МОДЕЛЬ КВАНТОВЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ НАЦИОНАЛЬНЫХ БЛОКЧЕЙН-ЭКОСИСТЕМ И ПЛАТФОРМ

Петренко С. А.[1], Балябин А. А.[2]

DOI: 10.21681/2311-3456-2025-1-7-17

Цель исследования: *разработка математической модели квантовых угроз безопасности информации на основе сетей Петри для национальных блокчейн-экосистем и платформ «Экономики данных» Российской Федерации.*

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

Полученные результаты: *модель ранее неизвестных квантовых угроз безопасности информации на основе сетей Петри для национальных блокчейн-экосистем и платформ «Экономики данных» Российской Федерации.*

Научная новизна: *представлена и обоснована математическая модель квантовых угроз безопасности на основе сетей Петри, которая позволила задать метрику и меру обеспечения киберустойчивости для типовой блокчейн-системы в условиях новых кибератак злоумышленников с применением квантового компьютера.*

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

Введение

В настоящее время наблюдается беспрецедентный рост угроз безопасности информации в отношении объектов критической информационной инфраструктуры Российской Федерации, в том числе национальных блокчейн-экосистем и платформ [1, 2].

Общее количество инцидентов информационной безопасности (ИБ) возросло на 64% по отношению к аналогичному показателю предыдущего года (см. рис. 1) [3].

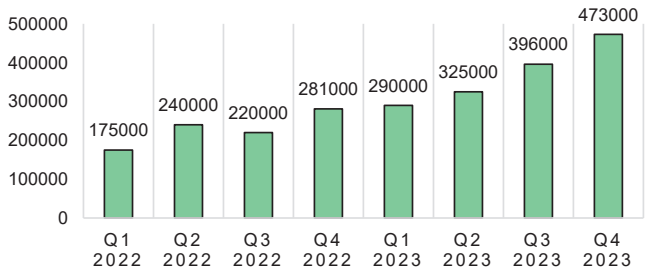

Рис. 1. События ИБ по кварталам в 2022-2023 гг.

Сегодня технологии блокчейн нашли различное применение в области криптовалют [4], смарт-контрактов [5], интернета вещей (IoT) [6], систем электронного голосования [7] и др. Криптографические преобразования, лежащие в основе технологии блокчейн, обеспечивают один из фундаментальных принципов информационной безопасности – неотказуемость, – а распределенная децентрализованная архитектура позволяет всем участникам сети верифицировать хранящиеся в ней записи без необходимости в едином «удостоверяющем центре» [8]. Несмотря на это, наблюдается рост количества инцидентов, связанных с атаками на блокчейн-платформы. Так в результате атаки на криптобиржу MtGox злоумышленниками было похищено более 450 млн долларов США [9], а всего суммарно было похищено с различных криптобирж порядка 2 млрд долларов США [10]. При этом большинство атак злоумышленников на блокчейн экосистемы и платформы осуществляется с применением классических СуперЭВМ архитектуры фон Неймана. Однако в 2023-2024 гг. были впервые зафиксированы атаки злоумышленников с применением квантового компьютера [11].

Криптостойкость алгоритмов цифровой подписи и хэширования, лежащих в основе технологии блокчейн, обеспечивается сложностью задач разложения большого числа на простые сомножители и дискретного логарифмирования. Однако применение квантовых алгоритмов, таких как алгоритм Шора, позволяет экспоненциально сократить время решения данных задач. Это представляет собой новую угрозу для блокчейн-платформ, для противодействия которой требуется внедрение квантово-устойчивых криптографических преобразований [12].

1 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

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

В целом рост количества и сложности кибератак на блокчейн экосистемы и платформы является общемировой тенденцией. Существующие платформы блокчейн уже не обладают требуемой киберустойчивостью в условиях роста угроз безопасности, в том числе квантовых, а применяемых классических методов и средств защиты зачастую недостаточно для предотвращения катастрофических последствий кибератак.

Особенности структуры и поведения блокчейн-экосистем и платформ

Функционирование типовой блокчейн-системы можно поэтапно представить следующим образом:

1) создание транзакции;
2) верификация и валидация транзакции;
3) формирование блока транзакций;
4) подтверждение блока транзакций по алгоритму консенсуса;
5) добавление блока в распределенный реестр.

Транзакции в блокчейн объединяются в блоки, как показано на рис. 2. Каждый блок состоит из заголовка и основой части, в которой содержатся записи обо всех входящих в этот блок транзакциях. Каждый вновь создаваемый блок транзакций хранит в себе хэш предыдущего блока так, что цепочку блоков транзакций возможно восстановить вплоть до первого блока в системе, называемого генезис-блоком.

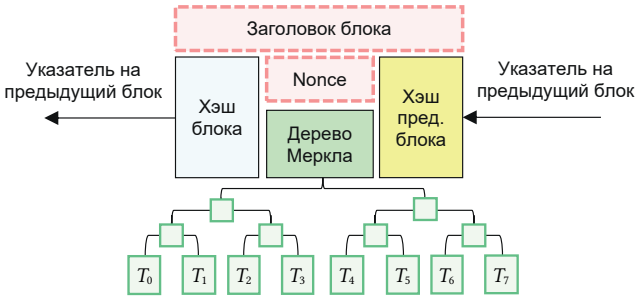

Рис. 2. Представление блокчейн в виде цепочки блоков

При формировании блока транзакций в блокчейн используется один из алгоритмов консенсуса. Наиболее распространенными алгоритмами консенсуса являются [13]:

- *Proof of Work (PoW);*
- *Proof of Stake (PoS);*
- *Delegated Proof of Stake (DPoS).*

Типовая блокчейн-система представляет собой распределенный реестр, между узлами которого осуществляется сетевое взаимодействие, поэтому в ее архитектуре возможно выделить уровни, аналогичные уровням сетевой модели OSI, включающие сверху вниз: уровень приложений, уровень сервисов, уровень протоколов, уровень сети и уровень инфраструктуры [14]. Укрупненная архитектура типовой блокчейн-системы представлена на рис. 3.

Таким образом, к особенностям национальных блокчейн-экосистем и платформ можно отнести:

- высокая сложность структуры и поведения;
- преимущественно вычислительный характер обработки данных;
- беспрецедентный рост угроз безопасности информации;
- высокие требования к безопасности и киберустойчивости и др.

Данные особенности необходимо учитывать при разработке модели квантовых угроз безопасности информации для национальных блокчейн-экосистем и платформ.

Предлагаемый способ решения задачи

Состояния типовой блокчейн-системы предлагается моделировать с помощью математического аппарата сетей Петри [15]:

$$N = (P,T,F,M_0), \quad (1)$$

где $P = \{p_1,...,p_i,...,p_n\}$ – конечное множество позиций, $n > 0$; $T = \{t_1,...,t_j,...,t_m\}$ – конечное множество переходов,

Уровень приложений	dApp Browsers	Decentralized Applications	Application Hosting	Programming Languages	
Сервисы и решения	Multi signatures	Data Feeds	Off-chain Computing	Governance, DAOs	State Channels
	Oracles	Wallets	Digital Assets	Smart Contracts	Digital IDs
Уровень протоколов	Consensus Algorithms	Side Chains	Permissioned and Permissionless	EVMs	
Уровень сети	RPLx	Roll Your Own	Block Delivery Networks	Trusted Execution Environment	Peer-to-Peer
Уровень инфраструктуры	Mining	Network	Virtualization	Nodes	Tokens	Storage

Рис. 3. Укрупненная архитектура типовой блокчейн-системы

$m > 0$, $P \cap T = \varnothing$; F – функция инцидентности, $F \subseteq (P \times T) \cup (T \times P)$; M_0 – первоначальная маркировка, $M_0 : P \longrightarrow \{1,2,3,...\}$.

При этом следует отметить, что одними из самых серьезных угроз являются угрозы эксплуатации ранее неизвестных уязвимостей «нулевого дня» (0-day) и НДВ. Как известно, такие уязвимости возникают вследствие наличия программных ошибок, меняющих поведение программы. Схема жизненного цикла уязвимости «нулевого дня» приведена на рис. 4.

В случае с блокчейн-платформами, к новым, ранее неизвестным уязвимостям могут быть отнесены архитектурные уязвимости алгоритмов, связанные с недостаточной их стойкостью в условиях воздействий с применением квантовых вычислений.

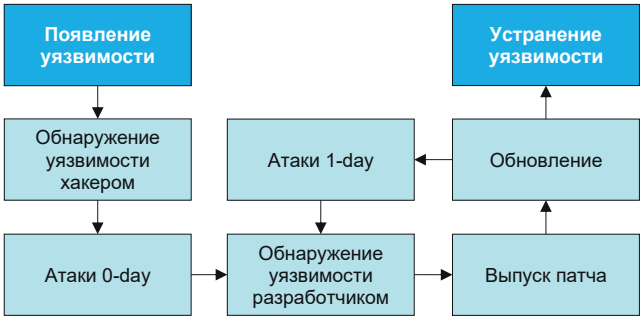

Рис. 4. Схема жизненного цикла уязвимости «нулевого дня»

Функционирование системы блокчейн опирается на допущения о ничтожно малой вероятности коллизии хэш-функций и невозможности подбора требуемого

Таблица 1.

Квантовые преобразователи

Наименование преобразователя	Обозначение	Матричное представление
Однокубитные вентили		
Вентиль Паули X	X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Вентиль Паули Y	Y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Вентиль Паули Z	Z	$\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$
Вентиль Адамара	H	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Фазовый сдвиг π/4	S	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
Фазовый сдвиг π/8	T	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
Вентиль CNOT	$CNOT$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
Многокубитные вентили		
Вентиль Controlled-Z	CZ	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$
Вентиль SWAP	$SWAP$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

значения односторонней функции за разумное время [16, 17].

Однако данные допущения справедливы лишь для фон Неймановских компьютерных систем, одновременно обрабатывающих лишь одно состояние. Квантовые же компьютеры оперируют состояниями кубитов $|\psi\rangle$ на комплексной плоскости, при этом состояния кубитов $|0\rangle$ и $|1\rangle$ соответствуют значениям бит 0 и 1. Так квантовый компьютер, состоящий из N кубитов, способен оперировать 2^N квантовыми состояниями одновременно.

Для выполнения практических вычислений на квантовом компьютере к кубитам применяется ряд линейных преобразований, которые в широком смысле соответствуют решениям уравнения Шредингера. В табл. 1 представлены основные квантовые преобразователи, их обозначения и представление в матричной форме.

В квантовых вычислениях также применяются некоторые известные алгоритмы, которые позволяют значительно сократить время решения вычислительно-сложных криптографических задач.

Квантовый алгоритм Дойча-Йожи используется для определения того, к какому типу относится функция $f: \{0,1\}^n \longrightarrow \{0,1\}$ – постоянному или сбалансированному [18]. Известно, что сбалансированная булева функция на всей области определения возвращает значения 0 и 1 одинаковое количество раз. Для вычислений в алгоритме применяется квантовый оракул $U_f: |x,y\rangle \longrightarrow |x,y \oplus f(x)\rangle$. Последовательность шагов вычисления выглядит следующим образом:

1) начальное состояние с $n + 1$ кубитами: $|\psi_0\rangle = |0\rangle^{\oplus n} \otimes |1\rangle$;
2) преобразование Адамара над n входными кубитами приводит их в состояние суперпозиции:
$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \sum_{x=0}^{2^n-1} |x\rangle \oplus |1\rangle;$$
3) применение квантового оракула U_f и получение результата:
$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \oplus |1\rangle;$$
4) повторное преобразование Адамара над n входными кубитами и измерение состояния кубитов.

Если при измерении все значения кубитов оказались равными 0, то функция $f(x)$ является постоянной, иначе – сбалансированной.

Квантовый алгоритм Шора применяется при решении задачи разложения целого числа N на простые сомножители p и q так, что $N = p \times q$. Последовательность шагов вычисления выглядит следующим образом:

1) к n входными кубитам в начальном состоянии $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ применяется квантовое преобразование Фурье;
2) поиск периода r функции $f(x) = a^x \bmod N$, где a – случайно выбранное число, взаимно простое с N.

Квантовый алгоритм Шора способен решать задачу вычисления дискретного логарифма за полиномиальное время, в частности, временная сложность факторизации числа N оценивается как $O(\log^2 N \log\log N \log\log N)$ [19].

Квантовый алгоритм Гровера применяется для решения задачи поиска элемента в неупорядоченном множестве. Математически это можно записать в виде функции $f: \{0,1\}^n \longrightarrow \{0,1\}$, при этом алгоритм Гровера решает задачу поиска x, такого, что $f(x) = 1$ [20]. Последовательность шагов вычисления выглядит следующим образом:

1) начальное состояние с n кубитами: $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$;
2) применение квантового оракула U_f для поиска состояний, удовлетворяющих условию $f(x) = 1$;
3) применение оператора диффузии Гровера D, переход к шагу 2;
4) измерение состояния кубитов и определение значения x.

Временная сложность решения задачи на множестве мощности N оценивается как $O(\sqrt{N})$, что означает возможность решения на квантовом компьютере NP-полной задачи с квадратичным приростом скорости по сравнению с решением аналогичной задачи на компьютере с фон Неймановской архитектурой.

Применение квантовых алгоритмов позволяет значительно ускорить решение ряда вычислительно-сложных задач, что приводит к возникновению отдельного класса уязвимостей архитектурного характера, эксплуатация которых представляет угрозу для блокчейн-экосистем и платформ КИИ РФ. Для наглядности в табл. 2 и 3 приведено сравнение вычислительной сложности некоторых алгоритмов решения задач факторизации числа, состоящего из $N = \log_2 n$ символов, где n – количество двоичных разрядов числа, и дискретного логарифмирования.

Таблица 2.

Временная сложность решения задачи факторизации

Наименование алгоритма	Оценка временной сложности
Алгоритм Ферма	$O\left(N^{\frac{1}{3}}\right)$
Алгоритм квадратичного решета	$O(e^{(1+0(1))\sqrt{\log n \log\log n}})$
Алгоритм решета числового поля	$O(n \log n \log N)$
Алгоритм Шора	$O(\log^3 N)$

Таблица 3.

Временная сложность решения задачи дискретного логарифмирования

Наименование алгоритма	Оценка временной сложности
Алгоритм Адлемана	$O\left(c^{\ln p^{\frac{1}{2}}}\right)$
Алгоритм COS	$O(e^{(\log p \log\log p)^{\frac{1}{2}}})$
Алгоритм решета числового поля	$O(n \log n \log N)$
Алгоритм Шора	$O(\log^3 N)$

Формирование перечня актуальных угроз безопасности

Стратифицированное представление блокчейн-платформ по уровням возникновения уязвимостей, эксплуатируемых в ходе осуществления атак, представлено на рис. 5.

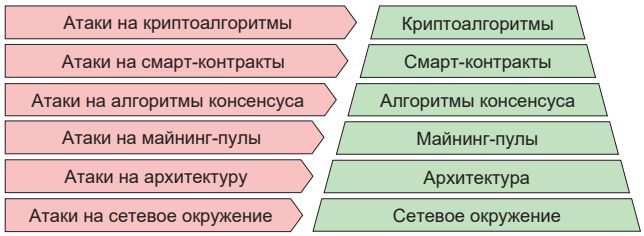

Рис. 5. Стратификация блокчейн-платформ по уровням возникновения эксплуатируемых уязвимости

Уязвимости криптографических алгоритмов. Большинство современных блокчейн-платформ (Bitcoin, Ethereum, Litecoin, Dash, Ripple, Cardano и др.) используют для генерации ключевой пары алгоритм цифровой подписи на основе эллиптических кривых (ECDSA). Криптостойкость таких алгоритмов основана на допущении о сложности вычисления дискретного логарифма на эллиптической кривой, то есть решения уравнения вида:

$$S = nT(\mathrm{mod}\ m) \qquad (2)$$

относительно n, где S, T – известные точки на эллиптической кривой, соответствующие зашифрованному и начальному сообщениям. Временная сложность дискретного логарифмирования на эллиптической кривой с помощью ρ-алгоритма Полларда составляет $O(\sqrt{n})$, где n – длина ключа в битах, в то время как применение квантового алгоритма Шора позволяет свести ее к $O(\log^3 n)$. Это может позволить злоумышленнику, имеющему квантовый вычислитель и открытый ключ, отыскать соответствующий ему закрытый ключ из ключевой пары и осуществить атаку подмены личности [21].

Другим примером уязвимостей криптографических алгоритмов является недостаточная криптостойкость применяемых в блокчейн-платформах хэш-функций (SHA256, Ethash, SCrypt, Equihash, X11 и др.) к атаке нахождения коллизии с помощью квантового алгоритма Гровера. В этом случае злоумышленник может сгенерировать вредоносный блок, обладающий такой же хэш-суммой, как и изначальный, и осуществить атаку 51 %, двойного расходования и эгоистичного майнинга [22].

Уязвимости смарт-контрактов. Смарт-контракты, используемые в таких блокчейн-платформах, как Ethereum, считаются одним из самых уязвимых элементов блокчейн [5, 23]. К причинам возникновения уязвимостей данного уровня относятся недостатки, связанные с зависимостью временных меток, порядком следования транзакций, реентерантностью и необработанными исключениями, что может позволить злоумышленнику осуществить атаку повторного воспроизведения смарт-контракта.

Уязвимости алгоритмов консенсуса. Алгоритмы консенсуса (PoW, PoS, DPoS и др.) являются одними из центральных элементов блокчейн-платформ и выполняют функции верификации блоков. В зависимости от конкретных типов алгоритмов консенсуса возможны реализации таких атак, как атака 51 %, Финни и атака двойного расходования [13, 24].

Уязвимости майнинг-пулов. Вычислительная сложность майнинга в современных блокчейн-платформах (Bitcoin, Ethereum и др.) может быть достаточно высока, что заставляет узлы объединять вычислительные мощности в пулы. С другой стороны, это представляет опасность для блокчейн-экосистемы, поскольку вычислительная мощность одного пула может превысить вычислительную мощность остальной сети блокчейн, что позволит злоумышленнику, имеющему возможность управления пулом, осуществить такие атаки, как атака 51 %, двойного расходования и удержания блока [25].

Уязвимости архитектуры. К архитектурным недостаткам блокчейн-систем можно отнести недостатки, связанные с некорректной идентификацией узлов, перезапуском системы, отсутствием ограничений размеров блока [26]. Используя эти недостатки, злоумышленник может осуществить атаки, такие как атака информационного затмения и DDoS-атака.

Уязвимости сетевого окружения. Поскольку блокчейн-платформа представляет собой одноранговую сеть взаимосвязанных узлов, распространение информации по которой осуществляется с некоторой задержкой, то она может быть уязвима для таких атак, как атака Сивиллы, двойного расходования и DNS-атака [26].

Учитывая рассмотренные уязвимости, сформируем перечень актуальных угроз устойчивости блокчейн-экосистем и платформ КИИ РФ, как показано

Таблица 4.

Перечень актуальных угроз устойчивости блокчейн-экосистем и платформ КИИ РФ

Уязвимости по уровням возникновения Атаки	Криптоалгоритмы	Смарт-контракты	Алгоритмы консенсуса	Майнинг-пулы	Архитектура	Сетевое окружение
Атака 51%	+	–	+	+	–	–
Атака подмены личности	+	–	–	–	–	–
Атака Сивиллы	–	–	–	–	–	+
Атака информационного затмения	–	–	–	–	+	+
Атака эгоистичного майнинга	+	–	+	+	–	–
Атака двойного расходования	+	–	+	+	–	–
Атака Финни	+	–	+	–	–	–
DDoS-атака	–	–	–	–	+	+
DNS-атака	–	–	–	–	–	+
Атака BGP-hijacking	–	–	–	–	+	+
Атака удержания блока	+	–	–	+	–	–
Атака на баланс	+	–	+	+	–	+
Атака повторного воспроизведения	–	+	–	–	+	–

в табл. 4. Символы «+» и «–» означают, что данная уязвимость соответственно может или не может эксплуатироваться при атаке на определенный уровень блокчейн-платформы.

Отметим, что большинство кибератак осуществляется с территорий иностранных государств, что подразумевает наличие удаленного доступа к объектам критической информационной инфраструктуры (КИИ) РФ и сетевой вектор воздействия. Значимую угрозу представляют нарушители, обладающие высоким потенциалом, в распоряжении которых имеются достаточные ресурсы для подготовки и осуществления кибератак с использованием средств эксплуатации известных и ранее неизвестных уязвимостей блокчейн-экосистем и платформ:

- специальные службы иностранных государств;
- террористические и экстремистские организации;
- организованные хакерские группировки.

Моделирование кибератак злоумышленников на блокчейн-экосистемы

Типовая схема компьютерной атаки в соответствии с MITRE ATT&CK имеет 14 этапов (тактик) и более 400 техник [27], однако, в реальных кибератаках могут задействоваться не все этапы. На рис. 6 представлена схема типового целенаправленного ИТВ на блокчейн-платформу КИИ РФ, состоящего из 5 этапов, характерных для подавляющего большинства целенаправленных ИТВ.

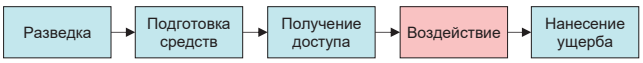

Рис. 6. Обобщенная схема ИТВ на типовую блокчейн-платформу КИИ РФ

Рассмотрим подробнее этап непосредственного воздействия на целевую систему, а также примеры кибератак злоумышленников на типовые блокчейн-платформы.

Атака 51 %. Данная атака характерна для блокчейн-платформ, использующих алгоритмы консенсуса типа PoW, PoS, DPoS, и предполагает наличие у злоумышленника 51 % или более вычислительной мощности блокчейн-платформы. Такое превосходство достижимо несколькими способами:

- увеличение количества вычислителей в пуле;
- применение квантового алгоритма Гровера.

Применение злоумышленником квантового алгоритма Гровера для поиска коллизий хэш-функций может позволить ему значительно быстрее подбирать значение параметра *Nonce* создаваемого блока и формировать произвольные вредоносные блоки

с требуемыми хэш-суммами. Сформируем модель данной атаки на основе сети Петри.

- Предусловия (условия осуществимости атаки):
  - P_1 – злоумышленник обладает 51 % или более вычислительной мощности сети блокчейн:
    - P_{11} – для алгоритмов консенсуса типа PoW:
      - P_{111} – злоумышленник контролирует более 50 % вычислительной мощности блокчейн-платформы;
      - P_{112} – злоумышленник обладает вычислительными ресурсами квантового компьютера;
    - P_{12} – злоумышленник обладает более 50 % долей владения для алгоритмов консенсуса типа PoS;
    - P_{13} – злоумышленник обладает более 50 % прав голоса для алгоритмов консенсуса типа DPoS;
  - P_2 – злоумышленник знает хэш-сумму предыдущего блока;
- Переходы (шаги осуществления атаки):
  - T_1 – синтез вредоносного блока с требуемой хэш-суммой без передачи его в блокчейн;
  - T_2 – синтез вредоносной цепочки блоков, более длинной, чем существующая;
  - T_3 – передача созданной вредоносной цепочки блоков в блокчейн;
- Постусловия (возможные направления развития атаки):
  - P_3 – блокировка транзакций;
  - P_4 – препятствование деятельности иных узлов блокчейн;
  - P_5 – обращение транзакций для подготовки атаки двойного расходования;
  - P_6 – принуждение узлов блокчейн-платформы к присоединению к вычислительным мощностям злоумышленника.

Полученная модель атаки 51 % на основе сети Петри представлена на рис. 7.

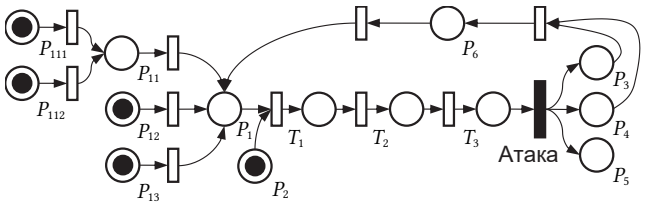

Рис. 7. Модель сети Петри для атаки 51 %

Атака двойного расходования. Одной из задач алгоритмов консенсуса является обеспечение невозможности дублирования транзакций (двойного расходования средств). Так, если $B_0,\ldots,B_i,\ldots,B_N$ – существующая цепочка блоков и целью злоумышленника является дублирование транзакции, содержащейся в блоке B_i, то ему придется заново сформировать блок B_i', не содержащий данной транзакции, а также более длинную цепочку, состоящую из блоков B_j', v с соответствующими хэш-суммами, где n – длина существующей цепочки блоков. Классическими вычислительными средствами данная атака практически не реализуема, однако, злоумышленник, обладающий возможностью осуществления квантовых вычислений, может применить алгоритм Гровера для нахождения коллизий хэш-функций. Сформируем модель данной атаки на основе сети Петри.

- Предусловия (условия осуществления атаки):
  - P_1 – злоумышленник обладает достаточными вычислительными ресурсами:
    - P_{11} – классическими;
    - P_{12} – квантовыми;
  - P_2 – транзакция записана в блок B_i и подтверждена получателем;
- Переходы (шаги осуществления атаки):
  - T_1 – синтез цепочки блоков B_i', $j = \overline{(i, n+1)}$, где блок B_i' не содержит предыдущей транзакции и распространение новой цепочки в блокчейн;
- Постусловия (возможные направления развития атаки):
  - P_3 – повторное использование средств злоумышленником.

Полученная модель атаки двойного расходования на основе сети Петри представлена на рис. 8.

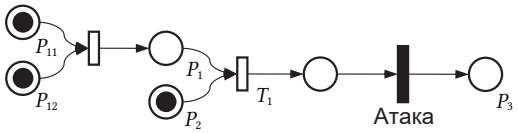

Рис. 8. Модель сети Петри для атаки двойного расходования

Атака подмены личности. Правом владения цифровых активов в блокчейн наделены обладатели закрытого ключа, а с помощью открытого ключа это право возможно проверить. Для данной атаки злоумышленнику необходимо восстановить закрытый ключ по известному открытому ключу одним из способов:

- кража данных о ключевой паре (например, в результате предварительного ИТВ);
- применение квантового алгоритма Шора для решения задачи дискретного логарифмирования за полиномиальное время.

Восстановив закрытый ключ, злоумышленник сможет действовать от имени его владельца. Сформируем модель данной атаки на основе сети Петри.

- Предусловия (условия осуществления атаки):
  - P_1 – злоумышленник обладает сведениями о параметрах эллиптической кривой для восстановления ключевой пары алгоритма ECDSA;
  - P_2 – злоумышленник обладает достаточными квантовыми вычислительными ресурсами для решения задачи дискретного логарифмирования;
  - P_3 – злоумышленник осуществил вспомогательное ИТВ и получил сведения о ключевой паре;
- Постусловия (возможные направления развития атаки):
  - P_4 – злоумышленник применил квантовый алгоритм Шора, решил задачу дискретного логарифмирования и получил закрытый ключ из ключевой пары;
  - P_5 – выполнение операций с цифровыми активами от имени владельца закрытого ключа.

Полученная модель атаки подмены личности на основе сети Петри представлена на рис. 9.

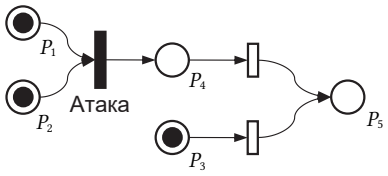

Рис. 9. Модель сети Петри для атаки подмены личности

Оценка киберустойчивости блокчейн-систем

Как правило, под устойчивостью некоторой технической системы понимают ее способность сохранять значения параметров своего функционирования в заданных пределах в условиях дестабилизирующих воздействий. Применительно к блокчейн-системам такими дестабилизирующими воздействиями являются кибератаки злоумышленников, в том числе с применением квантового компьютера. Проводя аналогию с динамическими системами, будем оценивать устойчивость функционирования блокчейн-системы в условиях кибератак злоумышленников по показателю вероятности P нахождения невосстанавливаемой системы в работоспособном состоянии в течение заданного времени t:

$$P(t) = e^{-\lambda t}, \quad (3)$$

где λ – интенсивность потока ИТВ.

Здесь мерой устойчивости является число в отрезке [0,1], где 0 обозначает абсолютно неустойчивую, а 1 – абсолютно устойчивую системы.

Примем допущение о том, что поток нарушений является простейшим. Интенсивность потока нарушений λ постоянна и зависит от вероятности искажений, которая, в свою очередь, пропорциональна количеству перебираемых хэш-сумм $N_{хэш}$ в единицу времени:

$$\lambda(t) \sim P_{иск} = const, P_{иск} = \frac{N_{хэш}}{T}. \quad (4)$$

Результаты оценки устойчивости функционирования типовой блокчейн-системы в условиях кибератак злоумышленников по показателю вероятности нахождения системы в работоспособном состоянии в зависимости от времени при различных значения $P_{иск}$ представлены на рис. 10.

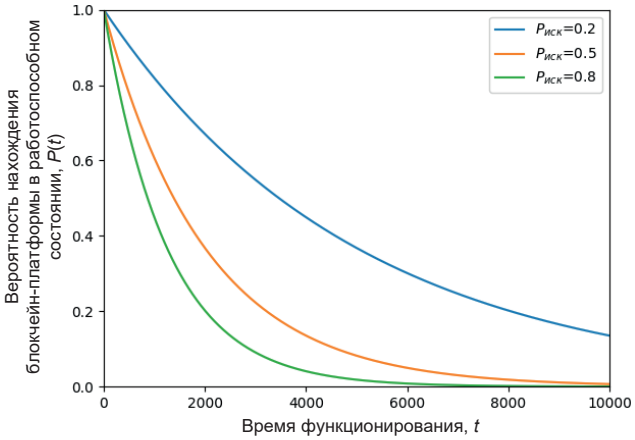

Рис. 10. Результаты оценки устойчивости функционирования типовой блокчейн-системы в условиях кибератак злоумышленников

Вероятность нахождения блокчейн-платформы КИИ РФ в работоспособном состоянии с течением времени снижается так, что $\lim_{t\to\infty} P(t) = 0$. При уменьшении количества хэш-сумм $N_{хэш}$, проверяемых в единицу времени, снижается вероятность искажения $P_{иск}$, а снижение устойчивости с течением времени замедляется. Полученные результаты позволяют подтвердить гипотезу о снижении киберустойчивости блокчейн-экосистем и платформ в условиях целенаправленных кибератак злоумышленников.

Выводы

В настоящей работе была поставлена задача разработки новой модели квантовых угроз безопасности информации на основе сетей Петри на примере некоторой типовой блокчейн-экосистемы и платформы. Приведено возможное формализованное описание источников угроз безопасности информации, сформирован перечень актуальных угроз безопасности информации. Проведено моделирование квантовых угроз безопасности, что позволило определить возможные метрику и меру обеспечения киберустойчивости блокчейн-систем в условиях кибератак злоумышленников с применением квантового компьютера.

Результаты экспериментов позволили выявить ряд количественных закономерностей снижения киберустойчивости блокчейн-экосистем и платформ «Экономики данных» РФ в условиях атак злоумышленников с применением квантового компьютера.

Статья подготовлена по результатам Проекта ФТС-2024-2.3-VY-1160-5744 «Технологии противодействия ранее неизвестным квантовым киберугрозам» в рамках реализации мероприятия 2.3 государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус».

Литература

1. *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.*
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. *Балябин, А. А. Модель облачной платформы КИИ РФ с кибериммунитетом в условиях информационно-технических воздействий // Защита информации. Инсайд. 2024. № 5 (119). С. 35–44.*
4. *Verma A. et al. Blockchain for Industry 5.0: Vision, Opportunities, Key Enablers, and Future Directions // IEEE Access. 2022. Vol. 10. Pp. 69160–69199. DOI: 10.1109/ACCESS.2022.3186892.*
5. *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.*
6. *Ali M. S., Vecchio M., Pincheira M., Dolui K., Antonelli F., Rehmani M. H. Applications of blockchains in the internet of things: A comprehensive survey // IEEE Communications Surveys & Tutorials. 2019. Vol. 21. No. 2. Pp. 1676–1717. DOI: 10.1109/COMST.2018.2886932.*
7. *Vladucu M. -V., Dong Z., Medina J., Rojas-Cessa R. E-Voting Meets Blockchain: A Survey // IEEE Access. 2023. Vol. 11. Pp. 23293–23308. DOI: 10.1109/ACCESS.2023.3253682.*
8. *Petrenko S., Khismatullina E. Cyber-resilience concept for Industry 4.0 digital platforms in the face of growing cybersecurity threats // Software Technology: Methods and Tools, 51st International Conference, TOOLS 2019, Innopolis, Russia, October 15–17, 2019. 420 p. DOI: 10.1007/978-3-030-29852-4.*
9. *Петренко А. С., Петренко С. А. Оценка квантовой угрозы для современных блокчейн-систем // Информационные системы и технологии в моделировании и управлении: Сборник трудов VII Международной научно-практической конференции, Ялта, 24–25 мая 2023 года. 2023. С. 171–173.*
10. *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.*
11. *Петренко А. С., Петренко С. А., Костюков А. Д., Ожиганова М. И. Модель квантовых угроз безопасности для современных блокчейн-платформ // Защита информации. Инсайд. 2022. № 3 (105). С. 10–20.*
12. *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.*
13. *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.*
14. *Xie J., Tang H., Huang T., Yu F., Xie R., Liu J., Liu Y. A survey of blockchain technology applied to smart cities: Research issues and challenges // IEEE Communications Surveys & Tutorials. 2019. Vol. 21. No. 3. Pp. 2794–2830. DOI: 10.1109/COMST.2019.2899617.*
15. *Shahriar M. A. et al. Modelling Attacks in Blockchain Systems using Petri Nets // 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China. 2020. Pp. 1069–1078. DOI: 10.1109/TrustCom50675.2020.00142.*
16. *Younis M. M., Salim Jamil A., Abdulrazzaq A. H., Ahmed Mawla N., Khudhair R. M., Vasiliu Y. Progress and Challenges in Quantum Computing Algorithms for NP-Hard Problems // 2024 36th Conference of Open Innovations Association (FRUCT), Lappeenranta, Finland. 2024. Pp. 460–468. DOI: 10.23919/FRUCT64283.2024.10749878.*
17. *Молдовян А. А., Молдовян Н. А. Новые формы скрытой задачи дискретного логарифмирования // Труды СПИИРАН 2019. Т. 2, № 18. С. 504–529. DOI: 10.15622/sp.18.2.504-529.*
18. *Savo G. Glisic; Beatriz Lorenzo. Quantum Search Algorithms // Artificial Intelligence and Quantum Computing for Advanced Wireless Networks, Wiley. 2022. Pp. 499–542. DOI: 10.1002/9781119790327.ch11.*
19. *Петренко А. С., Романченко А. М. Перспективный метод криптоанализа на основе алгоритма Шора // Защита информации. Инсайд. 2020. № 2 (92). С. 17–23.*
20. *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.*
21. *Borges F., Reis P. R., Pereira D. A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography // IEEE Access. 2020. Vol. 8. Pp. 142413–142422. DOI: 10.1109/ACCESS.2020.3013250.*
22. *Kearney J. J., Perez-Delgado C. A. Vulnerability of blockchain technologies to quantum attacks // Array. 2021. Vol. 10. P. 100065. DOI: 10.1016/j.array.2021.100065.*
23. *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.*
24. *Sayeed S., Marco-Gisbert H. Assessing blockchain consensus and security mechanisms against the 51 % attack // Applied Sciences. 2019. Vol. 9. No. 9. P. 1788. DOI: 10.3390/app9091788.*
25. *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.*
26. *Mollajafari S.; Bechkoum K. Blockchain Technology and Related Security Risks: Towards a Seven-Layer Perspective and Taxonomy // Sustainability 2023. Vol. 15 (18). 13401. DOI: 10.3390/su151813401.*
27. *Al-Shaer R., Spring J. M., Christou E. Learning the Associations of MITRE ATT&CK Adversarial Techniques // 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France. 2020. Pp. 1–9. DOI: 10.1109/CNS48642.2020.9162207.*

A MODEL OF QUANTUM THREATS TO INFORMATION SECURITY FOR NATIONAL BLOCKCHAIN ECOSYSTEMS AND PLATFORMS

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

The purpose of the research: *development of a mathematical model of quantum threats to information security based on Petri nets for national blockchain ecosystems and platforms of the «Data Economy» of the Russian Federation.*

The method of the research: *methods of system analysis, methods of Petri net theory, methods of probability theory and mathematical statistics, methods of the theory of stability of complex systems.*

The result of the research: *a mathematical model of quantum threats to security based on Petri nets is presented and substantiated, which made it possible to set a metric and measure of ensuring cyber resilience for a typical national blockchain system in the face of new cyber attacks by intruders using a quantum computer.*

References

1. *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.*
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. *Balyabin A. A. Model' oblachnoy platformy KII RF s kiberimmunitetom v usloviyakh informatsionno-tekhnicheskikh vozdeystviy // Zashchita informatsii. Insayd. 2024. № 5 (119). Pp. 35–44.*
4. *Verma A. et al. Blockchain for Industry 5.0: Vision, Opportunities, Key Enablers, and Future Directions // IEEE Access. 2022. Vol. 10. Pp. 69160–69199. DOI: 10.1109/ACCESS.2022.3186892.*
5. *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.*
6. *Ali M. S., Vecchio M., Pincheira M., Dolui K., Antonelli F., Rehmani M. H. Applications of blockchains in the internet of things: A comprehensive survey // IEEE Communications Surveys & Tutorials. 2019. Vol. 21. No. 2. Pp. 1676–1717. DOI: 10.1109/COMST.2018.2886932.*
7. *Vladucu M. -V., Dong Z., Medina J., Rojas-Cessa R. E-Voting Meets Blockchain: A Survey // IEEE Access. 2023. Vol. 11. Pp. 23293–23308. DOI: 10.1109/ACCESS.2023.3253682.*
8. *Petrenko S., Khismatullina E. Cyber-resilience concept for Industry 4.0 digital platforms in the face of growing cybersecurity threats // Software Technology: Methods and Tools, 51st International Conference, TOOLS 2019, Innopolis, Russia, October 15–17, 2019. 420 p. DOI: 10.1007/978-3-030-29852-4.*
9. *Petrenko A. S., Petrenko S. A. Otsenka kvantovoy ugrozy dlya sovremennykh blokcheyn-sistem // Informatsionnye sistemy i tekhnologii v modelirovanii i upravlenii : Sbornik trudov VII Mezhdunarodnoy nauchno-prakticheskoy konferentsii, Yalta, May 24–25, 2023. Pp. 171–173.*
10. *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.*
11. *Petrenko A. S., Petrenko S. A., Kostyukov A. D., Ozhiganova M. I. Model' kvantovykh ugroz bezopasnosti dlya sovremennykh blokcheyn-platform // Zashchita informatsii. Insayd. 2022. № 3 (105). Pp. 10–20.*
12. *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.*
13. *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.*
14. *Xie J., Tang H., Huang T., Yu F., Xie R., Liu J., Liu Y. A survey of blockchain technology applied to smart cities: Research issues and challenges // IEEE Communications Surveys & Tutorials. 2019. Vol. 21. No. 3. Pp. 2794–2830. DOI: 10.1109/COMST.2019.2899617.*
15. *Shahriar M. A. et al. Modelling Attacks in Blockchain Systems using Petri Nets // 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China. 2020. Pp. 1069–1078. DOI: 10.1109/TrustCom50675.2020.00142.*
16. *Younis M. M., Salim Jamil A., Abdulrazzaq A. H., Ahmed Mawla N., Khudhair R. M., Vasiliu Y. Progress and Challenges in Quantum Computing Algorithms for NP-Hard Problems // 2024 36th Conference of Open Innovations Association (FRUCT), Lappeenranta, Finland. 2024. Pp. 460–468. DOI: 10.23919/FRUCT64283.2024.10749878.*
17. *Moldovyan A. A., Moldovyan N. A. Novye formy skrytoy zadachi diskretnogo logarifmirovaniya // Trudy SPIIRAN 2019. No.5. Vol. 18. Pp. 504–529. DOI: 10.15622/sp.18.2.504-529.*

3 Sergei 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

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

18. *Savo G. Glisic; Beatriz Lorenzo. Quantum Search Algorithms // Artificial Intelligence and Quantum Computing for Advanced Wireless Networks, Wiley. 2022. Pp. 499–542. DOI: 10.1002/9781119790327.ch11.*
19. *Petrenko A. S., Romanchenko A. M. Perspektivnyy metod kriptoanaliza na osnove algoritma Shora // Zashchita informatsii. Insayd. 2020. № 2 (92). Pp. 17–23.*
20. *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.*
21. *Borges F., Reis P. R., Pereira D. A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography // IEEE Access. 2020. Vol. 8. Pp. 142413–142422. DOI: 10.1109/ACCESS.2020.3013250.*
22. *Kearney J. J., Perez-Delgado C. A. Vulnerability of blockchain technologies to quantum attacks // Array. 2021. Vol. 10. P. 100065. DOI: 10.1016/j.array.2021.100065.*
23. *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.*
24. *Sayeed S., Marco-Gisbert H. Assessing blockchain consensus and security mechanisms against the 51 % attack // Applied Sciences. 2019. Vol. 9. No. 9. P. 1788. DOI: 10.3390/app9091788.*
25. *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.*
26. *Mollajafari S.; Bechkoum K. Blockchain Technology and Related Security Risks: Towards a Seven-Layer Perspective and Taxonomy // Sustainability 2023. Vol. 15 (18). 13401. DOI: 10.3390/su151813401.*
27. *Al-Shaer R., Spring J. M., Christou E. Learning the Associations of MITRE ATT&CK Adversarial Techniques // 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France. 2020. Pp. 1–9. DOI: 10.1109/CNS48642.2020.9162207.*