УДК 004.056.5
DOI 10.33764/2618-981X-2025-6-129-138

А. И. Подлегаев[1]✉, В. В. Селифанов[1]

Аудит информационной безопасности в оптотехнических системах, созданных с использованием технологии квантового распределения ключей

[1]Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: sanyi.p@yandex.ru

Аннотация. В современном мире информационная безопасность становится одним из ключевых факторов, обеспечивающих устойчивость и надежность функционирования различных информационных систем. С развитием технологий передачи данных и ростом объемов обрабатываемой информации возрастает и сложность задач по защите конфиденциальности, целостности и доступности данных. В этом контексте квантовые технологии, в частности квантовое распределение ключей, открывают новые перспективы для создания практически неуязвимых систем защиты информации. Оптотехнические системы, использующие технологию квантового распределения ключей, представляют собой уникальное сочетание классических и квантовых компонентов, обеспечивающих высокий уровень безопасности передачи данных. Однако, несмотря на теоретическую защищенность, такие системы остаются уязвимыми к ряду специфических угроз, связанных с физическими особенностями квантовых каналов, аппаратными ограничениями и возможными атаками на классические элементы инфраструктуры. В связи с этим возникает необходимость проведения комплексного аудита информационной безопасности, позволяющего выявить потенциальные уязвимости и оценить эффективность существующих защитных мер. Актуальность исследования обусловлена растущей потребностью в надежной защите данных в условиях развития квантовых технологий и угроз, связанных с возможными атаками на квантовые каналы связи, основной проблемой является необходимость комплексной оценки их безопасности с учетом специфики квантовых протоколов и физических характеристик оборудования. Результаты исследования подтверждают высокую степень защищенности систем с квантовым распределением ключей, однако выявляют ряд факторов, влияющих на снижение уровня безопасности, таких как параметры оптических каналов и особенности реализации протоколов. Главный вывод состоит в том, что имитационное моделирование является эффективным инструментом для проведения аудита и оптимизации защиты квантово-оптических систем. Данная работа способствует развитию методологии оценки безопасности современных квантовых коммуникаций и может быть полезна для специалистов в области информационной безопасности и квантовой криптографии.

Ключевые слова: аудит, оценка защищенности, имитационное моделирование, оптотехнические системы, квантовое распределение ключей

A. I. Podlegaev[1]✉, V. V. Selifanov[1]

Information security audit in optotechnical systems created using quantum key distribution technology

[1]Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: sanyi.p@yandex.ru

Abstract. In the modern world, information security is becoming one of the key factors ensuring the stability and reliability of various information systems. With the development of data transmission technologies and the increasing volume of processed information, the complexity of tasks related to

protecting the confidentiality, integrity, and availability of data is also growing. In this context, quantum technologies, in particular quantum key distribution (QKD), open up new prospects for creating practically invulnerable information protection systems.
Optotechnical systems that use quantum key distribution technology represent a unique combination of classical and quantum components, providing a high level of data transmission security. However, despite their theoretical security, such systems remain vulnerable to a number of specific threats related to the physical characteristics of quantum channels, hardware limitations, and possible attacks on classical elements of the infrastructure. In this regard, it becomes necessary to conduct a comprehensive information security audit to identify potential vulnerabilities and assess the effectiveness of existing protective measures. The relevance of this research is driven by the growing need for reliable data protection amid the development of quantum technologies and threats associated with possible attacks on quantum communication channels. The main challenge is the necessity of a comprehensive security assessment, taking into account the specifics of quantum protocols and the physical characteristics of the equipment. The research results confirm the high level of security of QKD systems, but also reveal several factors that can reduce the level of protection, such as the parameters of optical channels and the specifics of protocol implementation. The main conclusion is that simulation modeling is an effective tool for auditing and optimizing the protection of quantum-optical systems. This work contributes to the development of methodologies for assessing the security of modern quantum communications and may be useful for specialists in information security and quantum cryptography.

Keywords: audit, security assessment, simulation modeling, optotechnical systems, quantum key distribution

Введение

Современные вызовы информационной безопасности требуют принципиально новых подходов к защите данных, особенно в условиях развития квантовых технологий. Квантовое распределение ключей (КРК), основанное на фундаментальных принципах квантовой механики, рассматривается как перспективное решение для создания неуязвимых систем передачи информации [1]. Протоколы типа BB84, предложенные еще в 1984 году, заложили основу для реализации ε-секретности, однако их практическое внедрение в оптотехнические системы выявило ряд проблем, связанных с аппаратными ограничениями и атаками на классические компоненты инфраструктуры [2].

Работы Науменко А.П. и Щербаченко А.А. [3] демонстрируют, что стойкость КРК-систем зависит не только от квантовых протоколов, но и от корректности реализации классических алгоритмов аутентификации. Исследования Positive Technologies [4] выявили уязвимости, связанные с генерацией псевдослучайных чисел и атаками на оптоволоконные линии, что требует интеграции квантовых генераторов случайности. При этом анализ уязвимостей протоколов BB84, SARG04 и E91 указывает на необходимость совершенствования методов обнаружения атак типа «intercept-resend».

Несмотря на теоретическую защищенность КРК, практические реализации сталкиваются с проблемами:

– зависимость безопасности от параметров оптических каналов (затухание, шумы);

– уязвимости классических компонентов (аутентификация, управление ключами);

– отсутствие стандартизированных методик аудита, учитывающих гибридную природу оптотехнических систем [5].

Данная работа направлена на разработку комплексного подхода к аудиту безопасности КРК-систем, объединяющего анализ квантовых протоколов, физических характеристик оборудования и классических инфраструктурных элементов. Задачи включают:

– разработку имитационной модели для оценки влияния параметров оптических каналов на стойкость ключа;

– формирование критериев оценки эффективности защитных механизмов в гибридных квантово-классических системах.

Теоретическая значимость работы заключается в систематизации требований к безопасности КРК-систем, а практическая – в создании инструментария для аудита, адаптированного к специфике оптотехнических решений. Результаты исследования могут быть применены при проектировании квантовых сетей связи и сертификации оборудования в соответствии с нормативными требованиями.

Методы и материалы

В данном исследовании применен комплекс теоретических и имитационных методов для анализа и оценки информационной безопасности оптотехнических систем, использующих технологию КРК.

Основой исследования послужил систематический обзор научных публикаций в области квантовой криптографии и информационной безопасности [6–19], включая работы по протоколам КРК (BB84, E91 и др.), а также современные стандарты и рекомендации по аудиту безопасности (ISO/IEC 27001, ETSI QKD 007) [20, 21]. Анализ позволил выявить ключевые угрозы и уязвимости, а также определить требования к методам аудита.

Для оценки безопасности КРК-систем была разработана имитационная модель [22], которая учитывает:

– физические параметры оптических каналов (затухание, уровень шума);

– особенности реализации квантовых протоколов (выбор состояний, параметры измерений);

– влияние классических компонентов инфраструктуры (аутентификация, управление ключами);

– потенциальные сценарии атак (перехват, вмешательство, подмена данных).

Модель построена на основе алгоритмов Монте-Карло, позволяющих многократно имитировать процесс передачи и обработки ключей с учетом случайных факторов и ошибок.

Ниже приводятся основные формулы и показатели [23].

Квантовая ошибка рассчитывается как отношение числа ошибочных бит $N_{\text{ошибочных}}$ к общему числу переданных бит $N_{\text{всего}}$:

$$QBER = \frac{N_{\text{ошибочных}}}{N_{\text{всего}}}. \quad (1)$$

Скорость безопасного ключа определяется с учетом коррекции ошибок и приватной компрессии:

$$R_{secure} = R_{raw} \times \left(1 - \tau_{EC} - \tau_{PA}\right), \quad (2)$$

где R_{secure} – скорость безопасного ключа; R_{raw} – скорость передачи необработанных бит; τ_{EC} – доля бит, потерянных при коррекции ошибок; τ_{PA} – доля бит, потерянных при приватной компрессии.

Индекс безопасности *S*, характеризующий эффективность защиты, рассчитывается так:

$$S = \frac{R_{secure}}{R_{raw}} \times \left(1 - QBER\right). \quad (3)$$

В разработке имитационной модели для проведения аудита информационной безопасности квантово-оптических систем использовалась специализированная визуальная среда AnyLogic. Этот инструмент позволяет создавать гибкие и масштабируемые модели, интегрирующие вероятностные распределения, дискретно-событийные процессы и агентные модели, что важно для комплексного имитационного анализа сложных гибридных систем.

Результаты

В результате проведенного теоретического анализа и имитационного моделирования аудита безопасности оптотехнических систем с использованием технологии КРК получены данные о влиянии параметров оптического канала на уровень *QBER*, представленные в табл. 1.

Таблица 1

Результаты моделирования зависимости *QBER* от параметров оптического канала

Длина канала, км	Затухание, дБ	Средний *QBER*, %	Стандартное отклонение, %
5	1,0	1,2	0,15
10	2,0	2,5	0,22
15	3,0	4,1	0,30
20	4,0	6,8	0,45

Скорость безопасного ключа при различных сценариях атак представлена в табл. 2.

Таблица 2

Влияние атак на скорость безопасного ключа

Сценарий атаки	Потери при коррекции ошибок τ_{EC}, %	Потери при приватной компрессии τ_{PA}, %	R_{secure}, бит/сек
Отсутствие атак	5	10	8500
Атака «intercept-resend»	15	25	4200
Атака «man-in-the-middle»	20	30	3200

Индекс безопасности в зависимости от *QBER* и сценариев атак представлен на рис. 1.

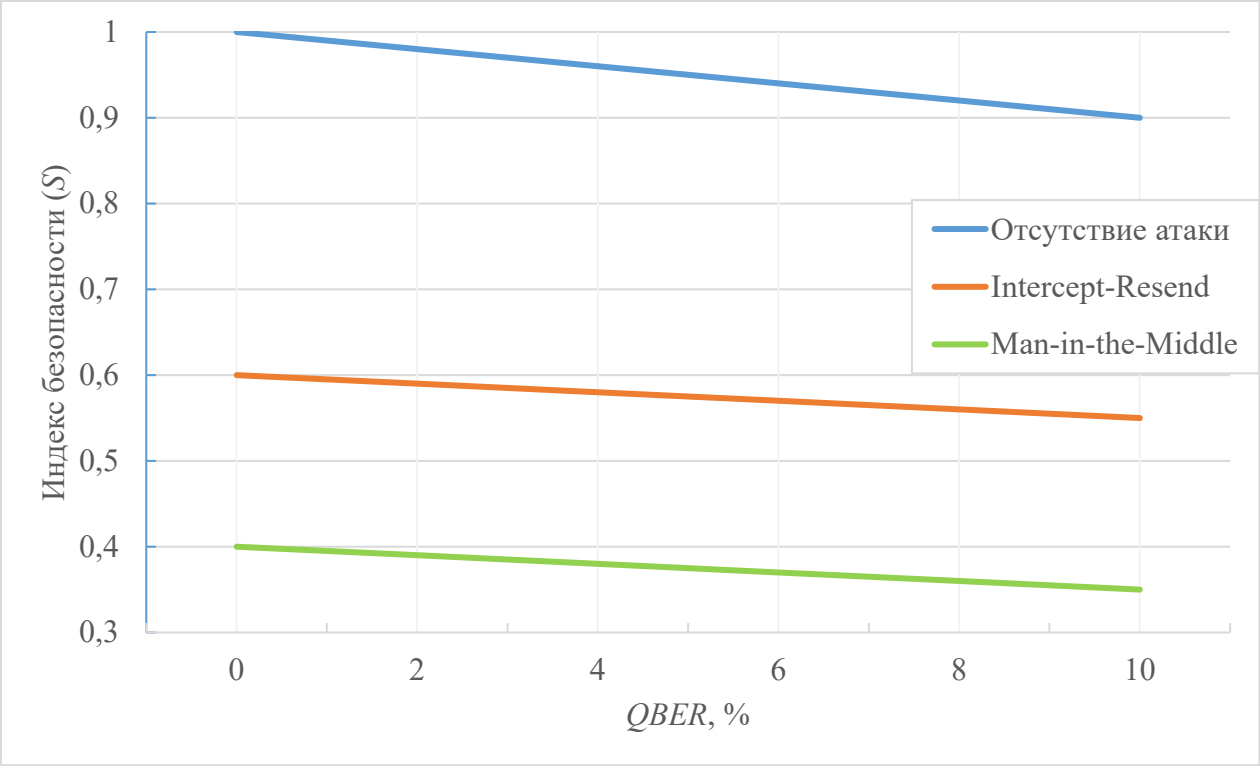

Рис. 1. Зависимость индекса безопасности *S* от *QBER* и сценариев атаки

Индекс безопасности *S* снижается с ростом *QBER* и при наличии атак, что подтверждает необходимость оптимизации параметров системы.

Блок-схема модели представлена на рис. 2.

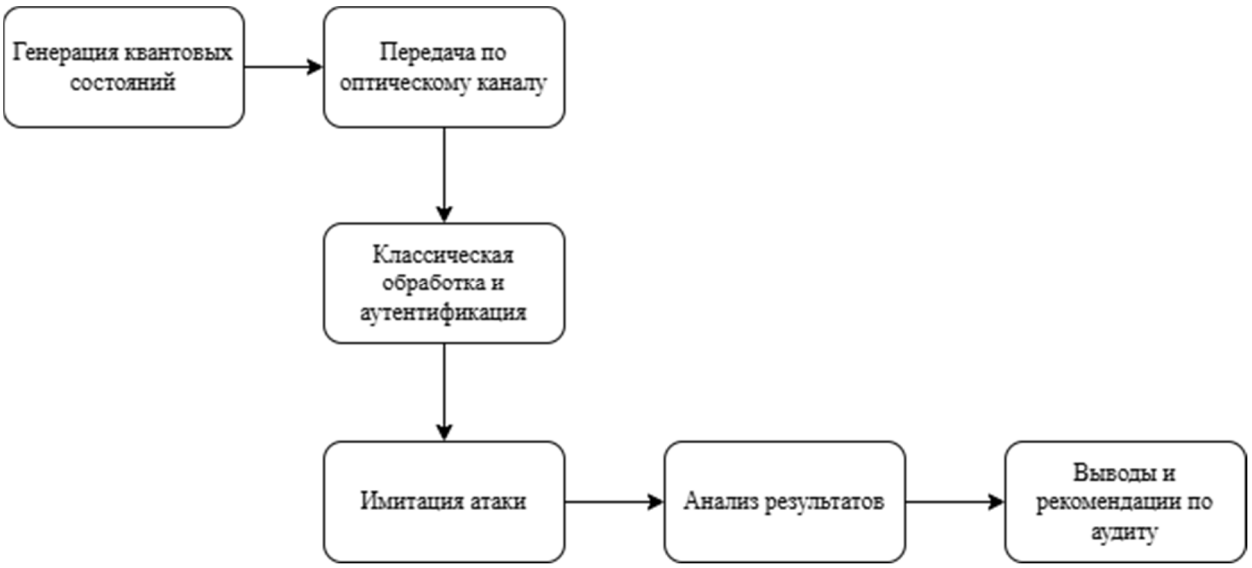

Рис. 2. Блок-схема аудита информационной безопасности при передаче информации по оптическому каналу с КРК

Основные компоненты блок-схемы: генерация квантовых состояний, передача по оптическому каналу, классическая обработка, имитация атак, анализ результатов.

Разработанная имитационная модель представлена на рис. 3 и 4.

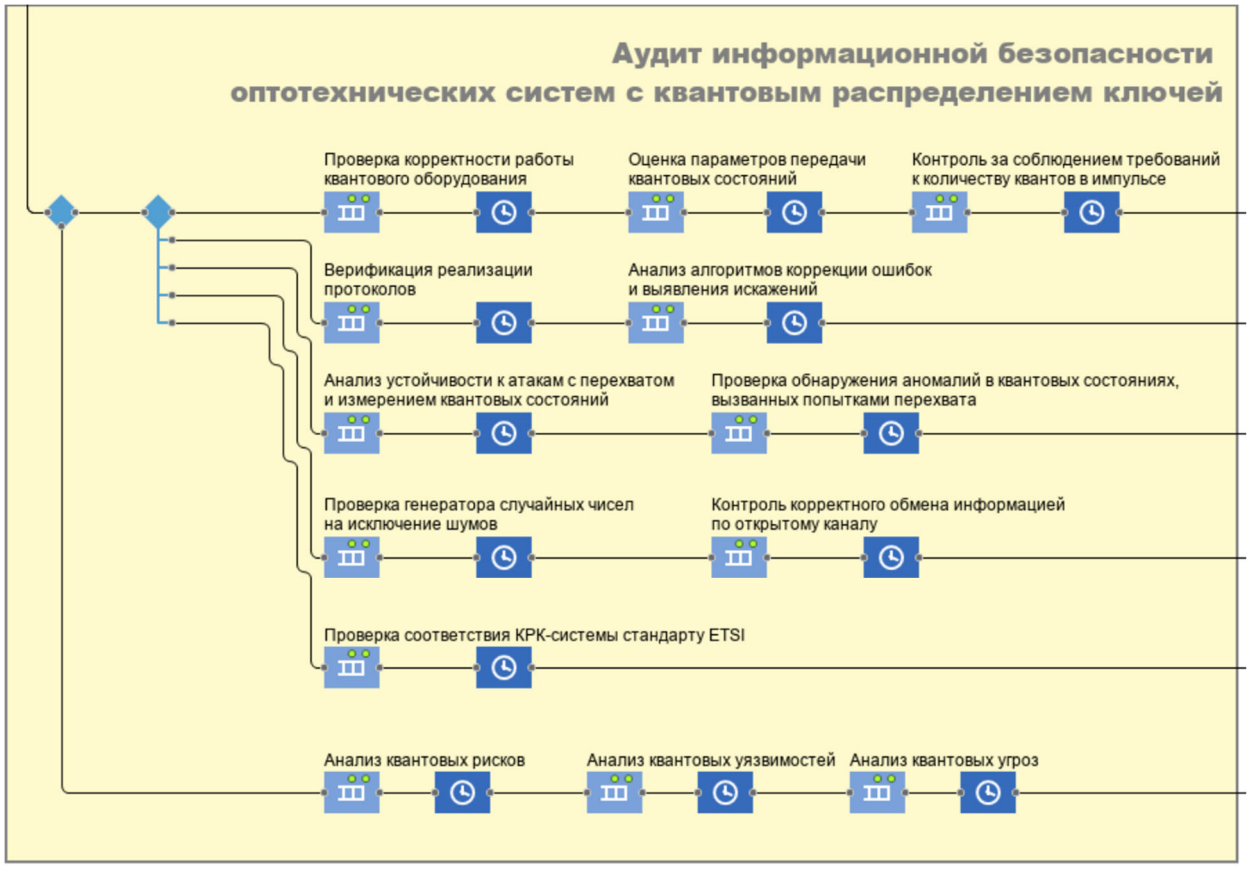

Рис. 3. Модуль имитационной модели для КРК-систем

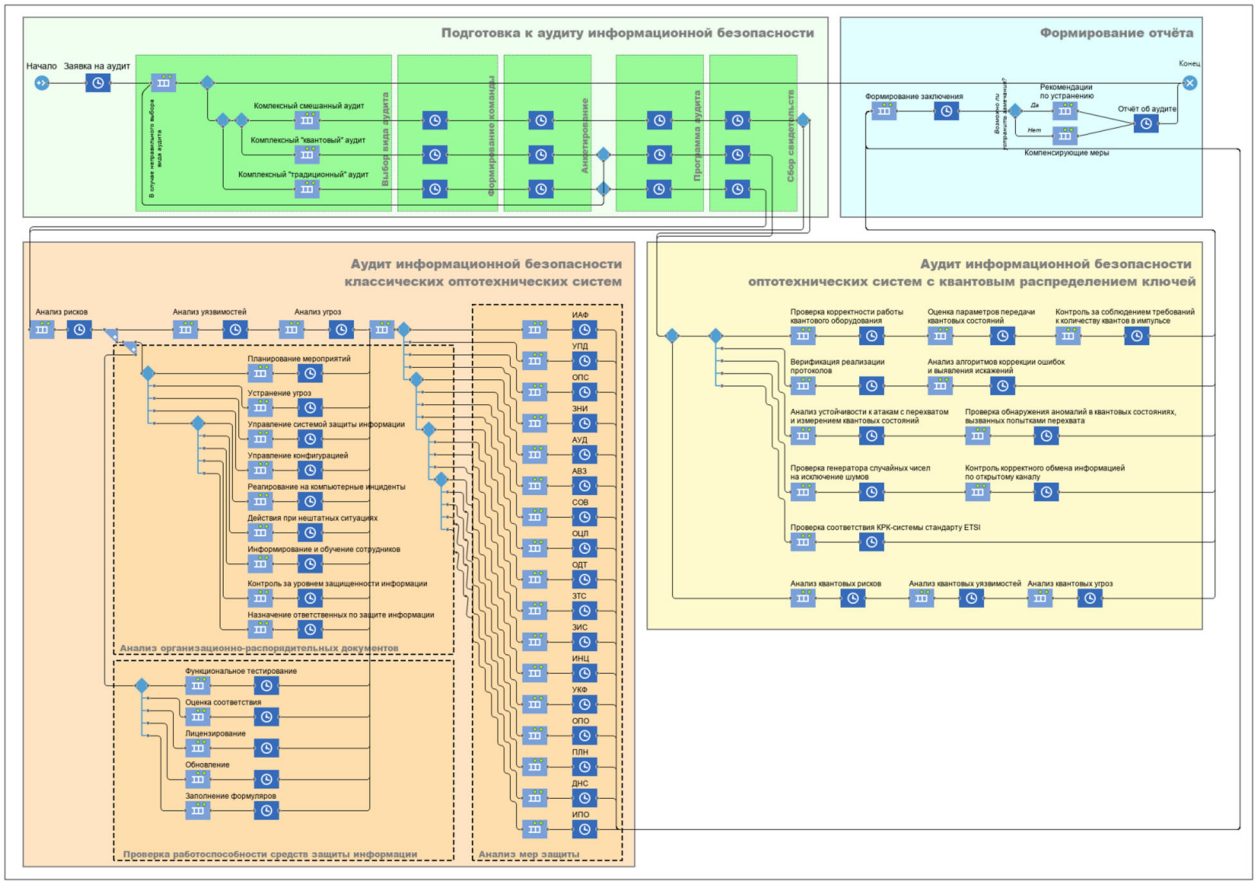

Рис. 4. Имитационная модель аудита информационной безопасности оптотехнических систем, созданных с использованием КРК

Результаты моделирования подтверждают высокую чувствительность КРК-систем к параметрам оптических каналов и типам атак, что требует тщательного аудита и адаптации защитных мер.

Заключение

В данной работе проведен теоретический анализ и имитационное моделирование аудита информационной безопасности оптотехнических систем, реализующих технологию КРК.

Основные выводы по результатам исследования следующие:

– уровень квантовой ошибки *QBER* существенно зависит от длины и качества оптического канала, что напрямую влияет на эффективность формирования безопасного ключа;

– различные сценарии атак (например, intercept-resend и man-in-the-middle) приводят к значительному снижению скорости безопасного ключа и индекса безопасности, что подчеркивает необходимость аудита с учетом гибридной природы систем;

– имитационное моделирование, реализованное в среде AnyLogic, доказало свою эффективность как инструмент для оценки уязвимостей и оптимизации параметров защиты в квантово-оптических системах [24, 25].

Рекомендации по практическому применению результатов включают:

– внедрение регулярного аудита безопасности с использованием имитационных моделей, адаптированных под конкретные параметры оборудования и каналов связи;

– усиление контроля и совершенствование классических элементов инфраструктуры, таких как аутентификация и управление ключами, для минимизации рисков атак на классическом уровне;

– оптимизация параметров оптических каналов и протоколов с целью снижения *QBER* и повышения общей надежности системы.

Основные направления дальнейших исследований предполагают:

– исследование новых видов атак, специфичных для гибридных квантово-классических систем, и методов их обнаружения;

– расширение имитационных моделей с включением дополнительных критериев аудита информационной безопасности, анализа угроз и уязвимостей, внутренней организационно-распорядительной документации.

Таким образом, авторы надеются, что представленное исследование будет способствовать развитию методологии оценки и обеспечения безопасности современных систем квантовой коммуникации и может служить основой для дальнейшего совершенствования технологий и практик в области информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Евсиков К.С. Информационная безопасность цифрового государства в квантовую эпоху. Вестник Университета имени О.Е. Кутафина (МГЮА). – 2022. – С. 46–58.

2. Серикова Ю.И., Малыгина Е.А. Уязвимости криптографических систем с различными протоколами квантового распределения ключа и ключевая роль биометрии в квантовой криптографии // Universum: технические науки: электрон. научн. журн. – 2017. – С. 13–15.

3. Курс «Роль квантовой криптографии в информационных технологиях» // Квантовые технологии МГУ. – URL: https://quantum.msu.ru/ru/education/online/the-role-of-quantum-cryptography-in-IT (дата обращения: 25.04.2025).

4. Безопасность квантовых технологий в сфере IT / Positive Technologies, QApp, КуБорд, Российский квантовый центр. – 24.05.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/bezopasnost-kvantovyh-technologiy-v-sphere-it/ (дата обращения: 25.04.2025).

5. Что такое квантовая угроза? Атака с помощью квантового компьютера – квантовая атака простыми словами // База знаний QApp. – URL: https://qapp.tech/help/quantum-threat (дата обращения: 25.04.2025).

6. Аверьянов В. С. О некоторых вопросах, идеях и технологических решениях в области квантового распределения ключей безопасности / В. С. Аверьянов // Информационная безопасность: Сборник докладов Всероссийской Школы молодых ученых, Новосибирск, 14–18 ноября 2022 г. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2022. – С. 34–39.

7. Комарова А. В. Основные угрозы безопасности и устранение их методом аудита информационной безопасности / А. В. Комарова, К. В. Толокольникова // Взаимодействие науки и общества: проблемы и перспективы: сборник статей Международной научно-практической конференции: в 4 частях, Казань, 8 июня 2017 года. Т.4. – Казань: Общество с ограниченной ответственностью «ОМЕГА САЙНС», 2017. – С. 63–66.

8. Сети квантового распределения ключей в кибербезопасности. – (Серия «Технологии доверенного взаимодействия») / Жиляев А. Е., Сабанов А. Г., Шелупанов А. А., Конев А. А., Брагин Д. С. – Москва: Горячая линия, 2023. – 152 с.

9. Баранкова И. И. Сложности, возникающие при проведении аудита информационной безопасности на предприятии / И. И. Баранкова, У. В. Михайлова, Т. В. Быкова // Вестник УрФО. Безопасность в информационной сфере. – 2019. – № 1(31). – С. 53–56.

10. Егоров М. А. Методика аудита информационной безопасности в современных условиях / М. А. Егоров // Вестник науки и образования. – 2019. – № 11-2(65). – С. 34–37.

11. Ефремов А. В. Анализ существующих методик оценки средств аудита информационной безопасности / А. В. Ефремов, Г. Е. Панамарев // Вестник Военного инновационного технополиса «Эра». – 2021. – Т. 2, № 4. – С. 38–45.

12. Зелинская Е. Л. Аудит безопасности информационных систем: виды и этапы работ / Е. Л. Зелинская, А. Г. Зелинский // Морская стратегия и политика России в контексте обеспечения национальной безопасности и устойчивого развития в XXI веке: Сборник научных трудов. ч. 2 . – Севастополь : Черноморское высшее военно-морское ордена Красной Звезды училище им. П.С. Нахимова, 2019. – С. 165–169.

13. Палканов И. С. Внутренний аудит информационной безопасности как инструмент получения объективных оценок состояния информационной безопасности организации / И. С. Палканов, В. Е. Рачков // Студенческая наука для развития информационного общества: Сборник материалов X Всероссийской научно-технической конференции с международным участием, Ставрополь, 07–08 ноября 2019 года. Ч. 1. – Ставрополь: Северо-Кавказский федеральный университет, 2019. – С. 153–161.

14. Белова, Е. А. Имитационное моделирование угроз информационной безопасности / Е. А. Белова, В. О. Крылов, О. А. Мартиросова // Актуальные научные исследования в современном мире. – 2020. – № 11-2(67). – С. 32–36.

15. Галиуллин Н. Имитационное моделирование в обеспечении информационной безопасности предприятия / Н. Галиуллин // Collegium linguisticum – 2019: тезисы докладов Ежегодной конференции Студенческого научного общества МГЛУ, Москва, 17–19 октября 2019 года. – Москва: Московский государственный лингвистический университет, 2019. – С. 286.

16. Хубиева М. Д. Анализ методов проведения аудита информационной безопасности предприятия / М. Д. Хубиева, Ф. Б. Тебуева // Новые технологии и проблемы технических наук: Сборник научных трудов по итогам международной научно-практической конференции, Красноярск, 11 ноября 2016 года. Ч. 3. – Красноярск: Инновационный центр развития образования и наук, 2016. – С. 33–37.

17. Стукалов, В. Е. Цели и задачи аудита информационной безопасности / В. Е. Стукалов. – Текст: непосредственный // Молодой ученый. – 2024. – № 2 (501). – С. 16–19.

18. Огнев, И. А. Имитационная модель процесса аудита информационной безопасности / И. А. Огнев, В. В. Селифанов // Сборник избранных статей научной сессии ТУСУР. – 2024. – № 1–3. – С. 103–107.

19. Иванов, А. В. Вопросы оценки эффективности аудита информационной безопасности / А. В. Иванов, И. А. Огнев, В. В. Селифанов // Вестник УрФО. Безопасность в информационной сфере. – 2024. – № 4(54). – С. 37–48.

20. ГОСТ Р ИСО/МЭК 27001–2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Москва: Росстандарт, 2021. – 28 с.

21. ETSI GR QKD 007 V1.1.1 (2018-12). Quantum Key Distribution (QKD); Vocabulary. European Telecommunications Standards Institute, 2018. 60 p.

22. Свидетельство о государственной регистрации программы для ЭВМ № 2024663736 Российская Федерация. Имитационная модель аудита информационной безопасности: № 2024662969: заявл. 11.06.2024: опубл. 11.06.2024 / А.А. Микула, А.И. Подлегаев, В.В. Селифа-

нов; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет геосистем и технологий».

23. Исследование компании RAND «Безопасность коммуникаций в эпоху квантовых компьютерных технологий» / RAND Corporation. – 2021. – URL: https://rdc.grfc.ru/2021/03/rand-quantum-comps/ (дата обращения: 25.04.2025).

24. Микула, А. А. Вопросы моделирования процедур аудита информационной безопасности / А. А. Микула, А. И. Подлегаев, В. В. Селифанов // Интерэкспо Гео-Сибирь. – 2024. – Т. 7, № 3. – С. 146–152.

25. Подлегаев, А. И. Вопросы моделирования системы управления аудитом / А.И. Подлегаев, А.А. Микула, В.В. Селифанов // Интерэкспо Гео-Сибирь. – 2024. – Т. 6. – С. 210–217.