МОДЕЛЬ БЛОКЧЕЙН-ПЛАТФОРМЫ С КИБЕРИММУНИТЕТОМ В УСЛОВИЯХ КВАНТОВЫХ АТАК

Балябин А. А.[1], Петренко С. А.[2]

DOI: 10.21681/2311-3456-2025-3-72-82

Цель исследования: *разработка математической модели блокчейн-платформы с кибериммунитетом для исследования свойства киберустойчивости национальных блокчейн-экосистем и платформ «Экономики данных» Российской Федерации в условиях новой квантовой угрозы.*

Методы исследования: *методы системного анализа, методы теории вероятностей и математической статистики, методы теории устойчивости сложных систем.*

Полученные результаты: *проведено исследование текущего состояния технологий блокчейн; сформирована концептуальная четырехуровневая модель блокчейн-платформы, включающая уровни: криптографических алгоритмов, алгоритмов консенсуса, смарт-контрактов и децентрализованных приложений; сформулирована гипотеза об обеспечении киберустойчивости на различных уровнях блокчейн-платформы; разработана математическая модель блокчейн-платформы с кибериммунитетом для национальных блокчейн-экосистем и платформ «Экономики данных» Российской Федерации; проведена оценка киберустойчивости блокчейн-платформ с кибериммунитетом в условиях квантовых атак, результаты которой позволили подтвердить гипотезу исследования.*

Научная новизна: *предложенная модель отличается от существующих тем, что формализует процесс функционирования блокчейн-платформы как сложной многоуровневой системы с учетом нового фактора – наличия атакующего, обладающего квантовым вычислительным потенциалом, что обеспечивает возможность исследования свойства киберустойчивости блокчейн-платформ в условиях квантовых атак. К элементам новизны модели также относится введение в нее новых операций по обнаружению аномального состояния и по восстановлению штатного функционирования, которые в совокупности впервые реализуют механизмы кибериммунной защиты блокчейн-платформы.*

Ключевые слова: *угрозы безопасности информации, квантовые угрозы безопасности, блокчейн-экосистемы и платформы, кибербезопасность, киберустойчивость, методы анализа и синтеза квантово-устойчивого блокчейн.*

Введение

Активное развитие технологий блокчейн началось в 2008 году с публикации *Nakamoto S.* «*Bitcoin: A Peer-to-Peer Electronic Cash System*». В работе описывалась концепция цифровой валюты Bitcoin, использующая технологию распределенного реестра (DLT) для обеспечения безопасности транзакций без необходимости в доверенных центрах. В 2009 году был запущен первый блокчейн Bitcoin, что ознаменовало начало эры блокчейн-технологий.

В 2015 году с запуском платформы Ethereum, появились такие понятия, как смарт-контракты, токены, системы децентрализованных финансов (DeFi), децентрализованные автономные организации (DAO), децентрализованные приложения (dApps) и др. С развитием блокчейн-экосистем и платформ возникла потребность в интероперабельности – обеспечении возможности разных блокчейн-сетей обмениваться данными и активами между собой.

В работе [1] представлена схема эволюции технологий блокчейн, включающая 5 этапов. Данная схема, однако, не учитывает развитие искусственного интеллекта, квантовых вычислений, а также повышенные требования, предъявляемые к киберустойчивости значимых информационно-технических систем в условиях роста киберугроз. Авторская схема эволюции технологий блокчейн, учитывающая данные актуальные тенденции, представлена на рис. 1.

Современное состояние развития технологий блокчейн соответствует этапу «Блокчейн 4.0» и характеризуется активным внедрением данных технологий в объекты Индустрии 4.0 [2], системы интернета вещей (IoT) [3] и облачные платформы [4], а также исследованием перспектив создания децентрализованной сети Интернет (Web3) [5]. В Российской Федерации технологии блокчейн применяются в рамках реализации национального проекта «Экономика данных» с целью перевода экономики страны, социальной сферы и органов власти на новые принципы работы.

1 Балябин Артём Алексеевич, младший научный сотрудник, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Федеральная территория «Сириус», Россия. E-mail: Balyabin.AA@talantiuspeh.ru

2 Петренко Сергей Анатольевич, доктор технических наук, профессор, руководитель группы, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Федеральная территория «Сириус», Россия. Orcid.org/0000- 0003-0644-1731. E mail: Petrenko.SA@talantiuspeh.ru

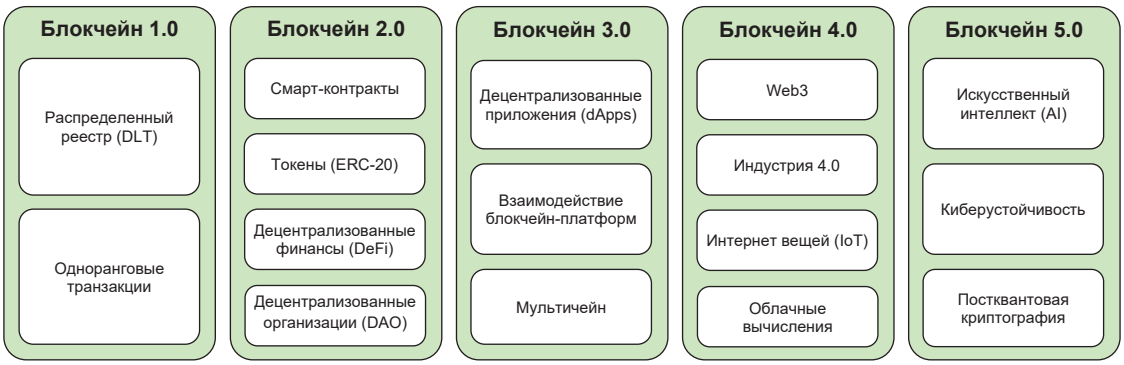

Рис. 1. Эволюция технологий блокчейн

В настоящем исследовании учитываются также и новейшие вызовы, такие как рост квантовых угроз, и предлагается модель блокчейн-платформы, отвечающей требованиям к киберустойчивости в условиях квантовых атак, в рамках следующего этапа развития технологий «Блокчейн 5.0».

1. Системный анализ блокчейн-платформ

Существует множество различных блокчейн-платформ (Bitcoin, Ethereum, Polkadot, Cardano, Solana, Tezos, EOS, Конфидент, InnoChain, Мастерчейн и др.), в каждой которых применяется свой стек технологий. Рассмотрим подробнее основные уровни блокчейн-платформ, значимые с точки зрения новой квантовой угрозы.

Фундаментом любой блокчейн-платформы являются криптографические алгоритмы хэширования (SHA-256, Ethash, Keccak, RIPEMD-160), шифрования (AES) и цифровой подписи (ECDSA). Ведутся исследования по применению в блокчейн постквантовых алгоритмов хэширования (NTRU, FrodoKEM), шифрования (FrodoKEM, Saber, BIKE, HQC, CRYSTALS-Kyber, SIKE) и цифровой подписи (CRYSTALS-Dilithium, SPHINCS+, FALCON, Picnic, Гиперикум, Шиповник, Крыжовник), устойчивых к атакам с применением квантового компьютера [6–9]. Данные криптоалгоритмы применяются для аутентификации узлов, формирования и проверки корректности транзакций и блоков и составляют основу алгоритмов консенсуса.

Следующий уровень блокчейн-платформ представлен алгоритмами консенсуса, которые необходимы для создания и проверки корректности блоков транзакций, а также согласования действий узлов. К наиболее распространенным из них относятся PoW, PoS, DPoS, BFT и PoA [10]. Алгоритмы консенсуса являются важнейшей частью блокчейн-платформы, позволяющей узлам принимать согласованное решение о добавлении в сеть нового блока.

Смарт-контракты активируются транзакциями и служат для автоматического исполнения последовательностей других транзакций (ERC-20, ERC-721, BEP-20). В своей работе они могут использовать сведения из внешнего мира, запрашиваемые у оракулов – программных или аппаратных источников данных (Chainlink, Band Protocol). Смарт-контракты служат основой для децентрализованных приложений и в то же время являются одним из самых уязвимых уровней блокчейн, поскольку подвержены, например, ошибкам численного переполнения, реентерантности и управления правами доступа [11, 12].

Уровень децентрализованных приложений (dApps) является надстройкой над смарт-контрактами, предназначенной для управления их совместным выполнением. Децентрализованные приложения также

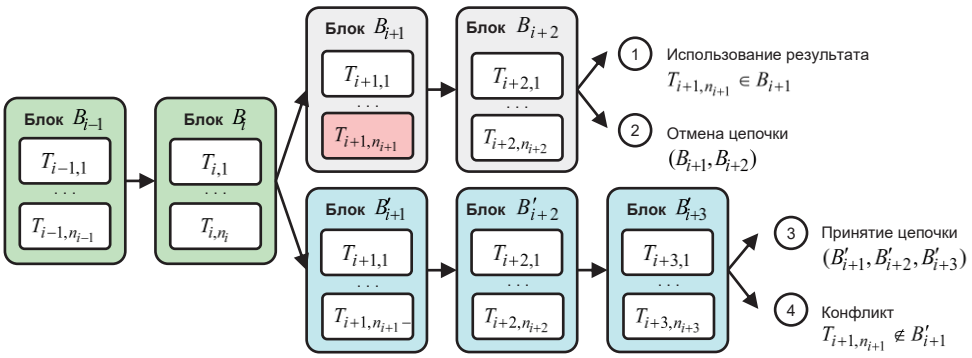

Рис. 2. Пример эмерджентного эффекта в блокчейн-платформе

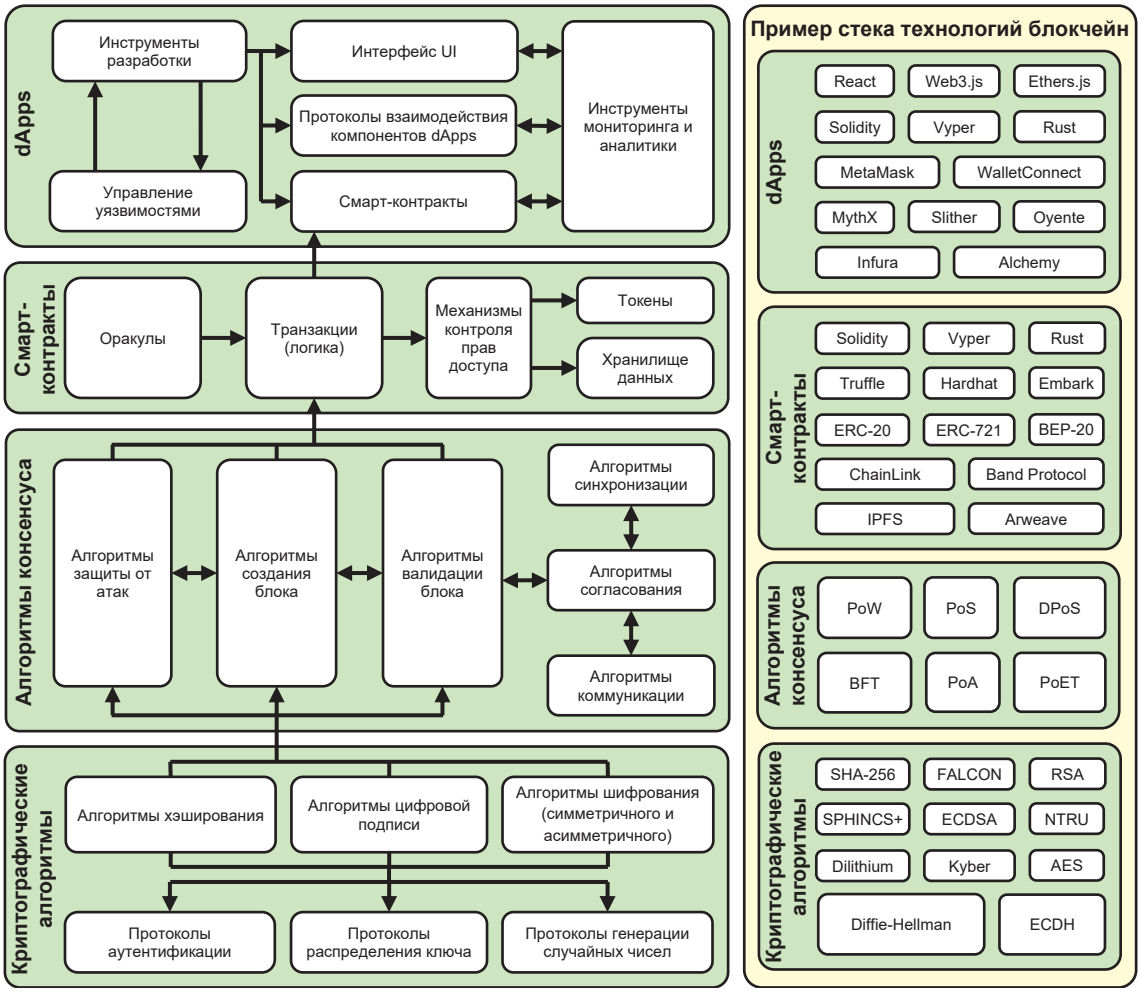

Рис. 3. Концептуальная модель блокчейн-платформы как сложной многоуровневой системы

подвержены ряду уязвимостей, в том числе уязвимостям вида «man-in-the-middle» [13, 14].

Совместное функционирование взаимосвязанных уровней блокчейн-платформы приводит к возникновению различных эмерджентных эффектов. Например, при штатном функционировании блокчейн может возникнуть следующая ситуация. Результат транзакции $T_{i+1,n_{i+1}}$, присутствующей в короткой цепочке блоков (B_{i+1}, B_{i+2}), используется для подтверждения некоторых операций. Транзакция отменяется при появлении более длинной цепочки $(B'_{i+1}, B'_{i+2}, B'_{i+3})$, в которой она отсутствует. При дальнейшем выполнении действий, опирающихся на ранее подтвержденный результат данной транзакции, возникает конфликтная ситуация, как показано на рис. 2.

Все это позволяет рассматривать блокчейн-платформу как сложную многоуровневую систему. Концептуальная четырехуровневая модель блокчейн-платформы представлена на рис. 3.

Далее необходимо определить понятие киберустойчивости блокчейн-платформ в условиях квантовых атак.

2. Квантовые атаки на блокчейн-платформы

Криптостойкость алгоритмов блокчейн, обеспечивается сложностью задач факторизации больших чисел и дискретного логарифмирования. Однако применение квантовых алгоритмов, таких как алгоритмы Шора и Гровера, позволяет значительно сократить время решения данных задач, что представляет новую угрозу для блокчейн-платформ [15].

Квантовый алгоритм Гровера предназначен для решения задачи поиска элемента в неупорядоченном множестве $\mathrm{f}:\{0,1\}^n \longrightarrow \{0,1\}$ и позволяет сократить вычислительную сложность поиска с $O(2^n)$ до $O(2^{n/2})$, где n – размерность пространства поиска в битах. Так, простой перебор 256-битной хэш-суммы SHA-256, используемой в алгоритме консенсуса PoW, будет иметь вычислительную сложность $O(2^{256})$, а с применением алгоритма Гровера – $O(2^{128})$.

Квантовый алгоритм Шора предназначен для решения задачи факторизации большого числа $N = 2^n$ и имеет полиномиальную вычислительную сложность $O(n^3)$, где n – количество бит числа. Это делает алгоритм ECDSA, основанный на сложности решения проблемы дискретного логарифмирования,

Таблица 1

Квантовые атаки на блокчейн-платформы

Уровень	Результат атаки	Последствие атаки
Децентрализованные приложения (dApps)	Обход аутентификации пользователя	Раскрытие защищенной информации (конфиденциальность) Появление в блокчейн вредоносного блока транзакций (целостность) Снижение или утрата работоспособности блокчейн-платформы (доступность)
	Фальсификация узла	
Смарт-контракты	Фальсификация данных о внешней среде (компрометация оракула)	
	Фальсификация токена	
	Нарушение логики смарт-контракта	
Алгоритмы консенсуса	Синтез произвольного блока транзакций, удовлетворяющего требованиям	
	Получение превосходства вычислительной мощности (установление контроля над сетью)	
Криптографические алгоритмы	Решение задачи факторизации большого числа	
	Решение задачи дискретного логарифмирования	
	Отыскание коллизии хэш-функции	

неустойчивым при наличии достаточного количества логических кубитов.

Квантовые атаки на блокчейн-платформу могут осуществляться на различных уровнях ее функционирования. Описание результатов и последствий квантовых атак на данных уровнях представлено в табл. 1.

Таким образом, с точки зрения нарушения свойства конфиденциальности конечная цель атаки на различные уровни блокчейн-платформы состоит в раскрытии защищенной информации, например, приватного ключа пользователя, с точки зрения нарушения свойства доступности – в снижении или нарушении работоспособности блокчейн-платформы, а с точки зрения нарушения свойства целостности – во внедрении вредоносного блока транзакций. Под вредоносным блоком, в частности, понимается блок с корректной хэш-суммой, содержащий транзакцию, противоречащую логике функционирования блокчейн-платформы, например транзакцию траты несуществующих средств. В дальнейшем в работе

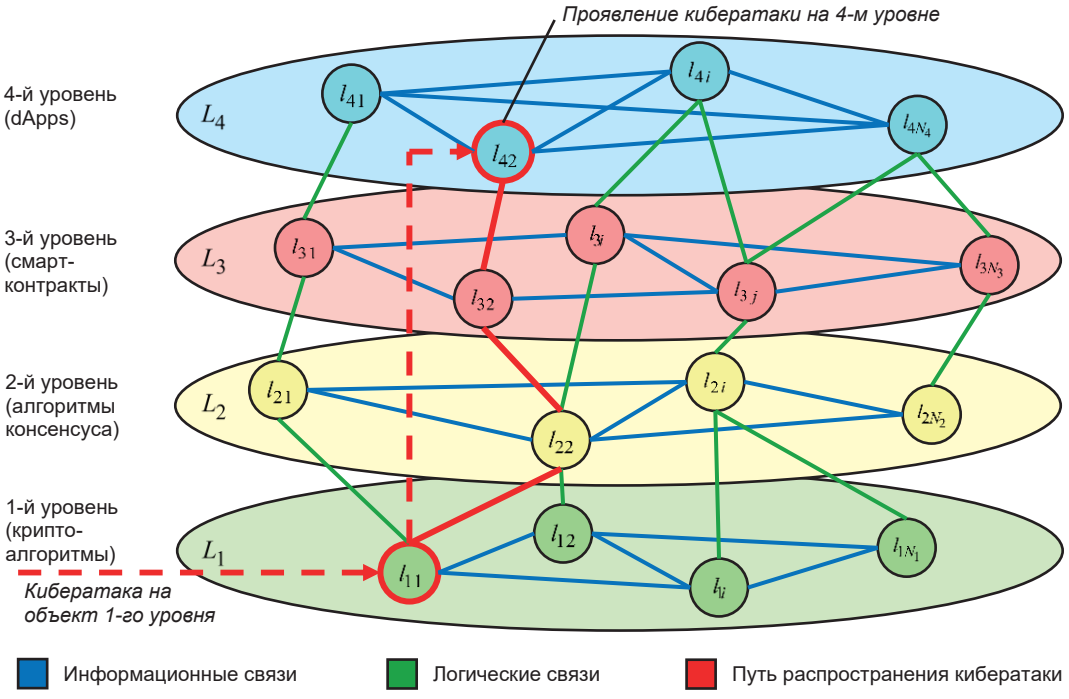

Рис. 4. Схема межуровневого отображения кибератаки на блокчейн-платформу

в основном будут подразумеваться атаки, направленные на нарушение свойства целостности.

Учитывая сложный, иерархический и децентрализованный характер блокчейн-платформы, дестабилизирующее воздействие, оказываемое на одном уровне, может проявляться на другом ее уровне, как показано на рис. 4.

Известно, что под киберустойчивостью информационно-технической системы понимается ее способность сохранять показатели своего функционирования в пределах допустимых значений в условиях дестабилизирующих воздействий (кибератак). Сформулируем определение для квантовой атаки и квантовой устойчивости блокчейн-платформы.

Определение 1. Под *квантовой атакой* на блокчейн-платформу будем понимать кибератаку, для достижения целей которой используется вычислительный потенциал квантового компьютера.

Определение 2. Под *квантовой устойчивостью блокчейн-платформы* (*киберустойчивостью в условиях квантовых атак*) будем понимать ее способность сохранять показатели своего функционирования в пределах допустимых значений в условиях дестабилизирующих воздействий (кибератак) с использованием квантового компьютера.

3. Постановка задачи исследования

Исследование возможностей обеспечения киберустойчивости блокчейн в условиях квантовых атак является перспективным научным направлением. Известны, например, работы [16, 17], посвященные организации квантово-устойчивого блокчейн с применением постквантовых криптографических алгоритмов. Одним из подходов к созданию киберустойчивых информационно-технических систем также является подход на основе кибериммунитета, заключающийся в наделении системы способностью обнаруживать аномалии и восстанавливать штатное функционирование [18–20].

Дано: L – блокчейн-платформа, функционирующая на четырех уровнях, так что $L = \{L_i | i \in [1,4]\}$; $X = \{X_i | i \in [1,4]\}$ – множество входных данных на каждом уровне; $Y = \{Y_i | i \in [1,4]\}$ – множество выходных данных на каждом уровне; $E = \{E_i | i \in [1,4]\}$ – множество параметров среды на каждом уровне; $A = \{A_i | i \in [1,4]\}$ – множество параметров дестабилизирующих воздействий на каждом уровне; $D = \{D_i | i \in [1,4]\}$ – множество параметров нейтрализующих воздействий на каждом уровне; $R = \{R_i | i \in [1,4]\}$ – множество показателей киберустойчивости функционирования блокчейн-платформы на каждом уровне.

Необходимо: разработать модель M блокчейн-платформы L с кибериммунитетом, устанавливающую закономерность изменения множества выходных данных Y и множества показателей киберустойчивости функционирования системы R от множества значений входных данных X, множества значений параметров среды E, множества значений параметров дестабилизирующих воздействий A и множества параметров нейтрализующих воздействий D. При этом на значения X, Y, E, A, D наложены условия допустимости: $X \subseteq X_{\text{доп}}$, $Y \subseteq Y_{\text{доп}}$, $E \subseteq E_{\text{доп}}$, $A \subseteq A_{\text{доп}}$, $D \subseteq D_{\text{доп}}$.

Формальная постановка научной задачи: найти

$$M: <L,X,E,A,D> \longrightarrow Y, R \mid \\ \mid X \subseteq X_{\text{доп}}, Y \subseteq Y_{\text{доп}}, E \subseteq E_{\text{доп}}, A \subseteq A_{\text{доп}}, D \subseteq D_{\text{доп}}. \quad (1)$$

Гипотеза исследования: киберустойчивость блокчейн-платформы на i-м уровне может быть эффективно обеспечена только при обеспечении ее на $(i-1)$-м уровне.

4. Модель блокчейн-платформы с кибериммунитетом

4.1. Уровень криптографических алгоритмов

Формализуем модель блокчейн-платформы на уровне криптографических алгоритмов (1-й уровень):

$X_1 = (x_1, \ldots, x_{n_1})$ – входные данные, представленные последовательностью транзакций x_i, $i \in [1,n_1]$ блока, где n_1 – количество транзакций;

$Y_1 = f_1(X_1)$ – выходные данные, представленные результатом применения функции хэширования f_1 к входным данным X_1;

$A_1 = \{(x_1, \ldots, x_{i-1}, a_i, x_{i+1}, \ldots, x_{n_1}), I_{\text{атак}_1}\}$ – параметры воздействия атакующего;

$(x_1, \ldots, x_{i-1}, a_i, x_{i+1}, \ldots, x_{n_1})$ – последовательность транзакций в блоке, включая вредоносную транзакцию a_i;

$I_{\text{атак}_1}$ – степень «влияния» атакующего на 1-й уровень блокчейн-платформы (например, $I_{\text{атак}_1} = H_{\text{атак}_1}$ – скорость перебора хэш-сумм (PoW), $I_{\text{атак}_1} = S_{\text{атак}_1}$ – доля владения активами (PoS));

$E_1 = \{I_{\text{сети}_1}, C, z_1\}$ – параметры среды функционирования;

$I_{\text{сети}_1}$ – степень «влияния» остальных участников, за исключением атакующего, на 1-й уровень блокчейн-платформы, $I_{\text{атак}_1} < I_{\text{сети}_1}$;

$C = 2^{z_1}$ – целевая сложность перебора хэш-сумм (PoW);

z_1 – количество требуемых нулевых бит в начале хэш-суммы блока;

$D_1 = \{w_1\}$ – параметры противодействия кибератакам, где w_1 – коэффициент доверия к узлу;

$E_2 = \{I_{\text{атак}_1}, I_{\text{сети}_1}\}$ – параметры среды функционирования для 2-го уровня блокчейн-платформы;

$U_1 = \{I_{\text{атак}_1}, I_{\text{сети}_1}\}$ – показатели функционирования блокчейн-платформы;

$q_1 = I_{\text{атак}_1} / (I_{\text{атак}_1} + I_{\text{сети}_1})$ – вероятность синтеза блока атакующим быстрее сети;

$R_1 = 1 - w_1 q_1$ – показатель киберустойчивости;

$\chi_1(Y_1) = \begin{cases} 1, \text{ если } \exists a_i \in X_1 : Y_1 = f_1(X_1),\ f(a_i, B) = 1; \\ 0, \text{ иначе.} \end{cases}$ – функция выявления аномалии, где f – функция проверки корректности транзакции a_i относительно всей имеющейся цепочки блоков B.

Утверждение 1. Показатель киберустойчивости блокчейн-платформы на 1-м уровне функционирования, вычисляемый с учетом вероятности синтеза и принятия блока атакующего в качестве основного, зависит только от степени «влияния» его на блокчейн-платформу и не зависит от целевой сложности перебора C.

Доказательство. Для блокчейн-платформ типа PoS это очевидно, поскольку узел, имеющий право синтеза блока, выбирается с вероятностью, пропорциональной доле владения ($S_{\text{атак}_1}$), и не зависит от сложности перебора хэш-суммы блока:

$$R_1 = 1 - w_1 q_1 = 1 - w_1 S_{\text{атак}_1} / (S_{\text{атак}_1} + S_{\text{сети}_1}). \quad (2)$$

Для блокчейн-платформ типа PoW вероятность синтеза и принятия блока атакующего быстрее сети можно определить как:

$$R_1 = 1 - w_1 T_{\text{общ}_1} / T_{\text{атак}_1}, \quad (3)$$

где $T_{\text{общ}_1} = C / (H_{\text{атак}_1} + H_{\text{сети}_1})$ – среднее время синтеза блока сетью, включая атакующего; $T_{\text{атак}_1} = C / H_{\text{атак}_1}$ – среднее время синтеза блока атакующим. То есть:

$$R_1 = 1 - w_1 q_1 = 1 - w_1 H_{\text{атак}_1} / (H_{\text{атак}_1} + H_{\text{сети}_1}). \quad (4)$$

Ч.т.д.

Таким образом, киберустойчивость блокчейн-платформы на 1-м уровне определяется ее способностью противодействовать принятию созданного атакующим вредоносного блока.

4.2. Уровень алгоритмов консенсуса

Формализуем модель блокчейн-платформы на уровне алгоритмов консенсуса (2-й уровень):

$X_2 = (x_1, \ldots, x_{n_2})$ – входные данные, представленные последовательностью блоков транзакций x_i, $i \in [1, n_2]$, где n_2 – количество блоков в цепочке;

$Y_2 = f_2(X_2)$ – выходные данные, представленные результатом согласования (консенсуса) узлами блокчейн цепочки блоков ;

$A_2 = \{(x_1, \ldots, x_{i-1}, a_i, x_{i+1}, \ldots, x_{n_2}), I_{\text{атак}_2}\}$ – параметры воздействия атакующего;

$(x_1, \ldots, x_{i-1}, a_i, x_{i+1}, \ldots, x_{n_2})$ – цепочка блоков, включая вредоносный блок a_i;

$I_{\text{атак}_2}$ – степень «влияния» атакующего на 2-й уровень блокчейн-платформы;

$E_2 = \{I_{\text{сети}_1}, z_2, R_1\}$ – параметры среды функционирования;

$I_{\text{сети}_2}$ – степень «влияния» остальных участников, за исключением атакующего, на 2-й уровень блокчейн-платформы, $I_{\text{атак}_2} < I_{\text{сети}_2}$;

z_2 – длина цепочки блоков для принятия ее в качестве основной;

$D_2 = \{w_2\}$ – параметры противодействия кибератакам, где w_2 – коэффициент доверия к узлу;

$E_3 = \{I_{\text{атак}_2}, I_{\text{сети}_2}, R_2\}$ – параметры среды функционирования для 3-го уровня блокчейн-платформы;

$U_2 = \{P_{\text{атак}_2}, P_{\text{сети}_2}, z_2, \lambda\}$ – показатели функционирования блокчейн-платформы;

$q_2 = I_{\text{атак}_2} / (I_{\text{атак}_2} + I_{\text{сети}_2})$ – вероятность синтеза блока атакующим быстрее сети;

$P_{\text{атак}_2} = w_2 q_2$ – вероятность синтеза и принятия блока атакующего;

$P_{\text{сети}_2} = 1 - P_{\text{атак}_2}$ – вероятность синтеза и принятия блока легитимных узлов сети, за исключением атакующего, $P_{\text{атак}_2} < P_{\text{сети}_2}$;

$\lambda = z_2 \frac{P_{\text{атак}_2}}{P_{\text{сети}_2}}$ – мат. ожидание длины цепочки блоков атакующего;

$R_2 = \varphi(U_2) = \sum_{k=0}^{z_2} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (P_{\text{атак}_2} / P_{\text{сети}_2})^{z_2 - k}\right)$ – показатель киберустойчивости;

$\chi_2(Y_2) = \begin{cases} 1, \text{ если } \exists a_i \in X_2 : Y_2 = f_2(X_2),\ f(a_i, B) = 1; \\ 0, \text{ иначе.} \end{cases}$ – функция выявления аномалии, где f – функция проверки корректности блока a_i относительно всей имеющейся цепочки блоков B, принимающая значение 1 в случае, если блок содержит некорректную транзакцию.

Таким образом, киберустойчивость блокчейн-платформы на 2-м уровне определяется ее способностью противодействовать принятию созданной атакующим вредоносной цепочки блоков.

4.3. Уровень смарт-контрактов

Формализуем модель блокчейн-платформы на уровне смарт-контрактов (3-й уровень):

$X_3 = \{X_{3i} | i \in [1, n_3]\}$ – множество входных данных, где $X_{3i} = \{x_{3ij} | j \in [1, \#X_{3i}]\}$, $i \in [1, n_3]$ – множество входных данных i-го смарт-контракта, n_3 – количество смарт-контрактов, при этом $X_{3i} = X_{3i}^{+} \cup X_{3i}^{-}$, где X_{3i}^{-} – подмножество вредоносных входных данных;

$Y_3 = f_3(X_3) = \{y_{3i} | y_{3i} = f_{3i}(x_{3i}),\ i \in [1, n_3]\}$ – выходные данные, представленные результатом выполнения смарт-контрактов с входными данными x_3, f_{3i} – функция i-го смарт-контракта;

$A_3 = (a_{31}, \ldots, a_{3n_3})$ – параметры воздействия, представленные вредоносными входными данными, передаваемыми атакующим в смарт-контракты, $a_{3i} \in X_{3i}^{-}$;

$E_3 = \{(\#X_{31}, \#X_{31}^{-}), \ldots, (\#X_{3n_3}, \#X_{3n_3}^{-}), R_2\}$ – параметры среды функционирования;

$D_3 = (D_{3i} | i \in [1, n_3])$ – параметры противодействия кибератакам, где $\{d_{3ij} | j \in [1, \#D_{3i}]\}$, $\#D_{3i} \in [0, \#X_{3i}^{-}]$, $i \in [1, n_3]$ – множество обнаруженных и заблокированных вредоносных входных данных i-го смарт-контракта;

$E_4 = \{\{P_{3i}^{a} | i \in [1, n_3]\}, R_3\}$ – параметры среды функционирования для 4-го уровня блокчейн-платформы;

$U_3 = \{P^a_{3i} | i \in [1,n_3]\}$ – показатели функционирования блокчейн-платформы;

$P^a_{3i} = P(S^a_{3i}) = (\#X^-_{3i} - \#D_{3i}) / \#X_{3i}$ – вероятность нарушения в i-м смарт-контракте (событие S^a_{3i});

$R_3 = \varphi(U_3) = R_2 \frac{1}{n_3} \sum_{i=1}^{n_3} (1 - P^a_{3i})$ – показатель киберустойчивости;

$\chi_3(Y_3) = \begin{cases} 1, \text{ если } \exists y'_{3i} \in Y_3 : f(x_{3i}, y'_{3i}) = 1; \\ 0, \text{ иначе.} \end{cases}$ – функция выявления аномалии, где f –функция проверки корректности результата выполнения смарт-контракта.

Таким образом, киберустойчивость блокчейн-платформы на 3-м уровне определяется ее способностью противодействовать выполнению смарт-контрактов с вредоносными входными данными.

4.4. Уровень децентрализованных приложений

Формализуем модель блокчейн-платформы на уровне децентрализованных приложений (dApps) (4-й уровень):

$X_4 = \{X_{4i} | i \in [1,n_4]\}$ – множество входных данных, где $X_{4i} = \{X_{4ij} | j \in [1,\#X_{4i}]\}$, $i \in [1,n_4]$ – множество входных данных i-го приложения, n_4 – количество приложений, при этом $X_{4i} = X^+_{4i} \cup X^-_{4i}$, где X^-_{4i} – подмножество вредоносных входных данных;

$Y_4 = f_4(X_4) = \{y_{4i} | y_{4i} = f_{4i}(x_{4i}),\ i \in [1,n_4]\}$ – выходные данные, представленные результатом выполнения приложений с входными данными X_4, f_{4i} – функция i-го приложения;

$A_4 = (a_{41}, ..., a_{4n_4})$ – параметры воздействия атакующего, представленные вредоносными входными данными, передаваемыми атакующим в приложения, $a_{4i} \in X^-_{4i}$;

$E_4 = \{\{P^a_{3i} | i \in [1,n_3]\}, R_3, (X_{41}, X^-_{41}), ..., (X_{4n_4}, X^-_{4n_4})\}$ – параметры среды функционирования блокчейн-платформы;

$D_4 = (D_{4i} | i \in [1,n_4])$ – параметры противодействия кибератакам, где $\{d_{4ij} | j \in [1,\#D_{4i}]\}$, $\#D_{4i} \in [0,\#X^-_{4i}]$, $i \in [1,n_4]$ – множество обнаруженных и заблокированных вредоносных входных данных i-го приложения;

$U_4 = \{P^a_{4i} | i \in [1,n_4]\}$ – показатели функционирования блокчейн-платформы на, где $P^a_{4i} = P(S^a_{4i})$ – вероятность нарушения в i-м приложении, вызванного обработкой вредоносных входных данных a (событие S^a_{4i});

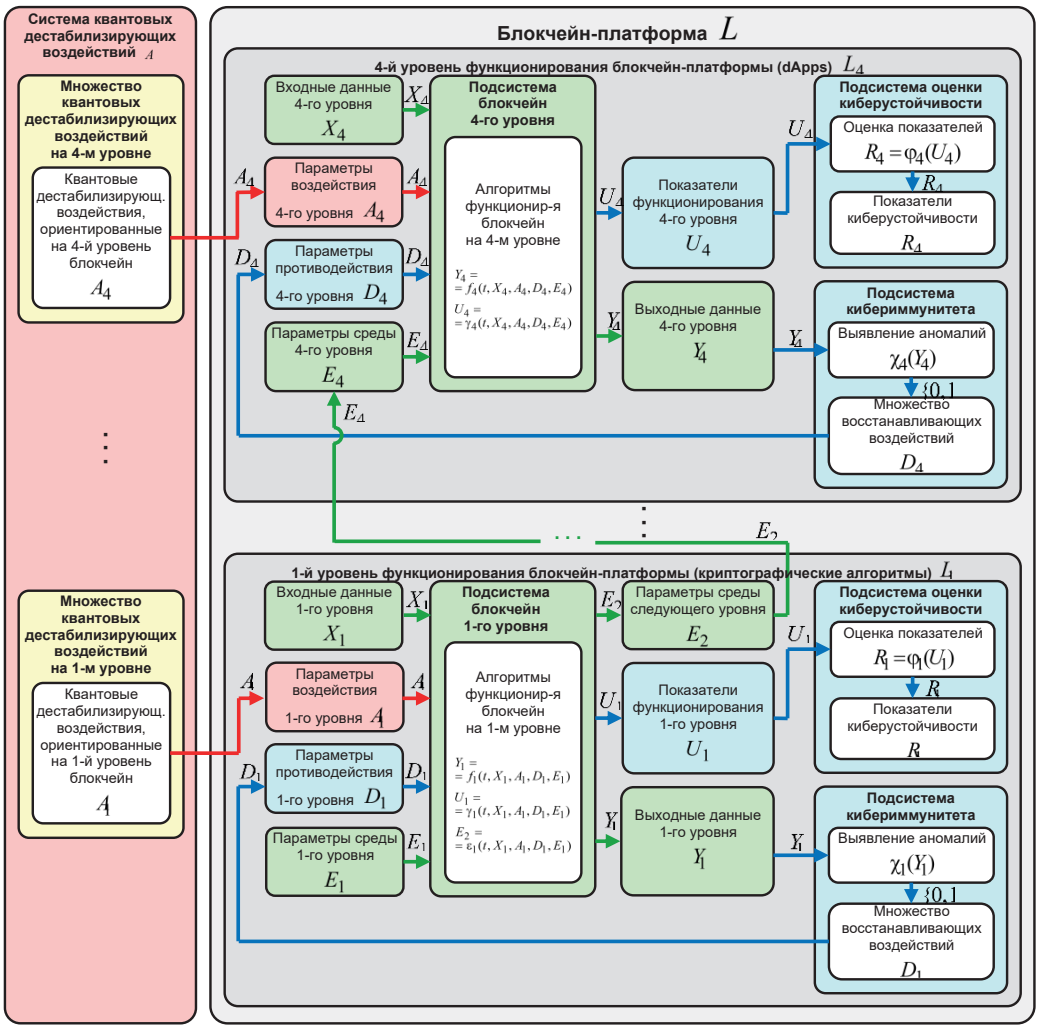

Рис. 5. Многоуровневая модель блокчейн-платформы в условиях квантовых атак

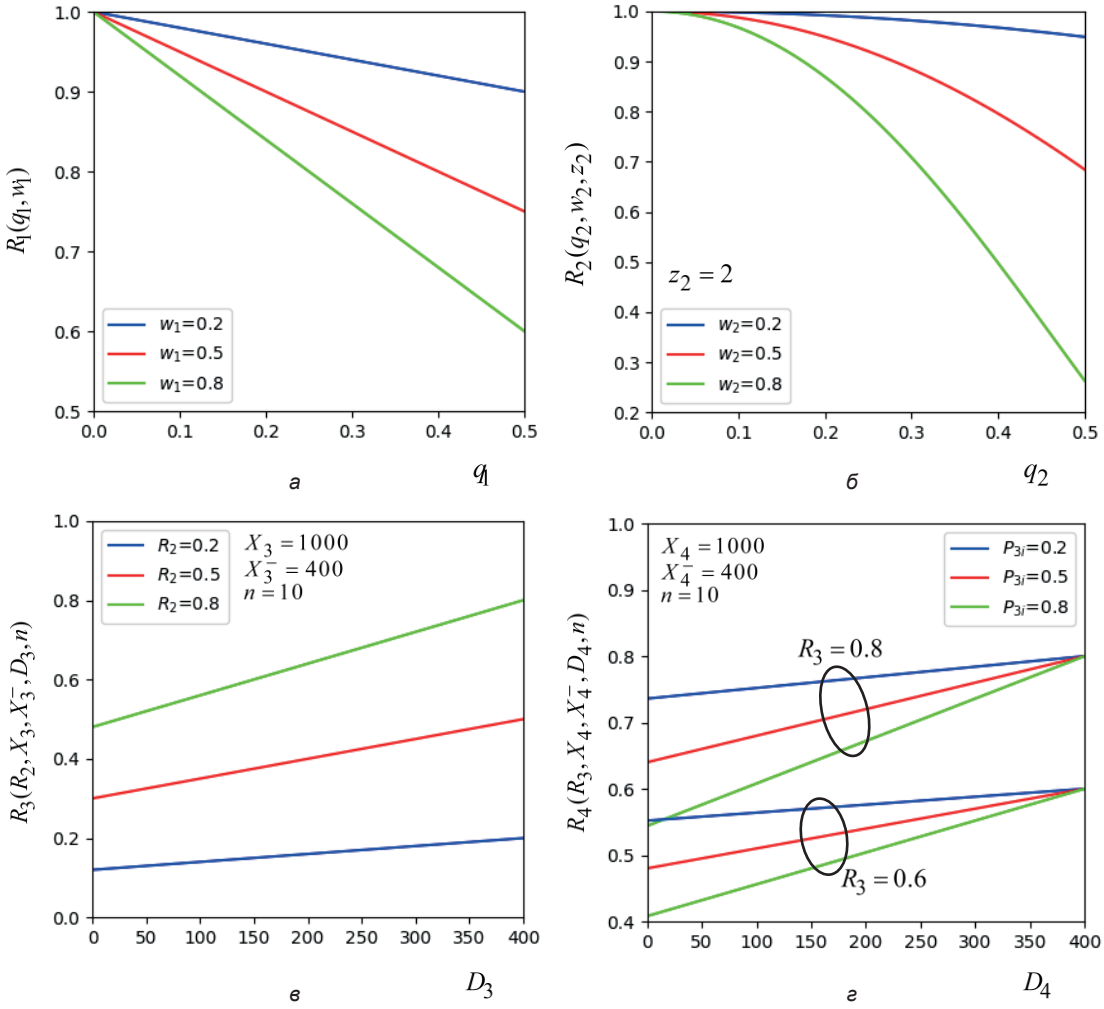

Рис. 6. Результаты экспериментальных исследований киберустойчивости: а – на 1-м уровне (криптоалгоритмов); б – на 2-м уровне (алгоритмов консенсуса); в – на 3-м уровне (смарт-контрактов); г – на 4-м уровне (децентрализованных приложений, dApps)

$P_{4i}^a = P(S_{4i}^a) = \frac{(\#X_{4i}^- - \#D_{4i})}{\#X_{4i}} \frac{1}{l_i} \sum_{r=1}^{l_i} P_{3ir}^a$ – вероятность нарушения в i-м приложении, состоящем из l_i смарт-контрактов, где P_{3ir}^a – вероятность нарушения в i-м смарт-контракте $r \in [1, l_i]$.

$R_4 = \varphi(U_4) = R_3 \frac{1}{n_4} \sum_{i=1}^{n_4} (1 - P_{4i}^a)$ – показатель киберустойчивости;

$\chi_4(Y_4) = \begin{cases} 1, \text{ если } \exists y'_{4i} \in Y_4 : f(x_{4i}, y'_{4i}) = 1; \\ 0, \text{ иначе.} \end{cases}$ – функция выявления аномалии, где f – функция проверки корректности результата выполнения децентрализованного приложения, принимающая значение 1 в случае, если результат некорректен, и 0 – иначе.

Таким образом, киберустойчивость блокчейн-платформы на 4-м уровне определяется ее способностью противодействовать выполнению децентрализованных приложений с вредоносными входными данными.

4.5. Многоуровневая модель блокчейн-платформы

Схема многоуровневой модели блокчейн-платформы в условиях квантовых атак представлена на рис. 5.

Учитывая сложный многоуровневый характер блокчейн-платформ, при выполнении практических расчетов можно оценивать лишь показатель киберустойчивости верхнего уровня, представляющий собой свертку: $R_1 \longrightarrow R_2 \longrightarrow R3_1 \longrightarrow R_4$.

5. Исследование квантовой устойчивости блокчейн-платформ с кибериммунитетом

Результаты экспериментальных исследований квантовой устойчивости блокчейн-платформы на различных уровнях функционирования приведены на рис. 6.

Киберустойчивость блокчейн-платформы в условиях квантовых атак на 1-м уровне снижается по мере увеличения вероятности q_1 того, что атакующий создаст вредоносный блок раньше остальной сети и этот блок будет принят в блокчейн. Противодействие принятию вредоносного блока оказывается с помощью снижения коэффициента доверия w_1 к атакующему узлу (рис. 6а).

На 2-м уровне киберустойчивость также зависит от вероятности принятия вредоносного блока q_2 и коэффициента доверия w_2, однако наблюдается нелинейная зависимость, поскольку атакующему необходимо синтезировать цепочку из z_2 блоков и «убедить» остальную сеть принять ее (рис. 6б).

На 3-м уровне киберустойчивость зависит от количества обнаруженных и нейтрализованных вредоносных входных данных D_3. Как видно, при нейтрализации все большего количества вредоносных входных данных значение показателя киберустойчивости уровня смарт-контрактов стремится к значению показателя предыдущего уровня R_2 (рис. 6в).

На 4-м уровне киберустойчивость оценивалась аналогично предыдущему уровню для двух различных значений R_3 с учетом вероятностей P_{3i} возникновения нарушений в смарт-контрактах, составляющих децентрализованные приложения. Показатель киберустойчивости R_4 при этом так же стремится к значению R_3 (рис. 6г).

Таким образом:

- в блокчейн-платформе существуют межуровневые связи, что характеризует ее как сложную многоуровневую систему;
- кибератака, осуществляемая на нижележащем уровне, оказывает влияние на все вышележащие уровни блокчейн-платформы;
- киберустойчивость на i-м уровне может быть эффективно обеспечена только при условии обеспечения ее на $(i-1)$-м уровне.

Результаты экспериментальных исследований позволяют подтвердить выдвинутую гипотезу.

Выводы

В настоящем исследовании поставлена задача синтеза математической модели блокчейн-платформы с кибериммунитетом в условиях квантовых атак. Проведен системный анализ и сформирована концептуальная четырехуровневая модель блокчейн-платформы, включающая уровни: криптографических алгоритмов, алгоритмов консенсуса, смарт-контрактов и децентрализованных приложений. Выдвинута гипотеза об обеспечении киберустойчивости на различных уровнях блокчейн-платформы. Разработана многоуровневая модель блокчейн-платформы с кибериммунитетом, отличающаяся от существующих учетом наличия атакующего, обладающего квантовым вычислительным потенциалом, и внедрением новых операций по обнаружению аномалий и восстановлению штатного функционирования системы.

В результате экспериментов выявлен ряд количественных закономерностей снижения киберустойчивости блокчейн-экосистем и платформ «Экономики данных» РФ в условиях атак злоумышленников с применением квантового компьютера, что позволило подтвердить выдвинутую гипотезу.

В дальнейшем результаты исследования будут использованы для синтеза методов и методик обеспечения киберустойчивости блокчейн-платформ в условиях квантовых атак на основе кибериммунитета.

Результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение №23-03 от 27.09.2024 г.).

Литература

1. Mourtzis D., Angelopoulos J., Panopoulos N. Blockchain Integration in the Era of Industrial Metaverse // Applied Sciences. 2023. Vol. 13. No. 3. P. 1353. DOI: 10.3390/app13031353.
2. Марков А.С. Важная веха в безопасности открытого программного обеспечения // Вопросы кибербезопасности. 2023. № 1(53). С. 2–12. DOI: 10.21681/2311-3456-2023-1-2-12.
3. Nguyen D.C. et al. 6G Internet of Things: A Comprehensive Survey // IEEE Internet of Things Journal. 2022. Vol. 9. No. 1. Pp. 359–383. DOI: 10.1109/JIOT.2021.3103320.
4. Балябин А.А., Петренко С.А., Костюков А.Д. Модель угроз безопасности и киберустойчивости облачных платформ КИИ РФ // Защита информации. Инсайд. 2024. № 5 (119). С. 26–34.
5. Chen C. et al. When Digital Economy Meets Web3.0: Applications and Challenges // IEEE Open Journal of the Computer Society. 2022. Vol. 3. Pp. 233–245. DOI: 10.1109/OJCS.2022.3217565.
6. Петренко А.С., Ломако А.Г., Петренко С.А. Анализ современного состояния исследований проблемы квантовой устойчивости блокчейна. Часть 1 // Защита информации. Инсайд. 2023. № 3 (111). С. 38–46.
7. Петренко А.С., Петренко С.А., Костюков А.Д. Эталонная модель блокчейн-платформы // Защита информации. Инсайд. 2022. № 4 (106). С. 34–44.
8. Петренко А.С., Петренко С.А. Метод оценивания квантовой устойчивости блокчейн-платформ // Вопросы кибербезопасности. 2022. № 3(49). С. 2–22. DOI: 10.21681/2311-3456-2022-3-2-22.
9. Петренко А.С., Петренко С.А. Basic Algorithms Quantum Cryptanalysis (Основные алгоритмы квантового криптоанализа) // Вопросы кибербезопасности. 2023. № 1(53). С. 100–115. DOI: 10.21681/2311-3456-2023-1-100-115.

10. Lashkari B., Musilek P. A Comprehensive Review of Blockchain Consensus Mechanisms // IEEE Access. 2021. Vol. 9. Pp. 43620–43652. DOI: 10.1109/ACCESS.2021.3065880.
11. Zou W. et al., Smart Contract Development: Challenges and Opportunities // IEEE Transactions on Software Engineering. 2021. Vol. 47. No. 10. Pp. 2084–2106. DOI: 10.1109/TSE.2019.2942301.
12. Kushwaha S.S., Joshi S., Singh D., Kaur M. Lee H.-N. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract // IEEE Access. 2022. Vol. 10. Pp. 6605–6621. DOI: 10.1109/ACCESS.2021.3140091.
13. Маркова С.В. Выявления уязвимостей в децентрализованных информационных системах на основе смарт-контрактов с помощью методов обработки больших данных // Фундаментальные исследования. 2022. № 9. С. 47–53.
14. Zheng P., Jiang Z., Wu J., Zheng Z. Blockchain-Based Decentralized Application: A Survey // IEEE Open Journal of the Computer Society. 2023. Vol. 4. Pp. 121–133. DOI: 10.1109/OJCS.2023.3251854.
15. Петренко А.С., Романченко А.М. Перспективный метод криптоанализа на основе алгоритма Шора // Защита информации. Инсайд. 2020. № 2(92). С. 17–23.
16. Петренко А.С. Квантово-устойчивый блокчейн: научная монография // Санкт-Петербург: Питер, 2023. 384 с.
17. Fernandez-Carames T.M., Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks // IEEE Access. 2020. Vol. 8. Pp. 21091–21116. DOI: 10.1109/ACCESS.2020.2968985.
18. Петренко С.А. Киберустойчивость Индустрии 4.0: научная монография // «Издательский Дом «Афина». 2020. 256 с.
19. Балябин, А.А. Модель облачной платформы КИИ РФ с кибериммунитетом в условиях информационно-технических воздействий // Защита информации. Инсайд. 2024. № 5(119). С. 35–44.
20. Балябин А.А., Петренко С.А., Костюков А. Д. Метод восстановления облачных и пограничных вычислений на основе кибериммунитета // Защита информации. Инсайд. 2022. № 6(108). С. 26–31.

MODEL OF A BLOCKCHAIN PLATFORM WITH CYBER-IMMUNITY UNDER QUANTUM ATTACKS

Balyabin A.A.[3], Petrenko S.A.[4]

Keywords: *threats to information security, quantum threats to security, blockchain ecosystems and platforms, cybersecurity, cyber resilience, methods of analysis and synthesis of quantum-resistant blockchain.*

Purpose of work *is to review new aspects for the task of information extraction from ensembles of quantum states, dictated by practical tasks of quantum cryptography.*

Research methods: *mathematical methods of quantum information theory, in particular, unambiguous discrimination of quantum states.*

Results of the study: *the paper analyzes the literature on the topic of eavesdropper information bounds in quantum cryptography in the presence of channel attenuation, including in the absence of quantum memory. The features of application of the fundamental information bound to the eavesdropper information in the presence of attenuation, the threats of application of ad hoc countermeasures for unambiguous state discrimination attack are demonstrated. The problems of finding an effective postselective eavesdropping transformation, as well as measurement in the absence of eavesdropper's quantum memory, are formulated.*

Scientific novelty: *the scientific novelty consists in the integration of disparate approaches to the problem of eavesdropper information bounds in quantum cryptography and resisting attacks in case of lossy channel. The review describes the peculiarities of applying information bound to quantum cryptography problems and formalizes the challenges facing the eavesdropper under attenuation conditions.*

References

1. Mourtzis D., Angelopoulos J., Panopoulos N. Blockchain Integration in the Era of Industrial Metaverse // Applied Sciences. 2023. Vol. 13. No. 3. P. 1353. DOI: 10.3390/app13031353.
2. Markov A.S. Vazhnaya vekha v bezopasnosti otkrytogo programmnogo obespecheniya // Voprosy kiberbezopasnosti. 2023. № 1 (53). Pp. 2–12. DOI: 10.21681/2311-3456-2023-1-2-12.
3. Nguyen D.C. et al. 6G Internet of Things: A Comprehensive Survey // IEEE Internet of Things Journal. 2022. Vol. 9. No. 1. Pp. 359–383. DOI: 10.1109/JIOT.2021.3103320.
4. Balyabin A.A., Petrenko S.A., Kostyukov A.D. Model' ugroz bezopasnosti i kiberustoychivosti oblachnykh platform KII RF // Zashchita informatsii. Insayd. 2024. № 5 (119). Pp. 26–34.
5. Chen C. et al. When Digital Economy Meets Web3.0: Applications and Challenges // IEEE Open Journal of the Computer Society. 2022. Vol. 3. Pp. 233–245. DOI: 10.1109/OJCS.2022.3217565.

3 Artyom A. Balyabin, Junior Researcher, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, E-mail: Balyabin.AA@talantiuspeh.ru

4 Sergei A. Petrenko, Dr.Sc. (in Tech.) (Grand Doctor, Full Professor), Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, Orcid.org/0000- 0003-0644-1731, E-mail: Petrenko.SA@talantiuspeh.ru

6. Petrenko A. S., Lomako A. G., Petrenko S. A. Analiz sovremennogo sostoyaniya issledovaniy problemy kvantovoy ustoychivosti blokcheyna. Chast' 1. // Zashchita informatsii. Insayd. 2023. № 3(111). Pp. 38–46.
7. Petrenko A. S., Petrenko S. A., Kostyukov A. D. Etalonnaya model' blokcheyn-platformy // Zashchita informatsii. Insayd. 2022. № 4(106). Pp. 34–44.
8. Petrenko A. S., Petrenko S. A. Metod otsenivaniya kvantovoy ustoychivosti blokcheyn-platform // Voprosy kiberbezopasnosti. 2022. № 3(49). Pp. 2–22. DOI 10.21681/2311-3456-2022-3-2-22.
9. Petrenko A., Petrenko S. Basic Algorithms Quantum Cryptanalysis // Voprosy Kiberbezopasnosti. 2023. No. 1 (53). Pp. 100–115. DOI 10.21681/2311-3456-2023-1-100-115.
10. Lashkari B., Musilek P. A Comprehensive Review of Blockchain Consensus Mechanisms // IEEE Access. 2021. Vol. 9. Pp. 43620–43652. DOI: 10.1109/ACCESS.2021.3065880.
11. Zou W. et al., Smart Contract Development: Challenges and Opportunities // IEEE Transactions on Software Engineering. 2021. Vol. 47. No. 10. Pp. 2084–2106. DOI: 10.1109/TSE.2019.2942301.
12. Kushwaha S. S., Joshi S., Singh D., Kaur M. Lee H.-N. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract // IEEE Access. 2022. Vol. 10. Pp. 6605–6621. DOI: 10.1109/ACCESS.2021.3140091.
13. Markova S. V. Vyyavleniya uyazvimostey v detsentralizovannykh informatsionnykh sistemakh na osnove smart-kontraktov s pomoshch'yu metodov obrabotki bol'shikh dannykh // Fundamental'nye issledovaniya. 2022. № 9. Pp. 47–53.
14. Zheng P., Jiang Z., Wu J., Zheng Z. Blockchain-Based Decentralized Application: A Survey // IEEE Open Journal of the Computer Society. 2023. Vol. 4. Pp. 121–133. DOI: 10.1109/OJCS.2023.3251854.
15. Petrenko A. S., Romanchenko A. M. Perspektivnyy metod kriptoanaliza na osnove algoritma Shora // Zashchita informatsii. Insayd. 2020. № 2(92). Pp. 17–23.
16. Petrenko A. S. Kvantovo-ustoychivyy blokcheyn: nauchnaya monografiya. // Sankt-Peterburg : Piter, 2023. 384 p.
17. Fernandez-Carames T. M., Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks // IEEE Access. 2020. Vol. 8. Pp. 21091–21116. DOI: 10.1109/ACCESS.2020.2968985.
18. Petrenko S. A. Kiberustoychivost' Industrii 4.0: nauchnaya monografiya // «Izdatel'skiy Dom «Afina». 2020. 256 p.
19. Balyabin A. A. Model' oblachnoy platformy KII RF s kiberimmunitetom v usloviyakh informatsionno-tekhnicheskikh vozdeystviy // Zashchita informatsii. Insayd. 2024. № 5(119). Pp. 35–44.
20. Balyabin A. A., Petrenko S. A., Kostyukov A. D. Metod vosstanovleniya oblachnykh i pogranichnykh vychisleniy na osnove kiberimmuniteta // Zashchita informatsii. Insayd. 2022. № 6(108). Pp. 26–31.