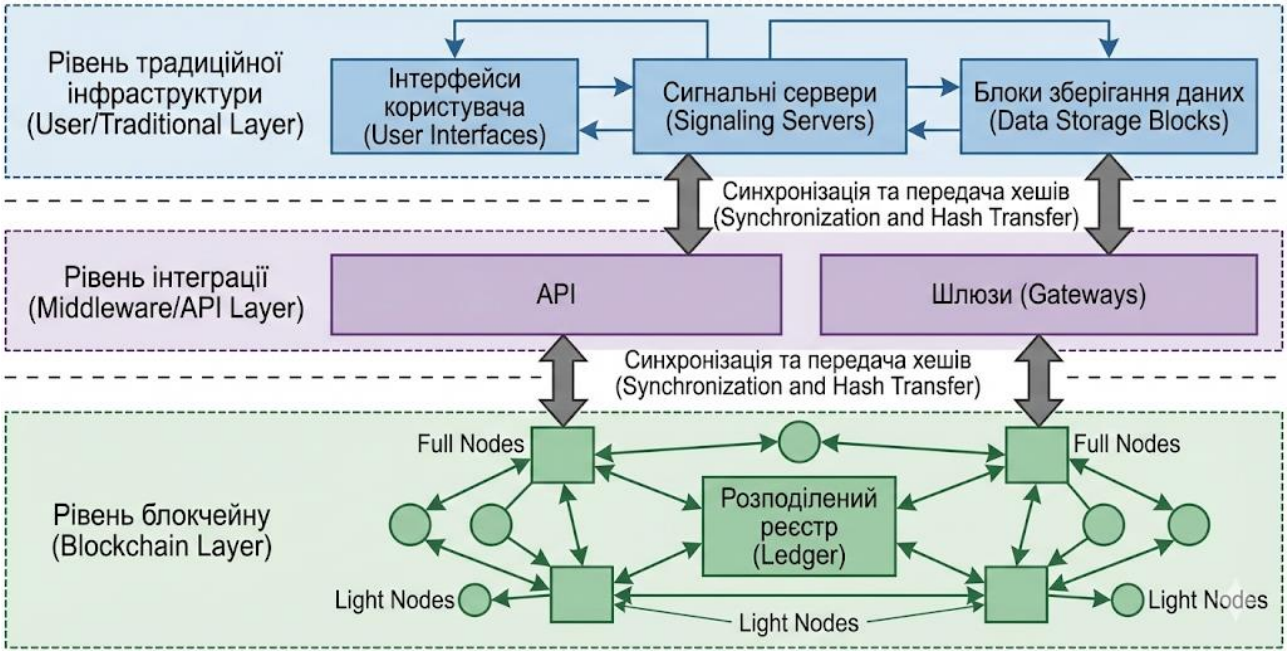


Рис. 3.1. Загальна схема архітектури гібридної системи електронних комунікацій

Наприклад, коли користувач ініціює виклик або сеанс передачі даних, система фіксує та записує цю подію в блокчейні, яку пізніше можна перевірити на автентичність, тим самим зміцнюючи довіру в мережі зв'язку. Архітектура блокчейн-компонента в системі зв'язку обертається навколо логічного реєстру, який веде вичерпний, захищений від несанкціонованого втручання запис усіх відповідних подій та транзакцій.

Цей реєстр працює за допомогою механізму, де нові записи, такі як журнали сеансів, токени автентифікації або хеші повідомлень, додаються через консенсусні протоколи, гарантуючи, що включено лише перевірені записи. Децентралізована природа блокчейну означає, що кілька вузлів, розподілених географічно, беруть участь у підтримці реєстру, тим самим усуваючи єдині точки відмови та зменшуючи

ризик зловмисного втручання. Вузли класифікуються на повні вузли, які зберігають весь блокчейн та перевіряють транзакції, та легкі вузли, які зберігають часткові дані, необхідні для рутинних операцій, та покладаються на повні вузли для перевірки. Повні вузли активно беруть участь у консенсусних алгоритмах, таких як Proof-of-Work або Proof-of-Stake, допомагаючи узгодити стан реєстру в мережі та забезпечуючи узгодженість. Легкі вузли, з іншого боку, оптимізують використання ресурсів та сприяють масштабованості, підтримуючи швидкість реагування системи, надаючи швидкий доступ до служб перевірки без підтримки всього ланцюга. Ця архітектура гарантує, що всі записи зв'язку синхронізовані в мережі, сприяючи створенню надійного середовища для безпечного та прозорого обміну. Використання принципів блокчейну для обробки даних, автентифікації та маршрутизації забезпечує підвищену безпеку та надійність у системах зв'язку. Криптографічні основи блокчейну дозволяють перевіряти джерела даних, де кожна подія зв'язку підписується цифровим підписом та записується в розподіленому реєстрі, що робить практично неможливим для зловмисників підробку або зміну інформації непоміченими. Наприклад, коли сеанс встановлено, блокчейн реєструє початок сеансу, перевіряючи особи учасників за допомогою криптографічних доказів, тим самим запобігаючи атакам «імперсонації» або «людина посередині». Транзакції, включаючи обмін повідомленнями та оновлення сеансу, реєструються в розподіленому реєстрі, забезпечуючи прозору, хронологічну історію, яку можна перевірити в будь-який час. Цей реєстр також підтримує процеси узгодження, де вузли періодично порівнюють свої стани для виявлення та усунення розбіжностей, підтримуючи узгодженість у мережі. Крім того, підсистема блокчейну взаємодіє з традиційними механізмами маршрутизації, надаючи перевірені метадані, які керують пересиланням пакетів та управлінням сеансом. Наприклад, рішення щодо маршрутизації можуть базуватися на перевірених блокчейном облікових даних сеансу, що гарантує, що пакети даних спрямовуються лише через довірені вузли, значно знижуючи ризик перехоплення або перенаправлення. Загалом, інтегруючи блокчейн в обробку даних та маршрутизацію, системи зв'язку досягають вищого

ступеня надійності, стійкості та відстежуваності, що є важливим для безпечної цифрової взаємодії.

Інтеграція криптографічних механізмів у компонент блокчейну значно підвищує безпеку та конфіденційність систем зв'язку. Шифрування транзакцій та даних гарантує, що конфіденційна інформація залишається захищеною від несанкціонованого доступу під час передачі та зберігання. Використовуючи передові криптографічні алгоритми, такі як AES для симетричного шифрування, система може захистити контент зв'язку, зробивши його нечитабельним для зловмисників. Крім того, смарт-контракти — самовиконуваний код, що зберігається в блокчейні — відіграють ключову роль в автоматизації таких процесів, як контроль доступу, робочі процеси автентифікації та перевірка транзакцій. Ці контракти працюють на основі попередньо визначених умов, зменшуючи потребу в ручному втручанні та мінімізуючи людські помилки. Децентралізована природа блокчейну ще більше підвищує безпеку системи, оскільки усуває централізовані точки збою та зменшує ризик фальсифікації даних або саботажу. Коли криптографічними ключами та протоколами належним чином керують у розподіленій мережі, загальна стійкість до кіберзагроз значно зростає. Таке поєднання криптографії та децентралізації створює надійну основу, де цілісність даних, конфіденційність та операційна автоматизація безперешкодно інтегровані, забезпечуючи безпечне та надійне середовище зв'язку [24].

Інтеграція системи електронного зв'язку з компонентом блокчейну значною мірою залежить від криптографічних функцій, таких як алгоритми хешування та асиметричне шифрування, для забезпечення цілісності та автентичності даних. Хеш-функції, такі як SHA-256, генерують унікальні дайджести фіксованої довжини для повідомлень та транзакцій, які служать цифровими відбитками пальців, що перевіряють цілісність даних зв'язку. Коли повідомлення передається, його хеш-значення обчислюється та зберігається в блокчейні, що дозволяє одержувачам підтвердити, що повідомлення не було змінено під час передачі, шляхом перерахунку та порівняння хешів. Асиметричне шифрування, що використовує пару відкритого та закритого ключів, сприяє безпечному підписанню та перевірці

повідомлень. Відправники цифровим способом підписують свої повідомлення своїми закритими ключами, надаючи доказ походження, тоді як одержувачі використовують відповідні відкриті ключі для перевірки дійсності підпису. Цей криптографічний підхід гарантує, що лише авторизовані учасники можуть створювати автентичні повідомлення, створюючи надійне середовище зв'язку. Безпека системи також залежить від ефективної генерації, управління та безпечного зберігання криптографічних ключів. Закриті ключі надійно зберігаються в апаратних модулях безпеки або спеціалізованих системах управління ключами, запобігаючи несанкціонованому доступу, тоді як відкриті ключі поширюються відкрито для полегшення перевірки. Правильне управління життєвим циклом ключів, що охоплює генерацію, розповсюдження, поновлення та скасування, є важливим для підтримки стійкої, безпечної комунікаційної інфраструктури, інтегрованої з блокчейном [25].

Архітектурні моделі взаємодії між учасниками системи, такими як клієнти, вузли та мережа, є основоположними для встановлення безпечної та ефективної комунікації в середовищі, що підтримує блокчейн (табл. 3.1). Загальна модель взаємодії, яку часто описують як «клієнт-вузол-мережа», передбачає, що клієнти ініціюють сеанси зв'язку, вузли перевіряють та передають повідомлення, а мережа підтримує консенсус через протоколи блокчейну. У цьому контексті клієнти взаємодіють з вузлами, які служать посередниками, перевіряючи криптографічні підписи, керуючи станами сеансів та синхронізуючи дані з реєстром блокчейну. Механізми доступу розроблені для забезпечення дозволів на основі ролей, гарантуючи, що учасники можуть виконувати лише дії, що відповідають їхнім призначеним ролям — будь то кінцеві користувачі, валідатори чи адміністратори. Рольові моделі допомагають визначити рівні доступу, контролювати видимість даних та керувати дозволами для криптографічних операцій. Крім того, обмін метаданими, такими як ідентифікатори сеансів, інформація про маршрутизацію та хеші транзакцій, відбувається між комунікаційними пристроями та реєстром блокчейну.

Таблиця 3.1.

Функціональний розподіл компонентів системи зв’язку

Компонент системи	Основна функція	Роль у забезпеченні безпеки
Традиційні модулі (Сигнальні сервери, UI)	Передача повідомлень, управління сеансами, маршрутизація пакетів.	Початкова автентифікація, шифрування каналу зв'язку.
Проміжне ПЗ (API, Middleware)	Синхронізація даних, перетворення запитів у транзакції.	Фільтрація запитів, забезпечення сумісності форматів даних.
Блокчейн-реєстр (Distributed Ledger)	Незмінний запис подій (логів), зберігання хешів повідомлень.	Захист від підробки історії, забезпечення аудиту та "незмінності" (immutability).
Вузли мережі (Повні та легкі)	Перевірка транзакцій, досягнення консенсусу, зберігання копій реєстру.	Усунення єдиної точки відмови, децентралізована верифікація даних.

Ця архітектурна структура підтримує масштабовану, безпечну та прозору екосистему зв'язку, де роль кожного учасника та обмін криптографічними метаданими зміцнюють довіру та операційну цілісність. Забезпечення стабільності, надійності та відмовостійкості системи електронного зв'язку, інтегрованої з технологією блокчейн, вимагає комплексного підходу до реплікації даних, синхронізації та механізмів консенсусу. Реплікація даних між кількома вузлами блокчейну є фундаментальною для підтримки стійкості системи; шляхом розподілу ідентичних копій реєстру система може витримувати збої або атаки окремих вузлів без втрати критичної інформації. Протоколи синхронізації гарантують, що всі вузли працюють на узгодженій та актуальній версії блокчейну, запобігаючи розбіжностям, які можуть поставити під загрозу цілісність даних або порушити потік зв'язку. Алгоритми консенсусу, такі як proof-of-work, proof-of-stake або

візантійська відмовостійкість, відіграють життєво важливу роль у перевірці нових транзакцій та підтримці угоди між розподіленими вузлами, тим самим запобігаючи потраплянню шкідливих або помилкових даних до реєстру. Ці алгоритми сприяють вирішенню конфліктів і гарантують остаточну узгодженість, навіть за наявності збоїв у роботі мережевих розділів або вузлів. Для подальшого підвищення відмовостійкості гібридні системи використовують схеми резервного копіювання, такі як періодичні знімки, позаланцюжкове сховище для менш критичних даних і надлишкові канали зв'язку, що мінімізує точки відмови. Впровадження надійних стратегій відновлення після відмови та децентралізованих структур управління гарантує, що система зв'язку залишається працездатною, безпечною та надійною навіть за несприятливих умов. Разом ці механізми утворюють стійку архітектуру, здатну підтримувати безперервний, надійний зв'язок у динамічних та потенційно агресивних середовищах [26].

На завершення, інтеграція технології блокчейн в системи електронного зв'язку фундаментально змінює те, як дані керуються, перевіряються та захищаються. Загальна архітектура поєднує традиційні модулі, такі як інтерфейси користувача, маршрутизація та зберігання, з децентралізованим шаром блокчейну, який забезпечує незмінний, прозорий запис подій зв'язку. Детальне проектування компонента блокчейн, що включає розподілені реєстри, механізми перевірки та ролі вузлів, забезпечує цілісність даних та стійкість до несанкціонованого доступу. Принципи криптографії, такі як хешування та асиметричне шифрування, підвищують автентичність даних, конфіденційність та безпечну маршрутизацію, тоді як смарт-контракти автоматизують критичні процеси, зменшуючи ручне втручання та людські помилки. Архітектурні моделі взаємодії учасників підкреслюють рольовий контроль доступу та обмін метаданими, сприяючи створенню надійного середовища. Нарешті, впровадження надійних механізмів реплікації даних, консенсусу та відмовостійкості гарантує стабільність та безперервність роботи системи навіть під час збоїв або атак. У сукупності ці елементи демонструють, що добре розроблена, інтегрована в блокчейн система зв'язку може значно підвищити безпеку, прозорість та надійність, прокладаючи

шлях для більш надійних та стійких цифрових взаємодій у все більш пов'язаному світі.

3.2. Реалізація механізмів автентифікації, цілісності та обміну даними на основі блокчейну

В епоху швидкої цифрової трансформації забезпечення безпечної та надійної взаємодії в інформаційних системах є надзвичайно важливим. Технологія блокчейн, відома своєю децентралізованою та незмінною природою, пропонує інноваційні рішення для покращення автентифікації, цілісності даних та безпечного обміну даними. Використовуючи можливості блокчейну, організації можуть створити прозорі, захищені від несанкціонованого доступу механізми, які зміцнюють протоколи безпеки та сприяють довірі між учасниками системи. У цьому есе досліджуються стратегії впровадження механізмів автентифікації, перевірки цілісності та обміну даними на основі блокчейну, підкреслюючи їхню важливість у створенні стійких цифрових інфраструктур [27].

Фундаментальний крок у розгортанні блокчейну для безпечних систем включає надійну автентифікацію користувачів та пристроїв (рис. 3.2). Цей процес починається з реєстрації унікальних ідентифікаторів, таких як криптографічні ключі, ідентифікатори пристроїв або біометричні хеші, в реєстрі блокчейну, який функціонує як централізований реєстр авторизованих об'єктів. Наприклад, мережа охорони здоров'я може зберігати унікальні ідентифікатори пацієнтів та ідентифікатори медичних пристроїв у блокчейні, щоб запобігти видаванню себе за іншу особу або несанкціонованому доступу. Потім автентифікація відбувається через перевірку цифрових підписів, згенерованих користувачами або пристроями, які служать криптографічним доказом ідентифікації. Коли користувач намагається отримати доступ до системи, його цифровий підпис перевіряється на відповідність збереженим обліковим даним у блокчейні, що гарантує автентичність. Крім того, смарт-контракти – самовиконуваний код, що зберігається в блокчейні – можуть автоматизувати процедури доступу, такі як надання або скасування дозволів на

основі попередньо визначених умов. Наприклад, смарт-контракт може автоматично скасовувати доступ, якщо облікові дані пристрою скомпрометовані, зменшуючи потребу в ручному втручанні. Цей багаторівневий підхід не тільки підвищує безпеку, але й оптимізує робочі процеси автентифікації, роблячи системи більш стійкими до несанкціонованого вторгнення.

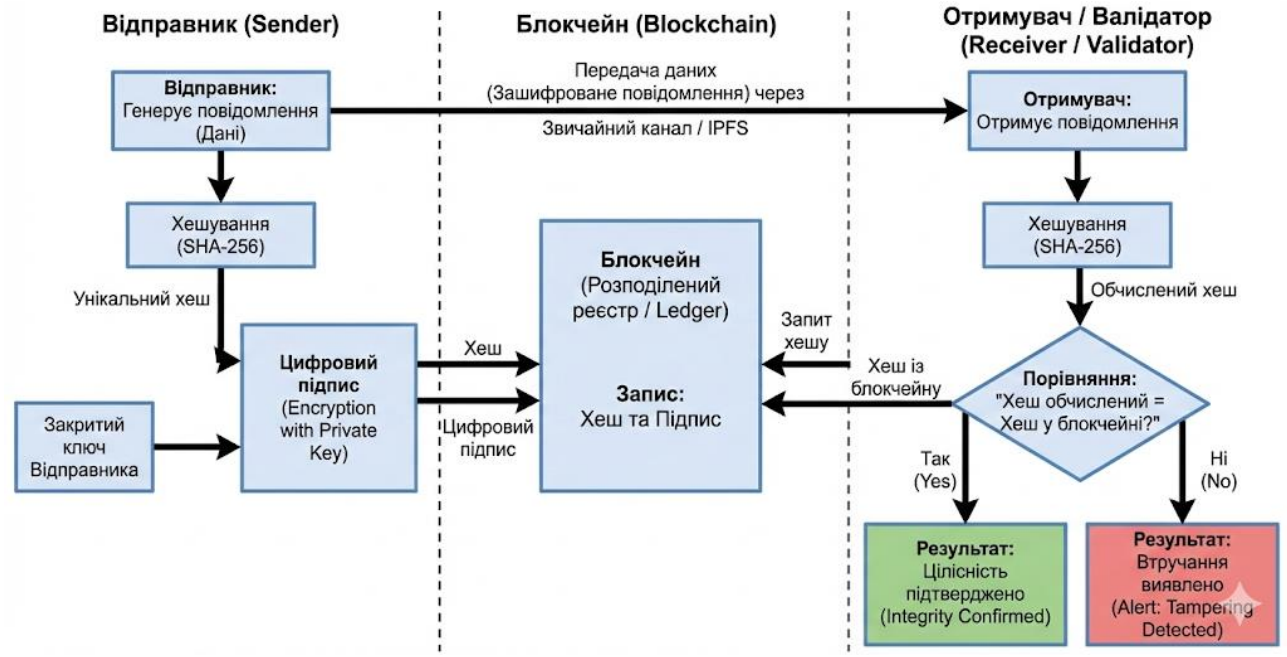


Рис. 3.2. Алгоритм забезпечення цілісності та автентифікації повідомлення

Підтримка цілісності даних є критично важливою для надійних цифрових операцій, і блокчейн забезпечує надійні механізми для досягнення цього. Один з основних методів включає хешування блоків інформації – застосування криптографічних алгоритмів для створення унікальних цифрових відбитків – а потім зберігання цих хешів у блокчейні. Коли дані пізніше отримуються або змінюються, їх поточний хеш можна перерахувати та порівняти зі збереженим записом, що дозволяє оперативно виявити будь-які втручання. Наприклад, у фінансових транзакціях хешування деталей транзакцій та їх запис у блокчейн гарантує, що будь-які несанкціоновані зміни будуть негайно очевидні. Крім того, запис журналів подій та історії сеансів у незмінному реєстрі блокчейну забезпечує незмінний запис діяльності, що є безцінним для журналів аудиту та судово-

медичних розслідувань. Ці журнали, після запису, не можуть бути змінені або видалені, що забезпечує підзвітність. Для подальшого підвищення цілісності системи часто використовують перевірку хеш-ланцюга – послідовне зв'язування хешів таким чином, щоб будь-яка зміна в попередньому блоці впливала на наступні хеші, що робить несанкціоновані зміни виявними за допомогою механізмів контролю версій. Такі комплексні заходи цілісності є життєво важливими в чутливих секторах, таких як охорона здоров'я та фінанси, де точність даних безпосередньо впливає на безпеку та відповідність вимогам.

Безпечний обмін даними між учасниками системи – це ще один критичний аспект, який сприяє блокчейн, забезпечуючи надійне середовище для комунікації. Асиметричне шифрування — використання пари відкритого та закритого ключів — є основою безпеки передачі повідомлень. Наприклад, відправник шифрує повідомлення відкритим ключем одержувача, гарантуючи, що лише одержувач може розшифрувати його своїм закритим ключем, що гарантує конфіденційність. Крім того, цифрові підписи, створені шляхом підписання повідомлень закритим ключем відправника, автентифікують походження даних та запобігають видаванню себе за іншу особу. Технологія блокчейн ще більше підвищує безпеку, керуючи сеансами, криптографічними ключами та сертифікатами за допомогою незмінних записів. Ці записи дозволяють учасникам перевіряти дійсність та походження ключів і сертифікатів, зменшуючи ризики, пов'язані з крадіжкою або неправильним використанням ключів. Під час спілкування транзакції, такі як обмін даними або команди, формуються та підтверджуються за допомогою процесів на основі блокчейну, що гарантує, що кожна взаємодія записана, перевірена та захищена від несанкціонованого доступу.

Наприклад, в управлінні ланцюгами поставок кожна транзакція, записана в блокчейні, підтверджує передачу товарів та пов'язаних з ними даних, забезпечуючи прозорий та безпечний слід. Інтегруючи ці криптографічні та блокчейн-методи ведення обліку, організації можуть сприяти безпечному, надійному та перевіреному обміну даними між розподіленими системами. Розумні контракти відіграють ключову роль в автоматизації процесів безпеки в системах на основі блокчейну,

значно підвищуючи ефективність та зменшуючи залежність від ручного контролю. Ці самовиконувані контракти, закодовані з попередньо визначеними правилами та умовами, забезпечують різні функції безпеки, такі як контроль доступу та авторизація. Наприклад, розумний контракт може автоматично надавати або скасовувати дозволи користувачів на основі перевірених облікових даних або певних подій, таких як проходження програми навчання з безпеки. Ця автоматизація гарантує, що права доступу послідовно застосовуються без втручання людини, мінімізуючи помилки та затримки. Крім того, розумні контракти можуть генерувати та записувати журнали, події та операційні записи безпосередньо в реєстр блокчейну, забезпечуючи незмінний та прозорий журнал аудиту. Ця функція автоматичного ведення журналу спрощує розслідування відповідності та судово-медичні розслідування, надаючи інформацію про несанкціоноване втручання.

Докази діяльності, пов'язаної з безпекою. Крім того, смарт-контракти можуть перевіряти сеанси зв'язку, перевіряючи автентичність учасників та цілісність обмінюваних даних, тим самим гарантуючи, що лише уповноважені особи беруть участь у конфіденційних взаємодіях. Наприклад, у фінансовій установі смарт-контракт може перевірити легітимність транзакції перед виконанням, запобігаючи шахрайській діяльності. Загалом, інтеграція смарт-контрактів у робочі процеси безпеки автоматизує рутинні процедури, підвищує прозорість та захищає систему від зловмисних маніпуляцій.

Забезпечення безперервності та довіри в обміні даними є фундаментальним для стійких реалізацій блокчейну, особливо в розподілених мережах, де вузли можуть бути географічно розподілені. Реплікація даних між кількома вузлами підтримує надійність системи, запобігаючи появі єдиних точок відмови; якщо один вузол скомпрометовано або зазнає простою, інші можуть продовжувати надавати послідовну та точну інформацію. Ця надмірність є критично важливою в таких секторах, як охорона здоров'я чи фінанси, де доступність даних життєво важлива для безперервності роботи. Цілісність реплікованих даних додатково посилюється за допомогою консенсусних алгоритмів, таких як Proof of Work, Proof of Stake або

Practical Byzantine Fault Tolerance, які разом перевіряють автентичність транзакцій, перш ніж вони будуть передані в блокчейн. Ці алгоритми дозволяють учасникам мережі узгоджувати достовірність даних, запобігаючи внесенню зловмисниками неправдивої або шахрайської інформації. Крім того, децентралізовані механізми довіри усувають залежність від центральних органів влади, розподіляючи контроль між кількома незалежними вузлами. Така децентралізація зменшує ризики цензури, корупції або одностороннього маніпулювання даними, сприяючи створенню більш стійкого та надійного середовища обміну даними (табл. 3.2) [28].

Таблиця 3.2.

Інструменти блокчейн-технологій для реалізації сервісів безпеки

Сервіс безпеки	Використаний механізм / Технологія	Принцип дії в розробленій системі
Цілісність даних (Integrity)	Криптографічне хешування (SHA-256)	Створення унікальних дайджестів повідомлень; будь-яка зміна вхідних даних змінює хеш, що фіксується реєстром .
Автентифікація (Authentication)	Асиметричне шифрування (PKI) та Цифрові підписи	Перевірка особи користувача або пристрою через валідацію підпису відкритим ключем .
Контроль доступу (Access Control)	Смарт-контракти (Smart Contracts)	Автоматичне надання або скасування прав доступу на основі попередньо прописаних умов без втручання людини .
Конфіденційність (Confidentiality)	Шифрування повідомлень	Шифрування змісту відкритим ключем отримувача, щоб лише власник закритого ключа міг прочитати дані .
Стійкість (Availability/Resilience)	Реплікація даних та Консенсус (PoW/PoS)	Розподілене зберігання копій реєстру на багатьох вузлах унеможливлює втрату даних при атаці на один вузол .

Наприклад, в управлінні ланцюгами поставок перевірка на основі консенсусу гарантує надійність записів про походження продукції та транзакції, сприяючи

впевненості зацікавлених сторін у тому, що дані є точними та захищеними від несанкціонованого доступу.

Захист від атак підміни, перезапису або блокування даних є основною перевагою технології блокчейн, яка використовує кілька стратегій для захисту цілісності даних та безперервності роботи. Одна з таких стратегій передбачає реєстрацію ключових подій та транзакцій у незмінному реєстрі, що унеможливлює для зловмисників відтворення, зміну або видалення критично важливих даних без виявлення. Цей підхід ефективно протидіє атакам повторного відтворення, коли раніше дійсні дані зловмисно передаються повторно для обману систем, гарантуючи, що кожна транзакція унікально записана та перевірена. Крім того, системи використовують записи історії транзакцій для автентифікації зв'язку; переглядаючи хронологічну послідовність записаних транзакцій, уповноважені сторони можуть виявляти розбіжності або несанкціоновані зміни. Ця історична відстежуваність має вирішальне значення для підтримки довіри та проведення ретельних розслідувань інцидентів, коли відбуваються порушення безпеки. Доступ до незмінної історії операцій не лише стримує зловмисну діяльність, але й надає вичерпний запис, який слідчі можуть аналізувати для виявлення векторів атак, скомпрометованих вузлів або внутрішніх загроз. Разом ці механізми створюють надійне середовище безпеки, яке підтримує автентичність даних та цілісність системи, навіть за умови складних кіберзагроз.

Ефективне управління ролями, політиками доступу та авторизацією в системі на основі блокчейну є важливим для підтримки структурованої та безпечної взаємодії між користувачами, вузлами та сервісами. Технологія блокчейн дозволяє формувати моделі доступу на основі ролей за допомогою децентралізованих механізмів, усуваючи потребу в центральному органі та зменшуючи вразливості, пов'язані з централізованим контролем. Наприклад, блокчейн охорони здоров'я може призначати певні ролі, такі як лікарі, медсестри та адміністратори, кожна з яких має попередньо визначені дозволи, що автоматично застосовуються за допомогою смарт-контрактів. Ці ролі закодовані в блокчейні, що гарантує прозорість, захист від несанкціонованого доступу та легкість аудиту прав доступу.

Крім того, в блокчейні встановлюються політики взаємодії, такі як протоколи для обміну даними, робочі процеси затвердження запитів або правила виклику сервісів, для регулювання того, як учасники системи спілкуються та співпрацюють. Ці політики зберігаються у вигляді смарт-контрактів або правил консенсусу, які автоматично забезпечують дотримання вимог щоразу, коли відбувається взаємодія. Крім того, система блокчейн відіграє життєво важливу роль у реєстрації всіх дій користувачів, таких як запити на доступ, зміни даних або зміни авторизації, створюючи вичерпний та незмінний журнал аудиту. Перевірка авторизацій передбачає перехресне посилання цих журналів на попередньо визначені ролі та політики, що зберігаються в блокчейні, що гарантує, що кожна дія є легітимною та відповідає організаційним стандартам. Такий децентралізований та прозорий підхід до управління ролями та доступом значно підвищує безпеку, підзвітність та операційну ефективність в екосистемах блокчейну [29].

На завершення, впровадження механізмів автентифікації, цілісності даних та безпечного обміну даними на основі блокчейну пропонує комплексний підхід до підвищення кібербезпеки в цифрових інфраструктурах. Розгортання надійних протоколів автентифікації користувачів та пристроїв у поєднанні з незмінними заходами цілісності даних, такими як хешування та перевірка хеш-ланцюжка, гарантує, що інформація залишається точною та захищеною від несанкціонованого доступу. Безпечний обмін даними додатково посилюється за допомогою криптографічних методів, таких як асиметричне шифрування та цифрові підписи, що підтримуються записами блокчейну, що перевіряють автентичність транзакцій. Розумні контракти автоматизують життєво важливі процеси безпеки, включаючи контроль доступу, реєстрацію подій та перевірку сеансів зв'язку, тим самим зменшуючи ручний нагляд та підвищуючи надійність системи. Забезпечення безперервності та довіри даних за допомогою реплікації даних, алгоритмів консенсусу та децентралізованих механізмів довіри сприяє створенню стійких та надійних мереж, особливо важливих у розподілених середовищах. Захист від зловмисних атак, таких як підміна або перезапис даних, досягається за допомогою незмінних історій транзакцій та протоколів перевірки, що захищає цілісність

системи. Нарешті, управління ролями, політиками доступу та авторизаціями за допомогою децентралізованих моделей та прозорих журналів підвищує безпеку, підзвітність та операційну чіткість. Разом ці механізми на основі блокчейну створюють безпечну, прозору та ефективну систему, яка не лише вирішує поточні проблеми кібербезпеки, але й прокладає шлях для майбутніх інновацій в управлінні цифровою безпекою.

3.3. Оцінка ефективності блокчейн-орієнтованої системи безпеки

Оскільки технологія блокчейн продовжує революціонізувати безпечний обмін даними та цілісність транзакцій, розробка надійних систем безпеки на основі принципів блокчейну стала надзвичайно важливою. Щоб забезпечити надійність, ефективність та стійкість цих систем до потенційних загроз, необхідний комплексний підхід, що включає тестування, моделювання та оцінку. У цьому есе досліджуються критичні кроки, пов'язані з оцінкою ефективності системи безпеки на основі блокчейну, від розробки реалістичних сценаріїв тестування до побудови детальних моделей поведінки та проведення ретельних функціональних оцінок. За допомогою цього дослідження ми підкреслимо важливість методичних стратегій тестування для перевірки безпеки, продуктивності та операційної коректності рішень безпеки блокчейну, тим самим надаючи уявлення про найкращі практики їх розгортання в реальних додатках [30].

Основа оцінки системи безпеки, орієнтованої на блокчейн, починається з розробки ретельно розроблених сценаріїв тестування. Ці сценарії повинні охоплювати як типові схеми комунікації, так і критичні граничні випадки, щоб забезпечити повне покриття. Типові сценарії включають рутинні транзакції, такі як обмін даними між довіреними вузлами, оновлення консенсусу та рутинне виконання смарт-контрактів, що відображають повсякденні операційні умови. Критичні сценарії, з іншого боку, моделюють потенційні вектори атак та режими збоїв, включаючи розділення мережі, поведінку зловмисних вузлів та спроби втручання в транзакції. Для точної оцінки стійкості системи життєво важливо

визначити параметри навантаження, які відображають пікове використання мережі, такі як пропускна здатність транзакцій, затримка та споживання пропускної здатності мережі. Також необхідно визначити моделі загроз для моделювання поведінки зловмисників, включаючи атаки 51%, подвійні витрати та атаки Sybil. Підготовка тестового середовища, яке імітує реальні умови мережі, використовуючи віртуалізовані вузли, контрольовану затримку та імітовані збої мережі, є важливою для фіксації автентичних реакцій системи. Наприклад, розгортання тестових мереж з налаштовуваними параметрами дозволяє проводити стрес-тестування системи за різних умов навантаження, виявляючи потенційні вузькі місця та вразливості перед розгортанням.

Для перевірки масштабованості та стійкості системи в умовах стресу було проведено аналіз залежності часу обробки транзакцій від зростання навантаження на мережу. Важливим аспектом оцінки було порівняння часових характеристик запропонованої архітектури з традиційними централізованими рішеннями.

Результати порівняльного аналізу затримок (latency) при різній інтенсивності запитів наведено на рис. 3.3.



Рис. 3.3. Залежність середнього часу обробки транзакції від навантаження на систему

Як видно з наведеного графіка, система з інтегрованим блокчейн-компонентом демонструє дещо вищі показники затримки порівняно з традиційною архітектурою, особливо на етапах ініціації транзакцій. Це пояснюється додатковими обчислювальними витратами на виконання криптографічних операцій (хешування, підпис) та досягнення консенсусу між вузлами мережі.

Проте, варто зазначити, що при пікових навантаженнях графік демонструє стабільність блокчейн-системи без критичних збоїв, що підтверджує її здатність ефективно працювати в умовах високого трафіку, забезпечуючи при цьому незмінність та верифікованість даних, чого не можуть гарантувати традиційні системи без додаткових надбудов безпеки. Таким чином, незначне збільшення часу обробки є прийнятним компромісом для забезпечення високого рівня захищеності комунікацій

Побудова детальної моделі поведінки системи під час обміну даними є критичним кроком у розумінні та прогнозуванні її атрибутів продуктивності та безпеки. Це включає моделювання потоків даних в інфраструктурі блокчейну, включаючи те, як транзакції створюються, перевіряються та поширюються між вузлами. Наприклад, моделювання процесу створення транзакцій включає моделювання того, як клієнти генерують запити на транзакції, як вузли перевіряють підписи транзакцій та як механізми консенсусу визначають включення транзакцій до блоків. Взаємодія між вузлами під час підтвердження транзакцій включає розуміння протоколів зв'язку між вузлами, затримок поширення блоків та процедур перевірки. Аналіз цих взаємодій дає уявлення про ефективність мережі та потенційні точки відмови. Крім того, моделювання затримок та пропускної здатності в різних режимах роботи, таких як при нормальному навантаженні, під час великих обсягів транзакцій або за наявності збоїв у мережі, допомагає оцінити масштабованість та стійкість системи. Кількісні показники, такі як час підтвердження транзакцій, затримка поширення блоків та швидкість пропускної здатності транзакцій, служать ключовими показниками. Наприклад, моделювання сценаріїв високого навантаження може показати, чи підтримує система прийнятний рівень продуктивності, чи виникають вузькі місця, спрямовуючи зусилля з

оптимізації. Після встановлення моделей та сценаріїв, проведення ретельного функціонального тестування підсистеми блокчейну має вирішальне значення для підтвердження її робочої коректності та функцій безпеки. Цей етап тестування включає перевірку того, що транзакції точно зареєстровані в блокчейні та що переходи їх станів відображають заплановані операції без помилок. Наприклад, забезпечення того, щоб передача цифрових активів правильно оновлювала баланси рахунків, а такі зміни незмінно реєструвалися, демонструє цілісність системи. Крім того, оцінка роботи механізмів автентифікації, таких як цифрові підписи, багатофакторна автентифікація та криптографічні ключі, є важливою для підтвердження того, що лише уповноважені особи можуть ініціювати транзакції або змінювати дані. Здатність системи виявляти та запобігати втручанню або несанкціонованому доступу повинна бути ретельно оцінена за допомогою цілеспрямованих симуляцій атак. Крім того, тестування смарт-контрактів — програмованих компонентів, що керують доступом до даних та обміном ними — гарантує їхню правильність та безпеку. Це включає перевірку того, що смарт-контракти виконуються належним чином, коректно обробляють крайні випадки та не містять вразливостей, які можна було б використати, таких як помилки повторного входу або переповнення. Наприклад, розгортання тестових смарт-контрактів у контрольованих середовищах допомагає виявити логічні недоліки, перш ніж вони вплинуть на робочі системи, забезпечуючи як функціональну правильність, так і стійкість безпеки. Важливим компонентом оцінки системи безпеки на основі блокчейну є ретельне тестування системного навантаження, щоб зрозуміти її масштабованість та стійкість в умовах стресу. Цей процес починається з розробки сценаріїв високого навантаження, де обсяг транзакцій поступово збільшується для імітації пікових робочих умов. Такі сценарії допомагають визначити обмеження пропускної здатності мережі, показуючи, наскільки добре вузли та механізми консенсусу справляються зі стрибками активності. Під час цих тестів ретельно контролюються такі показники продуктивності, як швидкість обробки транзакцій, час підтвердження блоків та пропускна здатність мережі. Зі зростанням навантаження стає критично важливим спостерігати за поведінкою

системи під час затримок та перевантажень, перевіряючи, чи підтримують вузли синхронізацію, якщо затримки спричиняють відставання транзакцій або якщо виникають мережеві розділи. Оцінка цих аспектів надає цінну інформацію про потенційні вузькі місця та точки відмови, спрямовуючи стратегії оптимізації для підвищення стійкості. Наприклад, якщо вузли демонструють значні затримки за високих обсягів транзакцій, для підтримки продуктивності може знадобитися коригування алгоритмів консенсусу або мережевої інфраструктури. Систематично аналізуючи реакції системи на зростання навантажень, розробники можуть забезпечити надійність та ефективність системи безпеки блокчейну навіть у складних умовах експлуатації.

Оцінка стійкості системи безпеки блокчейну до різних векторів атак та операційних збоїв є критично важливою для сертифікації її надійності. Це включає моделювання поширених кіберзагроз, таких як підміна даних, атаки типу «людина посередині» (MitM) та атаки повторного відтворення. Наприклад, зловмисники можуть намагатися змінити дані транзакцій або перехопити зв'язок, прагнучи порушити цілісність даних або викрасти конфіденційну інформацію. Навмисно впроваджуючи ці загрози в контрольованих середовищах, тестувальники можуть оцінити здатність системи виявляти, запобігати та реагувати на такі вторгнення. Безпека смарт-контрактів від спотворення або несанкціонованого доступу також ретельно перевіряється за допомогою симуляцій атак, спрямованих на такі вразливості, як повторний вхід, переповнення або логічні недоліки. Ці тести перевіряють, чи смарт-контракти виконуються безпечно та не наражають систему на експлойти. Крім того, відмовостійкість перевіряється шляхом моделювання збоїв окремих вузлів, таких як збої обладнання або відключення мережі, щоб оцінити, чи може система підтримувати цілісність та узгодженість, незважаючи на часткові збої. Це включає тестування відновлення консенсусу, процедур відновлення даних та здатності системи запобігати подвійним витратам або втраті даних під час збоїв вузлів. Такі комплексні оцінки є життєво важливими для підтвердження стійкості системи як до зловмисних атак, так і до операційних збоїв, забезпечуючи довгострокову безпеку та стабільність.

Порівняльний аналіз системи безпеки на основі блокчейну з традиційними рішеннями безпеки забезпечує глибше розуміння її практичних переваг та обмежень (табл. 3.3).

Таблиця 3.3.

Порівняльна характеристика традиційної та розробленої систем захисту

Критерій порівняння	Традиційна система зв'язку	Система з блокчейн-компонентом (Розроблена)
Централізація даних	Висока (єдина точка відмови)	Відсутня (розподілений реєстр)
Стійкість до модифікації даних	Низька (залежить від адміна БД)	Висока (незмінність хешів)
Прозорість аудиту	Обмежена (логи можна видалити)	Повна (публічний/приватний ланцюжок)
Автоматизація доступу	Ручна або скриптова	Смарт-контракти
Стійкість до DDoS/Single point failure	Низька	Висока (через реплікацію вузлів)

Це включає оцінку ключових показників ефективності, таких як пропускна здатність транзакцій, затримка, масштабованість та стійкість до атак. Наприклад, системи блокчейну часто перевершують у забезпеченні незмінності та децентралізованої перевірки, що може перевершити можливості централізованих рішень, які можуть бути вразливими до точок одиночного збою. Однак вони також можуть зіткнутися з такими проблемами, як повільніший час обробки транзакцій або вищі обчислювальні витрати. Систематично порівнюючи ці аспекти, зацікавлені сторони можуть визначити, де системи безпеки блокчейну пропонують значні переваги, такі як підвищена прозорість та стійкість до несанкціонованого доступу, а де вони можуть бути недостатніми, особливо в середовищах з високою частотою або обмеженими ресурсами. Крім того, оцінка економічної доцільності

включає аналіз витрат на впровадження, експлуатаційних витрат та потенційної економії, досягнутої завдяки покращенню безпеки та зменшенню шахрайства. Це включає врахування таких факторів, як інвестиції в інфраструктуру, технічне обслуговування та потенційна рентабельність інвестицій. Загалом, цей порівняльний аналіз допомагає особам, що приймають рішення, оцінити, чи відповідає впровадження рішень безпеки на основі блокчейну їхнім операційним цілям та обмеженням ресурсів, забезпечуючи обґрунтований підхід до інтеграції нових технологій у системи зв'язку.

Кульмінацією тестування, моделювання та оцінки системи безпеки на основі блокчейну є формування комплексних остаточних рекомендацій щодо її практичного впровадження. Центральним у цьому є визначення оптимальних режимів роботи та параметрів конфігурації, які максимізують безпеку, продуктивність та стабільність. Наприклад, визначення відповідних алгоритмів консенсусу, розміру блоку, структур комісій за транзакції та конфігурацій вузлів забезпечує ефективну роботу системи в реальних умовах. Крім того, ці рекомендації повинні включати стратегії масштабування системи для врахування зростаючих обсягів даних та потреб користувачів, такі як впровадження шардингу, рішень другого рівня або оптимізація архітектури мережі для підвищення пропускної здатності. Також важливими є належні рекомендації щодо інтеграції, що охоплюють такі аспекти, як сумісність з існуючою інфраструктурою, відповідність стандартам та процедури розгортання, що мінімізують перебої. Нарешті, на основі ретельного тестування та аналізу зацікавлені сторони можуть розробити обґрунтовані висновки щодо загальної ефективності та економічної доцільності системи безпеки блокчейну. Це включає оцінку того, чи система адекватно збалансовує безпеку та продуктивність, її готовність до розгортання та її потенційні переваги відносно витрат. Такі остаточні рекомендації слугують дорожньою картою для успішного впровадження. забезпечення того, щоб система не лише відповідала стандартам безпеки, але й відповідала цілям організації та операційним обмеженням.

ВИСНОВКИ

У магістерській роботі вирішено актуальне науково-прикладне завдання підвищення рівня захищеності систем електронних комунікацій шляхом інтеграції технології блокчейн. На основі проведених досліджень, моделювання та аналізу отримано наступні результати:

У першому розділі проведено комплексний аналіз теоретичних основ та сучасного стану безпеки електронних комунікацій.

Встановлено, що сучасні системи, незважаючи на впровадження нових технологій (IoT, 5G), залишаються вразливими через архітектурну централізацію та недоліки базових протоколів, таких як TCP/IP, DNS та SMTP.

Визначено основні вектори загроз, серед яких домінують технічні експлойти, атаки типу «людина посередині» (MitM), DDoS-атаки та методи соціальної інженерії.

З’ясовано, що традиційні засоби захисту (брандмауери, IDS/IPS, шифрування) хоч і створюють ешелоновану оборону, проте часто не можуть гарантувати повну незмінність історії транзакцій та захист від компрометації центральних вузлів.

У другому розділі обґрунтовано використання технології блокчейн як ефективного інструменту для забезпечення цілісності та довіри в розподілених системах.

Досліджено принципи децентралізації та використання розподіленого реєстру, які усувають єдину точку відмови та забезпечують прозорість операцій.

Проаналізовано механізми консенсусу (Proof of Work, Proof of Stake) та криптографічні методи (хешування SHA-256, асиметричне шифрування), які унеможливлюють непомітну модифікацію даних.

Визначено потенціал смарт-контрактів для автоматизації політик безпеки та контролю доступу, що дозволяє мінімізувати вплив людського фактору та адміністративних помилок.

У третьому розділі розроблено та досліджено архітектуру системи захищених електронних комунікацій з інтегрованим блокчейн-компонентом.

Запропоновано гібридну архітектуру, де традиційні модулі маршрутизації та інтерфейси поєднуються з рівнем блокчейну через API, що дозволяє фіксувати критичні події (початок сеансу, обмін ключами) у незмінному реєстрі.

Реалізовано алгоритми перевірки цілісності та автентичності повідомлень, де кожен акт комунікації підписується цифровим підписом і хешується, що захищає від атак підміни та повторного відтворення.

Проведено оцінку ефективності системи шляхом стрес-тестування та порівняльного аналізу. Результати показали, що запропонована система демонструє дещо вищу затримку на етапі ініціації транзакцій порівняно з традиційними рішеннями через витрати на консенсус, проте забезпечує стабільність роботи та збереження даних навіть при пікових навантаженнях, уникаючи критичних точок відмови.

Узагальнюючи, можна стверджувати, що інтеграція блокчейн-технологій у системи електронних комунікацій дозволяє створити довірене середовище обміну даними, яке гарантує високий рівень стійкості до кіберзагроз, прозорість аудиту та захист від несанкціонованих модифікацій.