

*Ю.І. ГОРБЕНКО, канд. техн. наук, М.В. ЄСІНА, канд. техн. наук,  
Д.В. МЯЛКОВСКИЙ, О.С. АКОЛЬЗІНА, В.А. ПОНОМАРЬ, канд. техн. наук*

## **СУЧАСНІ ПРОБЛЕМИ ЦЕНТРАЛІЗОВАНИХ ТЕХНОЛОГІЙ ТИПУ «КЛІЄНТ – СЕРВЕР» ТА МОЖЛИВОСТІ ЇХ УДОСКОНАЛЕННЯ НА ОСНОВІ ДЕЦЕНТРАЛІЗАЦІЇ**

### **Вступ**

Нині спостерігаються інтенсивні процеси розроблення та впровадження у різноманітні інформаційні технології (ІТ) принципів децентралізації. Основні з них закладені в технології блокчейн [1 – 5, 9]. Практично широке впровадження технології блокчейн (ТБЧ) зроблено в якості криптовалюти. Але, незважаючи на появу та впровадження на основі ТБЧ перспективних широкомасштабних розробок, продовжують існувати певні сумніви відносно перспектив застосування ТБЧ. Вони, як і більшість нових інформаційних технологій, можуть бути обмеженими в застосуванні, а то і непотрібними [1 – 6].

Нині широке розповсюдження та застосування знайшли ІТ, що ґрунтуються на технології типу «Клієнт – сервер» [7, 8]. Технології «Клієнт – сервер» (англ. Client-server) є обчислювальними або мережевими архітектурами, у яких завдання або мережеві навантаження розподілені між постачальниками послуг, яких називають серверами, та замовниками послуг, яких називають клієнтами. По суті, технології «Клієнт і сервер» є різної складності програмним забезпеченням, що розташовується на різних обчислювальних машинах і взаємодіють між собою через обчислювальну мережу за допомогою мережових протоколів. Вони можуть бути розташовані також і на одній машині. Сервери очікують від клієнтських програм певні запити і надають їм свої ресурси у вигляді даних, сервісних функцій. Оскільки одна програма-сервер може виконувати запити від безлічі програм-клієнтів, її розміщують на спеціально виділеній обчислювальній машині або машинах, налаштованих особливим чином, наприклад, спільно з іншими програмами-серверами. Тому, продуктивність та захищеність тощо, такої «машини – сервера» повинні бути високими. Враховуючи особливу роль такої машини в мережі, специфіки її обладнання та програмного забезпечення, її також називають сервером, а машини, які виконують клієнтські програми, відповідно, клієнтами. Технології «Клієнт – сервер» мають ряд переваг, але в останні роки проявились і ряд їх недоліків.

До основних переваг можна віднести [7, 8]:

- відсутність необхідності дублювання програмного забезпечення сервера клієнтами;
- вимоги до комп'ютерів, на яких встановлено клієнт, знижуються, так як усі обчислення виконуються на сервері;
- усі дані зберігаються на сервері, який, як правило, захищений набагато краще ніж клієнт;
- на сервері простіше організувати контроль повноважень, щоб вирішувати доступ до даних тільки клієнтам з відповідними правами доступу тощо.

Але, в останні роки щодо технологій клієнт – сервер виявлено і ряд недоліків [7, 8], до яких необхідно віднести:

- втрата працездатності сервера приводить до непрацездатності клієнтів або неякісного їх функціонування (непрацездатним сервером слід вважати сервер, продуктивності якого не вистачає на обслуговування всіх клієнтів, а також сервер, що знаходиться на ремонті, профілактиці тощо);
- при зниженні захищеності сервера появляється можливість несанкціонованого доступу до даних, що розміщені на клієнті та компрометації даних, ключів та ключових даних тощо;
- відновлення якісного надання основних послуг безпеки вимагає суттєвих часових та матеріально – технічних ресурсів ;

- підтримка роботи працездатності та безпеки даних ІТ технології клієнт – сервер вимагає використання окремих фахівців – системного адміністратора та адміністратора безпеки тощо;
- висока вартість обладнання та програмного забезпечення сервера тощо.

Тому важливими є відповіді на питання – чи можна та яким чином удосконалити системи «клієнт – сервер». При цьому першим питанням, на яке потрібно відповісти, це як оцінити покращення. Відповіді на дане питання можуть бути для звичайних користувачів та суспільства достатньо простими – нові технології повинні давати принципові та істотні покращення, в порівнянні з тими, що вже є.

Важливим є такий фактор, як людська звичка. Суспільство та суб'єкти (люди) переходять на нові технології тільки в разі, якщо вони дають суттєву перевагу, не просто на 5 – 10 %, а мінімум в 2-3 рази. При цьому, як підтверджено практикою, що для нових ІТ надважливими є такі критерії та показники оцінки та порівняння як вартість, складність (часова та просторова), швидкість, прибутковість, безпечність, анонімність, гнучкість, дизайн тощо [1, 9 – 12].

Наприклад, в найбільш поширеній децентралізованій технології «Біткоїн» необхідно вирішити проблеми курсу та ризику щодо криптовалюти, обміну в звичайні долари, легальності криптовалюти тощо [1, 9]. Також для певної цільової аудиторії необхідно щоб нові властивості, які дає технологія криптовалюти «Біткоїн», відповідали новим вимогам. Тому вже при проектуванні та розробленні і впровадженні нових ІТ, в першу чергу що ґрунтуються на децентралізації, потрібні як глибокі теоретичні дослідження, так і практичні результати щодо вказаних вище характеристик.

За результатами аналізу системних підходів та досвіду застосування нових ІТ спеціалістами [2, 4, 12] сформульовано наступні необхідні, (але недостатні) умови можливого широкого розповсюдження та застосування децентралізованих технологій, в тій чи іншій бізнес-сфері чи інформаційних системах. До них необхідно віднести такі [9, 1 – 6].

1. Застосування децентралізації повинне поліпшити хоча б один із важливих для цільового застосування параметрів: вартість, складність (часова та просторова), швидкість, прибутковість, безпечність, анонімність, гнучкість, дизайн тощо. При цьому важливо, щоб параметр повинен бути використаний не той, що пропонує розробник, а той, що пропонує користувач (замовник).

2. Покращення має бути суттєвим, децентралізація повинна покращувати хоча б один важливий для користувачів параметр, як мінімум в два рази.

3. Нова технологія, в нашому випадку ТБЧ, не повинна істотно програвати старим технологіям за іншими параметрами. Наприклад [9], якщо ТБЧ працює в три рази швидше, але якщо вона при цьому в два рази дорожче і в 1,5 рази складніше – вона, скоріше всього, не отримає визнання та застосування. В якості прийняттого порогу програшу можна взяти біля 30 – 50 %. У цілому нова технологія повинна бути в чомусь краще в 2-3 рази, а за всіма іншими параметрами програвати не більше ніж в 1,5 рази. Тобто, покращення повинне давати суттєві переваги, але ще і компенсувати побічні ефекти щодо програшу за іншими параметрами.

Таким чином, "кращість" і перевага нової технології – це суб'єктивна річ, вона формується користувачами, а не розробниками. Тільки продажі доводять наявність "кращості" та переваг. Відсутність продажів показує, що явної переваги цільовою аудиторією поки ще не визнано.

Таким чином, є проблема, сутність якої в тому, що децентралізація, в тому числі у вигляді ТБЧ, є начебто перспективною технологією, але де саме та як її краще використовувати, де вона буде мати в порівнянні з існуючими технологіями «Клієнт – сервер» кращою, на наш погляд, є не вирішеною .

Метою статті є:

- аналіз основних принципів побудування децентралізованих технологій з використанням ТБЧ та вимоги до них в частині безпеки;
- аналіз особливостей та умов застосування захищених ТБЧ;
- опис на аналіз потенційних атак, коли застосування БЧ є суттєвим механізмом захисту від них;
- сутність та пропозиції відносно протидії атакам спеціального виду.

Автори розуміють, що стаття носить характер первинного загальносистемного аналітичного огляду та відображає погляди авторів на ТБЧ. Ми сподіваємось, що в подальшому буде опубліковано серію науково-практичних статей щодо теорії та практики ТБЧ.

## **1. Основні принципи побудування ТБЧ**

З метою реалізації системного підходу до аналізу та оцінки захищеності розглянемо визнані основні принципи та вимоги щодо побудування ТБЧ. Згідно [4, 9 – 12] при побудуванні ТБЧ повинні бути застосовані чи рекомендовані до застосування такі базові принципи як : мережевої цілісності; розподілення влади; цінності як стимулу для користувачів; захисту (безпеки) інформації та ресурсів; приватності інформації та ресурсів. Важливими також є принципи створення програмного забезпечення; послуг технологій; бізнес моделей та ринків; організація функціонування; при необхідності також управління БЧ тощо. Вказані принципи в основоположній роботі Сатоші у явному вигляді [9,10] не виділялись, але вони використовуються практично для усіх платформ БЧ. Розглянемо базові з них детальніше та будемо враховувати їх при аналізі та оцінках в подальшому [2, 3].

### **1.1. Принцип мережевої цілісності**

Сутність цього принципу в тому, що довіра стосовно БЧ є внутрішньою, а не зовнішньою [3]. Цілісність забезпечується на кожному етапі процесу і є основною її цінністю. Учасники можуть обмінюватись такою цінністю, сподіваючись, що інша сторона діятиме також чесно. Основна її складова – цінність цілісності – чесність у своїх словах і вчинках, врахування інтересів інших, відповідальність за наслідки своїх рішень і дій, а також прозорість у прийнятті рішень та дій. Вона закладена в правах на рішення та в структурах стимулювання. Основна вимога полягає в тому, що діяти без цілісності неможливо або це потребує набагато більше часу, грошей, енергії та репутації [2, 3, 9], якщо вона не забезпечується.

### **1.2. Принцип розподілення влади**

Принцип розподілення влади у наступному [2, 3, 9 – 12]. В одноранговій мережі БЧ влада по суті розподілена, причому точка контролю відсутня. Будь – яка зі сторін не може припинити роботу системи БЧ. Якщо певному центральному управлінню вдасться компрометувати або відрізати індивідуума або групу, система БЧ все ще буде життєздатною. Якщо більше половини мережі спробує знищити всю мережу, то усі побачать, що діється, та будуть протидіяти.

### **1.3. Принцип цінності у якості стимулу для користувачів**

Принцип цінності міститься у наступному. В ТБЧ стимули однакові для всіх зацікавлених сторін. Так bitcoin або інша одиниця цінності є невід'ємною частиною цього вирівнювання та кореляції репутації [2, 3, 9 – 12]. Сатоші розробив програмне забезпечення таким чином, щоб винагородити тих, хто працює і належать до них, були більшими.

### **1.4. Принципи захисту (безпеки) інформації та ресурсів**

Принципи захисту (безпеки) інформації та ресурсів [2, 3, 8 – 12] повинні застосовуватись безумовно. Основним принципом (механізмом) захисту інформації та ресурсів у ТБЧ є застосування криптографічних методів – симетричних та асиметричних криптографічних перетворень та криптопротоколів. Причому, основним призначенням криптографічних механі-

змів є забезпечення цілісності, справжності, неспростовності, доступності та, в певному змісті, криптоживучості ключів та технології БЧ у цілому. Усі користувачі повинні застосовувати такі криптоперетворення як гешування, ЦП та асиметричне шифрування і протоколи встановлення та управління ключами.

На наш погляд, вказаного механізму для забезпечення кібербезпеки в ТБЧ недостатньо. В моделях порушника та загроз не враховуються можливі канали витоку та спеціальні атаки щодо криптографічних перетворень тощо [9, 17 – 20], а також вимоги щодо до криптографічних перетворень для постквантового періоду та їх стандартизації [ ].

Проблема, яку необхідно вирішити щодо криптографічних перетворень, у наступному. Зловмисники особливу увагу в своїх зловмисних діях звертають на крадіжку особистих даних, шахрайство, кібер-залякування, фішинг, спам, шкідливе програмне забезпечення, вимагання – все це підриває безпеку інформації та особистості в суспільстві. В останні роки ними використовуються можливі канали витоку інформації та небезпечного впливу [12 – 13]. Недостатньо, а то і мало в ряді випадків, того, що робиться для підвищення безпеки клієнтів, установ, економічної безпеки та ІТ і ТБЧ.

### **1.5. Принципи приватності інформації та ресурсів**

Принцип приватності інформації та ресурсів у наступному [2, 3, 8 – 10]. Особа повинна контролювати свої власні дані. Причому особи повинні мати право вирішувати, що, коли, як і скільки стосовно своєї особистості вони повинні повідомляти кому-небудь іншому. Повага до права на приватність – це не одне й те ж, що повага до приватності. Необхідно забезпечити і те, і інше. Усуваючи необхідність довіряти іншим, Сатоші усунув необхідність знати справжність особистості, щоб взаємодіяти з нею.

Проблема, яку необхідно вирішити у наступному. Визнано, що приватність – це основне право людини і фундамент вільного суспільства. Нині існує порушення конфіденційності, коли спочатку збираються і використовуються наші дані без згоди або дозволу особи, а потім інформація надійно не захищається від хакерів.

Наслідки для економіки БЧ критичні. Безумовно, що БЧ надає можливості зупинити тиск та спостереження за суспільством. Це, наприклад, для корпорацій дозволяє мати повну інформацію про особу. Швидко з'являються особисті дані про здоров'я та фітнес, щоденні поїздки, життя всередині будинків тощо.

Завдяки технології БЧ можна володіти своїми особистими правами як у віртуальному світі Second Life, але з реальними наслідками. Віртуальний користувач може захистити свою особисту інформацію, роздаючи лише інформацію, необхідну для будь-якої соціально-економічної роботи. При цьому можна переконатись, що отримує особа компенсацію за будь-які дані, які мають значення для іншої сторони.

### **1.6. Особливості блокчейн, які повинні бути враховані при аналізі захищеності**

Розглянемо деякі особливості БЧ, що пов'язані з його рекламою щодо переваг при застосуванні тощо [3, 8 – 15].

Важливою особливістю є необґрунтованість застосування ТБЧ. Існує тенденція до непомірного пропагування щодо використання ТБЧ, яка нині розвивається. Виконано значне число проєктів, що рекламуються та впроваджуються [2, 3]. Іноді є намагання включати ТБЧ, навіть, якщо вона не зовсім потрібна чи не потрібна. Вказане пов'язано з тим, що технологія ТБЧ є відносно новою і не дуже зрозумілою. Нижче розглянемо деякі обмеження і, можливо, необґрунтовані погляди, що пов'язані з технологією БЧ.

Незмінність технології. Більшість джерел, що стосуються ТБЧ, описують реєстри ланцюга блоків як незмінні. Насправді, це не зовсім так. Вказане можна пояснити тим, що вони захищені від несанкціонованого доступу, внаслідок чого є довіра, наприклад через фінансові транзакції. Але ТБЧ не можуть вважатися повністю незмінними, тому що є ситуації, в яких ТБЧ може бути зміненою. Тому вкажемо на способи, за допомогою яких може бути порушена концепція незмінності щодо реєстрів БЧ.

## **1.7. Особливості забезпечення кібербезпеки в блокчейн**

Використання технологій БЧ не усуває властиві для кібербезпеки ризики [2, 3, 8 – 11], що вимагають продуманого та активного управління ними. Скоріше всього, більшість з них пов'язані з людським фактором. Тому повинна бути розроблена та використовуватись надійна програма кібербезпеки ТБЧ, захисту мережі та організацій – учасників від кіберзагроз. Це повинне бути зроблене з урахуванням того, що хакери отримують все більше знань про ТБЧ та їх вразливості.

Також існуючі стандарти і керівництва в області кібербезпеки, як і раніше, мають велике значення для забезпечення безпеки систем, що взаємодіють та/або покладаються на ТБЧ. За умови певних коригувань, для розгляду конкретних характеристик ТБЧ існуючі стандарти і рекомендації забезпечують значну основу для захисту мереж БЧ від кібератак.

На додаток до загальних принципів і засобів контролю також прийнятні конкретні стандарти кібербезпеки, що мають відношення до ТБЧ, які вже існують і широко використовуються в багатьох галузях, наприклад NIST Cybersecurity Framework [9]. В ньому стверджується, що не існує «єдиного підходу до усунення загроз кібербезпеки», через те, що «організації будуть і далі мати унікальні ризики: різноманітні загрози, вразливості, схильності до ризиків, а відповідно, спосіб практичного використання ТБЧ в рамках структури буде різним.

## **1.8. Особливості застосування інфраструктури відкритого ключа та ідентифікація**

Якщо ТБЧ включає інфраструктуру відкритого ключа (ІВК), то деякі користувачі відразу ж думають, що при її використанні здійснюється і ідентифікація особистості [9, 13 – 16]. Але це не зовсім так, оскільки відносин «один на один» з використанням особистих ключів може і не існувати (користувач може мати декілька особистих ключів), також як і може не бути відносин «один на один» між адресами в ТБЧ і відкритими ключами (множинні адреси можуть впливати з єдиного відкритого ключа).

Часто ЦП використовуються для підтвердження ідентичності у цифровому світі при забезпеченні кібербезпеки, що може призвести до плутанини відносно потенційного застосування ТБЧ для управління ідентифікацією. Процес перевірки ЕП транзакції в блокчейні пов'язує транзакції з власниками особистих ключів, але не надає можливості для зв'язування реальних ідентифікаторів з цими власниками. У деяких випадках можна пов'язувати ідентифікатори реального цифрового світу з особистими ключами, але ці зв'язки виконуються через зовнішні процеси, а не підтримуються БЧ напряму. Наприклад, правоохоронні органи можуть запитувати записи з біржі, які пов'язують транзакції з конкретними особами. Іншим прикладом є індивідуальна публікація криптовалютної адреси на своєму особистому веб-сайті або сторінці, наприклад для пожертвувань в соціальній мережі, що забезпечить зв'язок між адресою та ідентифікатором у реальному цифровому світі.

Хоча, ТБЧ можна використовувати в інфраструктурах управління ідентифікацією, для яких потрібен розподілений компонент реєстру, важливо розуміти, що типові реалізації БЧ не призначені для автономних систем управління ідентифікацією. Існує більше можливостей мати надійні цифрові ідентифікатори, ніж просто реалізувати ТБЧ.

Таким чином, як при аналізі, так і в процесі синтезу ТБЧ важливими є основоположні принципи, що визначають сутність, вимоги та можливості ТБЧ.

## **2. Особливості та умови застосування ТБЧ**

Як зазначалося вище, ТБЧ мають свої особливості та вразливості. Серед особливостей, що стосуються безпеки ТБЧ, слід відмітити такі [11 – 13]: складність системи, розміри мережі, швидкість і ефективність мережі, політика використання, зловмисні користувачі, відсутність довіри, ігнорування транзакцій конкретних користувачів, вузлів або навіть цілих держав, створення зміненого, альтернативного ланцюга щодо таємниці. Розглянемо та проаналізуємо їх.

*Складність системи.* Якщо вирішено створити систему на основі ТБЧ з нуля, то одна невелика помилка може стати фатальною та зруйнувати всю розробку. Звичайно ж, це не можна вважати недоліком самого БЧ – це, скоріше, стосується особливостей його використання. Розробник, що створює блокчейн або займається його розробкою та підтриманням дієздатності, має бути дуже досвідченим, бо вірогідність допустити помилку у такій складній системі підвищується. Це можна побачити у сфері криптовалют, де регулярно відбуваються викрадення криптовалюти у користувачів або загалом компрометація усієї мережі навіть у найбільших проектах [20].

*Розміри мережі.* Для роботи БЧ необхідні як мінімум кілька сотень, а ще краще кілька тисяч узгоджено працюючих вузлів. Саме через це ТБЧ є вкрай вразливою до атак на початкових етапах роботи. Наприклад, якщо який-небудь користувач зможе отримати контроль над 51 % вузлів системи, то він зможе повністю контролювати створення блоків у мережі БЧ. А якщо в системі всього 20 вузлів, то подібний варіант розвитку подій більш, ніж можливий. Проте навіть ця атака вже враховується при побудованні сучасних мереж БЧ та нівелюється за допомогою більш досконалих систем консенсусу.

*Швидкість і ефективність мережі.* Структура мереж БЧ – це також одна з причин, з використанням якої може бути порушено нормальне функціонування мережі БЧ. Так, якщо мережа БЧ отримує надто широке поширення, а інфраструктура БЧ виявиться не готовою до такого обсягу операцій, то в результаті може знизитися швидкість проведення транзакцій, можуть з'явитися проблеми зі зберіганням даних, що негативно вплине на ефективність мережі БЧ. Також, до цієї проблеми можна віднести ситуацію, коли кількість користувачів (транзакцій) в системі буде перевищувати теоретичну максимально можливу кількість транзакцій в мережі (транзакцій в секунду), що може призвести до довгого очікування підтвердження транзакцій.

*Політика використання.* З огляду на те, що валюта в мережі БЧ є міжнародною і децентралізованою, це, по суті є загрозою для контрольованих державою валют. На даний момент керівні органи деяких держав прагнуть ввести більш суворі обмеження на використання БЧ. У різних країнах сподіваються взяти систему під контроль до того, як вона стане серйозним конкурентом і почне загрожувати їхній економіці. Непрямим чином це також є суттєвою загрозою для сучасної банківської системи. Наразі ця загроза є вкрай реальною, наприклад, за неофіційними даними Китай контролює близько 60 % обчислювальних потужностей біткоіну та потенційно може його скомпрометувати [9].

*Застосування ключів.* В транзакціях в мережі БЧ використовуються асиметричні пари ключів – публічні і особисті криптографічні ключі. Самі по собі такі ключі зламати майже неможливо на звичайному комп'ютері, проте зловмисник може отримати їх більш простим і звичним способом. Наприклад, ключі можна дістати в тому випадку, якщо ви зберігаєте їх на небезпечній або незахищеній платформі. Використання соціальної інженерії та викрадення ключів із менш захищених ресурсів є найбільш популярним способом на сьогоднішній день серед криптовалютних зловмисників [1 – 6, 9, 19].

*Зловмисні користувачі.* Мережа БЧ не може нав'язувати правила та інструкції з проведення транзакцій, вона не може диктувати користувачам норми поведінки. Тому це проблематично для permissionless мереж БЧ через те, що користувачі виступають під псевдонімами і немає відповідності «один до одного» між ідентифікаторами користувачів мережі і іменами користувачів системи. Permissionless мережі часто надають винагороду (наприклад, криптовалюту), щоб мотивувати користувачів діяти справедливо; проте деякі можуть вибирати зловмисну поведінку, якщо це дає більшу винагороду. Найбільша проблема для зловмисних користувачів – отримати достатню потужність (чи то ставку в системі, обчислювальну потужність тощо), щоб завдати шкоди.

Аналіз показав, що якщо створюється досить велике зловмисне співтовариство, злочинні дії можуть зводитись до наступних дій та поведінки [1 – 6, 9].

*Ігнорування транзакцій конкретних користувачів, вузлів або навіть цілих держав.*

Створення зміненого, альтернативного ланцюга таємниці, а потім його відправка, як тільки альтернативний ланцюг довший реально побудованого. Чесні вузли будуть перемикатися на ланцюг, який має найбільшу «роботу» (за протоколом БЧ). Це може порушити основний принцип мережі БЧ – порушити її прозорість до підробки та захист від несанкціонованого використання [3].

*Відмова передавати блоки на інші вузли.* По суті, порушуючи розподіл інформації (це не є проблемою, якщо мережа БЧ є досить децентралізованою). У той час як зловмисні користувачі можуть створювати неприємності і наносити короточасну шкоду, мережі БЧ можуть виконувати жорсткі розгалуження для боротьби з ними. Чи будуть відшкодовані збитки (втрачені гроші), залежить від розробників і користувачів мережі БЧ [9].

*На додаток до наявності зловмисних користувачів в мережах,* адміністратори інфраструктури БЧ в permissioned мережах можуть також діяти зловмисно. Наприклад, адміністратор інфраструктури може (в залежності від точної конфігурації) мати можливість захопити виробництво блоків, виключати деяких користувачів з виконання транзакцій, переписувати історію блоків, двічі витратити монету, видаляти ресурси, переадресувати чи блокувати мережеві підключення [9, 19].

*Відсутність довіри.* Інша поширена невірна інтерпретація щодо роботи БЧ може надходити від осіб, які знають, що в БЧ немає «третьої довіреної сторони», а мережі БЧ є «не довіреними» середовищами. Не дивлячись на те, що третя довірена сторона не сертифікує транзакції в permissionless мережах блокчейн (в permissioned системах це менш помітно, оскільки адміністратори системи діють, як довірені особи, надаючи користувачам допуски і дозволи). Для правильного функціонування мережі БЧ все ж необхідний досить високий ступінь довіри всередині мережі, в тому числі коли [2 – 6, 9].

1) Існує довіра до криптографічної технології, що використовується, але криптографічні алгоритми або їх реалізації можуть мати недоліки.

2) Існує довіра до правильної і безперервної роботи смарт-контрактів, які можуть мати ненавмисні лазівки і недоліки.

3) Існує довіра до розробників, які виробляють програмне забезпечення якомога більш стабільним.

4) Існує впевненість в тому, що більшість користувачів блокчейну не вступають у таємну змову. Якщо окрема група або фізична особа може керувати більш, ніж 50 % всієї потужності створення блоків, виникає можливість підірвати permissionless мережу блокчейн. Однак, як правило, отримання необхідної обчислювальної потужності є надмірно дорогим.

5) Для користувачів мережі БЧ, які не мають повного вузла, існує довіра до того, що вузли приймають і обробляють транзакції справедливо.

## **2. Опис та аналіз потенційних атак, коли застосування БЧ є суттєвим механізмом захисту від них**

Аналіз показав [9 – 12], що проблема безпеки інформації та безпеки взагалі ІТ, стоїть перед сучасним цифровим світом досить гостро. Зростає кількість кіберзагроз, що пов'язані з крадіжкою ідентифікаційних даних. За інформацією аналітичного агентства Cybersecurity Venture, щорічний збиток від кіберзлочинів досягне до 2021 р. порядку шість трильйонів доларів. У 2017 р. збиток становив чотири трильйони. Тому зростає і кількість коштів, вкладених в кібербезпеку, – до 2021 р. витрати перевищать один трильйон доларів. Це пояснюється тим, що ТБЧ при їх застосуванні безпосередньо, а також у інших ІТ забезпечує захист від цілого спектру різних атак. Розглянемо та проаналізуємо основні із них [10 – 13, 21, 22].

### **3.1. Атаки типу «людина посередині»**

Нині для захисту з'єднань (наприклад, HTTPS і TLS) [23], тобто каналів зв'язку, використовується ІВК, що включає засвідчувальні центри (ЗС) та центри сертифікації ключів (ЦСК). Кожен учасник мережі має пару відкритий/особистий ключ. Особистий ключ він зберігає в таємниці. Відкритий ключ зберігає ЦС. Коли користувач хоче встановити безпечне з'єднання

(зайти на сайт), він відправляє запит на відкритий ключ ресурсу у сертифікаційного центру і шифрує дані перед відправкою, використовуючи свій особистий ключ та відкритий із сертифікату. Щоб розшифрувати дані, сервер (сайт) використовує свій особистий ключ та відкритий відправника.

У цьому випадку криптостійкість (надійність) системи залежить від того, наскільки добре захищений засвідчувальний центр. Якщо зловмиснику вдається компрометувати засвідчувальний центр, то він отримає можливість провести атаку man-in-the-middle – MITM («люди на посередині»). У цьому випадку виконується розсилка підроблених відкритих ключів, до яких у хакерів є відповідні особисті (із пари фальшивих) ключі. З їх допомогою виконується розшифрування інформації, що передається від клієнта до серверу чи навпаки.

Однак, проведений аналіз показав, що в системі, що побудована на блокчейні, MITM атаку не можна реалізувати. Коли користувач публікує відкритий ключ в БЧ, про це «дізнаються» всі вузли мережі (наприклад, БЧ біткоіна має 10 тисяч активних вузлів). Ця інформація записується в блок, і цілісність реєстру захищається криптографічно. Тому опублікувати підроблені ключі зловмисники з великою ймовірністю не зможуть, таку спробу відразу розпізнають користувачі та не приймуть вузли мережі БЧ. Це однак із основних переваг ТБЧ.

### 3.2. Маніпулювання даними

Важливою вимогою до даних ІТ є коректність даних у мережі. Наприклад, якщо завантажуються файл із Інтернету та для того, щоб перевірити його цілісність та автентичність, як правило використовується його геш-значення. Так як в ІТ «клієнт – сервер» файл і дані про його геш-значення зберігаються на сервері централізовано, то зростає вірогідність підробки цих даних [16 – 19]. Навіть використання простої перевірки геш-значення, що міститься на офіційному ресурсі цього файлу, несе в собі елемент довіри користувача до цього ресурсу. Наприклад, відомі випадки, коли подібний офіційний ресурс атакували та робили підміну геш – значення на своє. У результаті користувач, що хоче перевірити геш-значення файлу зловмисника потрапить на сайт, що знаходиться під контролем того самого зловмисника, пройде перевірку та інсталує шкідливе програмне забезпечення.

Блокчейн у свою чергу дозволяє записати геш-значення у БЧ та бути з великою вірогідністю певним, що воно залишиться незмінним, а вірогідність підробки його з часом буде майже нульовою, оскільки це буде вимагати також підробки усіх наступних блоків БЧ, що є майже неможливою задачею для сучасних комп'ютерних систем.

### 3.3. DDoS-атаки

Завданням розподілених мережових атак є обмеження пропускної здатності мережевого ресурсу, наприклад інфраструктури, що підтримує сайт компанії чи системи «клієнт – сервер» [12 – 14]. Так, веб-сервери завжди мають обмеження за кількістю запитів, що оброблюються одночасно (пропускна здатність). Якщо число звернень до сервера перевищує можливості будь-якого компонента інфраструктури, виникають проблеми з рівнем обслуговування. Причому масштаб цих проблем залежить від мети DDoS-атаки.

Наприклад, масована DDoS-атака на американського DNS-провайдера Dyn залишила мільйони користувачів без таких сервісів, як Twitter, PayPal, Netflix і GitHub [ ]. DDoS-атака на Dyn проводилася за допомогою гігантського ботнету Mirai, що включав десятки мільйонів пристроїв: роутери, принтери, IP-камери і інші пристрої, підключені до Інтернету. Всі разом вони трансливали дані на сервери Dyn зі швидкістю 1,2 Тбіт/с. А в жовтні цього року почав поширюватися вірус Reaper, що заражає «розумні» пристрої по всьому світу.

Атака на DNS-провайдера показує, наскільки централізовані системи роблять всю інтернет-інфраструктуру вразливою. Більш серйозним сценарієм розвитку атак на DNS-сервери є його компрометація з метою перенаправлення користувачів на сайти із шкідливим програмним забезпеченням.

Однак можна відмовитися від центральних DNS-серверів і реалізувати систему, в якій пари «ім'я – IP-адреса» реєструються в мережі БЧ та розподіляються по всіх вузлах. Це



забезпечить прозорість перетворень та і захищеність одночасно. Зловмисники не зможуть зруйнувати якусь одну певну інфраструктуру, атакувавши лише один із кластерів. Самі дані будуть захищені засобом застосування ЕП, гешування та криптографічних протоколів. Застосування БЧ також суттєво зменшить мережеві витрати, пов'язані з читанням DNS.

### **3.4. Захист пристроїв «інтернету речей»**

Згідно з результатами дослідження компанії F5 Networks, число атак на пристрої інтернет («інтернет речей», Internet of Things) та їх інфраструктуру зросло з початку 2018 р. на 280 % [3, 19]. Здебільшого це пов'язано з поширенням зловмисниками шкідливого програмного забезпечення. В цьому випадку Зловмисники атакують інтернет-пристрої та використовують їх для проведення DDoS-атак і хостингу інфраструктури різних вірусів [19, 22].

Вважається, що застосування БЧ дозволить захистити інтернет з тих же причин, за яких він використовується в криптовалютах – впевненість в легітимності даних і чіткий процес їх підтвердження. Однак необхідно враховувати, що простої реєстрації пристрою в БЧ – недостатньо. Необхідна ціла інфраструктура для управління пристроями і контролю доступу до даних. Проведений аналіз показав, що вже існують декілька рішень від публічних проєктів, що реалізують цю систему. Наприклад, одним з рішень може стати проєкт ChainAnchor [9]. Це фреймворк, який будуть підтримувати розробники «розумних пристроїв», провайдери даних і незалежні розробники. Ідея полягає в тому, що учасники мережі, в обмін на підтримання безпеки, отримують можливість продавати анонімні дані з інтернет-пристроїв. Фреймворк має механізми, що дозволяють блокувати компрометовані пристрої, а також відключати від БЧ легітимні пристрої при зміні власника. Він також дозволяє працювати в умовах необмеженого зростання даних [5, 9].

### **3.5. Кібер та мережеві атаки**

Нині ТБЧ [5, 9 – 12, 22, 23] рекламуються як дуже безпечні. Це можна пояснити в силу захищеності від несанкціонованого доступу (НСД) – як тільки транзакція у блокчейні здійснена, її взагалі не можна змінити. Однак це справедливо тільки для транзакцій, які були включені в опублікований блок. Транзакції, які ще не були включені в опублікований блок в ланцюгу, вразливі для декількох типів атак. Так у мережах БЧ, які мають мітки часу для транзакцій, підроблення часу або зміна годин користувача могло б мати негативний або позитивний вплив на транзакцію, роблячи час і повідомлення часу вектором атаки. Відмова в обслуговуванні, коли атака може проводитися на платформі БЧ або на інтелектуальному контракті, реалізованому на платформі.

Мережі БЧ та їх застосування не захищені від зловмисних учасників, які можуть проводити мережеве сканування і розвідку, щоб виявляти і використовувати вразливості, а також запускати атаки нульового дня. Служби, засновані на БЧ, та розгорнуті в поспіху, або тільки закодовані додатки (такі, як інтелектуальні контракти) можуть містити нові, а також відомі вразливості і слабкості розгортання. Вони і будуть знайдені і потім атаковані через мережу, так само, як атакують сайти і додатки в теперішній час.

### **3.6. Огляд та класифікація атак спеціального типу**

Атаки спеціального виду (side-channel attacks) можна віднести до атак аналітичного типу. Реалізація цих атак направлена на пошук вразливостей у практичній реалізації криптосистеми, в першу чергу засобу криптозахисту інформації (КЗІ). У [23] запропоновано класифікацію спеціальних атак за такими ознаками:

- контроль над обчислювальним процесом;
- спосіб доступу до системи чи засобу;
- метод безпосереднього здійснення атаки.

На рис. 1. наведено модель, яка пояснює атаки спеціального виду [23].

*Класифікація спеціальних атак за ступенем впливу на обчислювальний процес.* Аналіз показав [23], що за ступенем впливу на обчислювальний процес спеціальні атаки можна поділити:

- на пасивні, коли зловмисник отримує необхідну інформацію без помітного впливу на систему, але система при цьому продовжує функціонувати як і раніше;
- активні, коли зловмисник реалізує деякий вплив на систему, у результаті якого змінюється поведінка системи, але зміни такого роду можуть бути «прозорими» для системи, на яку відбувається напад.

При цьому зловмисник у змозі визначати та використати інформацію про систему БЧ.

*Класифікація спеціальних атак по способу доступу до системи.* В залежності від можливості доступу до апаратно-програмного чи апаратного засобу КЗІ можна виділити такі класи атак [36]:

- агресивні (англ. *invasive*) – коли здійснюється спроба розкриття системи зловмисником та отримання прямого доступу до внутрішніх компонентів;
- напівагресивні (англ. *semi-invasive*) – коли вплив на внутрішні компоненти засобу КЗІ здійснюється без посереднього контакту;
- не агресивні (англ. *non-invasive*) – коли використовується тільки зовнішня інформація – наприклад, час обчислення чи споживання енергії. Тобто безпосереднього впливу на систему, що досліджується, немає.

*Класифікація спеціальних атак за методом здійснення атаки.* Спеціальні атаки, в залежності від методів, які використовуються для аналізу отриманої інформації, можна поділити [23]:

- на прості (*simple side channel attack*) – коли здійснюється дослідження прямої залежності між процесами в пристрої та отриманої зловмисником інформації, а результатом атаки є виділення корисної інформації, наприклад, від рівня шумів;
- диференційні (*differential side channel attack*) – коли використовуються статистичні методи дослідження залежностей між вхідними даними та інформацією, яка отримана під час спостереження.

Як правило, при цьому здійснюється велика кількість вимірювань, а також спеціальна обробка сигналу і корекція помилок. В процесі здійснення атак на реалізацію засобу КЗІ може здійснюватись аналіз усіх зовнішніх параметрів засобу, а також усі можливі методи порушення його нормального функціонування, аж до його руйнування з метою отримання секретного ключа.

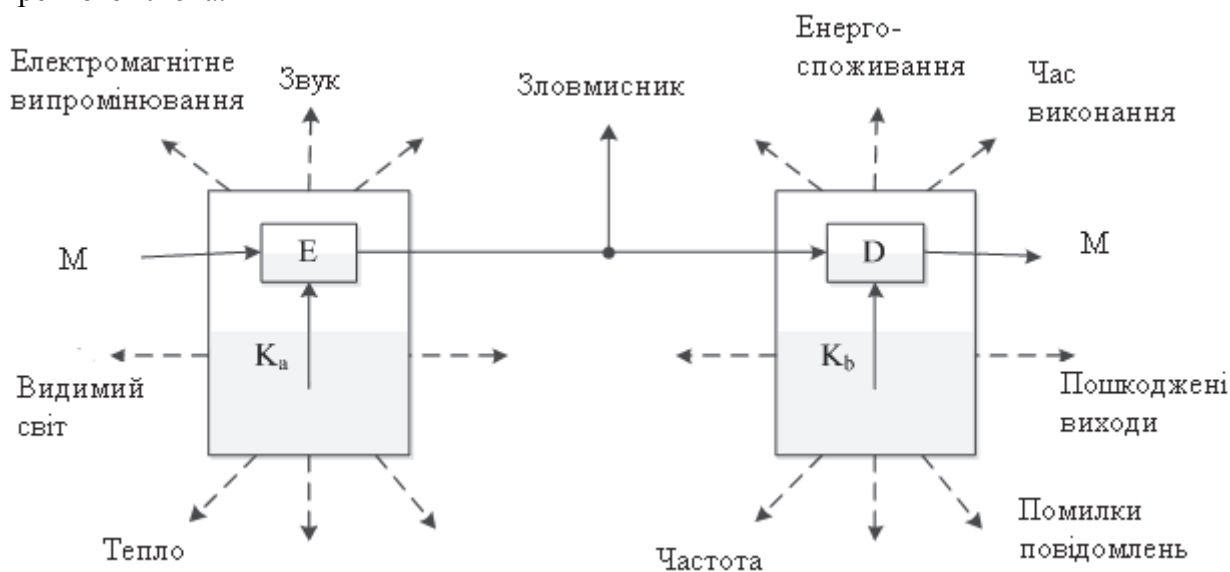


Рис. 1. Криптографічна модель відносно атак спеціального виду

При виконанні атак за часом [23] вимірюється час виконання алгоритму криптоперетворення. У реалізаціях асиметричних алгоритмів час виконання операцій також може залежати як від оброблюваних даних, так і від ключа криптоперетворення (ЕП, АСШ, ПІК). При використанні апаратного рішення у вигляді автомата з жорсткою логікою навіть час складання за деяким модулем може змінюватися у залежності від реалізації ланцюгів перенесення.

Атаки на реалізацію можуть ґрунтуватись на аналізі всіх споживаних потужностей сучасних обчислювальних пристроїв КЗІ, особливо таких, що побудовані на використанні елементів схемотехніки TTL (TTL), TTLШ (TTL(S)), а також частково і КМОП (CMOS). Вона також залежить від оброблюваних даних. Тому у зловмисника з'являється можливість отримати інформацію про внутрішній стан автомата, у тому числі секретний ключ, наприклад шляхом аналізу енергоспоживання при АСШ чи ЦП. Так, атака, що описана у [23], дозволяє на основі аналізу енергоспоживання обчислити вагу Хемінга (кількість одиничних бітів) оброблюваного блоку. Ця інформація, а також знання виключно відкритих текстів (без знання шифротексту), дає зловмисникові можливість відтворити таємний ключ шифрування. Крім того, якщо у порушника є можливість порушувати нормальну роботу пристрою (наприклад, вносити збої), то за допомогою спеціальних методів можна відновити практично будь-який секретний параметр системи.

Основною метою фізичної атаки є дослідження особливостей реалізації пристрою КЗІ (мікросхеми), що потрібно для отримання інформації відносно особистого або таємного ключів, наприклад, шляхом дослідження області всередині кристалу ПЛІС. Як правило, такі атаки орієнтовані на специфічні області ПЛІС, які в режимі нормального функціонування є не доступними.

#### **4. Сутність та пропозиції відносно протидії атакам спеціального виду**

Наші попередні дослідження показали, що існуючі криптографічні механізми, що застосовуються в ТБЧ, не забезпечують захист від атак спеціального виду. Для забезпечення захисту потрібно застосовувати, як мінімум, постквантову криптографію – асиметричні перетворення типу ЕП, АСШ та криптографічні протоколи інкапсуляції ключів. Детальніше ці питання висвітлені в [9, 17 – 20, 23]. Відмітимо, що в основу захисту від атак спеціального виду можуть бути покладені методи, що розглядаються нижче.

##### **4.1. Фіксована кількість звернень до геш-функції**

В [23] розглянуто атаку спеціального виду за часом, яка може розкрити секретний ключ NTRU. Ця атака можлива завдяки тому, що у розшифруванні різних шифротекстів використовується різна кількість звернень до геш-функції. Методом протидії таким атакам є використання механізму доповнення. Розмір доповнення повинен відповідати необхідному рівню криптостійкості. В цьому випадку використовується схема доповнення NAEP, а розмір доповнення дорівнює розміру геш-значення, яке задовольняє умові

$$Hlen = \begin{cases} 160 & k \leq 112 \\ 256 & k > 112 \end{cases} \quad (1)$$

де  $k$  – рівень криптостійкості.

За умови виконання (1) можна сподіватись, що криптоперетворення і, як наслідок, криптосистема, може бути захищеною від атак за часом.

##### **4.2. Рандомізація даних**

Метод рандомізації зводиться до «засліплення» даних [24 – 28]. По суті, воно зводиться до зміни вхідних даних в деякий непередбачуваний стан. Залежно від характеристик функції «засліплення», вона може виключити деякі або всі витoki корисної інформації. Основною властивістю вхідних даних є їх псевдовипадковість. У криптосистемі «NTRU Prime ІТ

Ukraine»[25] застосовується засліплюючий поліном, що запобігає витоку інформації про секретний ключ.

#### 4.3. Незалежність від значень

Якщо усі перетворення із особистим ключем та поліномом засліплення при зашифруванні та розшифруванні не залежать від значень засліплюючого поліному та особистого ключа, то про них неможливо по стороннім каналам дізнатися будь-яку інформацію. Також, якщо в операції множення не використовується значення секретного ключа, то неможливо отримати інформацію про секретний ключ, аналізуючи операцію множення по стороннім каналам.

#### 4.4. Вплив заходів стійкості на кількість ключів NTRU-подібного алгоритму

Аналіз показав, що в будь-якому разі ключі криптоперетворення повинні задовольняти властивостям випадкових послідовностей. До таких властивостей належать: випадковість, рівномірність та незалежність. В «NTRU Prime ІТ Ukraine» [25 – 27] це забезпечується за рахунок фіксованих значень кількостей ненульових елементів у секретних ключах  $f$  та  $g$ . Так, кількість 1, -1, 0 приблизно є рівною.

У табл. 1 – 3 у якості прикладу наведено конкретні значення параметрів для першого, середнього та останнього набору параметрів згідно [26 – 27]. У [25, 26] визначено наступне співвідношення (1, -1, 0) для секретних ключів  $f$  та  $g$ : для  $f$  кількість 1 та -1 позначається як  $df$  та дорівнює  $df=2t$ , для  $g$  кількість одиниць дорівнює  $dg1=n/3+1$ , кількість -1 дорівнює  $dg-1=n/3$ .

Таблиця 1

Приклади параметрів NTRU Prime ІТ Ukraine

Параметри				
n	q	t	рівень стійкості k	
439	6833	142	112	1
727	5827	121	205	2
1021	8819	183	298	3

Таблиця 2

Стійкість NTRU Prime ІТ Ukraine

Число ненульових елементів	Рівень стійкості		
	1	2	3
$df=2t$	184	242	366
$dg1=n/3+1$	147	243	341
$dg-1=n/3$	146	242	340

У табл. 3 наведено значення кількості можливих ключів, які отримані при застосуванні формули (1).

Таблиця 3

Кількість ключів NTRU Prime ІТ Ukraine

Число ненульових елементів	Рівень стійкості		
	1	2	3
для $f$	$0,3 * 10^{193}$	$0,9 * 10^{344}$	$0,3 * 10^{482}$
для $g$	$0,5 * 10^{207}$	$0,9 * 10^{344}$	$0,1 * 10^{485}$

Якщо немає обмеження на кількість 1, -1 для ключів, наприклад, як для схеми Crystals-Kyber то для підрахунку треба використовувати формулу (2) розміщення з повторенням:

$$A_n^m = n^m, \quad (2)$$

де  $n$  – для ключів це кількість елементів, тобто 3, а  $m$  – кількість позицій, тобто розмір ключа.

У табл. 4 наведено значення кількості секретних ключів при відсутності обмежень на кількість коефіцієнтів.

Таблиця 4

Кількості секретних ключів без обмеження на кількість коефіцієнтів

	Рівень стійкості		
	1	2	3
Кількість секретних ключів	$0,3 * 10^{210}$	$0,7 * 10^{347}$	$0,1 * 10^{488}$

Аналіз показав, що при введенні обмежень розмір простору ключів зменшується. У табл. 5 наведено значення, у скільки разів зменшується кількість ключів, якщо ввести обмеження на коефіцієнти згідно з наведеним вище.

Таблиця 5

Зменшення розміру ключового простору

Число ненульових елементів	Рівень стійкості		
	1	2	3
для f	$10^{17}$	$0,8 * 10^3$	$0,3 * 10^6$
для g	$0,6 * 10^3$	$0,8 * 10^3$	$10^3$

Таким чином, обмеження на кількість ненульових коефіцієнтів призводить до зменшення кількості ключів від 17-ти до 3-х десяткових порядків. Однак ця міра є необхідною задля захисту перспективних криптоперетворень постквантового періоду від атак по стороннім каналам. Але, для реалізації наведених пропозицій щодо захисту від спеціальних атак потрібно використовувати принципово нові криптографічні механізми, скоріше всього постквантового періоду [17, 18, 26 – 28].

## Висновки

1. Впровадження у різноманітні інформаційні технології принципів децентралізації має суттєві перспективи. Основні з них закладені в технології БЧ. Але, незважаючи на появу та впровадження на основі ТБЧ перспективних широкомасштабних розробок, продовжують існувати певні сумніви відносно перспектив застосування ТБЧ. Вони, як і більшість нових інформаційних технологій, можуть бути обмеженими в застосуванні, а то і непотрібними.

2. Відносно застосування БЧ важливими є відповіді на питання – чи можна та яким чином удосконалити системи «клієнт – сервер». При цьому першим питання, на яке потрібно відповісти, це як оцінити покращення. Відповіді на дане питання можуть бути для звичайних користувачів та суспільства достатньо простими – нові технології повинні давати принципові та істотні покращення, в порівнянні з тими, що уже існують.

3. Важливим є такий фактор, як людська звичка. Суспільство та суб'єкти) переходять на нові технології, тільки в разі, якщо вони дають суттєву перевагу, не просто на 5 – 10 %, а мінімум в 2-3 рази. При цьому, як підтверджено практикою, що для нових ІТ надважливими є такі критерії та показники оцінки та порівняння як вартість, складність (часова та просторова), швидкість, прибутковість, безпечність, анонімність, гнучкість, дизайн тощо.

4. Нова технологія, в нашому випадку ТБЧ, не повинна істотно програти існуючим технологіям за іншими параметрами. Наприклад, якщо ТБЧ працює в три рази швидше, але якщо вона при цьому в два рази дорожче і в 1,5 рази складніше – вона, скоріше всього, не отримає визнання та застосування. В якості прийняттого порогу програшу можна взяти біля 30 – 50 %. У цілому нова технологія повинна бути в чомусь краще в 2-3 рази, а за всіма іншими параметрами програти не більше ніж в 1,5 рази. Тобто, покращення повинне давати суттєві переваги, але ще і компенсувати побічні ефекти щодо програшу за іншими параметрами.

5. З метою реалізації системного підходу до аналізу та оцінки захищеності розглянемо визнані основні принципи та вимоги щодо побудування ТБЧ. При побудуванні ТБЧ повинні бути застосовані чи рекомендовані до застосування такі базові принципи як: мережевої цілісності; розподілення влади; цінності як стимулу для користувачів; захисту (безпеки) інформації та ресурсів; приватності інформації та ресурсів. Важливими також є принципи створення програмного забезпечення; послуг технологій; бізнес моделей та ринків; організація функціонування; при необхідності також управління БЧ тощо.

6. Серед особливостей, що стосуються безпеки ТБЧ, слід відмітити: складність системи, розміри мережі, швидкість і ефективність мережі, політика використання, зловмисні користувачі, відсутність довіри, ігнорування транзакцій конкретних користувачів, вузлів або навіть цілих держав, створення зміненого, альтернативного ланцюга щодо таємниці.

7. Атаки спеціального виду (side-channel attacks) можна віднести до атак аналітичного типу. Реалізація цих атак направлена на пошук вразливостей у практичній реалізації криптосистеми, в першу чергу засобу криптозахисту інформації (КЗІ). У [23] запропоновано класифікацію спеціальних атак за такими ознаками:

- контроль над обчислювальним процесом;
- спосіб доступу до системи чи засобу;
- метод безпосереднього здійснення атаки.

8. Для захисту криптосистеми «NTRU Prime ІТ Ukraine» від атак за часом пропонується під час шифрування здійснювати фіксовану кількість звернень до геш-функції, а також здійснювати засліплення даних (що вносить додаткову випадковість). Також усі перетворення, що здійснюються з секретними параметрами, не повинні залежати від конкретних значень цих параметрів.

9. Якщо усі перетворення із особистим ключем та поліномом засліплення при зашифруванні та розшифруванні не залежать від значень засліплюючого поліному та особистого ключа, то про них неможливо по стороннім каналам дізнатися будь-яку інформацію. Також, якщо в операції множення не використовується значення секретного ключа, то неможливо отримати інформацію про секретний ключ аналізуючи операцію множення по стороннім каналам.

10. Для забезпечення захисту потрібно застосовувати як мінімум постквантову криптографію – асиметричні перетворення типу ЕП, АСШ та криптографічні протоколи інкапсуляції ключів. Детальніше ці питання висвітлені в [9, 17 – 20, 23].

#### Список літератури:

1. Andreas M. Antonopoulos Mastering Bitcoin: Unlocking Digital Cryptocurrencies / Andreas M. Antonopoulos Kyiv : NGITS, 2014. – С. 10 – 150.

2. Що таке децентралізований додаток? [Електронний ресурс]. Режим доступу: <https://www.coindesk.com/information/what-is-a-decentralized-application-dapp>.

3. Don Tapscott, Alex Tapscott Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World / Don Tapscott, Alex Tapscott Blockchain. Kyiv : Information Systems, 2016. С. 65 – 102.

4. 20 основних застосувань БЧ [Електронний ресурс]. Режим доступу: <https://biznesmodeli.ru/blockchain-cto-eto-cases-crypto-top10/>.

5. БЧ: атаки, безопасность и криптография [Електронний ресурс]. Режим доступу: [https://www.securitylab.ru/blog/personal/Informacionnaya\\_bezopasnost\\_v\\_detalyah/343072.php](https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/343072.php).

6. Распределённые реестры и информационная безопасность: от чего защищает БЧ [Электронный ресурс]. Режим доступа: <https://habr.com/company/bitfury/blog/341902/>.
7. Клиент-сервер:  
[https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B8%D0%B5%D0%BD%D1%82\\_%E2%80%94%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B8%D0%B5%D0%BD%D1%82_%E2%80%94%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80).
8. Коржов В. Многоуровневые системы клиент-сервер. Издательство : Открытые системы. Дата обращения 31 января 2010. Архивировано 26 августа 2011 г.
9. NISTIR 8202 – Blockchain Technology Overview, 2018, 68 p. Access mode: <https://doi.org/10.6028/NIST.IR.8202>.
10. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. <https://bitcoin.org/bitcoin.pdf>.
11. Pavan Duggal Blockchain Contracts and Cyberlaw / Pavan Duggal. Kyiv : Information Systems, 2015. С. 15 – 39.
12. Quantum attacks on Bitcoin, and how to protect against them / Divesh Aggarwal, Gavin K. Brennen, Troy Lee, Miklos Santha, Marco Tomamichel; National University of Singapore. Singapore, 2017.
13. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005, № 2594-IV.
14. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради (ВВР). 2017. № 45, ст.403.
15. Регламент (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року «Про електронну ідентифікацію та довірчі послуги для електронних транзакцій у межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС» (1) (COM (2012) 0238-C7-0133/2012 – 2012 / 0146 (COD)).
16. Прикладна криптологія. Теорія. Практика. Застосування / І.Д. Горбенко, Ю.І. Горбенко. Харків, 2012. С. 352 – 359.
17. Lily Chen Report on Post-Quantum Cryptography. NISTIR 8105 (DRAFT) .
18. «Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process» Gorjan Alagic та ін. <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf>.
19. Алгоритмы шифрования – основа работы криптовалют [Электронный ресурс]. Режим доступа: <https://tgraph.io/Algoritmy-shifrovaniya--osnova-raboty-kriptovalyut-09-27>.
20. Blockchain 3.0 – 5 лучших проектов нового поколения: <https://privatfinance.com/blockchain-3-0-5-luchshih-proektov-novogo-pokoleniya/>.
21. Криптографические хэш-функции [Электронный ресурс]. Режим доступа: <http://bit.nmu.org.ua/ua/student/metod/cryptography.pdf>.
22. Возможные атаки на функции хэширования [Электронный ресурс]. Режим доступа: <https://studfiles.net/preview/2157418/page/2/>.
23. Горбенко Ю. І. Методи побудовання та аналізу криптографічних систем. Харків : Форт, 2015. – 959 с.
24. American National Standard X9.98-2010. Lattice-based polynomial public key encryption algorithm, Part 1: key establishment, Part 2: data encryption. 2010.
25. Daniel J. Bernstein NTRU Prime / Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal // Электронный ресурс. Режим доступа: <https://ntruprime.cr.yt.to/ntruprime-20160511.pdf>. <https://bench.cr.yt.to/results-encrypt.html>.
26. Горбенко И.Д. Общие положения и анализ алгоритма направленного шифрования NTRU Prime ПТ Ukraine / І.Д. Горбенко, Е.Г. Качко, М.В. Есина // Радиотехника. 2018. Вып. 193. С. 5-16
27. Gorbenko I. D. Calculation of general parameters for NTRU Prime Ukraine of 6-7 levels of stability / I. D. Gorbenko, A. N. Alekseychuk, O. G. Kachko, M. V. Yesina, I. V. Stelnik, S. O. Kandy, V. A. Bobukh, V. A. Ponomar // Telecommunications and Radio Engineering, 2019. Volume 78, Issue 4. P.327-340. DOI: 10.1615/TelecomRadEng.v78.i4.40.
28. Gorbenko I.D. Methods of building general parameters and keys for NTRU Prime Ukraine of 5th-7th levels of stability. Product form / І.Д. Горбенко, О.Г. Качко, Ю.І. Горбенко, І.В. Стелник, С.О. Канди, М.В. Есина // Telecommunications and Radio Engineering, 2019. Volume 78, Issue 7. P. 579-594. DOI: 10.1615/TelecomRadEng.v78.i7.30.98.

*АТ «Інститут інформаційних технологій»;  
Харківський національний університет імені В.Н. Каразіна;  
Адміністрація Державної служби спеціального зв'язку та захисту  
інформації України.*

*Надійшла до редколегії 19.09.2019*