УДК 004.057.44:343.98

5.2.2. Математические, статистические и инструментальные методы экономики (физико-математические науки, экономические науки)

МАТЕМАТИЧЕСКИЕ ОСНОВЫ БЛОКЧЕЙН-ПРОТОКОЛОВ В ДЕЯТЕЛЬНОСТИ ОВД: ТЕОРЕТИЧЕСКИЕ МОДЕЛИ КОНСЕНСУСА, КРИПТОГРАФИЧЕСКИЕ ПРИМИТИВЫ И МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ СЛЕДСТВЕННОЙ ТАЙНЫ

Лаптев Владимир Николаевич
к.т.н., доцент
SPIN-код: 8905-8271
ФГБОУ ВО «Кубанский ГАУ им. И.Т. Трубилина», Краснодар, Россия

Жмурко Даниил Юрьевич
к.э.н., доцент
РИНЦ SPIN-код: 1543-2028

Хромых Анна Алексеевна
к.ф-м.н.

Назаров Артур Карапетович
к.ф-м.н.

Куминов Михаил Владимирович
ФГКОУ ВО «Краснодарский университет МВД России», Краснодар, Россия

В настоящем исследовании проводится комплексный анализ математического аппарата блокчейн-технологий в контексте цифровой трансформации правоохранительной деятельности. Работа базируется на интеграции теоретических моделей государственного управления, таких как ресурсный подход (RBV), единая теория принятия и использования технологий (UTAUT) и концепция технологического, организационного и экологического контекста (TOE). В центре внимания находятся формализованные описания протоколов консенсуса (PBFT, PoA, Raft), их классификация в рамках теоремы CAP и устойчивость к византийским ошибкам. Особое место уделено адаптации российских криптографических стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 для архитектур распределенных реестров, используемых в органах внутренних дел (ОВД). Исследуются математические свойства доказательств с нулевым разглашением (ZKP) и гомоморфного шифрования как инструментов обеспечения следственной тайны и защиты персональных данных. Предложена модель динамического управления сложностью майнинга

UDC 004.057.44:343.98

5.2.2. Mathematical, statistical and instrumental methods of economics (physical and mathematical sciences, economic sciences)

MATHEMATICAL FOUNDATIONS OF BLOCKCHAIN PROTOCOLS IN LAW ENFORCEMENT ACTIVITIES: THEORETICAL CONSENSUS MODELS, CRYPTOGRAPHIC PRIMITIVES, AND MECHANISMS FOR ENSURING INVESTIGATIVE CONFIDENTIALITY

Laptev Vladimir Nikolaevich
Cand.Tech.Sci., Associate professor
RSCI SPIN Code: 8905-8271
Federal State Budgetary Educational Institution of Higher Education "Kuban State Agrarian University named after I.T. Trubilin", Krasnodar, Russia

Zhmurko Daniil Yuryevich
Cand.Econ.Sci., Associate Professor
RSCI SPIN Code: 1543-2028

Khromykh Anna Alekseevna
Candidate in Physics and Mathematics

Nazarov Artur Karapetovich
Candidate in Physics and Mathematics

Kuminov Mikhail Vladimirovich
Krasnodar University of the Ministry of Internal Affairs of Russia, Krasnodar, Russia

This study presents a comprehensive analysis of the mathematical framework underlying blockchain technologies in the context of the digital transformation of law enforcement activities. The research is based on the integration of theoretical models of public administration, including the Resource-Based View (RBV), the Unified Theory of Acceptance and Use of Technology (UTAUT), and the Technology–Organization–Environment (TOE) framework. The focus is placed on formalized descriptions of consensus protocols (PBFT, PoA, Raft), their classification within the CAP theorem, and their resilience to Byzantine faults. Particular attention is given to the adaptation of Russian cryptographic standards GOST R 34.11-2012 and GOST R 34.10-2012 for distributed ledger architectures used by internal affairs bodies. The mathematical properties of zero-knowledge proofs (ZKP) and homomorphic encryption are examined as tools for ensuring investigative confidentiality and protecting personal data. A model of dynamic mining difficulty management for digital evidence management systems (DEMS) is proposed, based on information sensitivity levels

для систем хранения цифровых доказательств (DEMS) на основе уровней чувствительности информации

Ключевые слова: БЛОКЧЕЙН-ПРОТОКОЛЫ, ОРГАНЫ ВНУТРЕННИХ ДЕЛ, ЦИФРОВАЯ ТРАНСФОРМАЦИЯ, АЛГОРИТМЫ КОНСЕНСУСА, ГОСТ Р 34.11-2012, ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ, КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ, ЦИФРОВАЯ ФОРЕНЗИКА

Keywords: BLOCKCHAIN PROTOCOLS, LAW ENFORCEMENT AGENCIES, DIGITAL TRANSFORMATION, CONSENSUS ALGORITHMS, GOST R 34.11-2012, ZERO-KNOWLEDGE PROOFS, CRYPTOGRAPHIC DATA PROTECTION, DIGITAL FORENSICS

http://dx.doi.org/10.21515/1990-4665-216-017

Теоретические модели цифровой трансформации в государственном секторе и правоохранительной деятельности

Цифровая трансформация в государственном управлении представляет собой многогранный процесс, выходящий за рамки простого внедрения информационных систем. Она радикально перестраивает стратегические подходы к управлению данными и взаимодействию институтов власти. «В деятельности органов внутренних дел этот процесс сталкивается с уникальными вызовами: необходимостью обеспечения абсолютной целостности доказательной базы, защитой прав участников процесса и соблюдением строгих регуляторных требований» [1].

Для понимания механизмов внедрения блокчейна в ОВД целесообразно использовать интегративную модель, объединяющую три фундаментальные теоретические базы:

1. **Ресурсный подход (Resource-Based View, RBV)**. «Согласно этой модели, блокчейн рассматривается как стратегический актив, позволяющий трансформировать операционные возможности (эффективность процессов, безопасность системы) в стратегические преимущества (масштабируемость технологий, децентрализованное доверие)» [1]. В контексте ОВД это означает переход от статических методов верификации данных к динамическим процессам, где доверие обеспечивается алгоритмиче-

ски.

2. **Единая теория принятия и использования технологий (UTAUT)**. Данная модель объясняет намерения пользователей через такие факторы, как ожидаемая производительность и условия содействия. В правоохранительных органах ожидаемая производительность напрямую коррелирует с масштабируемостью и безопасностью блокчейн-сети, а условия содействия – с качеством организационного управления.
3. **Модель TOE (Technology-Organization-Environment)**. Она описывает технологический, организационный и экологический контексты, влияющие на внедрение инноваций. Технологический контекст включает возможности ИТ-инфраструктуры, организационный – стратегическое планирование и бюджетную поддержку, а экологический (внешний) – уровень осведомленности о конфиденциальности данных и правовое поле.

«Применение блокчейна позволяет перейти от централизованных моделей верификации, уязвимых перед «единой точкой отказа» и внутренними злоупотреблениями, к децентрализованным системам, где множество независимых узлов подтверждают легитимность транзакций. Это кардинально меняет ландшафт цифровых транзакций в государственном секторе, минимизируя проблемы доверия к центральным администраторам» [2].

Математическая формализация алгоритмов консенсуса в ведомственных сетях

Выбор механизма консенсуса является критическим решением при проектировании блокчейн-системы для ОВД. «В отличие от публичных сетей, где доминирует Proof-of-Work (PoW), для правоохранительных нужд наиболее применимы протоколы для частных (permissioned) сетей, где участники идентифицированы и обладают определенными правами доступа» [4].

Модель Practical byzantine fault tolerance (PBFT)

Алгоритм PBFT остается золотым стандартом для консорциумных блокчейнов, обеспечивая высокую пропускную способность и устойчивость к вредоносному поведению узлов. Математически доказано, что система может достичь консенсуса, если количество византийских (неисправных или злонамеренных) узлов f не превышает одной трети от общего числа узлов N:

$$N \geq 3f + 1$$

Это условие является оптимальным для обеспечения отказоустойчивости в распределенных системах. Протокол PBFT функционирует в три фазы:

1. *Pre-prepare* – лидер (primary) рассылает предложение о новом блоке всем узлам.
2. *Prepare* – узлы обмениваются сообщениями, подтверждая получение и корректность предложения.
3. *Commit* – узлы обмениваются подтверждениями готовности зафиксировать блок в реестре.

«С точки зрения теоремы CAP, PBFT является *CP-системой* (Consistency и Partition Tolerance), отдавая приоритет согласованности данных перед доступностью. Это означает, что при серьезном разделении сети система скорее остановится, чем допустит ветвление (форк) реестра, что критически важно для юридической чистоты следственных данных» [4].

Протоколы Proof-of-Authority (PoA): Aura и Clique

Алгоритмы семейства PoA полагаются на список доверенных «авторитетов» (authority nodes), которые по очереди создают блоки. В контексте ОВД такими авторитетами могут выступать региональные управления или серти-

фицированные криптографические узлы [6].

- *Aura (Authority Round)* – работает в два этапа: предложение блока лидером и подтверждение его большинством авторитетов. Временная шкала разбивается на шаги длительностью *step_duration*. Лидер *l* для текущего шага *s* вычисляется как:

$$s = t / step\_duration$$

$$l = s \ (mod \ N)$$

где *t* – системное время. Aura классифицируется как AP-система, что делает её уязвимой к форкам в условиях асинхронности сети Интернет.

- *Clique* – реализован в клиентах Ethereum (Geth). Он разрешает форки, используя протокол GHOST для выбора самой «тяжелой» цепочки. «В Clique частота создания блоков ограничена значением *1 / (N/2 + 1)*, что математически предотвращает захват сети меньшинством византийских узлов» [4].

Параметр сравнения	**PBFT**	**PoA (Aura)**	**PoA (Clique)**
Задержка (message rounds)	3 раунда	*2(N/2 + 1)*	1 раунд
Тип завершенности	Немедленная	Вероятностная	Вероятностная
Пропускная способность (TPS)	200–500	Более 1500	Более 1500
Масштабируемость	Ограничена (≤ 10 узлов)	Ограничена	Умеренная

Анализ показывает, что для систем, требующих строгой непротиворечивости данных (например, реестр оружия или оперативные учеты), PBFT является более предпочтительным, несмотря на задержки [4].

Гибридные и высокопроизводительные модели (Raft, QuickBFT)

Протокол **Raft** широко применяется в частных блокчейнах благодаря своей простоте и высокой эффективности. Он не является византийски отказоустойчивым (защищает только от сбоев типа crash faults), но его интеграция с PBFT позволяет создавать гибридные модели. Например, модель, предложенная Вангом (2024), использует децентрализованное голосование Raft для быстрого выбора лидера и PBFT для подтверждения данных в агрессивных средах [8].

В современных исследованиях также выделяется протокол **QuickBFT**, который сокращает четырёхэтапную коммуникацию до трёхэтапной на основе методов многокритериального принятия решений и нечётких множеств (Vague sets). «Это позволяет снизить задержку консенсуса на 20% при сохранении устойчивости к вредоносным узлам» [9].

Криптографические основы блокчейн-протоколов по стандартам России

Применение блокчейн-технологий в ОВД требует соответствия национальным стандартам криптографической защиты информации (СКЗИ). Основными примитивами здесь выступают хеш-функция «Стрибог» и алгоритм электронной подписи на эллиптических кривых.

Алгебраическая структура хеш-функции ГОСТ Р 34.11-2012 («Стрибог»)

«Стрибог» построен на итерационной конструкции Меркла-Дамгора. «Для обработки данных любой длины используется процедура дополнения до размера блока 512 бит вектором вида (00…01). В основе функции сжатия лежит схема Миягучи-Пренеля с внутренним блочным шифром XSPL» [10].

Математические трансформации внутри раунда шифра:

1. *X (XOR)* – сложение по модулю 2 с раундовым ключом.

2. *S (Substitution)* – нелинейное преобразование на основе *S*-блоков. «Алгебраическая сложность *S*-блока значительно эволюционировала: с 1304 операций в 2012 г. до 169–179 операций в 2024 г., что существенно повышает производительность программных реализаций в блокчейн-сетях» [12].
3. *P (Permutation)* – байтовая перестановка.
4. *L (Linear transformation)* – линейное преобразование, реализуемое как умножение вектора на матрицу Коши *A* над полем $GF(2^8)$. Свойства матрицы Коши обеспечивают максимальное лавинное расстояние между входными и выходными данными.

Эквивалентная формула вычисления функции сжатия h_{i+1}:

$$h_{i+1} = F(F(h_{i-1} \oplus i, m_i) \oplus \Delta_i, m_{i+1}) \oplus \Delta_{i+1} \oplus (i+2)$$

где $\Delta_i = i \oplus$(i+1) – дифференциальное представление счетчика блоков [12].

Формирование и проверка подписи по ГОСТ Р 34.10-2012

«Для обеспечения аутентичности транзакций в блокчейне используется электронная подпись на базе группы точек эллиптической кривой *E* над простым полем Z_p» [14].

Математические параметры подписи:

- *Инвариант кривой J(E)*: $J(E) = 1728 \frac{4a^3}{4a^3+27b^2} (mod\ p)$, где a, b – коэффициенты уравнения кривой $y^2 = x^3 + ax + b$ [15].
- *Ключи:* секретный ключ d – случайное целое число ($0 < d < q$, где q – порядок группы точек). Публичный ключ $Q = d \times P$, где P – генератор группы [15].

Алгоритм подписи:

1. Вычисление хеша сообщения $h = H(M)$. Определение целого числа $e = h \pmod q$ (если $e = 0$, то $e = 1$).
2. Генерация случайного числа k ($0 < k < q$) и вычисление точки $C = kP$.
3. Вычисление координаты $r = x_c \pmod q$. Если $r = 0$, выбор нового k.
4. Вычисление $s = (rd + ke) \pmod q$. Если $s = 0$, выбор нового k.
5. Результат – конкатенация векторов $(\bar{r}|\bar{s})$.

«Применение данных стандартов гарантирует устойчивость блокчейн-протоколов к современным методам криптоанализа и обеспечивает юридическую значимость записей в рамках правового поля России» [13].

Математические модели обеспечения конфиденциальности и следственной тайны

Одной из главных проблем использования блокчейна в ОВД является конфликт между прозрачностью распределённого реестра и необходимостью защиты оперативной информации. Решением выступают доказательства с нулевым разглашением (Zero-Knowledge Proofs, ZKP).

Формальные свойства ZKP

«ZKP позволяют «Проверяющему» (Prover) убедить «Верификатора» (Verifier) в истинности утверждения, не раскрывая само утверждение. Математически это описывается через три свойства» [17]:

1. *Полнота (completeness)* – для любого истинного утверждения x и свидетеля w существует доказательство π, такое что Верификатор примет его с вероятностью [1].
2. *Надежность (soundness)* – для любого ложного утверждения вероятность того, что мошенник-Проверяющий убедит Верификатора, очень мала.
3. *Обоснованность знаний (Knowledge Soundness)* – если Проверяющий

может убедить Верификатора, то он действительно обладает секретным свидетельством *w* (это свойство отличает SNARKs от обычных интерактивных доказательств) [17].

«Для блокчейнов ОВД наиболее актуальны **zk-SNARKs** (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge). Они обладают свойством краткости, что означает малый размер доказательства и экстремально быструю проверку, не зависящую от сложности доказываемого вычисления» [18].

Применение ZKP в защите следственной тайны

В процессе расследования ZKP может использоваться для:

- Подтверждения того, что сотрудник ОВД обладает правами доступа к материалам дела, не раскрывая его ФИО остальным узлам сети.
- Проверки алиби или соответствия возрастным критериям (KYC) без раскрытия персональных данных.
- Верификации того, что цифровое доказательство получено из законного источника, при сохранении анонимности информатора.

Существует также синергия между ZKP и *полностью гомоморфным шифрованием (FHE).* «Если ZKP позволяет проверить корректность выполнения функции, то FHE позволяет выполнять саму функцию над зашифрованными данными. Это открывает путь к «программируемой приватности», где многосторонние смарт-контракты обрабатывают конфиденциальные улики, не имея к ним прямого доступа в открытом виде» [23].

Управление цифровыми доказательствами в блокчейн-системах (DEMS)

«Цифровая форензика требует строгого соблюдения «цепи владения» (Chain of Custody). Исследования показывают, что до 80% судебных дел могут потерпеть неудачу из-за проблем с документированием перемещения улик» [25].

Математическая модель идентификации улик

Для каждой улики I (например, изображения) строится уникальный идентификатор ρ, основанный на анализе метаданных и контента. В базовой модели это сумма интенсивностей пикселей для изображения размером $\rho = \sum_{x=1}^{W} \sum_{y=1}^{H} I(x, y)$. Для обеспечения анонимности и неподдельности используется механизм «соленого» хеширования с рандомным вызовом ψ от верификатора:

$$X = H(HASH_{image} + \psi)$$

где $HASH_{image} = H(\rho)$, а H – алгоритм SHA-256 или ГОСТ Р 34.11-2012.22 значение X записывается в блок в качестве полезной нагрузки данных.

Модель динамической сложности майнинга

В ведомственных блокчейнах ОВД целесообразно использовать механизм динамической настройки сложности доказательства работы (Proof of Work) или времени подтверждения в зависимости от чувствительности данных S [22].

Классификация чувствительности данных:

- *Высокая (H)* – финансовые отчеты, показания защищенных свидетелей, видео с мест преступлений.
- *Средняя (M)* – внутренняя переписка (e-mail), логи аудита.
- *Низкая (L)* – публичные документы, справочники.

Математически сложность D (количество ведущих нулей в хеше блока) устанавливается функцией от типа файла и тегов дела:

$$\mathrm{D} = \begin{cases} 5, \text{если } S = H \\ 4, \text{если } \mathrm{S} = \mathrm{M} \\ 3, \text{если } \mathrm{S} = \mathrm{L} \end{cases}$$

«Это позволяет оптимизировать вычислительные ресурсы сети: критические данные защищаются максимальной мощностью майнинга, в то время как рядовые события обрабатываются быстрее» [22].

Поле блока B_i	**Описание**	**Формализм**
Block Number	Порядковый номер	B_n
Previous Hash	Хеш предка	H_{prev}
Data Payload	Полезная нагрузка данных	$X = H(HASH_{image} + \psi)$
Nonce	Переменная майнинга	N
Difficulty	Текущая сложность	D
New Hash	Результат майнинга	$H_{new} = H(B\_n, X, D, H_{prev}, N)$

Анализ безопасности и моделирование рисков

Внедрение блокчейна в ОВД не устраняет угрозы полностью, но переводит их в плоскость математической борьбы с атакующими.

Количественная оценка векторов атак

«Для оценки устойчивости системы используется фреймворк *BVQRF* (Blockchain Variable Quantitative Risk Framework), который интегрирует принципы NIST с количественным скорингом рисков» [26].

1. *Атака 51%*. В публичных сетях вероятность успеха, атакующего с долей хешрейта q при ожидании z подтверждений, описывается как:

$$P = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{K!}\left(1 - \left(\frac{q}{p}\right)^{z-k}\right)$$

где $\lambda = z(q/p)$, $p = 1-q$. «В частных сетях ОВД риск смещается от мощности к количеству скомпрометированных узлов-авторитетов (> 1/3 для PBFT)» [27].

2. *Атака Сивиллы (Sybil Attack)*. «Математически предотвращается через

механизмы идентификации участников и привязки прав к ведомственным сертификатам. В PoA-сетях атака Сивиллы невозможна, пока список авторитетов защищен» [26].

3. *Атака затмения (Eclipse Attack)*. «Атакующий берет под контроль коммуникации узла, заставляя его принимать ложные данные. Защита обеспечивается через детерминированный выбор пиров и использование зашифрованных каналов TLS 1.3 на базе ГОСТ» [15].

Сравнение с централизованными БД

Сравнительный анализ по модели *STRIDE* демонстрирует преимущества блокчейн-архитектуры для ОВД [29].

Угроза (STRIDE)	**Централизованная БД**	**Блокчейн в ОВД**
Подмена или спуфинг (Spoofing)	Риск подмены администратора	Идентификация по ГОСТ Р 34.10-2012
Изменение данных или модификация, искажение (Tampering)	Прямое изменение записей в БД	Математическая неизменность хеш-цепочки
Отказ от действий (Repudiation)	Сложность доказательства авторства	Криптографическая неотрекаемость действий
Разглашение информации или утечка (Inf. Disclosure)	Утечка всей базы при взломе	Сокрытие данных через ZKP и FHE
Отказ в обслуживании (DoS)	Единая точка отказа сервера	Децентрализованная устойчивость узлов
Повышение привилегий (Elev. of Privilege)	Уязвимость суперпользователя	Консенсус большинства участников

Заключение

Математические основы блокчейн-протоколов предоставляют органам внутренних дел беспрецедентные возможности для построения доверенной цифровой среды. Анализ формализованных моделей консенсуса показывает, что алгоритм PBFT в сочетании с российскими криптографическими стандартами «Стрибог» и ГОСТ Р 34.10-2012 обеспечивает необходимый баланс между безопасностью и целостностью данных.

Внедрение доказательств с нулевым разглашением (ZKP) эффективно разрешает противоречие между прозрачностью распределённого реестра и режимом следственной тайны. Предложенная модель динамического управления сложностью в системах DEMS позволяет гибко адаптировать инфраструктуру под различные категории уголовных дел. В долгосрочной перспективе синергия блокчейна и гомоморфного шифрования создаст фундамент для безопасного межведомственного анализа больших данных, минимизируя риски утечек и несанкционированного доступа. Таким образом, блокчейн становится не просто технологией хранения, а математическим гарантом справедливости и законности в цифровую эпоху.

Список литературы

1. Баранов П. П. Цифровая криминалистика и электронные доказательства // Криминалистика. – 2020. – № 12. – С. 19–27.

2. Бахтизин Р. Н. Доказательства с нулевым разглашением в распределённых реестрах // Информационная безопасность. – 2022. – № 1. – С. 9–17.

3. Бычков В. С. Цифровые доказательства и блокчейн-реестры // Уголовный процесс. – 2021. – № 9. – С. 48–55.

4. Горбачёв А. В., Кузнецов Д. А. Блокчейн-технологии в системах государственного управления // Информационное общество. – 2021. – № 4. – С. 34–41.

5. ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М. : Стандартинформ, 2012. – 42 с.

6. ГОСТ Р 34.11–2012. Информационная технология. Криптографическая защита информации. Функция хэширования. – Введ. 01.01.2013. – М. : Стандартинформ, 2013. – 35 с.

7. ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) операций. Защита

информации. – М. : Стандартинформ, 2018. – 64 с.

8. Карпов А. В., Мясников В. В. Криптографические методы защиты информации в распределённых системах // Проблемы информационной безопасности. – 2020. – № 3. – С. 15–23.

9. Лукьянов С. А. Математические модели консенсуса в ведомственных сетях // Информационные технологии. – 2023. – № 6. – С. 22–30.

10. Молдовян Н. А., Молдовян А. А. Криптография: от примитивов к протоколам. – СПб. : БХВ-Петербург, 2020. – 512 с.

11. Соловьёв И. Н. Применение распределённых реестров в правоохранительной деятельности // Вестник МВД России. – 2022. – № 2. – С. 56–63.

12. Федеральный закон РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи» (ред. действ.).

13. Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. действ.).

14. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. – М. : Диалектика, 2019. – 784 с.

15. Androulaki E. et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains // EuroSys. – 2018. – P. 1–15.

16. Antonopoulos A. Mastering Blockchain. – Sebastopol : O’Reilly Media, 2022. – 416 p.

17. Ben-Sasson E. et al. Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture // USENIX Security. – 2014. – P. 781–796.

18. Bonneau J. et al. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies // IEEE S&P. – 2015. – P. 104–121.

19. Cachin C. Architecture of the Hyperledger Blockchain Fabric // Workshop on Distributed Cryptocurrencies. – 2016. – P. 1–4.

20. Casey E. Digital Evidence and Computer Crime. – London : Academic Press, 2020. – 832 p.

21. Castro M., Liskov B. Practical Byzantine Fault Tolerance // OSDI. – 1999. – P. 173–186.

22. Conti M., Kumar S., Lal C., Ruj S. A Survey on Security and Privacy Issues of Blockchain // IEEE Communications Surveys. – 2018. – Vol. 20, № 4. – P. 3416–3452.

23. Gentry C. Fully Homomorphic Encryption Using Ideal Lattices // STOC. – 2009. – P. 169–178.

24. Goldwasser S., Micali S., Rackoff C. The Knowledge Complexity of Interactive Proof Systems // SIAM J. Comput. – 1989. – Vol. 18. – P. 186–208.

25. Katz J., Lindell Y. Introduction to Modern Cryptography. – Boca Raton : CRC Press, 2021. – 623 p.

26. Lamport L. The Byzantine Generals Problem // ACM Transactions on Programming Languages and Systems. – 1982. – Vol. 4, № 3. – P. 382–401.

27. Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. Bitcoin and Cryptocurrency Technologies. – Princeton : Princeton Univ. Press, 2016. – 336 p.

28. NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. – 2018.

29. Ongaro D., Ousterhout J. In Search of an Understandable Consensus Algorithm (Raft) // USENIX ATC. – 2014. – P. 305–319.

30. Vukolić M. The Quest for Scalable Blockchain Fabric // Open Problems in Net-

work Security. – 2016. – P. 112–125.

References

1. Baranov P. P. Cifrovaja kriminalistika i jelektronnye dokazatel'stva // Krimi-nalistika. – 2020. – № 12. – S. 19–27.
2. Bahtizin R. N. Dokazatel'stva s nulevym razglasheniem v raspredeljonnyh reestrah // Informacionnaja bezopasnost'. – 2022. – № 1. – S. 9–17.
3. Bychkov V. S. Cifrovye dokazatel'stva i blokchejn-reestry // Ugolovnyj process. – 2021. – № 9. – S. 48–55.
4. Gorbachjov A. V., Kuznecov D. A. Blokchejn-tehnologii v sistemah gosudarstvennogo upravlenija // Informacionnoe obshhestvo. – 2021. – № 4. – S. 34–41.
5. GOST R 34.10–2012. Informacionnaja tehnologija. Kriptograficheskaja zashhita informacii. Processy formirovanija i proverki jelektronnoj cifrovoj podpisi. – M. : Standartinform, 2012. – 42 s.
6. GOST R 34.11–2012. Informacionnaja tehnologija. Kriptograficheskaja zashhita informacii. Funkcija hjeshirovanija. – Vved. 01.01.2013. – M. : Standartinform, 2013. – 35 s.
7. GOST R 57580.1–2017. Bezopasnost' finansovyh (bankovskih) operacij. Zashhita informacii. – M. : Standartinform, 2018. – 64 s.
8. Karpov A. V., Mjasnikov V. V. Kriptograficheskie metody zashhity informacii v raspredeljonnyh sistemah // Problemy informacionnoj bezopasnosti. – 2020. – № 3. – S. 15–23.
9. Luk'janov S. A. Matematicheskie modeli konsensusa v vedomstvennyh setjah // Informacionnye tehnologii. – 2023. – № 6. – S. 22–30.
10. Moldovjan N. A., Moldovjan A. A. Kriptografija: ot primitivov k protokolam. – SPb. : BHV-Peterburg, 2020. – 512 s.
11. Solov'jov I. N. Primenenie raspredeljonnyh reestrov v pravoohranitel'noj dejatel'nosti // Vestnik MVD Rossii. – 2022. – № 2. – S. 56–63.
12. Federal'nyj zakon RF ot 06.04.2011 № 63-FZ «Ob jelektronnoj podpisi» (red. dejstv.).
13. Federal'nyj zakon RF ot 27.07.2006 № 149-FZ «Ob informacii, informacion-nyh tehnologijah i o zashhite informacii» (red. dejstv.).
14. Shnajer B. Prikladnaja kriptografija. Protokoly, algoritmy i ishodnye teksty na jazyke C. – M. : Dialektika, 2019. – 784 s.
15. Androulaki E. et al. Hyperledger Fabric: A Distributed Operating System for Permis-sioned Blockchains // EuroSys. – 2018. – P. 1–15.
16. Antonopoulos A. Mastering Blockchain. – Sebastopol : O'Reilly Media, 2022. – 416 p.
17. Ben-Sasson E. et al. Succinct Non-Interactive Zero Knowledge for a von Neumann Archi-tecture // USENIX Security. – 2014. – P. 781–796.
18. Bonneau J. et al. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocur-rencies // IEEE S&P. – 2015. – P. 104–121.
19. Cachin C. Architecture of the Hyperledger Blockchain Fabric // Workshop on Distributed Cryptocurrencies. – 2016. – P. 1–4.
20. Casey E. Digital Evidence and Computer Crime. – London : Academic Press, 2020. – 832 p.
21. Castro M., Liskov B. Practical Byzantine Fault Tolerance // OSDI. – 1999. – P. 173–186.

22. Conti M., Kumar S., Lal C., Ruj S. A Survey on Security and Privacy Issues of Block-chain // IEEE Communications Surveys. – 2018. – Vol. 20, № 4. – P. 3416–3452.
23. Gentry C. Fully Homomorphic Encryption Using Ideal Lattices // STOC. – 2009. – P. 169–178.
24. Goldwasser S., Micali S., Rackoff C. The Knowledge Complexity of Interactive Proof Systems // SIAM J. Comput. – 1989. – Vol. 18. – P. 186–208.
25. Katz J., Lindell Y. Introduction to Modern Cryptography. – Boca Raton : CRC Press, 2021. – 623 p.
26. Lamport L. The Byzantine Generals Problem // ACM Transactions on Programming Lan-guages and Systems. – 1982. – Vol. 4, № 3. – P. 382–401.
27. Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. Bitcoin and Cryptocurrency Technologies. – Princeton : Princeton Univ. Press, 2016. – 336 p.
28. NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. – 2018.
29. Ongaro D., Ousterhout J. In Search of an Understandable Consensus Algorithm (Raft) // USENIX ATC. – 2014. – P. 305–319.
30. Vukolić M. The Quest for Scalable Blockchain Fabric // Open Problems in Network Se-curity. – 2016. – P. 112–125.