Модель квантовых угроз безопасности информации на основе сетей Петри для национальных блокчейн-экосистем

Петренко Алексей Сергеевич[1, 2],
аспирант, м.н.с.
Petrenko.AS@talantiuspeh.ru

Балябин Артем Алексеевич[1, 2],
аспирант, м.н.с.
Balyabin.AA@talantiuspeh.ru

[1] *Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)*
[2] *Научно-технологический университет «Сириус»*

Показано, что известных организационных и технических мер информационной безопасности уже недостаточно для обеспечения требуемой киберустойчивости блокчейн-экосистем и платформ «Экономики данных» Российской Федерации в условиях ранее неизвестных атак злоумышленников с применением квантового компьютера. Представлена и обоснована новая авторская модель квантовых угроз безопасности информации на основе математического аппарата сетей Петри для упомянутых блокчейн–экосистем и платформ. Приведены доказательства полноты, непротиворечивости и разрешимости этой математической модели. Выработан ряд рекомендаций для пополнения Банка угроз безопасности информации ФСТЭК России, https://bdu.fstec.ru/threat перечнем новых квантовых угроз безопасности.

Ключевые слова: *экономика данных, технологический суверенитет, информационная безопасность, национальная программа технологического развития, технология блокчейн, распределенный реестр, угрозы безопасности информации, модель квантовых угроз безопасности, квантово-устойчивый блокчейн*

Состояние вопроса

Проведен ряд исследований, посвященных угрозам безопасности блокчейн-экосистем и платформ как объектов КИИ. Например, в работах [1, 4, 6–10, 15 18, 20–38, 43, 70, 75, 77, 78] рассматривается текущее состояние постквантовой криптографии и ее возможные применения в блокчейн-экосистемах, предлагаются подходы к обеспечению квантовой устойчивости блокчейн. В работе [1, 11, 69–80] оцениваются потенциальные риски для блокчейн-платформ, связанные с внедрением квантовых вычислений, а также уязвимость асимметричных криптосистем и хэш-функций к атакам с использованием квантового компьютера. В работах [1, 12–18, 20–38, 51–72] исследуются возможности применения различных алгоритмов консенсуса, основанных на постквантовых криптосистемах, для обеспечения квантовой устойчивости блокчейн-платформ.

Работы [1–14, 43–61, 64–80] посвящены систематизации угроз информационной безопасности КИИ в целом, однако детали реализации кибератак в них не рассматриваются. Работы посвящены анализу моделей и методов обеспечения устойчивости КИИ, однако не рассматриваются особенности блокчейн-экосистем и платформ. В работе [20] предложена модель нарушителя ИБ, позволяющая оценить безопасность объекта КИИ с учетом потенциала нарушителя. В работах [7, 21–29, 38–72] рассмотрены основные угрозы безопасности КИИ, а также проблемы защиты их компонентов, в частности, гипервизоров, виртуальных сред, приложений, средств сетевого взаимодействия.

Таким образом, существующие исследования в основном посвящены анализу угроз безопасности либо для блокчейн-платформ, либо для объектов КИИ в целом. Формализованное описание причин возникновения уязвимостей и способов их эксплуатации применительно к блокчейн-экосистемам и платформам не проводилось.

Характеристика объекта исследования

Объектом исследования являются национальные блокчейн-экосистемы и платформы, относящиеся к КИИ РФ. Технологии блокчейн универсальны, поэтому угрозы, актуальные для настоящего объекта исследования, могут быть актуальны также и для иных блокчейн-платформ.

Функционирование системы блокчейн может быть охарактеризовано 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. 1. 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.

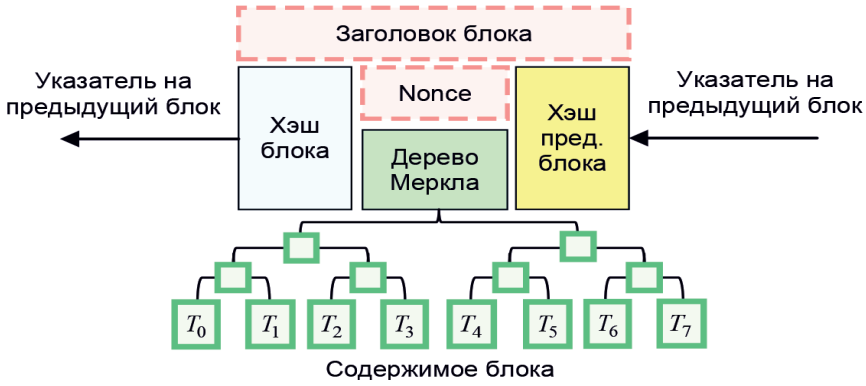

Рис. 1. ***Представление блокчейн в виде цепочки блоков***

При формировании блока транзакций в блокчейн используется один из алгоритмов консенсуса. Наиболее распространенными алгоритмами консенсуса являются [1–16, 28–54]:

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

Типовая блокчейн-платформа 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.* Укрупненная схема архитектуры типовой блокчейн-экосистемы представлена на рис. 2.

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

- информационно-вычислительная система;
- многоуровневая архитектура;
- динамическая система с обратной связью;
- система с повышенными требованиями к устойчивости функционирования;
- система, функционирующая в условиях целенаправленных воздействий.

Данные особенности необходимо учитывать при разработке модели квантовых угроз безопасности национальных блокчейн экосистем и платформ КИИ РФ.

Постановка задачи исследования

Введем обозначения. Будем моделировать состояния блокчейн-платформы с помощью сети Петри [25, 26]:

$$N = (P, T, F, M_0),$$

где $P = \{p_1, \ldots, p_i, \ldots, p_n\}$ – конечное множество позиций, $n > 0$; $T = \{t_1, \ldots, t_j, \ldots, t_m\}$ – конечное множество переходов, $m > 0$, $P \cap T = \varnothing$; F – функция инцидентности, $F \subseteq (P \times T) \cup (T \times P)$; M_0 – первоначальная маркировка, $M_0 : P \to \{1, 2, 3, \ldots\}$.

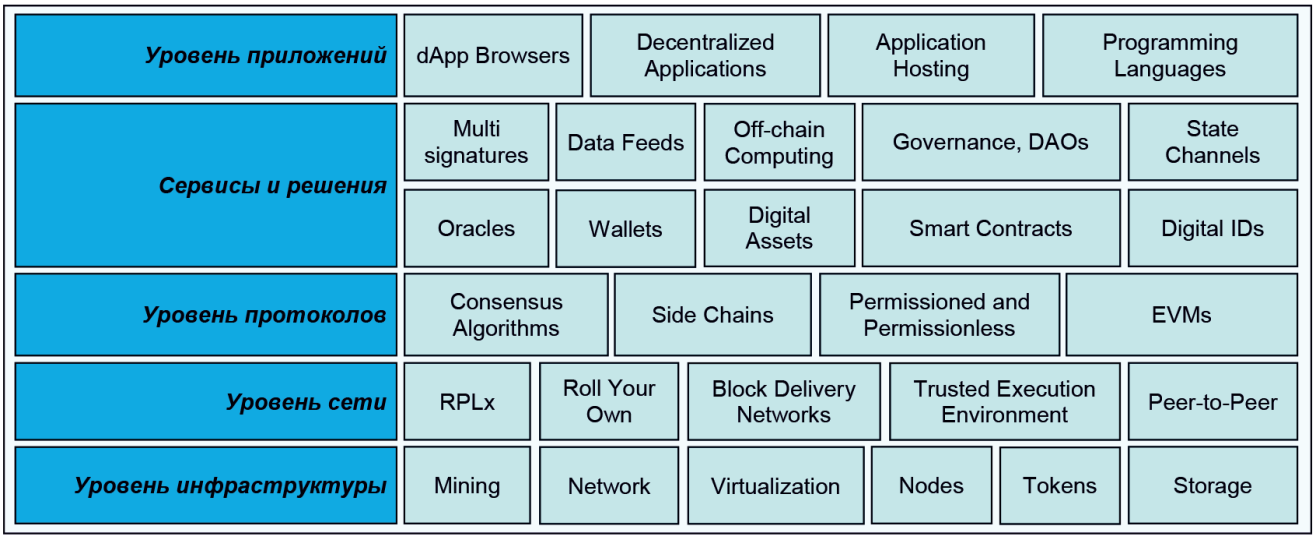

Рис. 2. ***Укрупненная архитектура типовой блокчейн-экосистемы***

Задачей исследования является разработка модели новых угроз и оценка устойчивости функционирования блокчейн-экосистем и платформ КИИ РФ в условиях роста угроз безопасности, в том числе квантовой угрозы безопасности, на примере типовой блокчейн-платформы.

Частные задачи исследования:

- сформировать перечень актуальных угроз устойчивости функционирования блокчейн-экосистем и платформ КИИ РФ;
- определить показатель, метрику и меру устойчивости блокчейн-экосистем и платформ КИИ РФ;
- оценить устойчивость блокчейн-экосистем и платформ КИИ РФ в условиях ИТВ на примере типовой блокчейн-платформы.

Гипотеза исследования: целенаправленные информационно-технические воздействия снижают устойчивость функционирования блокчейн-экосистем и платформ КИИ РФ.

Характеристика угроз безопасности блокчейн

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. 3.

В случае с блокчейн-экосистемами и платформами, к новым, ранее неизвестным уязвимостям могут быть отнесены архитектурные уязвимости алгоритмов, связанные с недостаточной их стойкостью в условиях воздействий с применением квантовых вычислений. Функционирование системы блокчейн опирается на принятые допущения, связанные с особенностями криптографических алгоритмов, такие как ничтожно малая вероятность коллизии хэш-функций или невозможность подбора значения односторонней функции, удовлетворяющего заданным условиям, за разумное время [1–14, 28–37, 39–41].

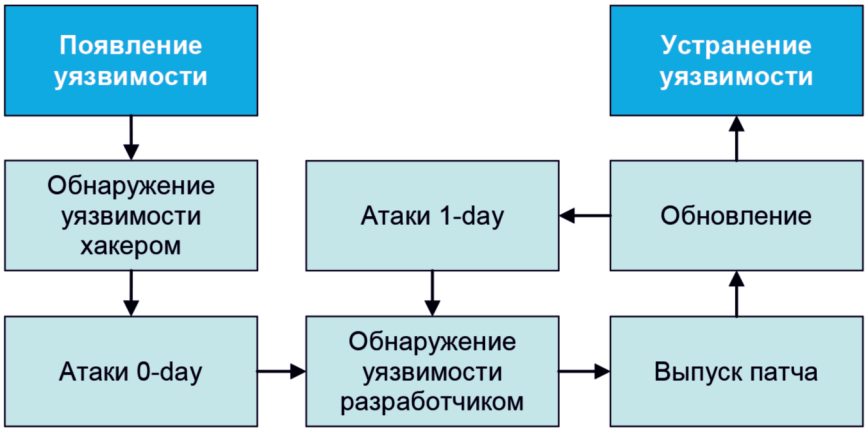

Рис. 3. ***Схема жизненного цикла уязвимости «нулевого дня»***

Однако, данные допущения справедливы лишь для фон Неймановских компьютерных систем. Квантовые компьютеры, в отличие от

классических, оперируют состояниями кубитов $|\Psi\rangle$ на комплексной плоскости, при этом состояния кубитов $|0\rangle$ и $|1\rangle$ соответствуют значениям бит 0 и 1. Квантовый компьютер, состоящий из N кубитов, способен оперировать 2^N квантовыми состояниями одновременно, в то время как классический компьютер одномоментно обрабатывает лишь одно состояние. 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.

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	$\begin{pmatrix} 0 & -i \\ 1 & 0 \end{pmatrix}$
Вентиль Паули Z	Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Вентиль Адамара	H	$\frac{1}{\sqrt{1}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Фазовый сдвиг $\pi/4$	S	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
Фазовый сдвиг $\pi/8$	T	$\begin{pmatrix} 1 & 0 \\ 0 & e^{in/4} \end{pmatrix}$
Многокубитные вентили		
Вентиль CNOT	$CNOT$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
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	$SWAP$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

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: $\{0,1\}^n \to \{0,1\}$ – постоянному или сбалансированному [32]. 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: $|x, y\rangle \to |x, y \oplus f(x)\rangle$. Вычисление начинается с $n + 1$ кубитами в состоянии $|\psi_0\rangle = |0\rangle^{\oplus n} \otimes |1\rangle$, после чего к n входным кубитам применяется преобразование Адамара, приводя их в состояние суперпозиции

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \sum_{x=0}^{2^n-1} |x\rangle \oplus |1\rangle.$$

После этого вновь применяется квантовый оракул U_f, возвращая

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \oplus |1\rangle.$$

На последнем шаге к входным кубитам вновь применяется преобразование Адамара и осуществляется измерение состояние кубитов. Если при измерении все значения кубитов оказались равными 0, то функция $f(x)$ является постоянной (константной), иначе – сбалансированной.

Квантовый алгоритм Шора применяется при решении задачи факторизации целого числа N на простые сомножители p и q так, что $N = p \times q$ [33]. Алгоритм состоит из двух основных шагов. На первом шаге к n входным кубитам в состоянии

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

применяется квантовое преобразование Фурье. На втором этапе на основе результата преобразования осуществляется 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 $O(\log^2 N \log\log N \log\log N)$ или в терминах длины $n = \log N$ числа N в битах – как $O(n^2 \log n \log\log n)$ [34]. Важно учитывать это свойство алгоритма Шора, поскольку значительная часть существующих криптосистем с открытым ключом, таких как криптосистема Эль-Гамаля, RSA, Диффи-Хеллмана и криптосистемы на основе эллиптических кривых, опираются на допущения о сложности дискретного логарифмирования.

Квантовый алгоритм Гровера применяется для эффективного решения задачи поиска элемента в неупорядоченном множестве. Математически это можно записать в виде функции $f: \{0,1\}^n \to \{0,1\}$, сопоставляющей $N = 2^n$ элементам значение 0 или 1, при этом алгоритм Гровера решает задачу поиска x, такого, что $f(x) = 1$. Вычисление начинается с n кубитами в состоянии

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

Далее повторяются шаги: (1) применение квантового оракула U_f, определяющего состояния, удовлетворяющие условию $f(x) = 1$; (2) применение оператора диффузии Гровера D. Количество повторений шагов оценочно составляет $\pi/4\sqrt{N}$, после чего выполняется измерение состояния кубитов с нахождением значения x. Временная сложность решения задачи в 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, что представляет угрозу для блокчейн-платформ, поскольку многие алгоритмы консенсуса зависят от решения NP-полных задач.

Таким образом, 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	$O(N^{1/3})$
Алгоритм квадратичного решета	$O\left(e(1+0(1))^{\sqrt{\log n \log\log n}}\right)$
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	$O(c^{\ln p^{1/3}})$
Алгоритм COS	$O\left(e^{(\log p \log\log p)^{1/2}}\right)$
Алгоритм решета числового поля	$O(n \log n \log N)$
Алгоритм Шора	$O(\log^3 N)$

Квантовые угрозы безопасности блокчейн

Блокчейн-платформы представляют собой многоуровневые иерархические системы. Каждый из уровней может становиться объектом ИТВ по причине наличия в нем уязвимостей. Стратифицированное представление блокчейн-платформ по уровням возникновения уязвимостей, эксплуатируемых в ходе осуществления атак, представлено на рис. 4.

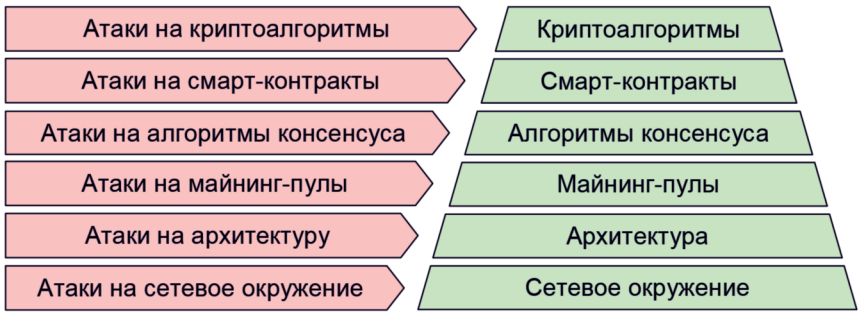

Рис. 4. ***Стратификация блокчейн-платформ по уровням возникновения эксплуатируемых уязвимости***

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

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

относительно n при известных значениях S и ,T где S, T – 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 временную сложность данной задачи к полиномиальной, оцениваемой как $O(\log^3 n)$. Это может позволить злоумышленнику, имеющему квантовый вычислитель и открытый ключ, отыскать соответствующий ему закрытый ключ из ключевой пары и осуществить атаку подмены личности [1–24, 35–41, 56–80].

Другим примером уязвимостей криптографических алгоритмов является недостаточная криптостойкость применяемых в блокчейн-платформах хэш-функций, таких как 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 [1–12, 28–51, 53–80].

Уязвимости смарт-контрактов. Смарт-контракты, используемые в таких блокчейн-платформах как Ethereum, считаются одним из самых уязвимых элементов блокчейн [37, 38]. 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.

Уязвимости майнинг-пулов. Вычислительная сложность майнинга в современных блокчейн-платформах, таких как 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.

Уязвимости архитектуры. К архитектурным недостаткам блокчейн-систем можно отнести недостатки, связанные с некорректной идентификацией узлов, перезапуском системы, отсутствием ограничений размеров блока. 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.

Учитывая рассмотренные уязвимости, сформируем перечень актуальных угроз устойчивости блокчейн-экосистем и платформ КИИ РФ, как показано в табл. 4, где символы «+» и «–» означают, что данная уязвимость соответственно может или не может эксплуатироваться при атаке на определенный уровень блокчейн-платформы.

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	–	+	–	–	+	–

Вероятные нарушители

Большинство кибератак на российские информационные ресурсы осуществляется с территорий иностранных государств, что подразумевает наличие удаленного доступа к элементам КИИ РФ и сетевой вектор воздействия [1, 4–21, 28–45, 51–78]. Значимую угрозу представляют нарушители, обладающие высоким потенциалом, в распоряжении которых имеются достаточные ресурсы для подготовки и осуществления ИТВ с использованием средств эксплуатации известных и ранее неизвестных уязвимостей блокчейн-экосистем и платформ. Таким образом, к вероятным нарушителям устойчивости функционирования блокчейн-экосистем и платформ КИИ РФ можно отнести:

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

Моделирование ИТВ на блокчейн-экосистемы с помощью сетей Петри

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

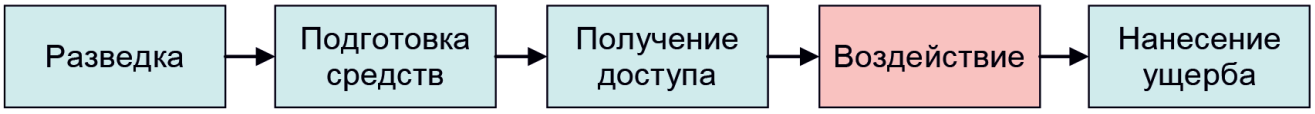

Рис. 5. ***Обобщенная схема ИТВ на типовую блокчейн-платформу КИИ РФ***

Область настоящего исследования ограничивается этапом непосредственного воздействия на целевую систему. Рассмотрим примеры ИТВ на типовые блокчейн-платформы.

Атака 51 %. Данная атака характерна для блокчейн-платформ, использующих алгоритмы консенсуса типа PoW, PoS, DPoS. Атака предполагает наличие у злоумышленника вычислительной мощности, составляющей 51 % или более от общей вычислительной мощности блокчейн-платформы. Данное 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 нужными 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. 6.

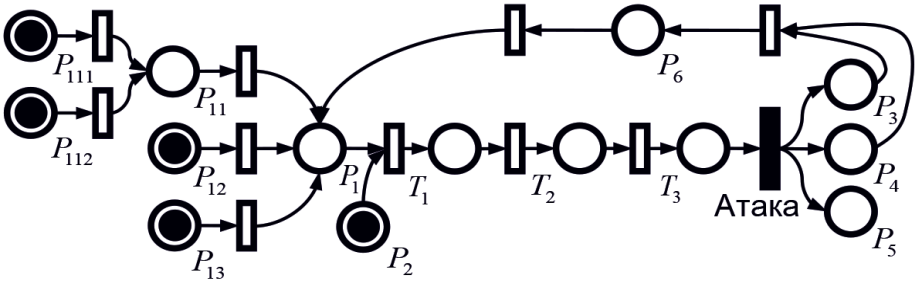

Рис. 6. ***Модель сети Петри для атаки 51 %***

Атака двойного расходования. На примере криптовалют, одной из основных задач алгоритмов консенсуса является обеспечение невозможности дублирования и повторного расходования уже потраченных средств. Так, если $B_0, \ldots, B_i, \ldots, B_N$ – существующая цепочка блоков, и целью злоумышленника является повторное расходование средств, запись о котором содержится 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', $j = \overline{i, n+1}$ с соответствующими хэш-суммами, где – длина существующей цепочки блоков. Классическими вычислительными средствами данная атака практически нереализуема, 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'_j, $j = \overline{i, n+1}$, 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. 7.

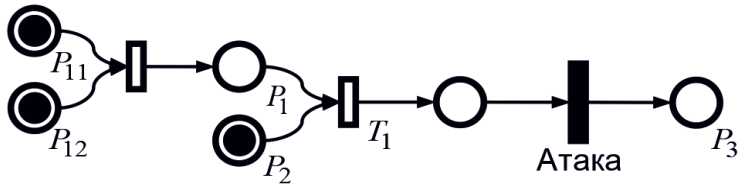

Рис. 7. ***Модель сети Петри для атаки двойного расходования***

Атака подмены личности. Известно, что правом владения цифровых активов в блокчейн наделены обладатели закрытого ключа, а с помощью открытого ключа из ключевой пары это право возможно проверить. Для данной атаки злоумышленнику необходимо по известному открытому ключу восстановить закрытый ключ, что достижимо несколькими способами:

● 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. 8.

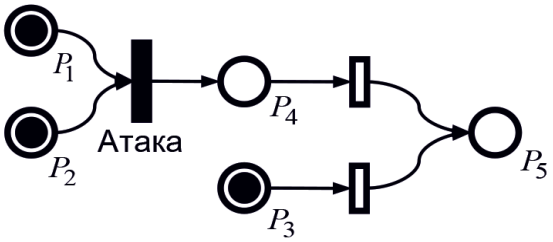

Рис. 7. ***Модель сети Петри для атаки двойного расходования***

Оценка киберустойчивости блокчейн-экосистем

Под устойчивостью технической системы понимают ее способность сохранять значения параметров своего функционирования в заданных пределах в условиях дестабилизирующих воздействий [1–24, 42–80]. Применительно к блокчейн-экосистемам и платформам КИИ РФ дестабилизирующими воздействиями являются ИТВ, в том числе с применением квантовых вычислительных средств. Проводя аналогию с динамическими системами, будем оценивать устойчивость функционирования блокчейн-платформ КИИ РФ в условиях ИТВ на примере типовой платформы по показателю вероятности P нахождения невосстанавливаемой системы в работоспособном состоянии в течение заданного времени t [80]:

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

где λ – интенсивность потока ИТВ.

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:

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

Результаты оценки устойчивости функционирования блокчейн-платформ КИИ РФ в условиях ИТВ на примере типовой блокчейн-платформы по показателю вероятности нахождения системы в работоспособном состоянии в зависимости от времени при различных значениях $P_{иск}$ представлены на рис. 9.

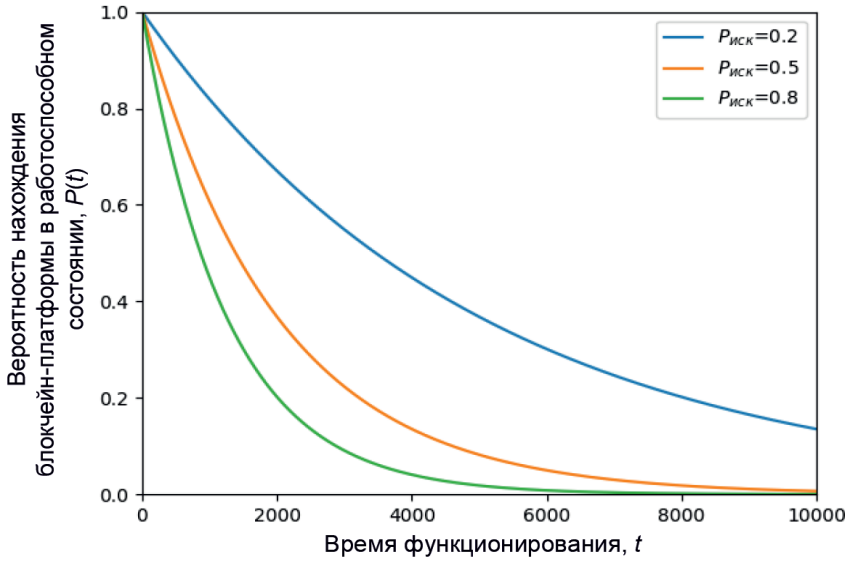

Рис. 9. ***Результаты оценки киберустойчивости блокчейн-платформы КИИ РФ в условиях ИТВ***

В условиях ИТВ 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 выдвинутую гипотезу исследования о снижении устойчивости функционирования блокчейн-экосистем и платформ КИИ РФ в условиях целенаправленных ИТВ.

Выводы

В настоящем исследовании была поставлена задача разработки модели новых квантовых угроз безопасности информации и количественной оценки киберустойчивости функционирования блокчейн-экосистем и платформ КИИ РФ в условиях ИТВ на примере типовой блокчейн-платформы.

Для выполнения поставленной задачи был решен ряд частных научных задач. Дано формализованное описание источников угроз устойчивости и ИТВ для блокчейн-платформ КИИ РФ. Сформирован перечень актуальных угроз и нарушителей устойчивости. Определены показатель, метрика и мера устойчивости, проведена количественная оценки устойчивости функционирования блокчейн-платформ КИИ РФ в условиях ИТВ на примере типовой блокчейн-платформы по показателю вероятности нахождения системы в работоспособном состоянии в течение заданного времени $P(t)$.

Результаты эксперимента показали, что в условиях целенаправленных ИТВ устойчивость блокчейн-платформ КИИ РФ снижается, что позволило подтвердить гипотезу исследования. Таким образом, все поставленные задачи были выполнены, а цель исследования – достигнута. В дальнейшем результаты настоящего исследования могут быть обобщены на другие экосистемы и платформы критической информационной инфраструктуры РФ.

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. Алексей Петренко, «Квантово-устойчивый блокчейн» (научная монография)/ А.С. Петренко. – Санкт-Петербург: Изд. Питер, 2022. - 384 с.

2. Балябин, А. А. Модель угроз безопасности и киберустойчивости облачных платформ КИИ РФ / А. А. Балябин, С. А. Петренко, А. Д. Костюков // Защита информации. Инсайд. – 2024. – № 5(119). – С. 26–34.

3. Балябин, А. А. Модель облачной платформы КИИ РФ с киберриммунитетом в условиях информационно-технических воздействий / А. А. Балябин // Защита информации. Инсайд. – 2024. – № 5(119). – С. 35–44.

4. Боев С.Ф., Петренко А.С., Петренко С.А., Ступин Д.Д. Квантовый криптоанализ криптосхем блокчейн-платформ. В сборнике: Многопроцессорные вычислительные и управляющие системы (МВУС-2022). Сборник материалов Всероссийской научно-технической конференции (Таганрог, 27–30 июня 2022 г.). Отв. редактор Академик И.А. Каляев, Южный федеральный университет. – Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2022. – С. 12–20.

5. Гончаренко, В. А. Модели и методы оценивания устойчивости критически важных информационных систем к информационно-техническим воздействиям / В. А. Гончаренко, С. И. Фомин, О. В. Суржанов // Современные тенденции в образовании и науке : сборник научных трудов по материалам Международной научно-практической конференции: в 10 частях, Тамбов, 28 декабря 2012 года. Том Часть 3. – Тамбов: ООО «Консалтинговая компания Юком», 2013. – С. 49–50.

6. Петренко, А. С. Оценка квантовой угрозы для современных блокчейн-систем / А. С. Петренко, С. А. Петренко // Информационные системы и технологии в моделировании и управлении : Сборник трудов VII Международной научно-практической конференции Отв. редактор К. А. Маковейчук , Ялта, 24–25 мая 2023 года. – Симферополь: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2023. – С. 171–173.

7. Петренко, А. С. Анализ современного состояния исследований проблемы квантовой устойчивости блокчейна. Часть 1 / А. С. Петренко, А. Г. Ломако, С. А. Петренко // Защита информации. Инсайд. – 2023. – № 3(111). – С. 38–46.

8. Петренко А.С., Петренко С.А., Костюков А.Д. Эталонная модель блокчейн-платформы. Журнал «Защита информации. Инсайд». 2022. № 4 (106). с. 34–44.

9. Петренко А.С., Петренко С.А., Костюков А.Д., Ожиганова М.И. Модель квантовых угроз безопасности для современных блокчейн-платформ. Журнал «Защита информации. Инсайд». 2022. № 3 (105). с. 10–20.

10. Петренко А.С., Петренко С.А., Костюков А.Д. Угрозы безопасности децентрализованным блокчейн-приложениям. Журнал «Защита информации. Инсайд». 2022. № 5 (107). с. 28–39.

11. Дубровин, А. С. Информационно-технические воздействия в автоматизированных системах специального назначения / А. С. Дубровин, Т. В. Мещерякова, В. И. Арутюнова // Вестник Воронежского института высоких технологий. – 2018. – № 3(26). – С. 28–33.

12. Зубарев, И. В. Основные угрозы безопасности информации в виртуальных средах и облачных платформах / И. В. Зубарев, П. К. Радин // Вопросы кибербезопасности. – 2014. – № 2(3). – С. 40–45.

13. Марков А.С. Важная веха в безопасности открытого программного обеспечения. Вопросы кибербезопасности. 2023, № 1(53), с. 2–12. DOI: http://dx.doi.org/10.21681/2311-3456-2023-1-2-12.

14. Максимова, Е. А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры / Е. А. Максимова // Труды учебных заведений связи. – 2020. – Т. 6, № 4. – С. 91-103. – DOI 10.31854/1813-324X-2020-6-4-91-103.

15. Молдовян А.А., Молдовян Н.А. Новые формы скрытой задачи дискретного логарифмирования. Труды СПИИРАН 2019. № 2(18). Стр. 504-529. doi: 10.15622/sp.18.2.504-529.

16. Молдовян Н.А., Введение в криптосистемы с открытым ключом /Молдовян Н.А., Молдовян А.А./, Изд. БХВ-Петербург, 2005, 286 с. – 2005.

17. Петренко А.С., Петренко С.А. Методика оценки квантовой устойчивости современных блокчейн-платформ. Методы и технические средства обеспечения безопасности информации. 2022. № 31. с. 167–169.

18. Петренко А.С., Петренко С.А. Метод оценивания квантовой устойчивости блокчейн-платформ. Журнал «Вопросы кибербезопасности». 2022. № 3 (49). с. 2–22.

19. Фоменко, К. Э. Подход к определению устойчивости функционирования элементов критической инфраструктуры в условиях компьютерных атак / К. Э. Фоменко, Т. Р. Сабиров, Д. Н. Бирюков // Методы и технические средства обеспечения безопасности информации. – 2019. – № 28. – С. 4–7.

20. Петренко А.С., Петренко С.А., Маковейчук Ян.Т. О создании квантово-устойчивых блокчейн-платформ. В сборнике: Повышение конкурентоспособности социально-экономических систем в условиях трансграничного сотрудничества регионов. Сборник материалов IX международной научно-практической конференции. Отв. редактор А.В. Олифиров. Симферополь, 2022. с. 139–142.

21. Петренко А.С., Петренко С.А., Антонова-Дружинина А.О., Ожиганова М.И. Метод параметрического выбора криптопримитивов для квантово-устойчивой блокчейн-платформы. Часть I. Журнал «Защита информации. Инсайд». 2022. № 4 (106). с. 24–33.

22. Петренко А.С., Петренко С.А., Антонова-Дружинина А.О., Ожиганова М.И. Метод параметрического выбора криптопримитивов для квантово-устойчивой блокчейн-платформы. Часть II. Журнал «Защита информации. Инсайд». 2022. № 5 (107). с. 20–27.

23. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов ассиметричного шифрования на основе криптосистемы «Classic McEliece». Свидетельство о регистрации программы для ЭВМ 2022668621, 10.10.2022. Заявка № 2022667670 от 30.09.2022.

24. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов ассиметричного шифрования на основе криптосистемы «CRYSTALS-Kyber». Свидетельство о регистрации программы для ЭВМ 2022668823, 12.10.2022. Заявка № 2022667709 от 30.09.2022.

25. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов ассиметричного шифрования на основе криптосистемы «NTRU». Свидетельство о регистрации программы для ЭВМ 2022668923, 13.10.2022. Заявка № 2022667716 от 30.09.2022.

26. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов ассиметричного шифрования на основе криптосистемы «Saber». Свидетельство о регистрации программы для ЭВМ 2022669031, 14.10.2022. Заявка № 2022667752 от 30.09.2022.

27. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов цифровой подписи на основе криптосистемы «CRYSTALS-Dilithium». Свидетельство о регистрации программы для ЭВМ 2022668253, 04.10.2022. Заявка № 2022667777 от 30.09.2022.

28. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов цифровой подписи на основе криптосистемы «Falcon». Свидетельство о регистрации программы для ЭВМ 2022669033, 14.10.2022. Заявка № 2022667701 от 30.09.2022.

29. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов цифровой подписи на основе криптосистемы «Rainbow». Свидетельство о регистрации программы для ЭВМ 2022668622, 10.10.2022. Заявка № 2022667676 от 30.09.2022.

30. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов ассиметричного шифрования на основе криптосистемы «BIKE». Свидетельство о регистрации программы для ЭВМ 2022669035, 14.10.2022. Заявка № 2022667755 от 30.09.2022.

31. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов ассиметричного шифрования на основе криптосистемы «FrodoKEM». Свидетельство о регистрации программы для ЭВМ 2022668803, 12.10.2022. Заявка № 2022667707 от 30.09.2022.

32. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов ассиметричного шифрования на основе криптосистемы «HQC». Свидетельство о регистрации программы для ЭВМ 2022610610, 10.10.2022. Заявка № 2021680315 от 30.09.2022.

33. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов ассиметричного шифрования на основе криптосистемы «NTRU Prime». Свидетельство о регистрации программы для ЭВМ 2022668555, 10.10.2022. Заявка № 2022667780 от 30.09.2022.

34. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов ассиметричного шифрования на основе криптосистемы «SIKE». Свидетельство о регистрации программы для ЭВМ 2022668699, 11.10.2022. Заявка № 2022667675 от 30.09.2022.

35. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов цифровой подписи на основе криптосистемы «SPHINCS+». Свидетельство о регистрации программы для ЭВМ 2022669011, 14.10.2022. Заявка № 2022667703 от 30.09.2022.

36. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов цифровой подписи на основе криптосистемы «Picnic». Свидетельство о регистрации программы для ЭВМ 2022668556, 10.10.2022. Заявка № 2022667692 от 30.09.2022.

37. Петренко А.С. и др. Набор инструментов разработки (SDK) постквантовых алгоритмов цифровой подписи на основе криптосистемы «GeMSS». Свидетельство о регистрации программы для ЭВМ 2022668625, 10.10.2022. Заявка № № 2022667681 от 30.09.2022.

38. Петренко А.С. и др. Программа для управления базой данных кибериммунитетов и знаний иммунной системы защиты гиперконвергентных цифровых платформ. Свидетельство о регистрации программы для ЭВМ 2022610610, 13.01.2022. Заявка № 2021680315 от 13.12.2021.

39. Петренко С. А. Кибериммунология: научная монография / Петренко С. А. – СПб: «Издательский Дом «Афина». 2021. 240 с.

40. Сергей Петренко, Киберустойчивость цифровой экономики. Научно-популярная монография/ – СПб.: Изд. Питер, 2021. – 384 с.: ил. ISBN 978-5-4461-1763-5.

41. Сергей Петренко, Киберустойчивость Индустрии 4.0: научная монография / «Издательский Дом «Афина», 2020. – 256 с. ISBN 978-5-9909868-7-9.

42. Сергей Петренко, Дмитрий Ступин. Национальная система раннего предупреждения о компьютерном нападении: научная монография / под редакцией С. Ф. Боева. «Издательский Дом «Афина», 2018. – 440 с.

43. Alexei Petrenko, Applied Quantum Cryptanalysis (научная монография «Прикладной квантовый криптоанализ»), ISBN: 9788770227933, e-ISBN: 9788770227926, River Publishers, 2022. – 256 pp. (SCOPUS) https://www.riverpublishers.com/book_details.php?book_id=1028

44. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, «SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies», in 2015 IEEE Symposium on Security and Privacy, 2015, pp. 104–121. doi: 10.1109/SP.2015.14.

45. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, «Hawk: The blockchain model of cryptography and privacy-preserving smart contracts», in 2016 IEEE Symposium on Security and Privacy (SP), 2016, pp. 839–858. doi: 10.1109/SP.2016.55.

46. M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, «Applications of blockchains in the internet of things: A comprehensive survey», IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1676–1717, 2019. doi:10.1109/COMST.2018.2886932.

47. F. S. Hardwick, A. Gioulis, R. Naeem Akram, and K. Markantonakis, «E-voting with blockchain: An E-Voting protocol with decentralization and voter privacy», in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1561–1567. doi: 10.1109/Cybermatics_2018.2018.00262.

48. 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, Proceedings. Editors: Mazzara, M., Bruel, J.-M., Meyer, B., Petrenko, A. (Eds.). 420 p. DOI: 10.1007/978-3-030-29852-4.

49. Petrenko A.S., Petrenko S.A., Taran V.N. Universal quantum gate as a tool for modeling quantum cryptanalysis algorithms on a quantum circuit. В сборнике: CEUR Workshop Proceedings. Сер. «AISMA 2021 – Proceedings of the International Workshop on Advanced in Information Security Management and Applications» 2022. с. 143–150.

50. Sergei Petrenko, Developing an Enterprise Continuity Program (научная монография: Разработка корпоративной программы непрерывности бизнеса, ©2021 River Publishers, River Publishers Series in Information Science and Technology. ISBN: 9788770223973, e-ISBN: 9788770223966, 496 p., Developing an Enterprise Continuity Program (riverpublishers.com) (Scopus).

51. Sergei Petrenko, Developing a Cybersecurity Immune System for Industry 4.0 (научная монография: Разработка иммунной системы защиты Индустрии 4.0.), ©2020 River Publishers, River Publishers Series in Security and Digital Forensics. ISBN: 9788770221887, e-ISBN: 9788770221870, 386 p., https://www.riverpublishers.com/book_details.php?book_id=764 (Scopus).

52. Sergei Petrenko. Cyber Resilience (научная монография: Киберустойчивость Индустрии 4.0.), ISBN: 978-87-7022-11-60 (Hardback) and 877-022-11-62 (Ebook) © 2019 River Publishers, River Publishers Series in Security and Digital Forensics, 1st ed. 2019, 492 p. 207 illus. (Scopus).

53. Sergei Petrenko. LA ADMINISTRACIyN DE LA CIBERSEGURIDAD. INDUSTRIA 4.0. (научная монография: Управление кибербезопасностью Индустрии 4.0.). Publicado segъn la decisiyn del consejo de redacciyn de la Universidad de Innopolis (Acta n.є 7 del 9 de mayo de 2017). Este trabajo ha recibido las siguientes subvenciones: concesiyn de RFBR (n.є 16-29-04268 de la oficina), concesiyn del presidente de la Federaciyn Rusa (NS-6831.2016.8) / Universidad de Oviedo, Universidad de Innopolis. Oviedo, Asturias, 1st ed. 2019, 276 p. 142 illus. (Scopus).

54. Sergei Petrenko. Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation (научная монография: Технологии обработки больших данных для мониторинга компьютерной безопасности), ISBN 978-3-319-79035-0 and ISBN 978-3-319-79036-7 (eBook), https://doi.org/10.1007/978-3-319-79036-7 © 2018 Springer Nature Switzerland AG, part of Springer Nature, 1st ed. 2018, XXVII, 249 p. 93 illus. (Scopus).

55. Sergei Petrenko. Cyber Security Innovation for the Digital Economy: A Case Study of the Russian Federation (научная монография: Инновационные технологии кибербезопасности для цифровой экономики), ISBN: 978-87-7022-022-4 (Hardback) and 978-87-7022-021-7 (Ebook) © 2018 River Publishers, River Publishers Series in Security and Digital Forensics, 1st ed. 2018, 490 p. 198 illus. (Scopus).

56. Sergei Petrenko [0000-0003-0644-1731] and Elvira Khismatullina [0000-0002-8765-1097]. 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, Proceedings. Editors: Mazzara, M., Bruel, J.-M., Meyer, B., Petrenko, A. (Eds.), eBook ISBN 978-3-030-29852-4, DOI 10.1007/978-3-030-29852-4, Softcover ISBN 978-3-030-29851-7, 420 p. (https://www.springer.com/gp/book/9783030298517). (Scopus).

57. Sergei Petrenko [0000-0003-0644-1731] and Elvira Khismatullina [0000-0002-8765-1097]. Method of improving the Cyber Resilience for Industry 4.0. Digital platforms. Software Technology: Methods and Tools, 51st International Conference, TOOLS 2019, Innopolis, Russia, October 15–17, 2019, Proceedings. Editors: Mazzara, M., Bruel, J.-M., Meyer, B., Petrenko, A. (Eds.), eBook ISBN 978-3-030-29852-4, DOI 10.1007/978-3-030-29852-4, Softcover ISBN 978-3-030-29851-7, 420 p.(https://www.springer.com/gp/book/9783030298517). (Scopus) № 4 (12). – С. 2–22.

58. T. M. Fernandez-Carames and P. Fraga-Lamas, «Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks», IEEE Access, vol. 8, pp. 21 091–21 116, 2020. doi: 10.1109/ACCESS.2020.2968985.

59. Z. Yang, T. Salman, R. Jain, and R. D. Pietro, «Decentralization using quantum blockchain: A theoretical analysis», IEEE Trans. on Quantum Engineering, vol. 3, pp. 1–16, 2022. doi: 10.1109/TQE.2022.3207111.

60. J. M. Jose and P. V, «A survey on consensus algorithms in blockchain based on post quantum cryptosystems», in 2022 5th International Conference on Computational Intelligence and Networks (CINE), 2022, pp. 1–6. doi: 10.1109/CINE56307.2022.10037353.

61. T. Srivastava, B. Bhushan, S. Bhatt, and A. K. M. B. Haque, Integration of Quantum Computing and Blockchain Technology: A Cryptographic Perspective. Springer Singapore, 2022, pp. 197–228. doi: 10.1007/978-981-19-0924-5_12.

62. B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami and M. Ayaz, «A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies», in IEEE Access, vol. 9, pp. 57792-57807, 2021, doi: 10.1109/ACCESS.2021.3073203.

63. Mishra, P., Pilli, E.S., & Joshi, R.C. (2021). Cloud Security: Attacks, Techniques, Tools, and Challenges (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781003004486.

64. Petrenko S. Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation. Cham, Switzerland: Springer International Publishing, 2018. 249 p. DOI: 10.1007/978-3-319-79036-7.

65. M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, «Blockchain consensus algorithms: A survey», arXiv preprint arXiv:2001.07091, 2020.

66. J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, «A survey of blockchain technology applied to smart cities: Research issues and challenges», IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2794–2830, 2019. doi: 10.1109/COMST.2019.2899617.

67. C. A. Petri, «Communication with automata», 1966.

68. J. P. McDermott, «Attack net penetration testing», in Proceedings of the 2000 workshop on New security paradigms, 2001, pp. 15–21. doi: 10.1145/366173.366183.

69. Petrenko S. Cyber Resilience / S. Petrenko. Denmark (Gistrup): River Publishers, 2019. – 444 p.

70. Shor P. Algorithms for quantum computation: discrete logarithms and factoring [Text] /Shor P.// Foundations of Computer Science. – 1994. – № 10. – 134p.

71. D. Deutsch and R. Jozsa, «Rapid solution of problems by quantum computation», Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 439, no. 1907, pp. 553–558, 1992. doi: 10.1098/rspa.1992.0167.

72. P. Shor, «Algorithms for quantum computation: Discrete logarithms and factoring», in Proceedings of FOCS, 1994, pp. 124–134.

73. J. J. Kearney and C. A. Perez-Delgado, «Vulnerability of blockchain technologies to quantum attacks», Array, vol. 10, p. 100065, 2021. doi: 10.1016/j.array.2021.100065.

74. H. Mayer, «ECDSA security in bitcoin and ethereum: a research survey», CoinFaabrik, June, vol. 28, p. 126, 2016.

75. P. W. Shor, «Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer», SIAM review, vol. 41, no. 2, pp. 303–332, 1999. doi: 10.1137/S0036144598347011.

76. M. A. Shahriar 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.

77. N. Atzei, M. Bartoletti, and T. Cimoli, «A survey of attacks on Ethereum smart contracts (sok)», in International conference on principles of security and trust. Springer, 2017, pp. 164–186. doi: 10.1007/978-3-662-54455-6_8.

78. M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, «Quantum resource estimates for computing elliptic curve discrete logarithms», in International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2017, pp. 241–270. doi: 10.48550/arXiv.1706.06752.

79. S. Sayeed and H. Marco-Gisbert, «Assessing blockchain consensus and security mechanisms against the 51 % attack», Applied Sciences, vol. 9, no. 9, p. 1788, 2019. doi: 10.3390/app9091788.

80. Половко А. М. Основы теории надёжности. – М.: Наука, 1964. – 446с.