ISSN 2079-4665, E-ISSN 2411-796X https://www.mir-nayka.com

Научная статья

УДК 338
JEL: L10, L20, L60, O14, O25, O33
https://doi.org/10.18184/2079-4665.2025.16.3.488–504

# Экономическая оценка целесообразности внедрения квантовых коммуникаций в энергетической отрасли

**Лобов Даниил Сергеевич** [1]

[1] Санкт-Петербургский государственный университет; Санкт-Петербург, Россия

[1] d.lobov96@yandex.ru, https://orcid.org/0000-0002-9548-2502

**Аннотация**

**Цель** – оценка экономической целесообразности проведения квантовой трансформации функции информационной безопасности на примере объектов энергетической отрасли.

**Методы.** В работе применяется авторская модель оценки экономической эффективности проведения квантовой трансформации функции информационной безопасности, основанная на подходах к анализу вероятности реализации рисков, связанных с созданием квантового компьютера, а также к оценке инвестиций, необходимых для внедрения инновационных решений в области квантовых коммуникаций. Расчет проведен на примере ПАО «Русгидро», данные по компании собраны в открытых источниках и годовых отчетах.

**Результаты работы.** Проведена апробация модели оценки экономической эффективности проведения квантовой трансформации функции информационной безопасности. Улучшена «теорема Моска» в области прогнозирования сроков квантовой трансформации с учетом фактора экономической эффективности инвестиционного проекта. Разработаны рекомендации по внедрению оборудования квантового распределения ключей и постквантовых алгоритмов в долгосрочной перспективе.

**Выводы.** Предложенная оригинальная модель позволяет оценить экономическую эффективность внедрения технологий квантовых коммуникаций, а обновленная «теорема Моска» – определить экономически обоснованные сроки реализации квантовой трансформации. Исследование показало, что квантовые коммуникации могут представлять наибольший интерес для компаний-владельцев ключевых объектов критической информационной инфраструктуры, обеспечивающих высокие показатели выручки. Чем выше децентрализация инфраструктурных объектов и ниже риск финансовых потерь в результате простоя, тем менее экономически эффективны проекты по внедрению квантовых коммуникаций. Так, для защиты множества интеллектуальных подстанций в рамках Smart Grid рекомендуется применять постквантовые математические алгоритмы, не требующие значительных капитальных вложений. Полученные результаты могут представлять практическую пользу для участников квантового рынка в России: регулятора, научно-исследовательских центров, коммерческих разработчиков решений, потенциальных клиентов.

**Ключевые слова:** квантовая трансформация, квантовые коммуникации, квантовый компьютер, экономическая модель, управление инновациями

**Конфликт интересов.** Автор заявляет об отсутствии конфликта интересов.

**Для цитирования:** *Лобов Д. С.* Экономическая оценка целесообразности внедрения квантовых коммуникаций в энергетической отрасли // МИР (Модернизация. Инновации. Развитие). 2025. Т. 16. № 3. С. 488–504

EDN: https://elibrary.ru/qtyvzq. https://doi.org/10.18184/2079-4665.2025.16.3.488-504

Original article

# Economic assessment of reasonability of introducing quantum communications in the energy sector

**Daniil S. Lobov** [1]

[1] Saint-Petersburg State University; Saint Petersburg, Russia

[1] d.lobov96@yandex.ru, https://orcid.org/0000-0002-9548-2502

**Abstract**

**Purpose:** evaluation of economic reasonability of quantum transformation of the information security function using the example of energy sector facilities.

**Methods:** the paper uses the author's model for assessing the economic efficiency of quantum transformation of the information security function, based on approaches to analyzing the probability of risks associated with the creation of a quantum computer, as well as to assessing the investments required to implement innovative solutions in the field of quantum communications. The calculation was carried out on the example of PJSC RusHydro; data on the company were collected from open sources and annual reports.

**Results:** the model for assessing the economic efficiency of quantum transformation of the information security function was tested. The Mosca's Theorem was improved in the field of forecasting the timing of quantum transformation, taking into account the factor of economic efficiency of investment projects. Recommendations for implementing quantum key distribution equipment and post-quantum algorithms in the long term were developed.

**Conclusions and Relevance:** the proposed original model allows assessing the economic efficiency of implementing quantum communications technologies, and the updated Mosca's Theorem allows determining the economically justified timeframes for quantum transformation. The study showed that quantum communications may be of greatest interest to companies that own key critical information infrastructure facilities that provide high revenue figures. The higher the decentralization of infrastructure facilities is and the lower the risk of financial losses due to downtime is, the less economically efficient the projects for implementing quantum communications are. Thus, to protect multiple intelligent substations within the Smart Grid, it is recommended to use post-quantum mathematical algorithms that do not require significant capital investments. The results obtained may be of practical use for participants in the quantum market in Russia: the regulator, research centers, commercial developers of solutions, and potential clients.

**Keywords:** quantum transformation, quantum communications, quantum computer, economic model, innovation management

**Conflict of Interest.** The author declares that there is no Conflict of Interest.

**For citation:** Lobov D. S. Economic assessment of reasonability of introducing quantum communications in the energy sector. *MIR (Modernization. Innovation. Research)*. 2025; 16(3):488–504. (In Russ.)

EDN: https://elibrary.ru/qtyvzq. https://doi.org/10.18184/2079-4665.2025.16.3.488-504



## Введение

Квантовые коммуникации – область знаний и технологий, связанных с передачей квантовых состояний в пространстве. Базовой технологией квантовых коммуникаций является квантовое распределение ключей: устройство передачи сигнала (источник фотонов) транслирует квантовое состояние с применением оптоволоконного или воздушного каналов на устройство приема (детектор фотонов). Переданная последовательность квантовых состояний служит основанием для формирования симметричного ключа шифрования [1]. Функциональные преимущества квантового распределения ключей заключаются в повышении устойчивости систем в условиях растущих рисков информационной безопасности.

Согласно авторскому определению, квантовая трансформация информационной безопасности – это процесс внедрения элементов квантовых коммуникаций в архитектуру информационной безопасности объекта. В результате квантовой трансформации изменяется подход к работе с ключами шифрования, повышается устойчивость криптографии: симметричные квантовые ключи автоматически передаются по закрытым каналам связи и загружаются в средства криптографической защиты информации (СКЗИ) с применением квантовых устройств и специальных интерфейсов. Традиционно симметричные ключи передаются либо вручную, доверенными курьерами, либо по открытым каналам связи, зашифрованные с помощью менее устойчивых симметричных алгоритмов, без использования дополнительной специализированной аппаратуры.

В настоящее время продолжаются попытки перехода от теории применения квантовых коммуникаций в системах интеллектуальных сетей энергоснабжения Smart Grid к практике [2, 3]. Еще в

2013 г. в США был реализован крупный проект по пилотированию устройств квантового распределения ключей с применением энергетических установок компании General Electric. В соответствии с планом НИОКР Национальная лаборатория Oak Ridge заявляла о возможности создания недорогих узлов квантового распределения ключей (КРК) – AQCESS (Accessible QKD for Cost-Effective Secret Sharing), доступных к одновременной работе на одном квантовом канале, а также совместимых с существующими на тот момент протоколами связи для бесшовной интеграции с существующими компонентами сети. Помимо Oak Ridge National Laboratory и GE Global Research, в проекте принял участие крупный поставщик квантового оборудования, ID Quantique. Реализация осуществлялась под эгидой Министерства энергетики США [1].

Можно предположить, что первые результаты НИОКР удовлетворили команду исследователей, так как в 2017 г. при поддержке Министерства энергетики США был запущен проект по увеличению протяженности квантового распределения ключа и разработке новых протоколов связи для обеспечения аутентификации и целостности данных с применением квантовых сетей [2].

Одним из результатов проекта стало успешное применение в 2021 г. оборудования Qubitekk на сети компании EPB Quantum Network для защиты связи между электрической подстанцией и распределительным центром. Квантовое распределение ключа позволило повысить устойчивость шифрования применяемой на предприятии системы SCADA. Расстояние между точками составило 3,4 км. Передача ключа осуществлялась по выделенному оптоволоконному каналу, проложенному по опорам, в связи с чем наблюдалось влияние агрессивной внешней среды, включая порывы ветра и изменение температур. Незначительное снижение скорости передачи ключа в результате работы в сложных условиях не оказало негативного влияния на достижение поставленной исследователями задачи [4].

В 2020 г. была опубликована статья китайских исследователей [5], посвященная применению устройств КРК на объектах энергетической отрасли. Целью проекта стало тестирование возможности применения квантового VPN для защиты процесса удаленного управления оборудованием с подключением Национального центра диспетчерского управления электроэнергией, Регионального центра диспетчерского управления и электростанции. Расстояние между точками составило более 60 км. Крупнейший поставщик квантового оборудования в Китае, QuantumCTEK, заявляет, что аналогичные решения компании по распределению ключей применяются для защиты систем SCADA как минимум 4-х объектов энергетической инфраструктуры.

Учитывая международный практический опыт, автор данной работы предполагает, что внедрение квантовых коммуникаций в качестве инструмента информационной безопасности может представлять интерес для энергетических компаний-владельцев объектов критической информационной инфраструктуры в связи с возможностью снижения экономических рисков, обусловленных потенциальными последствиями киберпреступлений, в результате применения устройств квантового распределения ключей, обеспечивающих автоматическую передачу и загрузку симметричных ключей в средства криптографической защиты информации, исключающих необходимость применения менее стабильных асимметричных алгоритмов, а также передачи токенов доверенными курьерами. Для доказательства данной гипотезы автор провел исследование места и роли квантовых коммуникаций в системе информационной безопасности энергетического предприятия, оценил объем затрат на трансформацию инфраструктуры с применением квантового компонента и дал экономическую оценку рисков, связанных с отсутствием квантового уровня безопасности сети в долгосрочной перспективе.

### Обзор литературы и исследований

Изучение источников, посвященных статистике инцидентов на объектах энергетической инфраструктуры [6, 7], показывает, что наиболее результативные атаки хакеров связаны с недостаточной подготовкой персонала и подрывными действиями сотрудников самих организаций. Борьба с наиболее актуальными угрозами лежит в первую очередь в периметре административной работы: своевременная установка патчей и обновление программного обеспечения сотрудниками ИТ, обучение персонала, а также сегментация сетей.

Возникает вопрос – необходимо ли применение квантовых коммуникаций для защиты от потенциальных угроз, например, квантового компьютера. Ключевые риски, связанные с квантовым компью-

[1] Practical Quantum Security for Grid Automation // U.S. Department of Energy. 2017. URL: https://www.energy.gov/sites/prod/files/2017/04/f34/ORNL_Practical_Quantum_Security_FactSheet_0.pdf (дата обращения: 18.02.2025)

[2] Quantum Physics Secured Communications for the Energy Sector // U.S. Department of Energy. 2021. URL: https://www.energy.gov/sites/default/files/2021-08/Quantum%20Physics%20Secured%20Communications%20for%20the%20Energy%20Sector%20-%20ORNL_508.pdf (дата обращения: 18.02.2025)

тером, заключаются прежде всего в возможном получении доступа к данным, зашифрованным асимметричным ключом RSA [8], в то время как, например, алгоритм симметричного шифрования AES останется устойчивым даже в новых условиях [9]. Таким образом, функциональное применение квантовых коммуникаций сужается до промышленных систем, применяющих шифрование RSA. Действительно, такие системы есть и довольно распространены в условиях развития Индустрии 4.0. Прежде всего, это SCADA (аббр. от англ. Supervisory Control And Data Acquisition) – программно-аппаратный комплекс сбора данных и диспетчерского контроля.

Роль технологии SCADA значительна в цифровизации промышленных объектов, в связи с чем аспекты ее информационной безопасности подробно исследуются экспертами. Опыт прошлых кибератак показывает [10], что компрометация систем SCADA может привести к экономическому и, в некоторых случаях, физическому ущербу для населения. Ряд авторов предлагает новые подходы к обеспечению защиты SCADA как с применением квантового распределения ключей, так и математических постквантовых алгоритмов [11–13].

Преимущества постквантовых алгоритмов заключаются в отсутствии необходимости закупки дорогостоящих устройств квантового распределения ключей [14, 15], а также в возможности защиты беспроводных сетей при отсутствии доступа к воздушным каналам [16]. При этом стоит отметить, что внедрение более «тяжелых» алгоритмов шифрования все же потребует выделения дополнительных вычислительных мощностей, также отсутствует гарантия долгосрочной устойчивости постквантового шифрования с учетом риска создания улучшенных квантовых компьютеров.

Большинство работ, посвященных вопросам стратегического развития квантовых коммуникаций, рассматривает факторы формирования рынка устройств квантового распределения ключей. Барьеры коммерциализации, выявленные в 2014-2015 гг., включали недостаточность сертификации и стандартизации оборудования и технологий, низкое качество послепродажного обслуживания, отсутствие необходимой телекоммуникационной инфраструктуры [17]. До сих пор нерешенной задачей остается создание «квантового повторителя», позволяющего транслировать состояние фотона на протяженные расстояния [18, 19]. Актуальные исследования отмечают зоны развития в области регуляторных мер поддержки (требуется разработка новых законодательных актов для интенсификации применения устройств квантового распределения ключей на объектах критической инфраструктуры) [20], повышения вовлеченности представителей науки, государственного управления и бизнеса в вопросы практического применения технологии [21].

При этом авторы отмечают позитивную динамику развития отрасли: осуществляется переход исследований с этапа научно-исследовательских работ (НИР) на опытно-конструкторские работы (ОКР) [22], наблюдается определенный прогресс в области стандартизации [3], что свидетельствует о росте уровня технологической готовности решений. Рост уровня коммерческой готовности подтверждается участием таких крупных технологических компаний, как Toshiba и Huawei, в создании квантовой инфраструктуры [23, 24]. При участии крупного бизнеса в 16-ти странах созданы тестовые полигоны для апробации квантовых сетей [25]. Исследователи уже сейчас рекомендуют организациям обратить внимание на повышение их уровня «квантовой готовности» [26]. Успешность развития высокотехнологичного направления подтверждается данными по рынку: совокупная выручка компаний квантовой экосистемы в Российской Федерации стремится к 1 млрд руб. в условиях реализации мер государственной поддержки, прогнозируется рост объема международного рынка до 36 млрд долл. в 2040 г. [4]

Ряд исследований затрагивает вопросы отраслевого применения технологий квантового распределения ключей. Отмечается значимая роль ОАО «РЖД» в развитии квантовых коммуникаций с учетом протяженности оптоволоконных сетей компании [27]. Проведены работы по анализу перспектив внедрения квантовых коммуникаций в транспортной [28], энергетической [5] и финансовой отраслях [6]. Подчеркиваются возможности применения технологии в целях защиты каналов

[3] *Popa A.B., Popescu P.G.* The Future of QKD Networks // arXiv preprint. arXiv:2407.00877. 01.07.2024. https://doi.org/10.48550/arXiv.2407.00877

[4] Там же

[5] *Салыгин В.И., Лобов Д.С.* Перспективы применения технологий квантового распределения ключей на примере объектов нефтегазовой отрасли // Друкеровский вестник. 2023. № 1(51). С. 246–253. EDN: https://elibrary.ru/whyeqq. https://doi.org/10.17213/2312-6469-2023-1-246-253

[6] *Bishwas A.K., Sen M.* Strategic roadmap for quantum-resistant security: a framework for preparing industries for the quantum threat // arXiv preprint arXiv:2411.09995. 15.10.2024.

центров обработки данных [18]. В долгосрочной перспективе развитие квантовых коммуникаций будет обеспечиваться не только за счет продажи решений квантового распределения ключей в сегменте информационной безопасности, но и благодаря формированию фундаментально новых рынков, созданию «квантового интернета» [7].

Недостаточное освещение получают вопросы экономической выгоды конечных клиентов от внедрения устройств квантового распределения ключей, являющейся основой спроса, силу которого на рынке квантовых коммуникаций можно поставить под сомнение в случае сокращения мер государственной поддержки. В соответствии с выводами Тайгелера Х. с соавторами [8], исследовавшего на примере облачных сервисов специфику действий регуляторов, ответственных за сертификацию, инновационные рынки могут столкнуться с замедлением принятия мер, направленных на создание регуляторного фреймворка, в том случае, если не наблюдается одновременного действия двух рыночных сил: технологического давления (англ. technology push), приводящего к созданию прорывных решений в результате научно-технического прогресса, и рыночного притяжения (англ. demand/market pull), вызванного нарастающим спросом клиентов на инновации для удовлетворения их потребностей [29]. Таким образом, недостаточная активность регулятора в области квантовых коммуникаций может свидетельствовать о низкой силе «рыночного притяжения» и ожиданиях слабого экономического эффекта от внедрения устройств квантового распределения ключей со стороны потребителей.

Хотя исследователи подчеркивают [9], что одним из ключевых факторов, ограничивающих силу рыночного притяжения в области квантовых коммуникаций, является высокая стоимость устройств квантового распределения ключей, отсутствует методология оценки оптимальной с точки зрения конечного клиента стоимости, отражающей ожидания потенциальных выгод от применения технологии в реальных условиях, к которой необходимо стремиться разработчикам при формировании коммерческих предложений. Представленная в данной работе авторская математическая модель позволяет закрыть выявленный пробел в научной литературе.

Автор также отмечает недостаток текущих теоретических положений в области долгосрочного планирования квантовой трансформации функции информационной безопасности квантовых технологий, заключающийся в отсутствии учета экономических параметров. Так, канадский физик Мишель Моска [30] предлагает теорему [10], в соответствии с которой дата установки устройств квантового распределения ключей определяется на основе прогноза создания квантового компьютера и требований к сроку хранения секретной информации:

$$(X + Y) > Z, \quad (1)$$

где $X$ – срок хранения чувствительных данных, $Y$ – ожидаемый срок осуществления квантовой трансформации, $Z$ – количество лет, оставшихся до создания квантового компьютера.

По мнению автора, теорема Моска не является достаточно актуальной для коммерческих организаций и может быть улучшена с учетом фактора экономической эффективности инвестиций.

## Материалы и методы

В работе применяется авторская модель оценки экономической эффективности проведения квантовой трансформации функции информационной безопасности, основанная на принципах методологии BIA (англ. Business Impact Analysis, рус. «анализ воздействия на бизнес») по исследованию влияния чрезвычайных ситуаций на бизнес. Стандарт проведения BIA (ISO/TS 22317:2015) включает рекомендации по оценке рисков воздействия угроз цифровой безопасности на непрерывность бизнеса (англ. business continuity). Простой оборудования, полученный в результате реализации кибер-угроз, приводит как к экономическим, так и репутационным издержкам организации. Подобный риск-ориентированный подход к оценке экономических эффектов является основным при обосновании внедрения решений цифровой безопасности.

В соответствии с авторской моделью расчет проводится в три этапа, в ходе которых осуществляется оценка:

[7] *Jiang J.L., Luo M.X., Ma S.Y.* Quantum network capacity of entangled quantum internet // IEEE Journal on Selected Areas in Communications. 2024. Vol. 42. Iss. 7. P. 1900–1918. https://doi.org/10.1109/jsac.2024.3380091

[8] *Teigeler H., Lins S., Sunyaev A.* Technology-Push or Market-Pull – What Drives Certification Authorities to Perform Continuous Service Certification? // In: Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm and Uppsala, Sweden, June 8-14, 2019. URL: https://aisel.aisnet.org/ecis2019_rp/29/ (дата обращения: 18.02.2025)

[9] *Henry E.* Economic Impact of Quantum Cryptography on Network Security Industries // SSRN. 24.09.2024. https://dx.doi.org/10.2139/ssrn.4966117

[10] What is the Mosca-theorem? // Utimaco. URL: https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-mosca-theorem (дата обращения: 22.06.2025)

- затрат на внедрение оборудования квантового распределения ключей (или постквантовых алгоритмов в качестве альтернативного решения);
- риска простоя оборудования, реализуемого в результате отсутствия проекта по внедрению квантового оборудования или постквантовых алгоритмов, в связи с применением квантового компьютера в ходе кибератаки на рассматриваемый объект критической инфраструктуры; стоит отметить, что на данном этапе также возможен учет риска репутационных издержек и падения стоимости ценных бумаг компании-владельца объекта;
- экономической эффективности квантовой трансформации на основе данных по затратам и рискам.

Исследование экономической эффективности квантовой трансформации было проведено на примере компании ПАО «Русгидро» – одного из ключевых участников рынка электроэнергии. Данные по количеству объектов критической инфраструктуры компании и результатам операционной деятельности были собраны из открытых источников и годовых отчетах.

### Результаты исследования

Модель оценки экономической эффективности проведения квантовой трансформации функции информационной безопасности

Оценка затрат на внедрение квантового оборудования производится по формуле:

$$QT_c = (A \times P_1) + (B \times P_2) + (C \times P_3) + \\ + (S \times P_4) + (PN \times P_5) + (L \times P_6) + (C \times P_7), \quad (2)$$

где $QT_c$ – затраты на осуществление квантовой трансформации; $A$ – количество квантовых узлов «$A$» – передача сигнала и сопряженных с ними модулей управления ключами (МУК), средств криптографической защиты информации (СКЗИ), для локальной сети; $P_1$ – стоимость внедрения одного квантового узла «$A$» и сопряженного с ним модуля управления ключами (МУК) и средства криптографической защиты информации (СКЗИ); $B$ – количество квантовых узлов «$B$» – прием сигнала и сопряженных с ними МУК и СКЗИ, для локальной сети; $P_2$ – стоимость внедрения одного квантового узла «$B$» и сопряженных с ним МУК и СКЗИ; $C$ – количество сопряженных квантовых узлов приема и передачи сигнала (модулей), применяемых для подключения локальной квантовой сети (через квантовые узлы «$B$») к магистральной; $P_3$ – стоимость внедрения квантового модуля «$C$» (узел приема и узел передачи); $S$ – количество оптических коммутаторов для локальной сети топологии «точка-многоточка»; $P_4$ – стоимость внедрения одного оптического коммутатора «$S$»; $PN$ – количество сотрудников информационной безопасности (ИБ) в организациях, проходящих квантовую трансформацию; $P_5$ – стоимость повышения квалификации одного сотрудника; $L$ – протяженность оптоволоконного канала, км; $P_6$ – стоимость прокладывания одного км оптоволоконного канала; $P_7$ – стоимость оказания услуги подключения локальной квантовой сети к магистральной квантовой сети в год (с применением узлов «$C$»).

Визуальное изображение компонентов сети и связи между ними представлены на рис. 1.

Риски отказа от внедрения квантового распределения ключей (КРК) и постквантовых алгоритмов оцениваются в соответствии с формулой:

$$ER = QR \times AL, \quad (3)$$

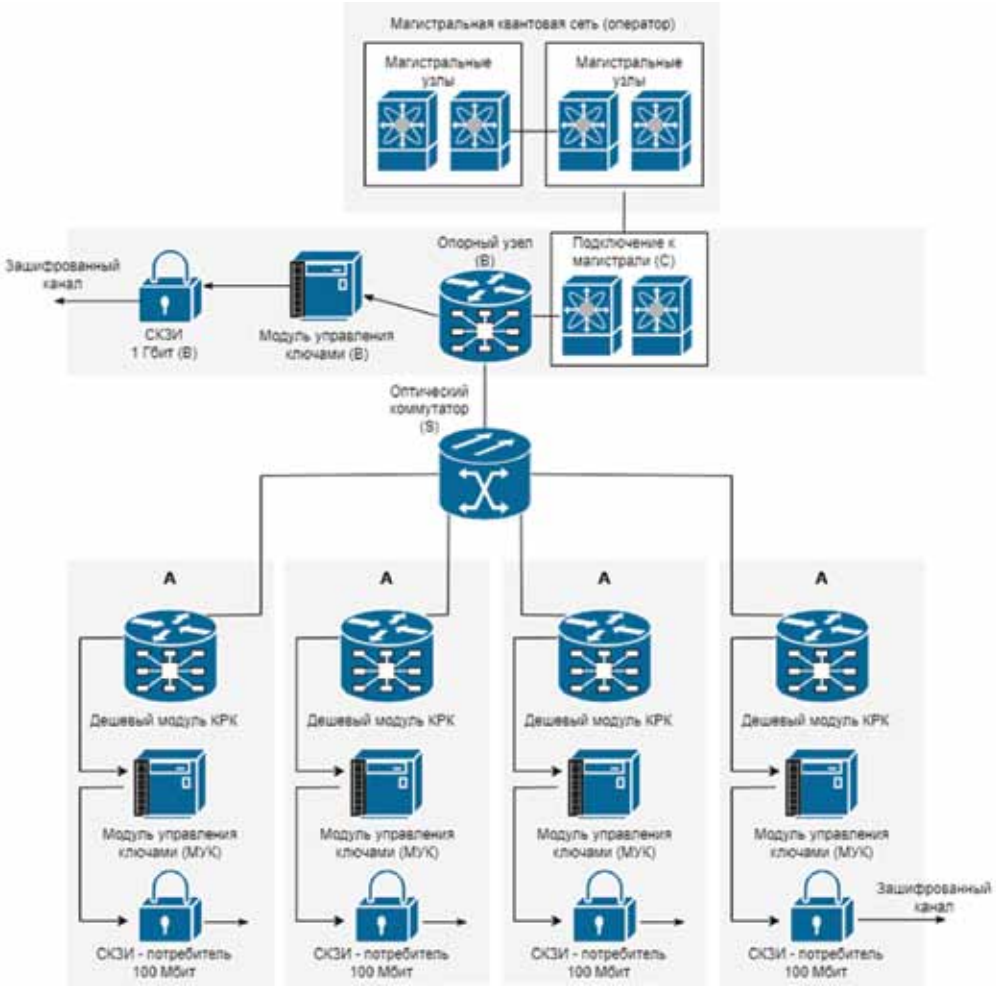
где $ER$ – экономическая оценка рисков отказа от внедрения КРК и постквантовых алгоритмов; $QR$ – риск применения квантового компьютера; $AL$ – ожидаемые потери выручки от простоя оборудования в результате успешной квантовой кибератаки.

Риск применения квантового компьютера определяется в соответствии с данными ведущих аналитических агентств, публикующих прогнозы создания квантового компьютера, способного снизить устойчивость алгоритмов RSA. Ожидаемые потери выручки от простоя оборудования в результате успешной квантовой кибератаки рассчитываются по формуле:

$$AL = \frac{R}{Количество\ часов\ работы\ в\ году} \times T, \quad (4)$$

где $AL$ – ожидаемые потери выручки от простоя оборудования в результате успешной квантовой кибератаки, руб.; $R$ – выручка компании, руб.; $T$ – максимальный ожидаемый простой оборудования в результате реализации успешной кибератаки, часов.

Показатель $ER$ ежегодно увеличивается по мере роста $QR$ (риска создания и применения квантового компьютера). Пересечение $ER$ и $QTc$ в определенном временном периоде свидетельствует о необходимости внедрения устройств квантовых коммуникаций для снижения рисков квантовой атаки. В случае, если пересечение $ER$ и $QTc$ не наблюдается в долгосрочном горизонте планирования (например, в течение 10 лет, то есть до 2035 г.), рекомендуется обратить внимание на возможность применения альтернативных методов защиты сетей от квантовой угрозы, например, на внедрение математических постквантовых алгоритмов. Стоимость внедрения постквантовых




*Составлено автором.*

**Рис. 1. Схема компонентов локальной квантовой сети**

*Compiled by the author.*

**Fig. 1. Components of a local quantum network**

алгоритмов можно оценить с применением метода бенчмаркинга по формуле:

$$PQ = ITB \times \alpha, \quad (5)$$

где $PQ$ – затраты на постквантовую трансформацию; $\alpha$ – бенчмарк стоимости постквантовой трансформации (% от бюджета в области информационных технологий (ИТ)); $ITB$ – бюджет ИТ-организаций, проходящих квантовую трансформацию.

Стоит отметить, что возможно развитие предложенной модели с учетом операционных затрат на поддержание работы квантовой сети. При выборе периода оценки предлагается ориентироваться на срок в 3 года (требование к сроку амортизации средств криптографической защиты информации):

$$QTtco = QTc + (QTqc \times \partial \times t) + (C \times P_7 \times t), \quad (6)$$

где $QTtco$ – полная стоимость владения квантовой сетью; $QTqc$ – затраты на осуществление квантовой трансформации за вычетом затрат на обучение персонала, прокладку оптоволоконного канала и закупку услуг квантовой сети (чистые затраты на внедрение квантовой сети); $\partial$ – бенчмарк ежегодной стоимости поддержания работы квантовой сети к чистым затратам на ее внедрение, %; $t$ – период оценки (предлагается ориентироваться на срок амортизации СКЗИ за вычетом первого года внедрения).

Стоимость подключения к магистральной квантовой сети $(C \times P_7 \times t)$ не учитывается в случае проекта по созданию изолированной локальной квантовой сети.

Риски отказа от внедрения КРК и постквантовых алгоритмов в рамках данного подхода также оцениваются кумулятивно:

$$ERc = \sum_{i=1}^{n} ER_i, \quad (7)$$

где $ERc$ – совокупная экономическая оценка рисков отказа от внедрения КРК и постквантовых алгоритмов; $ER_i$ – экономическая оценка рисков отказа от внедрения КРК и постквантовых алгоритмов за отдельный год.

*Сценарии проведения квантовой трансформации*

Применим авторскую модель оценки экономической эффективности квантовой трансформации на примере компании ПАО «Русгидро». Данные для проведения анализа взяты из открытых источников, преимущественно годовых отчетов компании.

Предположим, что руководство «Русгидро» примет решение внедрить квантовые коммуникации на сетях по следующим трем сценариям.

1. Защита канала между Южно-Сахалинской ТЭЦ-1 и 3-мя подстанциями («Южно-Сахалинская» ПС, ПС «Шахтерская», ПС «Южная») в рамках локальной квантовой сети. Требуется установка одного устройства приема сигнала и 3-х передатчиков.
2. Защита каналов между 66-ю [11] генерирующими объектами компании (гидроэлектростанции, тепловые электростанции, геотермальные электростанции, солнечные электростанции, ветровые электростанции) и 427-ю трансформаторными подстанциями мощностью от 110 до 220 кВ с подключением к магистральной квантовой сети. Требуется установка 66-ти устройств приема сигнала и 427-ми передатчиков. Осуществляется подключение локальных сетей к квантовой магистральной сети.
3. Защита каналов между 427-ю подстанциями мощностью от 110 до 220 кВ и 22525-ю подстанциями мощностью 6–35 кВ [12]. Необходимо установить 2253 устройства приема сигнала и 22525 передатчиков, так как к одному устройству приема может быть подключено не более 10-ти передатчиков (также на 1 устройство приема приходится 1 оптический коммутатор). Осуществляется подключение локальных сетей к квантовой магистральной сети.

В случае, если установка устройств квантового распределения ключей не будет представлять экономический интерес, предлагается оценить стоимость внедрения постквантовых алгоритмов.

Результаты предварительных расчетов приведены в табл. 1. Обоснование количества объектов квантовой инфраструктуры приведено выше по тексту, стоимости установки и обслуживания оборудования основываются на индикативной оценке автора в результате сбора информации от вендоров на рынке квантовых устройств в течение 2024 г. и могут изменяться. Показатели $L$ и $PN$ не учитываются в упрощенном расчете. В качестве ориентировочного периода предлагается взять 2 года функционирования оборудования плюс 1 год внедрения. Итоговые результаты анализа учитывают инфляционные ожидания и представлены в динамике до 2040 г. **далее.**

Оценим риски отказа от внедрения КРК и постквантовых алгоритмов с учетом вероятности создания квантового компьютера и потенциала простоя оборудования в результате успешной квантовой атаки.

Вероятность успешного создания квантового компьютера основана на опросах экспертов квантовой индустрии [13] (в основу оценки вероятности создания лег отчет McKinsey, применяется понижающий индикативный коэффициент х2, учитывающий консервативные прогнозы создания функционирующего квантового компьютера [14], а также заявления лидеров индустрии [15]), она увеличивается с 5% в 2025 г. до 69% в 2040 г., с неравномерными темпами роста в периодах 2025–2030 гг. и 2031–2040 гг.

Определим риски потери выручки от простоя оборудования в результате успешной квантовой кибератаки, учитывая, что бенчмарк по временным

[11] География деятельности. Годовой отчет 2022 // Русгидро. URL: https://ar2022.rushydro.ru/ru/company-profile/geography (дата обращения: 22.06.2025)

[12] Производственные и операционные результаты. Годовой отчет 2021 // Русгидро. URL: https://ar2021.rushydro.ru/3/Proizvodstvennye_i_operatsionnye_rezultaty/ (дата обращения: 22.06.2025)

[13] Enabling the next frontier of quantum computing // McKinsey. 19.09.2024. URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/enabling-the-next-frontier-of-quantum-computing (дата обращения: 18.02.2025)

[14] Timelines: When can we expect a useful quantum computer? // Introduction to Quantum Computing for Business. URL: https://introtoquantum.org/essentials/timelines/ (дата обращения: 18.05.2025)

[15] Is Nvidia's Jensen Huang Right About Quantum Computing? Huang predicted it will be 15 to 30 years before the technology is commercially viable // Observer. 14.01.2025. URL: https://observer.com/2025/01/is-nvidias-jensen-huang-right-about-quantum-computing/ (дата обращения: 18.05.2025)

Таблица 1

**Оценка затрат на внедрение оборудования квантового распределения ключей в соответствии с тремя сценариями на момент 2025 г.**

Table 1

**Cost estimation for implementing quantum key distribution equipment in accordance with 3 scenarios as of 2025**

| Показатель | Сценарий 1 | Сценарий 2 | Сценарий 3 |
|---|---|---|---|
| A | 3 ед. | 427 ед. | 22 525 ед. |
| $P_1$ | 6 млн руб. | 6 млн руб. | 6 млн руб. |
| $A*P_1$ | 18 млн руб. | 2562 млн руб. | 135150 млн руб. |
| B | 1 ед. | 66 ед. | 2253 ед. |
| $P_2$ | 40 млн руб. | 40 млн руб. | 40 млн руб. |
| $B*P_2$ | 40 млн руб. | 2640 млн руб. | 90120 млн руб. |
| C | - | 66 ед. | 2253 ед. |
| $P_3$ | - | 33 млн руб. | 33 млн руб. |
| $C*P_3$ | - | 2178 млн руб. | 74349 млн руб. |
| S | 1 ед. | 66 ед. | 1151 ед. |
| $P_4$ | 1 млн руб. | 1 млн руб. | 1 млн руб. |
| $S*P_4$ | 1 млн руб. | 66 млн руб. | 1151 млн руб. |
| PN; L | Отсутствуют в упрощенном расчете | | |
| $P_7$ | 1,5 млн руб. | 1,5 млн руб. | 1,5 млн руб. |
| $C*P_7$ | - | 99 млн руб. | 3380 млн руб. |
| QTc | 59 млн руб. | 7545 млн руб. | 304150 млн руб. |
| QTqc | 59 млн руб. | 7446 млн руб. | 300770 млн руб. |
| $\partial$ | 20% | 20% | 20% |
| t | 2 года | 2 года | 2 года |
| (QTqc*$\partial$*t) | 23,6 млн руб. | 2978,4 млн руб. | 120308 млн руб. |
| ($C*P_7$*t) | - | 198 млн руб. | 6759 млн руб. |
| QTtco | 82,6 млн руб. | 10721,4 млн руб. | 431217 млн руб. |

*Составлено автором.*

*Compiled by the author.*

показателям простоя оборудования промышленных компаний в результате реализации атак с применением программ-вымогателей (ransomware) – 5 дней [16].

Объем выручки в зоне риска по первому сценарию оценивается на основании данных по мощности ТЭЦ и стоимости электроэнергии в регионе. Так, при мощности 150 МВт и стоимости 6–7 руб. за кВт•ч, годовая выручка составляет около 8,5 млрд руб. С учетом коэффициента использования установленной мощности (КИУМ) 50% выручка составляет около 4,3 млрд руб. В более масштабных сценариях 2 и 3 предлагается применение упрощенного индикативного расчета: в 2024 г. выручка ПАО «Русгидро» составила 642,9 млрд рублей с темпом роста +12,9 % год к году [17]. Так как полный вывод инфраструктуры из строя на всех объектах в федеральном масштабе представляется маловероятным даже в сценарии квантовой атаки, предположим, что потенциальная угроза затронет 10% инфраструктуры или в зону риска попадет 10% выручки. Оценка потенциальных рисков в результате отсутствия проекта внедрения квантового оборудования, учитывающая данные вводные, представлена в табл. 2.

Предварительный анализ собранных материалов показал, что внедрение квантовых коммуникаций на объектах ПАО «Русгидро» не является экономически обоснованным решением в краткосрочной перспективе ни в одном из сценариев (табл. 3).

[16] Темные хроники: к чему привела атака на Colonial Pipeline // Kaspersky ICT CERT. 21.05.2021. URL: https://ics-cert.kaspersky.ru/publications/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/ (дата обращения: 23.06.2025)

[17] Финансовая отчетность по МСФО за 2024 год // Русгидро. 2024. URL: https://rushydro.ru/investors/events/finansovaya-otchetnost-po-msfo-za-2024-god/ (дата обращения: 23.06.2025)

Таблица 2

**Оценка потенциальных рисков в результате отсутствия проекта внедрения квантового оборудования и экономическая эффективность квантовой трансформации в соответствии с тремя сценариями на момент 2025 г.**

Table 2

**Assessment of potential risks resulting from the absence of a project for the introduction of quantum equipment and the economic efficiency of quantum transformation in accordance with 3 scenarios as of 2025**

| | Сценарий 1 | Сценарий 2 | Сценарий 3 |
|---|---|---|---|
| R | 4.3 млрд руб. | 725,8 млрд руб. | 725,8 млрд руб. |
| Под угрозой простоя | 100% | 10% | 100% |
| Потенциальная потеря выручки | 4.3 млрд руб. | 72,58 млрд руб. | 725,8 млрд руб. |
| Количество часов работы в году | 8760 | 8760 | 8760 |
| T | 120 | 120 | 120 |
| AL | 58,9 млн руб. | 994 млн руб. | 9942 млн руб. |
| QR | 5,14% | 5,14% | 5,14% |
| ER | 3 млн руб. | 51 млн руб. | 511 млн руб. |

*Составлено автором.*

*Compiled by the author.*

Таблица 3

**Оценка экономической целесообразности проведения квантовой трансформации функции информационной безопасности в соответствии с тремя сценариями на момент 2025 г.**

Table 3

**Assessment of the benefits of implementing quantum key distribution using a risk-based approach in accordance with 3 scenarios as of 2025**

| | Сценарий 1 | Сценарий 2 | Сценарий 3 |
|---|---|---|---|
| ER | 3 млн руб. | 51 млн руб. | 511 млн руб. |
| QTc | 59 млн руб. | 7545 млн руб. | 304150 млн руб. |

*Составлено автором.*

*Compiled by the author.*

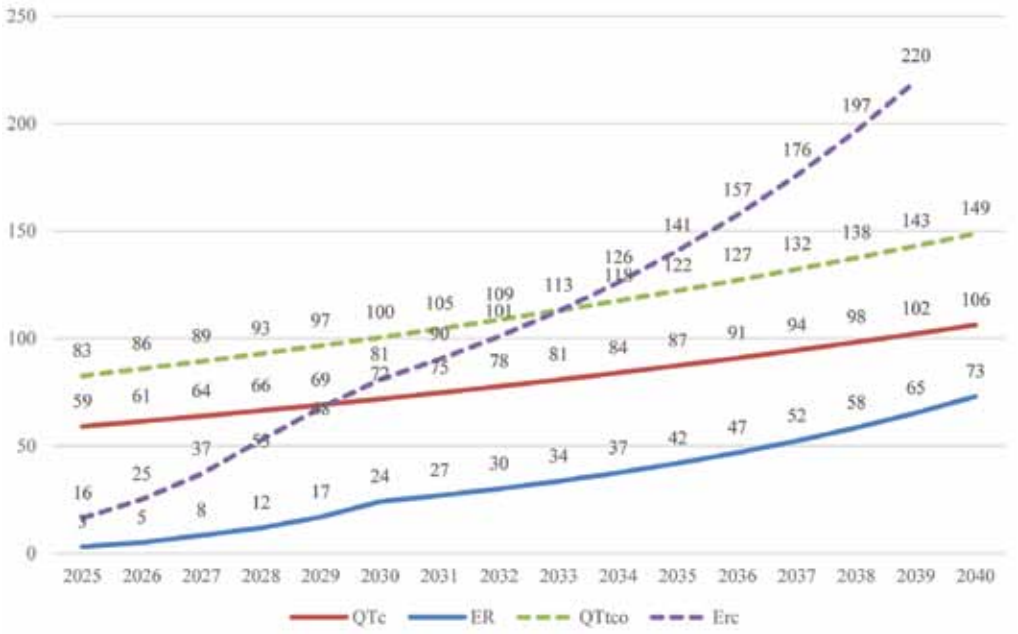
При этом очевидна зависимость: экономическая эффективность потенциальных проектов квантовой трансформации функции информационной безопасности увеличивается при точечной защите ключевых объектов критической информационной инфраструктуры. Покрытие многочисленных подстанций с незначительным весом в обеспечении выручки организации считается избыточным.

Далее предлагается рассмотреть прогноз экономической привлекательности проекта в динамике. Прогноз показателей до 2040 г. с учетом инфляции представлен на рис. 2. Согласно результатам расчета, проведение квантовой трансформации может представлять интерес в 2033 г. при учете совокупной экономической оценки рисков и полной стоимости владения локальной квантовой сетью.

Проведение расчета показало, что внедрение квантового оборудования по сценарию 2 не представляет экономического интереса: риски потери выручки от простоя значительно ниже, чем стоимость проведения квантовой трансформации. Проект может представлять интерес в том случае, если в зону риска применения квантового компьютера будет попадать более 10% всей информационной инфраструктуры компании (рис. 3). Однако сценарий, в котором успешная кибератака приводит к массовому простою промышленного оборудования на всех распределенных объектах компании, представляется маловероятным.

В случае сценария 3 даже 100% попадание инфраструктуры в зону риска может не привести к экономической эффективности квантовой трансформации в связи с большим количеством подстанций и высокой стоимостью оборудования квантового распределения ключей (рис. 4).

Таким образом, осуществление квантовой трансформации функции информационной безопасности может представлять интерес в сценарии 1, ограниченный интерес в сценарии 2, и не представляет интереса в сценарии 3.

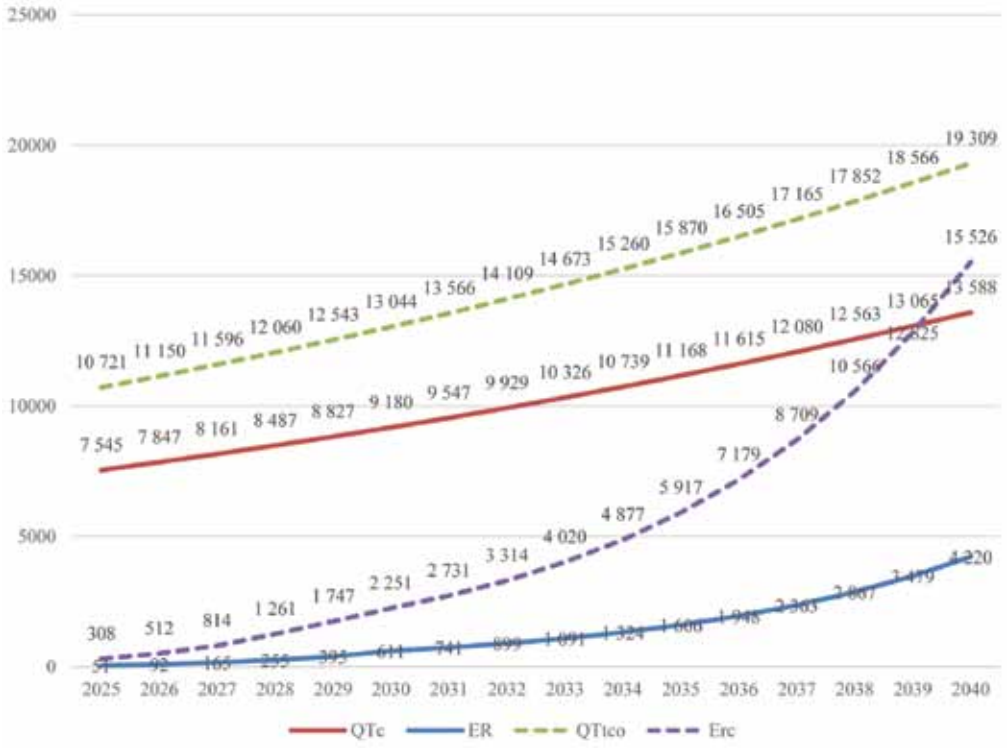



*Составлено автором.*

**Рис. 2. Сравнение стоимости рисков экономических потерь от простоя оборудования и проведения квантовой трансформации функции информационной безопасности, сценарий 1, млн руб.**

*Compiled by the author.*

**Fig. 2. Comparison of the cost of risks of economic losses from equipment downtime and the quantum transformation of the information security function, scenario 1, million rubles**




*Составлено автором.*

**Рис. 3. Сравнение стоимости рисков экономических потерь от простоя оборудования и проведения квантовой трансформации функции информационной безопасности, сценарий 2, млн руб.**

*Compiled by the author.*

**Fig. 3. Comparison of the cost of risks of economic losses from equipment downtime and the quantum transformation of the information security function, scenario 2, million rubles**


*Составлено автором.*

**Рис. 4. Сравнение стоимости рисков экономических потерь от простоя оборудования и проведения квантовой трансформации функции информационной безопасности, сценарий 3, млн руб.**

*Compiled by the author.*

**Fig. 4. Comparison of the cost of risks of economic losses from equipment downtime and the quantum transformation of the information security function, scenario 3, million rubles**

Для определения целевой даты внедрения квантового оборудования по сценарию 1 предлагается ориентироваться на модифицированную автором данного исследования «теорему Моска».

Ранее для определения целевой даты внедрения квантовых коммуникаций ученый Мишель Моска предлагал ориентироваться только на прогноз создания квантового компьютера и требования к срокам хранения секретной информации. Выбор года для начала проекта квантовой трансформации осуществлялся по формуле (1). Однако автор настоящей работы рекомендует учитывать срок достижения экономической эффективности квантовых сетей для конечных клиентов, пересмотрев переменную $Z$, то есть обозначить ею количество лет, оставшихся до $ER > QTc$ (альтернативно: $ERc > QTtco$). Данный подход к планированию квантовой трансформации представляется более актуальным для коммерческих организаций.

Следовательно, если экономическая эффективность наступает в 2033 г., срок хранения чувствительных данных различного характера (технологические параметры, аварийные ситуации, состояние оборудования), касающихся промышленного оборудования, в России составляет около 5-ти лет, а ожидаемый срок осуществления квантовой трансформации составляет около года, рекомендуемый год установки оборудования квантового распределения ключей на Южно-Сахалинской ТЭЦ-1 – 2027 г.

Далее оценим стоимость внедрения постквантовых алгоритмов как альтернативного инструмента защиты от квантовой угрозы для сценария 2. Преимущества данного решения заключаются в отсутствии необходимости закупки дорогостоящих устройств квантового распределения ключей, а также в возможности защиты беспроводных сетей при отсутствии доступа к воздушным и оптоволоконным каналам. При этом стоит отметить, что внедрение более «тяжелых» алгоритмов шифрования все же потребует выделения дополнительных вычислительных мощностей, также отсутствует гарантия долгосрочной устойчивости постквантового шифрования с учетом риска создания улучшенных квантовых компьютеров.

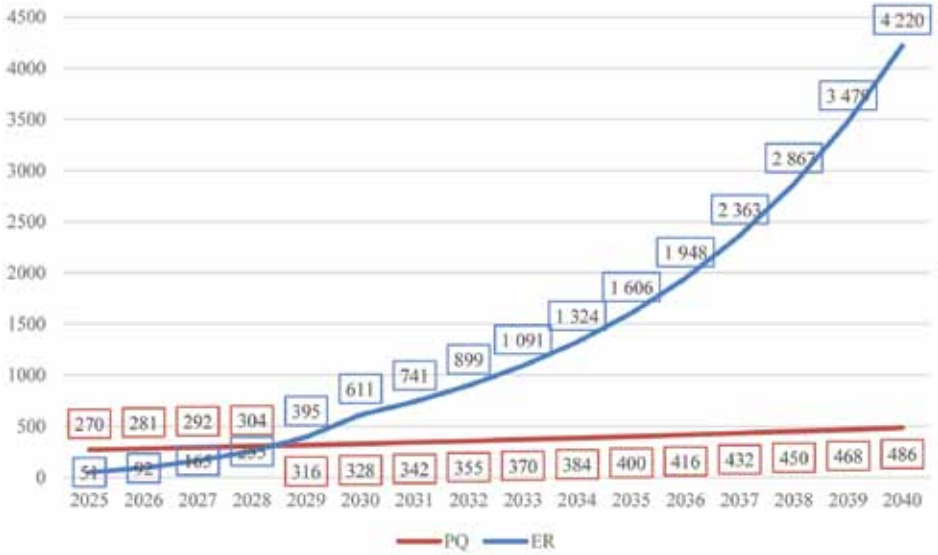
Для оценки стоимости внедрения постквантовых алгоритмов применяется метод бенчмаркинга: бюджет ИТ «Русгидро» составляет, как минимум, 2,7 млрд руб., в соответствии с выручкой дочерней ИТ-компании [18]. Бенчмарк равен 10%, так как

[18] Контрагент ООО «Русгидро ИТ сервис» // Аудит-ИТ. 2023. URL: https://www.audit-it.ru/contragent/1091902000772_ooo-rusgidro-it-servis (дата обращения: 18.02.2025)

Правительство США планирует выделить 7,1 млрд долл. на внедрение постквантовых алгоритмов [19], что равняется примерно 10% годового бюджета 2024 г. [20] Таким образом, затраты на постквантовую трансформацию ($PQ$) могут составить от 270 млн руб.:

$$PQ = 2700 \times 10\% . \quad (8)$$

Затраты на внедрение постквантовых алгоритмов несомненно ниже, чем на проведение квантовой трансформации, что позволяет сделать вывод о том, что масштабное обеспечение защиты будущей инфраструктуры умных сетей электроснабжения (Smart Grid) должно обеспечиваться прежде всего с применением данного инструмента. Рис. 5 подтверждает, что реализация подобного проекта может представлять экономический интерес для ПАО «Русгидро» уже в перспективе 2–3 лет, что, в свою очередь, соответствует планам правительственных организаций в США и Европейском союзе, предписывающих перевод критической информационной инфраструктуры на постквантовые алгоритмы в период до 2035 г. [21]




*Составлено автором.*

**Рис. 5. Сравнение стоимости рисков экономических потерь от простоя оборудования и внедрения постквантовых алгоритмов, сценарий 2, млн руб.**

*Compiled by the author.*

**Fig. 5. Comparison of the cost of risks of economic losses from equipment downtime and the implementation of post-quantum algorithms, scenario 2, million rubles**

## Выводы

Разработанная автором математическая модель позволяет оценить экономическую эффективность реализации квантовой трансформации функции информационной безопасности с учетом потенциальных потерь в результате реализации риска применения потенциальным противником квантового компьютера. Гипотеза о наличии ценностного предложения квантовых коммуникаций, основан-

[19] White House Report: U.S. Federal Agencies Brace for $7.1 Billion Post-Quantum Cryptography Migration // Quantum Insider. 09.05.2024. URL: https://thequantuminsider.com/2024/08/12/white-house-report-u-s-federal-agencies-brace-for-7-1-billion-post-quantum-cryptography-migration/ (дата обращения: 18.02.2025)

[20] Budget of the U.S. Government FISCAL YEAR 2024 // Novogradac. URL: https://www.novoco.com/public-media/documents/white-house-budget-fy-2024-03092023.pdf (дата обращения: 18.02.2025)

[21] EU Defines Clear Roadmap for Post Quantum Cryptography Transition by 2035 // Encryption Consulting. 16.06.2025. URL: https://www.encryptionconsulting.com/eu-defines-clear-roadmap-for-post-quantum-cryptography-transition-by-2035/; NSA sets 2035 deadline for adoption of post-quantum cryptography across national security systems // Fedscoop. 07.09.2022. URL: https://fedscoop.com/nsa-sets-2035-deadline-for-adoption-of-post-quantum-cryptography-across-natsec-systems/#:~:text=Emerging%20Tech-,NSA%20sets%202035%20deadline%20for%20adoption%20of%20post%2Dquantum%20cryptography,has%20secured%20most%20federal%20systems (дата обращения: 29.06.2025)

ного на экономических эффектах, подтвердилась только частично:

1) внедрение дорогостоящих устройств квантового распределения ключей представляет интерес прежде всего в целях долгосрочной защиты ключевых стратегических объектов критической информационной инфраструктуры, обеспечивающих реализацию основных операционных процессов, лежащих в основе получения основного потока выручки предприятия;
2) масштабные проекты по защите многочисленных объектов инфраструктуры рекомендуется осуществлять с применением постквантовых математических алгоритмов.

В соответствии с результатами применения доработанной автором «теоремой Моска», учитывающей экономические факторы в планировании внедрения решений защиты от квантовой угрозы, апробированной на примере ПАО «Русгидро», начало реализации подобных проектов может представлять наибольший интерес для коммерческих организаций с 2027 г., так как риски от применения потенциальным противником квантового компьютера будут выше, чем стоимость внедрения продвинутых математических алгоритмов и, в некоторых случаях, оборудования квантового распределения ключей.

В связи с этим предприятиям-владельцам объектов критической информационной инфраструктуры уже сегодня рекомендуется разрабатывать долгосрочные стратегии проведения квантовой трансформации, принимать участие в пилотных проектах в области квантовых коммуникаций и постквантовой криптографии.

**Список источников**

1. *Cao Y., Zhao, Y., Wang, Q., Zhang J., Ng S.X., Hanzo L.* The evolution of quantum key distribution networks: on the road to the qinternet // IEEE Communications Surveys and Tutorials. 2022. Vol. 24. Iss. 2. P. 839–894. https://doi.org/10.1109/comst.2022.3144219

2. *Evans P.G., Alshowkan M., Earl D., Mulkey D.D., Newell R., Peterson G.* Trusted node QKD at an electrical utility // IEEE Access. 2021. Vol. 9. P. 105220–105229. https://doi.org/10.1109/access.2021.3070222

3. *Prateek K., Maity S., Amin R.* An unconditionally secured privacy-preserving authentication scheme for smart metering infrastructure in smart grid // IEEE Transactions on Network Science and Engineering. 2022. Vol. 10. Iss. 2. P. 1085–1095. https://doi.org/10.1109/tnse.2022.3226902

4. *Alshowkan M., Evans P.G., Starke M., Earl D., Peters A.N.* Authentication of smart grid communications using quantum key distribution // Scientific Reports. 2022. Vol. 12. P. 12731. https://doi.org/10.1038/s41598-022-16090-w

5. *Zhao B., Zha X., Chen Z., Shi R., Wang D., Peng T., Yan L.* Performance analysis of quantum key distribution technology for power business // Applied Sciences. 2020. Vol. 10. Iss. 8. P. 2906. https://doi.org/10.3390/app10082906

6. *Jawad T.A., Mahmood A.N., Hameed A.N.* Detecting man-in-the-middle attacks via hybrid quantum-classical protocol in software-defined networks // Indonesian Journal of Electrical Engineering and Computer Science. 2023. Vol. 31. Iss. 1. P. 205–211. https://doi.org/10.11591/ijeecs.v31.i1.pp205-211

7. *Stergiopoulos G., Gritzalis D.A., Limnaios E.* Cyber-attacks on the oil & gas sector: a survey on incident assessment and attack patterns // IEEE Access. 2020. Vol. 8. P. 128440–128475. https://doi.org/10.1109/ACCESS.2020.3007960

8. *Sharma M., Choudhary V., Bhatia R.S., Malik S., Raina A., Khandelwal H.* Leveraging the power of quantum computing for breaking RSA encryption // Cyber-Physical Systems. 2021. Vol. 7. Iss. 2. P. 73–92. https://doi.org/10.1080/23335777.2020.1811384

9. *Bonnetain X., Naya-Plasencia M., Schrottenloher A.* Quantum security analysis of AES // IACR Transactions on Symmetric Cryptology. 2019. Vol. 2019. Iss. 2. P. 55–93. https://doi.org/10.46586/tosc.v2019.i2.55-93

10. *Ismail S., Sitnikova E., Slay J.* SCADA systems cyber security for critical infrastructures: case studies in the transport sector // In: Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications. Edited by Information Resources Management Association. Hershey, PA: IGI Global, 2020. P. 446–464. https://doi.org/10.4018/978-1-7998-2466-4.ch028

11. *Ghosh S., Sampalli S.* A survey of security in SCADA networks: current issues and future challenges // IEEE Access. 2019. Vol. 7. P. 135812–135831. https://doi.org/10.1109/ACCESS.2019.2926441

12. *Malina L., Dzurenda P., Ricci S., Hajny J., Srivastava G., Matulevičius R.* Post-quantum era privacy protection for intelligent infrastructures // IEEE Access. 2021. Vol. 9. P. 36038–36077. https://doi.org/10.1109/access.2021.3062201

13. *Naz M.T., Elmedany W., Ali M.* Securing SCADA systems in smart grids with iot integration: a self-defensive post-quantum blockchain architecture // Internet of Things. 2024. Vol. 28. P. 101381. https://doi.org/10.1016/j.iot.2024.101381

14. *Satrya G.B., Agus Y.M., Mnaouer A.B.* A comparative study of post-quantum cryptographic algorithm implementations for secure and efficient energy systems monitoring // Electronics. 2023. Vol. 12. Iss. 18. P. 3824. https://doi.org/10.3390/electronics12183824

15. *Ahn J., Kwon H.-Y., Ahn B., Park K., Kim T., Lee M.-K., Kim J., Chung J.* Toward quantum secured distributed energy resources: adoption of post-quantum cryptography (PQC) and quantum key distribution (QKD) // Energies. 2022. Vol. 15. Iss. 3. P. 714. https://doi.org/10.3390/en15030714

16. *Fakhruldeen H.F., Al-Kaabi R.A., Jabbar F.I., Al-Kharsan I.H., Shoja S.J.* Post-quantum techniques in wireless network security: an overview // Malaysian Journal of Fundamental and Applied Sciences. 2023. Vol. 19. Iss. 3. P. 337–344. https://doi.org/10.11113/mjfas.v19n3.2905

17. *Al Natsheh A., Gbadegeshin S.A., Rimpiläinen A., Imamovic-Tokalic I., Zambrano A.* Identifying the challenges in commercializing high technology: a case study of quantum key distribution technology // Technology Innovation Management Review. 2015. Vol. 5. P. 26–36. https://doi.org/10.22215/timreview864

18. *Cavaliere F., Prati E., Poti L., Muhammad I., Catuogno T.* Secure quantum communication technologies and systems: from labs to markets // Quantum Reports. 2020. Vol. 2. Iss. 1. P. 80–106. https://doi.org/10.3390/quantum2010007

19. *Azuma K., Economou S.E., Elkouss D., Hilaire P., Jiang L., Lo H.-K., Tzitrin I.* Quantum repeaters: from quantum networks to the quantum internet // Reviews of Modern Physics. 2023. Vol. 95. Iss. 4. P. 045006. https://doi.org/10.1103/revmodphys.95.045006

20. *Minbaleev A., Zenin S., Evsikov K.* Prospects for legal regulation of quantum communication // BRICS Law Journal. 2024. Vol. 11. Iss. 2. P. 11–54. https://doi.org/10.21684/2412-2343-2024-11-2-11-54

21. *Shahrul N.S., Hanefah M.M., Masruki R., Yaakub N.A., Mohamad N.* Awareness and readiness on quantum communication technology among the regulators, industry players and academicians in Malaysia // Journal of Information System and Technology Management. 2024. Vol. 9. Iss. 35. P. 21–37. https://doi.org/10.35631/JISTM.935002

22. *Shaji K.M., Dudhe R., Raina R.* Quantum communication technologies: future trends and prospects for innovation // In: 2023 9th International Conference on Optimization and Applications (ICOA). IEEE, 2023. P. 1–6. https://doi.org/10.1109/icoa58279.2023.10308831

23. *Mamiya A., Tanaka K., Yokote S., Sasaki M., Fujiwara M., Tanaka M.* Satellite-based QKD for global quantum cryptographic network construction // In: 2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS). Kyoto City, Japan, 2022. P. 47–50. https://doi.org/10.1109/icsos53063.2022.9749727

24. *Aguado A., López V., López D., Peev M., Poppe A., Pastor A., Folgueira J., Martín V.* The engineering of software-defined quantum key distribution networks // IEEE Communications Magazine. 2019. Vol. 57. Iss. 7. P. 20–26. URL: https://oa.upm.es/67027/1/INVE_MEM_2019_319360.pdf (дата обращения: 22.02.2025)

25. *Kim I., Ju J.* Trends in quantum communication testbeds // Electronics and Telecommunications Trends. 2024. Vol. 39. Iss. 5. P. 86–97. https://doi.org/10.22648/ETRI.2024.J.390509

26. *Purohit A., Kaur M., Seskir Z.C., Posner M.T., Venegas-Gomez A.* Building a quantum-ready ecosystem // IET Quantum Communication. 2024. Vol. 5. Iss. 1. P. 1–18. https://doi.org/10.1049/qtc2.12072

27. *Ермакова Е.О., Ерохина А.А.* Применение квантовых коммуникаций в ОАО «РЖД»: логистические аспекты // В сб.: Потенциал логистики XXI века: молодежное измерение. Вып. 3. СПб.: Санкт-Петербургский государственный экономический университет, 2022. С. 86–93. EDN: https://elibrary.ru/tmjflf

28. *Раткин Л.С.* Квантово-коммуникационные системы распределенных реестров для хранения и обработки данных о технических характеристиках и финансово-экономических параметрах инвестиционных проектов по разработке перспективных моделей автотранспорта // Транспорт: наука, техника, управление. Научный информационный сборник. 2021. № 5. С. 61–64. EDN: https://elibrary.ru/oxiuii. https://doi.org/10.36535/0236-1914-2021-05-10

29. *Hötte K.* Demand-pull, technology-push, and the direction of technological change // Research Policy. 2023. Vol. 52. Iss. 5. P. 104740. https://doi.org/10.1016/j.respol.2023.104740

30. *Kiviharju M.* Refining Mosca's theorem: risk management model for the quantum threat applied to IoT protocol security // In: Cyber Security. Computational Methods in Applied Sciences. Vol. 56. Cham: Springer International Publishing, 2022. P. 369–401. https://doi.org/10.1007/978-3-030-91293-2_16

Статья поступила в редакцию 18.02.2025; одобрена после рецензирования 17.07.2025; принята к публикации 23.07.2025

*Об авторе:*

**Лобов Даниил Сергеевич,** кандидат экономических наук, научный сотрудник лаборатории новых полупроводниковых материалов для квантовой информатики и телекоммуникаций; менеджер, ООО «Кэпт Налоги и Консультирование» (Москва); SPIN-код: 9143-7018; Scopus ID: 57353047600

*Автор прочитал и одобрил окончательный вариант рукописи.*

## References

1. Cao Y., Zhao Y., Wang Q., Zhang J., Ng S.X., Hanzo L. The evolution of quantum key distribution networks: on the road to the qinternet. *IEEE Communications Surveys and Tutorials*. 2022; 24(2):839–894. https://doi.org/10.1109/comst.2022.3144219 (In Eng.)

2. Evans P.G., Alshowkan M., Earl D., Mulkey D.D., Newell R., Peterson G. Trusted node QKD at an electrical utility. *IEEE Access.* 2021; 9:105220–105229. https://doi.org/10.1109/access.2021.3070222 (In Eng.)

3. Prateek K., Maity S., Amin R. An unonditionally secured privacy-preserving authentication scheme for smart metering infrastructure in smart grid. *IEEE Transactions on Network Science and Engineering*. 2022; 10(2):1085–1095. https://doi.org/10.1109/tnse.2022.3226902 (In Eng.)

4. Alshowkan M., Evans P.G., Starke M., Earl D., Peters A.N. Authentication of smart grid communications using quantum key distribution. *Scientific Reports*. 2022; 12:12731. https://doi.org/10.1038/s41598-022-16090-w (In Eng.)

5. Zhao B., Zha X., Chen Z., Shi R., Wang D., Peng T., Yan L. Performance analysis of quantum key distribution technology for power business. *Applied Sciences*. 2020; 10(8):2906. https://doi.org/10.3390/app10082906 (In Eng.)

6. Jawad T.A., Mahmood A.N., Hameed A.N. Detecting man-in-the-middle attacks via hybrid quantum-classical protocol in software-defined networks. *Indonesian Journal of Electrical Engineering and Computer Science*. 2023; 31(1):205–211. https://doi.org/10.11591/ijeecs.v31.i1.pp205-211 (In Eng.)

7. Stergiopoulos G., Gritzalis D.A., Limnaios E. Cyber-attacks on the oil & gas sector: a survey on incident assessment and attack patterns. IEEE Access. 2020; 8:128440–128475. https://doi.org/10.1109/ACCESS.2020.3007960 (In Eng.)

8. Sharma M., Choudhary V., Bhatia R.S., Malik S., Raina A., Khandelwal H. Leveraging the power of quantum computing for breaking RSA encryption. *Cyber-Physical Systems.* 2021; 7(2):73–92. https://doi.org/10.1080/23335777.2020.1811384 (In Eng.)

9. Bonnetain X., Naya-Plasencia M., Schrottenloher A. Quantum security analysis of AES. *IACR Transactions on Symmetric Cryptology*. 2019. 2019(2):55–93. https://doi.org/10.46586/tosc.v2019.i2.55-93 (In Eng.)

10. Ismail S., Sitnikova E., Slay J. SCADA systems cyber security for critical infrastructures: case studies in the transport sector. In: *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications*. Edited by Information Resources Management Association. Hershey, PA: IGI Global, 2020. P. 446–464. https://doi.org/10.4018/978-1-7998-2466-4.ch028 (In Eng.)

11. Ghosh S., Sampalli S. A survey of security in SCADA networks: current issues and future challenges. *IEEE Access.* 2019; 7:135812–135831. https://doi.org/10.1109/ACCESS.2019.2926441 (In Eng.)

12. Malina L., Dzurenda P., Ricci S., Hajny J., Srivastava G., Matulevičius R. Post-quantum era privacy protection for intelligent infrastructures. *IEEE Access.* 2021; 9:36038–36077. https://doi.org/10.1109/access.2021.3062201 (In Eng.)

13. Naz M.T., Elmedany W., Ali M. Securing scada systems in smart grids with iot integration: a self-defensive post-quantum blockchain architecture. *Internet of Things.* 2024; 28:101381. https://doi.org/10.1016/j.iot.2024.101381 (In Eng.)

14. Satrya G.B., Agus Y.M., Mnaouer A.B. A comparative study of post-quantum cryptographic algorithm implementations for secure and efficient energy systems monitoring. *Electronics*. 2023; 12(18):3824. https://doi.org/10.3390/electronics12183824 (In Eng.)

15. Ahn J., Kwon H.-Y., Ahn B., Park K., Kim T., Lee M.-K., Kim J., Chung J. Toward quantum secured distributed energy resources: adoption of post-quantum cryptography (PQC) and quantum key distribution (QKD). *Energies*. 2022; 15(3):714. https://doi.org/10.3390/en15030714 (In Eng.)

16. Fakhruldeen H.F., Al-Kaabi R.A., Jabbar F.I., Al-Kharsan I.H., Shoja S.J. Post-quantum techniques in wireless network security: an overview. *Malaysian Journal of Fundamental and Applied Sciences*. 2023; 19(3):337–344. https://doi.org/10.11113/mjfas.v19n3.2905 (In Eng.)

17. Al Natsheh A., Gbadegeshin S.A., Rimpiläinen A., Imamovic-Tokalic I., Zambrano A. Identifying the challenges in commercializing high technology: a case study of quantum key distribution technology. *Technology Innovation Management Review*. 2015; 5:26–36. https://doi.org/10.22215/timreview864 (In Eng.)

18. Cavaliere F., Prati E., Poti L., Muhammad I., Catuogno T. Secure quantum communication technologies and systems: from labs to markets. *Quantum Reports*. 2020; 2(1):80–106. https://doi.org/10.3390/quantum2010007 (In Eng.)

19. Azuma K., Economou S.E., Elkouss D., Hilaire P., Jiang L., Lo H.-K., Tzitrin I. Quantum repeaters: from quantum networks to the quantum internet. *Reviews of Modern Physics*. 2023; 95(4):045006. https://doi.org/10.1103/revmodphys.95.045006 (In Eng.)

20. Minbaleev A., Zenin S., Evsikov K. Prospects for legal regulation of quantum communication. *BRICS Law Journal*. 2024; 11(2):11–54. https://doi.org/10.21684/2412-2343-2024-11-2-11-54 (In Eng.)

21. Shahrul N. S., Hanefah M.M., Masruki R., Yaakub N.A., Mohamad N. Awareness and readiness on quantum communication technology among the regulators, industry players and academicians in Malaysia. *Journal of Information System and Technology Management*. 2024; 9(35):21–37. https://doi.org/10.35631/JISTM.935002 (In Eng.)

22. Shaji K.M., Dudhe R., Raina R. Quantum communication technologies: future trends and prospects for innovation. In: *2023 9th International Conference on Optimization and Applications (ICOA)*. IEEE, 2023. P. 1–6. https://doi.org/10.1109/icoa58279.2023.10308831 (In Eng.)

23. Mamiya A., Tanaka K., Yokote S., Sasaki M., Fujiwara M., Tanaka M. Satellite-based QKD for global quantum cryptographic network construction. In: *2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*. Kyoto City, Japan, 2022. P. 47–50. https://doi.org/10.1109/icsos53063.2022.9749727 (In Eng.)

24. Aguado A., López V., López D., Peev M., Poppe A., Pastor A., Folgueira J., Martín V. The engineering of software-defined quantum key distribution networks. I*EEE Communications Magazine*. 2019; 57(7):20–26. URL: https://oa.upm.es/67027/1/INVE_MEM_2019_319360.pdf (accessed: 22.02.2025) (In Eng.)

25. Kim I., Ju J. Trends in quantum communication testbeds. *Electronics and Telecommunications Trends*. 2024; 39(5):86–97. https://doi.org/10.22648/ETRI.2024.J.390509 (In Eng.)

26. Purohit A., Kaur M., Seskir Z.C., Posner M.T., Venegas-Gomez A. Building a quantum-ready ecosystem. *IET Quantum Communication*. 2024; 5(1):1–18. https://doi.org/10.1049/qtc2.12072 (In Eng.)

27. Ermakova E.O., Erokhina A.A. Quantum communications in JSC "Russian Railways": logistics aspects. In: *Potential of logistics of the 21st century: youth dimension*. Vol. 3. Saint Petersburg: Saint Petersburg State University of Economics, 2022. P. 86-93. EDN: https://elibrary.ru/tmjflf (In Russ.)

28. Rathkeen L.S. The quantum communication systems of distributed registers for storing and treatment of data of technical characteristics and financial and economical parameters of investment projects for development of perspective models of autotransport. *Transport: science, equipment, management. Scientific information collection.* 2021; (5):61–64. EDN: https://elibrary.ru/oxiuii. https://doi.org/10.36535/0236-1914-2021-05-10 (In Russ.)

29. Hötte K. Demand-pull, technology-push, and the direction of technological change. *Research Policy*. 2023; 52(5):104740. https://doi.org/10.1016/j.respol.2023.104740 (In Eng.)

30. Kiviharju M. Refining Mosca's theorem: risk management model for the quantum threat applied to IoT protocol security. In: *Cyber Security. Computational Methods in Applied Sciences*. Vol. 56. Cham: Springer International Publishing, 2022. P. 369-401. https://doi.org/10.1007/978-3-030-91293-2_16 (In Eng.)

The article was submitted 18.02.2025; approved after reviewing 17.07.2025; accepted for publication 23.07.2025

*About the author:*

**Daniil S. Lobov,** Candidate of Economic Sciences, Research Fellow, Laboratory of New Semiconductor Materials for Quantum Information Science and Telecommunications; Manager, Kept LLC (Moscow); SPIN: 9143-7018; Scopus ID: 57353047600

*The author has read and approved the final version of the manuscript.*